Explicit geometric and arithmetic properties of curves

Turku Ozlum Celik

▶ **To cite this version:**

Turku Ozlum Celik. Explicit geometric and arithmetic properties of curves. Algebraic Geometry [math.AG]. Universite Rennes 1, 2018. English. NNT : . tel-01871465

HAL Id: tel-01871465
https://theses.hal.science/tel-01871465

Submitted on 10 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ANNÉE 2018

UNIVERSITÉ DE RENNES 1

UNIVERSITE BRETAGNE LOIRE

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Bretagne Loire
pour le grade de
DOCTEUR DE L'UNIVERSITÉ DE RENNES 1
Mention : Mathématiques et applications
Ecole doctorale MathSTIC
présentée par

Türkü Özlüm Çelik

préparée à l'unite recherche 6625 du CNRS : IRMAR
Institut de Recherche Mathématique de Rennes
UFR de Mathématiques

Propriétés géométriques et arithmétiques explicites des courbes

Thèse soutenue à Rennes
le 31 Août 2018

Sorina IONICA
Maîtresse de conférences
Université de Picardie Amiens / rapporteuse

Riccardo SALVATI MANNI
Professeur
Università di Roma / rapporteur

Alp BASSA
Professeur associé
Boğaziçi Üniversitesi / examinateur

Elisa LORENZO GARCÍA
Maîtresse de conférences
Université de Rennes 1 / examinatrice

Rachel PRIES
Professeur
Colorado State University / examinatrice

Sylvain DUQUESNE
Professeur
Université de Rennes 1 / directeur de thèse

Christophe RITZENTHALER
Professeur
Université de Rennes 1 / co-directeur de thèse

Acknowledgements

Before anything else, I would like to thank my advisor Sylvain Duquesne for his enlightening advice and providing opportunities for the research direction in cryptography.

Second, I am deeply thankful to my co-advisor Christophe Ritzenthaler. He has introduced the beauties of computational aspects of algebraic geometry and number theory to me. Under no circumstances, he has never preserved his outstanding guidance and valuable support for my doctoral studies.

I owe Riccardo Salvati Manni and Sorina Ionica a debt of gratitude for their suggestions and remarks which were immensely important for the thesis to take its final form.

I am grateful to Alp Bassa, Elisa Lorenzo Garcia and Rachel Pries for accepting to be a part of my jury.

I am thankful to Henri Lebesgue Center for funding the 3-years stay in Rennes as well as ensuring many academic occasions.

This thesis has been comprised of three projects:

For the first project, I would like to thank Alessio Fiorentino. His mathematical and emotional support during his 1-year stay in Rennes as a postdoctoral researcher had been substantial. On the top of that, he has never stopped to share his knowledge store about the topic even with Skype. In addition, many thanks to my collaborators Avinash Kulkarni, Yue Ren and Mahsa Sayyary Namin. Our collaboration in a further project had made the whole picture of this part more apparent to me.

For the second one, many thanks to Gabriel Gallin and Arnaud Tisserand for their teamwork and navigation in the world of computer science.

And for the third project, I am thankful to the organisers of Women in Numbers Europe II for regulating such a productive scientific ambiance. Warm thanks to the members of our team, Yara Elias, Burçin Güneş, Rachel Newton, Ekin Ozman, Rachel Pries and Lara Thomas, for their cooperation. And special thanks to the leaders of our team, Ekin Ozman and Rachel Pries, for bringing the topic into our interest.

A huge thank you to the administrative team, the informatics service and the library team of not only IRMAR but also MPI MIS.

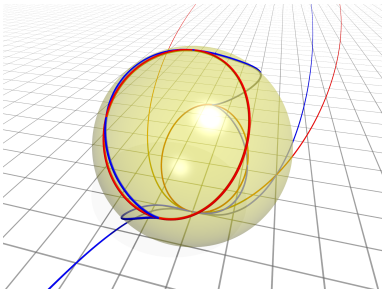
Sincere thanks to Nonlinear Algebra family at the Max Planck Institute for Mathematics in the Sciences for constituting an awesome scientific environment which played a role for the very last period of the dissertation study. I am especially grateful to the leader of this family, Bernd Sturmfels. His encouragement to begin postdoctoral research earlier than as planned had accelerated effectively the thesis to come to exist completely.

Beside all these, I feel extremely lucky due to my mother, my father, my brother, my husband and my friends. I owe them especially the emotional stability I need. And I do not dare to imagine a life without them! How can I thank them enough? (Bütün bunların yanısıra; annem, babam, kardeşim, eşim ve arkadaşlarım sayesinde kendimi çok şanslı hissediyorum. Özellikle gereksinim duyduğum duygusal dengeyi onlara borçluyum. Var olmadıkları bir hayat düşünemiyorum! Nasıl teşekkür etsem azdır...)

Contents

Introduction (en Français)

Les courbes algébriques sont des objets centraux de la géométrie algébrique qui apparaissent dans la géométrie arithmétique et également dans diverses applications. Parmi elles, on peut citer par exemple la cryptographie ou encore la physique théorique. Dans cette thèse, nous les étudions sous ces différents aspects.



Calcul des Constantes Thêta

Une façon de comprendre une courbe algébrique est d'étudier la structure de groupe appelé *jacobienne* associé à la courbe. *Les constantes thêta* jouent un rôle important pour comprendre la relation entre une courbe et sa jacobienne.

Les calculs explicites des constantes thêta sont étroitement liés à un problème classique qui demande quelles variétés abéliennes complexes principalement polarisées apparaissait comme des variétés jacobiennes de courbes. Le problème est appelé *le problème de Schottky* et remonte à Riemann [82, 83]. Le domaine a été amélioré par un large éventail des mathématiciens jusqu'à présent (voir [39] pour un historique bien écrit du sujet.). Une autre question connexe est d'essayer de récupérer explicitement la courbe à partir de sa jacobienne (voir [86] pour le cas $g = 2$, [93, 57] pour le cas hyperelliptique général, et [96, 48] pour le cas non-hyperelliptique lorsque $g = 3$). En outre, le sujet a de nombreuses applications dans différents domaines tels que la physique théorique [36] via des systèmes intégrables et la cryptographie [97] via des algorithmes de comptage de points de type AGM [84] et plus récemment la cryptographie basée sur les isogénies [69].

Soit $g \geq 0$ un entier. Notons $\mathcal{M}_g$ l'espace de modules sur $\mathbb{C}$ des courbes de genre g et $\mathcal{A}_g$ l'espace de modules des variétés abéliennes complexes principalement polarisées de dimension g. *L'application de Torelli*

$$j : \mathcal{M}_g \to \mathcal{A}_g \tag{1}$$

fait correspondre à la classe d'isomorphisme d'une courbe à la classe d'isomorphisme de sa jacobienne avec sa polarisation canonique. Le problème de Schottky est de caractériser

l'image de l'application j. L'approche classique du problème consiste à plonger $\mathcal{A}_g$ dans un espace projectif et d'essayer de trouver l'idéal définissant l'image.

Soit

$$\mathbb{H}_g = \{\tau \in \mathrm{GL}_g(\mathbb{C}) \mid {}^t\tau = \tau,\ \mathrm{Im}\tau > 0\}$$

le demi-espace supérieur de Siegel constitué des matrices complexes $g \times g$ avec une partie imaginaire définie positive.

Pour $\tau \in \mathbb{H}_g$, $z = (z_1, \ldots, z_g) \in \mathbb{C}^g$ et

$$[q] = \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} \in \mathbb{Z}^g \oplus \mathbb{Z}^g,$$

la fonction thêta avec caractéristique $[q]$ est

$$\vartheta[q](z,\tau) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i(n+\varepsilon/2)\tau^t(n+\varepsilon/2) + 2\pi i(n+\varepsilon/2)^t(z+\varepsilon'/2)\right).$$

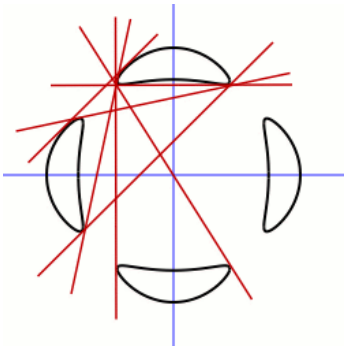
L'évaluation de cette fonction en $z = 0$, qui est $\vartheta[q](\tau) = \vartheta[q](0,\tau)$, est dite une constante thêta (*Thetanullwerte*) . La *caractéristique* $[q]$ est dite paire (resp. impaire) si le produit scalaire habituel $\varepsilon \cdot \varepsilon'$ est paire (resp. impaire). La constante thêta $\vartheta[q](\tau)$ est dite *paire* (resp. *impaire*) si la caractéristique $[q]$ est paire (resp. impaire). Notez que la constante thêta $\vartheta[q](\tau)$ est identiquement nulle pour tout $\tau \in \mathbb{H}_g$ si et seulement si la caractéristique $[q]$ est impaire.

D'autre part, tout $\tau \in \mathbb{H}_g$ définit une variété complexe abélienne principalement polarisée $\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$. Le groupe symplectique $\mathrm{Sp}(2g,\mathbb{Z})$ agit sur $\mathbb{H}_g$. Le quotient $\mathbb{H}_g/\mathrm{Sp}(2g,\mathbb{Z})$ est l'espace de modules $\mathcal{A}_g$. Il y a un revêtement fini $\mathcal{A}'_g \to \mathcal{A}_g$ où $\mathcal{A}'_g$ est le quotient de $\mathbb{H}_g$ par un certain sous-groupe (spécifiquement le sous-groupe $\Gamma_g(4,8)$) de $\mathrm{Sp}(2g,\mathbb{Z})$. Les caractéristiques thêta paires fournissent un application

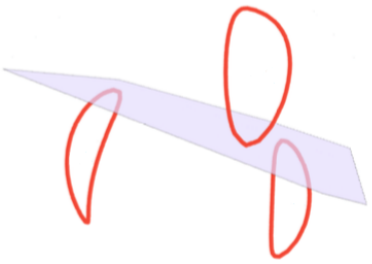
$$\begin{aligned} \Phi : \mathcal{A}'_g &\to \mathbb{P}^{2^{g-1}(2^g+1)}, \\ \tau &\mapsto (\vartheta[q](\tau))_q \end{aligned}$$

qui est une plongement lorsque q parcourt l'ensemble des caractéristiques thêta paires. L'étude pour déterminer toutes les relations entre les caractéristiques thêta paires revient alors à comprendre l'image de $\mathcal{A}_g$ par l'application Φ (voir [88]).

Dans le Chapitre 1, nous donnons un algorithme pour calculer la quatrième puissance du quotient de une donnée deux constantes thêta paires correspondant à une matrice de période dans $\mathbb{H}_g$ d'une courbe non-hyperelliptique de toute genre $g \geq 3$ dans le cas où une structure complète de niveau 2 est donnée. Soit $\mathcal{C}$ une courbe projective, lisse, non-hyperelliptique de genre g sur un corps $k \subseteq \mathbb{C}$. Nous définissons le *Jacobien* de $\mathcal{C}$ comme $\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$ par rapport à un *matrice de période normalisée* τ dans $\mathbb{H}_g$. Elle sera notée $\mathrm{Jac}(\mathcal{C})$. Une *structure complète de niveau 2* est représentée par les équations définissant de $\mathcal{C}$ sous le plongement canonique et certains diviseurs sur la courbe avec un étiquetage approprié comme suit. De tels diviseurs sont appelés *diviseurs thêta caractéristiques*. Il existe deux types de diviseurs thêta caractéristiques, *pair* et *impair*, qui dépendent de la dimension des espaces de Riemann-Roch associés. Notez que les diviseurs thêta caractéristiques impairs correspondent à certains objets géométriques appelé *multitangentes* sur la courbe. Par exemple, ces objets sont dits *bitangentes* quand $g = 3$ et *tritangentes* quand $g = 4$.



(a) Bitangentes sur la courbe Trott [85].



(b) Une tritangente d'une courbe avec trois ovals [60].

D'un autre côté, il existe une correspondance canonique entre les diviseurs thêta caractéristiques sur $\mathcal{C}$ et les formes quadratiques sur $\mathrm{Jac}[2](\mathcal{C})$ sur $\mathbb{F}_2$, où $\mathrm{Jac}[2](\mathcal{C})$ dénote les points de 2-torsion $\mathrm{Jac}(\mathcal{C})$. Les formes quadratiques sont *étiquetées* à travers une donnée combinatoire qui s'appelle une *base d'Aronhold*. La Section 1.1 rappelle une partie des prérequis mathématiques nécessaires pour l'algorithme.

Le calcul de ce quotient est bien connu et donné par une formule fermée pour une courbe de $g \leq 3$ et des courbes hyperelliptiques de n'importe quel genre, (voir [94, 96]). Ces formules peuvent être vues comme une description explicite de l'application de Torelli. En effet, une variété abélienne principalement polarisée peut être écrite comme une intersection de quadriques explicites dans un espace projectif [73]. Les coefficients de ces quadriques sont déterminés par des constantes thêta. Ces formules expriment des constantes thêta en termes de géométrie de la courbe. Dans le cas d'une courbe hyperelliptique donnée par $y^2 = \prod_{i=1}^{2g+2}(x - \alpha_i)$, nous avons

$$\vartheta[q](\tau)^4 = (2i\pi)^{-2g} \cdot \det(\Omega_1)^2 \cdot \prod_{i,j \in U} (\alpha_i - \alpha_j),$$

où Ω_1 est la première moitié d'une matrice de période et U est un ensemble d'indices dépendant du caractéristique $[q]$ [94, Page 218]. Cette formule, que nous appelons *la formule de Thomae absolue*, a ensuite été reprise par [41, 10, 40] en utilisant la méthode variationnelle. Une version plus simple exprimant le quotient $\vartheta[q](\tau)^8/\vartheta[q'](\tau)^8$, que nous appelons *la formule de Thomae relative*, a été établi dans [102, 75, 34] en utilisant des arguments élémentaires. Notez que cette formule, qui implique seulement les racines α_i, est généralement suffisante pour récupérer la jacobienne [91].

Pour une courbe non hyperelliptique $\mathcal{C}$ de $g = 3$, et pour deux caractéristiques thêta paires p_1, p_2 nous avons

$$\left(\frac{\vartheta[p_1](\tau)}{\vartheta[p_2](\tau)}\right)^4 = (-1)^n \cdot \frac{[\beta_1,\beta_2,\beta_3] \cdot [\beta_1,\beta_{12},\beta_{13}] \cdot [\beta_{12},\beta_2,\beta_{23}] \cdot [\beta_{13},\beta_{23},\beta_3]}{[\beta_{23},\beta_{13},\beta_{12}] \cdot [\beta_{23},\beta_3,\beta_2] \cdot [\beta_3,\beta_{13},\beta_1] \cdot [\beta_2,\beta_1,\beta_{12}]}, \qquad (\star)$$

où $[\beta_i,\beta_j,\beta_k]$ est le déterminant des coefficients de β_i, β_j et β_k qui sont certains bitangentes étiquetées via une base d'Aronhold [77, Théorème 3.1] et $n = 0, 1$ en fonction de p_1, p_2. Cette formule est appelée *formule de Weber*. Pour tout genre $g \geq 3$, le quotient $\left(\frac{\vartheta[p_1](\tau)}{\vartheta[p_2](\tau)}\right)^4$ est exprimé comme quotient des déterminants des sections régulières associées à certains fibrés sur $\mathcal{C}$. Pour les calculs explicites, nous traduisons cette expression algébrique en un quotient formé par des fonctions dans certains espaces de Riemann-Roch. Nous montrons le théorème suivant et donc obtenons l'algorithme.

Théorème. *Soit $\tilde{Q}_i^r$ et $\tilde{Q}_i^s$ les quotients des formes quadratiques ternaires, et A_i's (resp. B_i) des représentants fixes pour les points de contact de $\mathcal{C}$ avec une multitangente spécifique β_A (resp. β_B) pour $i = 1, ..., g-1$. Pour deux caractéristiques thêta impaires $p1, p2$, nous avons*

$$(-1)^n \cdot \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4}$$
$$= \frac{d_1 \begin{vmatrix} \tilde{Q}_1^s(B_1) & \cdots & \tilde{Q}_{g-1}^s(B_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^s(B_{g-1}) & \cdots & \tilde{Q}_{g-1}^s(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \tilde{Q}_1^r(A_1) & \cdots & \tilde{Q}_{g-1}^s(A_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^r(A_{g-1}) & \cdots & \tilde{Q}_{g-1}^r(A_{g-1}) \end{vmatrix}^2}{d_2 \begin{vmatrix} \tilde{Q}_1^r(B_1) & \cdots & \tilde{Q}_{g-1}^r(B_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^r(B_{g-1}) & \cdots & \tilde{Q}_{g-1}^r(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \tilde{Q}_1^s(A_1) & \cdots & \tilde{Q}_{g-1}^s(A_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^s(A_{g-1}) & \cdots & \tilde{Q}_{g-1}^s(A_{g-1}) \end{vmatrix}^2},$$

où d_1, d_2 sont les valeurs des produits de formes linéaires définissant β_A, β_B aux points A_i et B_i's et $n = 0, 1$ est donné uniquement en termes de p_1, p_2. (Pour l'énoncé complète, voir Théorème 1.2.4.)

Pour appliquer cet algorithme, il faut donc une structure complète de niveau 2 de genre g. Dans un premier temps, nous avons appliqué l'algorithme sur un exemple de courbe non-hyperelliptique du genre 3. Dans ce cas, une base d'Aronhold est suffisante pour la procédure de l'algorithme. En effet, cette base donne un modèle (*modèle de Riemann* [32, Chapitre 6]) pour la courbe, toutes les équations des 28 bitangentes de la courbe et un étiquetage élégant pour les diviseur thêta caractéristiques, c.-à-d. une structure complète de niveau 2. De plus, j'ai pu vérifier l'algorithme en composant le résultat avec la formule $(\star)$.

En genre supérieur, nous nous concentrons sur le cas $g = 4$. Nous avons étudié tout d'abord la courbe de Bring. Bien que nous disposions des équations de toutes les 120 tritangentes, nous ne pouvions pas surmonter efficacement le problème de l'étiquetage en général. Nous nous sommes donc concentrés sur une famille de courbes issues des surfaces de del Pezzo. Nous avons ainsi pu obtenir une structure complète de niveau 2 de genre 4. Dans la seconde partie du Chapitre 1, avec la motivation d'illustrer l'algorithme, nous expliquons brièvement la structure géométrique des surfaces de del Pezzo et montrons comment obtenir une structure complète de niveau 2 pour une courbe non-hyperelliptique de genre 4. Soit $\mathcal{S}$ une surface de del Pezzo de degré 1. La surface $\mathcal{S}$ est l'éclatement de huit points en position générale dans $\mathbb{P}^2$. Si $\kappa_{\mathcal{S}}$ est le diviseur canonique, alors le système linéaire $|-2\kappa_{\mathcal{S}}|$ donne un revêtement double de $\mathcal{S}$ sur un cône quadratique dans $\mathbb{P}^3$, et la courbe de branchement définit une courbe $\mathcal{C}$ du genre 4. Le point positif est qu'il y a une correspondance 2-1 entre les diviseurs exceptionnels de $\mathcal{S}$ et les diviseurs thêta caractéristiques impairs de $\mathcal{C}$ [101]. Nous calculons avec Magma les équations de toutes les tritangentes de $\mathcal{C}$ en calculant l'équation de la surface en partant de 8 points de $\mathbb{P}^2$ en position générale et les courbes exceptionnelles de $\mathcal{S}$. Dans ce cas, notez que les bases d'Aronhold viennent naturellement via la configuration de diviseurs exceptionnels sur $\mathcal{S}$. En effet, si $\rho : \operatorname{Pic}\mathcal{S} \to \operatorname{Pic}\mathcal{C}$ designe l'homomorphisme de restriction du groupe de Picard de $\mathcal{S}$ sur le groupe de Picard de $\mathcal{C}$, alors nous montrons la proposition suivante après quelques observations sur la structure de les points de 2-torsion $\operatorname{Pic}(\mathcal{C})[2]$ de $\operatorname{Pic}(\mathcal{C})$.

Proposition. *Supposons que $E_1, \ldots, E_8$ sont les diviseurs exceptionnels correspondant aux huit points sur l'éclatement. Soient $v_i = \rho(E_i + \kappa_{\mathcal{S}})$ pour $i = 1, \ldots, 8$ et $v_9 = v_1 + \cdots + v_8$.*

Pour tout diviseur thêta caractéristique D de $\mathcal{C}$, l'ensemble $\{D + v_i + v_9 \mid i = 1, \ldots, 9\}$ est une base d'Aronhold.

Ce résultat est obtenue par une proposition dans le contexte des formes quadratiques (voir Proposition 1.1.5). Cela nous permet d'avoir un étiquetage pour tous les diviseurs thêta caractéristiques. Puis nous obtenons une structure complète de niveau 2 de $\mathcal{C}$. La Section 1.2.2 est une introduction aux surfaces de del Pezzo de degré d puis plus spécifiquement de degré 1. La Section 1.2.3 relie la configuration des diviseurs exceptionnels de $\mathcal{S}$ avec les diviseurs thêta caractéristiques de $\mathcal{C}$ en se concentrant sur la façon de trouver une base d'Aronhold.

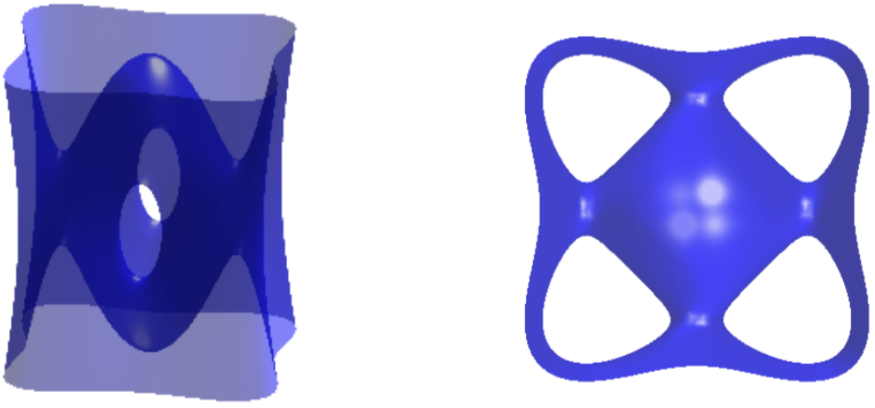


FIGURE 2: Une surface de del Pezzo de degré 2 [7].

Cryptographie sur les Courbes Hyperelliptiques

Les fonctions thêta apparaissent également dans *la cryptographie sur les courbes hyperelliptiques* (CCHE) [25]). À partir des remarques dans [22], Gaudry montre que la multiplication scalaire peut être accélérée en travaillant sur la variété de Kummer plutôt que sur la jacobienne d'une courbe de genre 2 [44]. Soit $\mathcal{A}$ une variété abélienne, *la variété de Kummer associée* à $\mathcal{A}$ est le quotient $\mathcal{K}_\mathcal{A} = \mathcal{A}/(-1)$ par l'automorphisme (-1) agissant sur $\mathcal{A}$. Considérons la jacobienne $\mathrm{Jac}(\mathcal{C})$ d'une courbe $\mathcal{C}$ de genre 2. Notons $\mathcal{K}_\mathcal{C}$ la variété de Kummer associée à $\mathrm{Jac}(\mathcal{C})$. Il est possible d'avoir un modèle de $\mathcal{K}_\mathcal{C}$ dans $\mathbb{P}^3$ par quatre fonctions thêta avec certaines caractéristiques, appelons-les *fonctions thêta fondamentales*. La structure de groupe de $\mathrm{Jac}(\mathcal{C})$ induit une structure de pseudo-groupe sur $\mathcal{K}_\mathcal{C}$. Cette structure de pseudo-groupe ainsi que certaines identités parmi les fonctions thêta fondamentales nous permet de faire de l'arithmétique sur $\mathcal{K}_\mathcal{C}$ grâce à des formules explicites [44, 81]. Dans la première partie du Chapitre 2, nous donnons une présentation courte, compact et autonome pour CCHE et *Kummer basée CCHE* (*KCCHE*) en le genre 2 en faisant un état de l'art du sujet afin de constituer un arrière-plan mathématique.

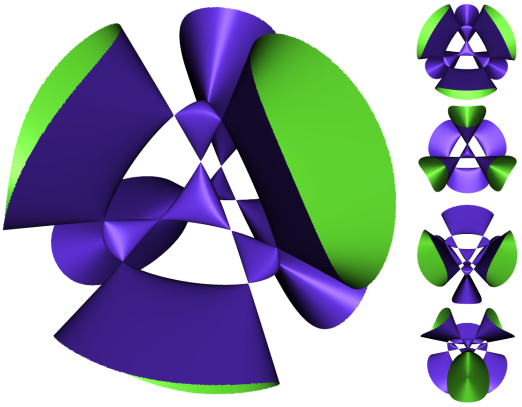


FIGURE 3: Une surface de Kummer [85].

La cryptographie asymétrique (voir [25, Chapitre 1]) est un système cryptographique qui utilise des paires de clés publiques et privées. Les clés publiques peuvent être distribuées et les clés privées sont seulement connues par le propriétaire. Le concept de la cryptographie asymétrique est apparu avec Diffie et Helman [31] en 1976. *La cryptographie sur les courbes elliptiques* (CCE) est devenue une approche courante et standard pour la cryptographie asymétrique. Les jacobiennes de courbes hyperelliptiques ont également été considérées pour des objectifs cryptographiques comme une alternative aux courbes elliptiques dans la cryptographie asymétrique. En effet, CCHE nécessite des corps finis plus petits que CCE à un niveau de sécurité similaire. Cependant, le nombre d'opérations sur le corp est plus important que dans CCHE. La comparaison CCE avec CCHE dépend donc non seulement des paramètres de la courbe, de l'optimisation de l'algorithme mais aussi de la manière de l'implémenter. En d'autres termes, en dehors de la complexité temporelle et de la sécurité mathématique des algorithmes. Par conséquent, il est également important de les analyser en les implémentant sur des plates-formes matérielles telles que des field *programmable gate arrays* (FPGAs [25]). KCCHE fournit des résultats prometteurs pour les implémentations de logiciels embarqués [81]. Les architectures matérielles pour KCCHE basées sur [81] pour la multiplication scalaire et leurs implémentations FPGA sont présentées dans [42] qui est un travail commun avec Gabriel Gallin et Arnaud Tisserand dans un projet *Hardware and Arithmetic for Hyperelliptic Curves Cryptography Project* (*HAH*) [62]. Je suis en effet un membre du projet HAH et j'avais mission de fournir les éléments mathématiques à l'implémentation de KCCHE. Le travail conjoint étudie et évalue l'impact de divers paramètres d'architecture sur le coût et les performances tels que le type, la taille et le nombre d'unités (arithmétique, mémoire, communications internes) ; topologie de l'architecture ; l'exploitation du parallélisme interne. Les architectures sont conçues pour $\mathbb{F}_p$ avec un nombre premier générique p et implémentées sur différents FPGA. Dans la deuxième partie du Chapitre 2, nous présentons les résultats de ces implémentations FPGA et les comparons avec des travaux similaires pour CCHE et CCE dans la littérature après avoir donné une courte description de [81]. La partie principale du travail, c'est-à-dire l'ingénierie, est réalisée par l'équipe d'informatique. J'ai écarté de ce travail les prérequis informatiques hors de ma spécialisation.

Calculs de p-rang

Il s'agit d'une collaboration avec Yara Elias, Burçin Güneş, Rachel Newton, Ekin Ozman, Rachel Pries et Lara Thomas, qui a débuté au Women in Numbers Europe 2 workshop au Centre Lorentz, Leiden [19].

Soit p un nombre premier et soit k un corps algébriquement clos de caractéristique p. Soit A une variété abélienne de dimension g définie sur k. Le *p-rang* de A est l'entier f défini par $\#A[p](k) = p^f$. On sait que $0 \leq f \leq g$. Quand $f = g$, on dit que A (ou X) est *ordinaire*. Soit X une courbe connexe projective lisse de genre g définie sur k. Alors le *p-rang de* X est le p-rang de sa jacobienne.

Exemple. *Supposons que X est une courbe hyperelliptique lisse du genre g, donné par $y^2 = f(x)$ pour un polynôme $f(x) \in k[x]$ ayant un degré $2g+1$ ou $2g+2$ qui a des racines distinctes. Soit c_s le coefficient de x^s dans le développement $f(x)^{\frac{p-1}{2}}$. Pour $0 \leq l \leq g-1$, soit M_l la matrice $g \times g$ dont l'entrée i, j est $(c_{ip-j})^{p^l}$. Le p-rang de X est le rang de $\prod_{i=0}^{g-1} M_{g-1-i}$.*

Le p-rang est un invariant pour les variétés abéliennes qui joue un rôle pour comprendre la structure de l'espace de modules $\mathcal{A}_g$ de variétés abéliennes principalement polarisées de dimension g définies sur un corps algébriquement clos k de caractéristique $p > 0$. Il induit des stratifications importantes de $\mathcal{A}_g$. Si l'on considère l'espace des modules $\mathcal{M}_g$ des courbes lisses, irréductibles, projectives du genre g alors l'application de Torelli $j : \mathcal{M}_g \to \mathcal{A}_g$, nous permet de définir les stratifications analogues sur $\mathcal{M}_g$ par les sous-structures $\mathcal{M}_g^f$ de $\mathcal{M}_g$ où chaque point correspond à des courbes de genre g et p-rang f (voir [1] et [2], pour la stratification de l'espace de modules des courbes hyperelliptiques du genre g par le p-rang). Pour des raisons de dimension, cela donne beaucoup d'informations quand $1 \leq g \leq 3$ et peu d'informations quand $g \geq 4$. Dans le Chapitre 3, nous nous considérons le probléme analogue sur l'espace de modules $\mathcal{R}_g$ des revêtements doubles non-ramifiés $\pi \colon Y \to X$ où X est une courbe lisse du genre g en étudiant la strate $\mathcal{R}_g^{(f,f')}$ pour laquelle X est de p-rang f et *la variété de Prym* P_π est de p-rang f'.

Plus précisément, considérons une revêtement double non-ramifié

$$\pi : Y \longrightarrow X.$$

Alors $\mathrm{Jac}(Y)$ est isogène à $\mathrm{Jac}(X) \oplus P_\pi$ où P_π est la variété de Prym de π. Dans ce contexte, P_π est une variété abélienne principalement polarisée de dimension $g-1$. Le p-rang f' de P_π satisfait $0 \leq f' \leq g-1$. Puisque le p-rang est un invariant d'isogénie, le p-rang de Y est égal à $f + f'$.

Maintenant, la question suivante se pose naturellement.

Question. *Supposons que p est un nombre premier impair et g, f, f' sont des entiers tels que $g \geq 2$, $0 \leq f \leq g$, et $0 \leq f' \leq g-1$ Existe-t-il une courbe X définie sur k de genre g et de p-rang f ayant une revêtement double non-ramifié $\pi : Y \longrightarrow X$ tel que P_π a p-rang f' ?*

La réponse à la question est oui pour $p \geq 3$ et $0 \leq f \leq g$ sous les restrictions suivantes,

- quand $g = 2$ [79, Proposition 6.1], sauf si $p = 3$ et $f = 0, 1$ et $f' = 0$, auquel cas la réponse est non [37, Exemple 7.1] ;

- quand $g \geq 3$ et $f' = g-1$, comme un cas particulier de [79, Théorème 1.1 (1)] ;

- quand $g \geq 3$ et $f' = g - 2$ (avec $f \geq 2$ quand $p = 3$), par [79, Théorème 7.1] ;

- quand $p \geq 5$ et $g \geq 4$ et $\frac{g}{2} - 1 \leq f' \leq g - 3$, par [79, Corollaire 7.3].

Nous étudions le premier cas ouvert de la question, qui se produit lorsque X a genre $g = 3$ et P_π a p-rang 0. Nous nous concentrons sur le cas où X est un quartique plane lisse ou, de façon équivalente, que X n'est pas hyperelliptique. En tant qu'application, nous vérifions que la réponse à la question est oui quand $g = 3$ et $3 \leq p \leq 19$.

Étant donné une courbe $Z : z^2 = D$ de genre 2 où $D \in k[x]$, il est possible de décrire toutes les quartiques planes lisses X ayant une revêtement double non-ramifié $\pi : Y \to X$ dont la variété de Prym P_π est isomorphe à $\mathrm{Jac}(Z)$. Plus précisément, la variété de Kummer $K = \mathrm{Jac}(Z)/\langle -1 \rangle$ de $\mathrm{Jac}(Z)$ est une surface quartique dans $\mathbb{P}^3$. Chaque plane lisse quartique X ayant une revêtement double non-ramifié $\pi : Y \to X$ tel que $P_\pi \simeq \mathrm{Jac}(Z)$, provient de l'intersection $V \cap K$, pour un plan $V \subset \mathbb{P}^3$ [76, 95, 18]. En se basant sur le travail de Kudo et Harashita [59], nous fournissons une méthode pour déterminer la matrice de Hasse-Witt de X à partir de V et Z dans la Proposition 3.4.3.

Supposons que $\pi : Y \to X$ est une revêtement double non-ramifié avec $P_\pi \simeq \mathrm{Jac}(Z)$ comme dans le paragraphe précédent. Dans la Section 3.5, nous choisissons d'abord $Z : z^2 = x^6 - 1$ et vérifions dans la Proposition 3.5.2 que la réponse à la question est oui quand $(g, f, f') = (3, 3, 0)$ et $p \equiv 5 \bmod 6$.

Dans la seconde partie de la Section 3.5, pour une courbe lisse arbitraire Z du genre 2, nous utilisons l'algèbre commutative pour analyser la condition suivant

$$X \text{ est non-ordinaire et } Z \text{ est de } p\text{-rang } 0. \qquad (\star\star)$$

Dans la Proposition 3.5.7, nous démontrons cette condition $(\star\star)$ est équivalente à l'annulation de 4 polynômes homogènes de degré $(p+1)(p-1)/2$ dans les coefficients de D et l'annulation d'un polynôme homogène de degré $6(p-1)$ dans les coefficients de D et V. Comme application, quand $p = 3$, on donne une caractérisation explicite des courbes Z et des plans V pour lesquels $\pi : Y \to X$ vérifie la condition (*), voir la Section 3.5.6.

Par souci d'exhaustivité, nous présentons tous les résultats suivants de [19] sans leurs preuves dans la dernière partie du Chapitre 3. C'est une application des résultats décrits ci-dessus pour les courbes de genre 3 en petite caractéristique pour étudier les p-rangs de variétés de Prym de courbes lisses de genre arbitraire $g \geq 3$. Pour cela, une méthode inductive développée dans [1] est utilisée. Ceci donne le Corollaire 3.7.7, qui étend [79, Corollary 7.3] pour de petites valeurs de p et donne l'application suivante.

Corollaire. *Soit $3 \leq p \leq 19$. La réponse à la question est oui, pour tout $g \geq 2$, sous les conditions suivantes sur (f, f'),*

1. *Si $g = 3r$ et (f, f') est tel que $2r \leq f \leq g$ et $r - 1 \leq f' \leq g - 1$;*

2. *Si $g = 3r + 2$ et (f, f') est tel que $2r \leq f \leq g$ et $r \leq f' \leq g - 1$, (avec $f \geq 2r + 2$ quand $p = 3$) ;*

3. *Si $g = 3r + 4$ et (f, f') est tel que $2r \leq f \leq g$ (avec $f \geq 2r + 4$ quand $p = 3$) et $r + 1 \leq f' \leq g - 1$.*

Tous les résultats d'existence pour les p-rangs décrits ci-dessus sont prouvés en utilisant un analyse géométrique de la stratification des espaces de modules de courbes et des revêtements doubles non-ramifiés par le p-rang. Par exemple, [37, Théorème 2.3] montre

que la strate $\mathcal{M}_g^f$ de $\mathcal{M}_g$ est non vide et chaque composant a une dimension $2g-3+f$, voir aussi [1, Section 3].

Considérons l'espace des modules $\mathcal{R}_g$. Une fois prouvé que $\mathcal{R}_g^{(f,f')} \neq \emptyset$ on peut s'intéresser à sa dimension.

Supposons que $\mathcal{R}_g^{(f,f')}$ est non vide. Comme application des résultats de pureté pour la stratification par les polygones de Newton, Ozman et Pries montrent que : si $\mathcal{R}_g^{(f,f')}$ n'est pas vide, alors chacun de ses composants a une dimension au moins $g-2+f+f'$ dans [79, Proposition 5.2] .

En fait, la dimension de $\mathcal{R}_g^{(f,f')}$ atteint cette borne inférieure dans les cas suivants,

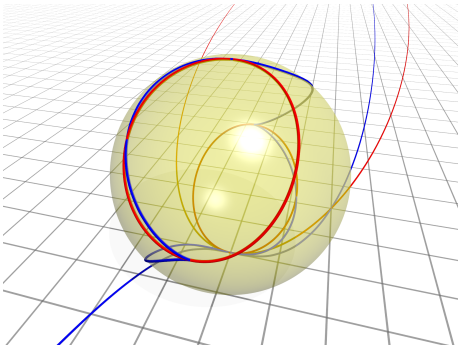
- quand $f'=g-1$, alors chaque composant de $\mathcal{R}_g^{(f,f')}$ a une dimension $2g-3+f$ comme un cas particulier de [79, Théorème 1.1 (1)] ;
- quand $f'=g-2$, avec $f\geq 2$ quand $p=3$, alors chaque composante de $\mathcal{R}_g^{(f,f')}$ a une dimension $2g-4+f$ [79, Théorème 7.1] ;
- quand $p\geq 5$ et $\frac{g}{2}-1\leq f'\leq g-3$, alors au moins une composante de $\mathcal{R}_g^{(f,f')}$ a une dimension $g-2+f+f'$ [79, Corollaire 7.3].

Le Théorème 3.7.6, valable pour tout nombre premier p et un résultat inductif permettent de tirer parti de l'information lorsque $g=3$ sur $\mathcal{R}_3^{(f,0)}$ afin d'obtenir des informations sur $\mathcal{R}_g^{(f,f')}$ pour tout genre g. Le résultat final est le Corollaire 3.7.7 ; il prouve l'existence des revêtements doubles non-ramifiés $\pi : Y \to X$ avec un contrôle sur le p-rang f de X et le p-rang f' de P_π si f est supérieur à environ $2g/3$ et f' est supérieur à environ $g/3$.

Corollaire. *Si $3\leq p\leq 19$, la strate $\mathcal{R}_g^{(f,f')}$ a une composante (non vide) de dimension $g-2+f+f'$ pour tout $g\geq 2$ sous les conditions pour (f,f') trouvées dans le corollaire précédent.*

Introduction

Algebraic curves are central objects in algebraic geometry which come into light also in arithmetic geometry and in various applications such as cryptography, theoretical physics etc. In this thesis, we study them under these different aspects.



Computations of Theta Constants

One way to understand an algebraic curve is to study the group structure called *Jacobian* associated to the curve. *Theta constants* play an important role to figure out the relation between a curve and its Jacobian.

Explicit computations of theta constants are closely related to a classical problem that asks which complex principally polarized abelian varieties arise as Jacobian varieties of curves. The problem is called the *Schottky problem* and that goes back to Riemann [82, 83]. The field has been improved by a wide range of mathematicians until present. See [39] for a well described history of the subject. Another related question is to try to recover the curve explicitly from its Jacobian. See [86] for the case $g = 2$, [93, 57] for the general hyperelliptic case, and [96, 48] for the non-hyperelliptic case when $g = 3$. In addition, the topic has many applications in different areas such as theoretical physics [36] via integrable systems, and cryptography [97] via AGM-style point counting algorithms [84] and more recently isogeny based cryptography [69].

Let $g \geq 0$ be an integer. Denote $\mathcal{M}_g$ the moduli space over $\mathbb{C}$ of curves of genus g and $\mathcal{A}_g$ the moduli space of complex principally polarized abelian varieties of dimension g. The *Torelli map*

$$j : \mathcal{M}_g \to \mathcal{A}_g \tag{2}$$

maps the isomorphism class of a curve to the isomorphism class of its Jacobian with its canonical polarization. The Schottky problem is to characterize the locus of Jacobians $\mathcal{J}_g$ which is defined to be the closure of $j(\mathcal{M}_g)$ in $\mathcal{A}_g$. The classical approach to the problem is to try to embed $\mathcal{A}_g$ in a projective space and try to find the defining ideal for $\mathcal{J}_g$.

Let

$$\mathbb{H}_g = \{\tau \in \mathrm{GL}_g(\mathbb{C}) \mid {}^t\tau = \tau,\ \mathrm{Im}\tau > 0\}$$

be the Siegel upper half space consisting of $g \times g$ complex matrices with positive definite imaginary part.

For $\tau \in \mathbb{H}_g$, $z = (z_1, \ldots, z_g) \in \mathbb{C}^g$ and

$$[q] = \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} \in \mathbb{Z}^g \oplus \mathbb{Z}^g,$$

the theta function with characteristic $[q]$ is

$$\vartheta[q](z,\tau) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i(n+\varepsilon/2)\tau^t(n+\varepsilon/2) + 2\pi i(n+\varepsilon/2)^t(z+\varepsilon'/2)\right).$$

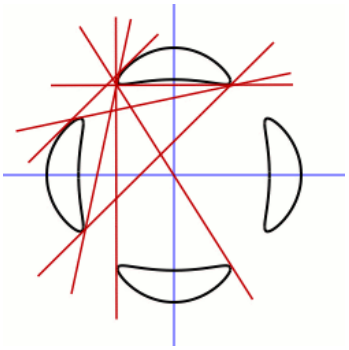
The evaluation of this function at $z = 0$, which is $\vartheta[q](\tau) = \vartheta[q](0,\tau)$, is called a *theta constant* (*Thetanullwert*). The *characteristic* $[q]$ is called *even* (resp. *odd*) if the usual scalar product $\varepsilon \cdot \varepsilon'$ is even (resp. odd). If the characteristic $[q]$ is even (resp. odd), the theta constant $\vartheta[q](\tau)$ is called *even* (resp. *odd*). Note that the theta constant $\vartheta[q](\tau)$ is identically zero for all $\tau \in \mathbb{H}_g$ if and only if the characteristic $[q]$ is odd.

On the other hand, any $\tau \in \mathbb{H}_g$ defines a complex principally polarized abelian variety $\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$. The symplectic group $\mathrm{Sp}(2g,\mathbb{Z})$ acts on $\mathbb{H}_g$. The quotient $\mathbb{H}_g/\mathrm{Sp}(2g,\mathbb{Z})$ is the moduli space $\mathcal{A}_g$. There is a level cover $\mathcal{A}'_g \to \mathcal{A}_g$, where $\mathcal{A}'_g$ is the quotient of $\mathbb{H}_g$ by a certain subgroup of $\mathrm{Sp}(2g,\mathbb{Z})$ denoted $\Gamma_g(4,8)$. Even theta characteristics provide a map

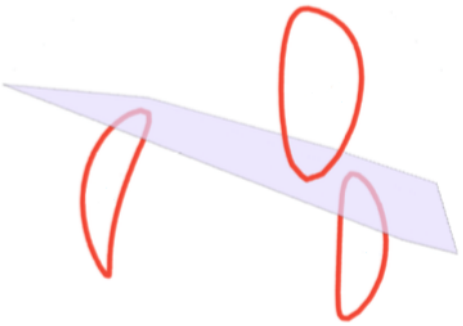
$$\begin{aligned} \Phi : \mathcal{A}'_g &\to \mathbb{P}^{2^{g-1}(2^g+1)}, \\ \tau &\mapsto (\vartheta[q](\tau))_q \end{aligned}$$

which is an embedding when q ranges over the set of even theta characteristics. Actually, the study to determine all the relations among the even theta characteristics amounts to try to understand the image under the map Φ (see [88]).

In Chapter 1, we give an algorithm to compute the fourth power of the quotient of any pair of even theta constants corresponding to a period matrix in $\mathbb{H}_g$ of a non-hyperelliptic curve of any genus $g \geq 3$ in the case that a complete 2-level structure is given. Let $\mathcal{C}$ be a projective, smooth, non-hyperellitic curve of genus g over a field $k \subseteq \mathbb{C}$. We define the *Jacobian* of $\mathcal{C}$ as $\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$ with respect to a *normalized period matrix* τ in $\mathbb{H}_g$. Denote it $\mathrm{Jac}(\mathcal{C})$. A *complete* 2*-level structure* is represented via the defining equations of the image of $\mathcal{C}$ under the canonical embedding and certain divisors on the curve with a suitable labelling as follows. Such divisors are called *theta characteristic divisors*. There are two kinds of theta characteristic divisors, *even* and *odd*, which depend on the dimension of the associated Riemann-Roch spaces. Note that the odd theta characteristic divisors correspond to some geometric objects called *multitangents* on the curve for arbitrary genus. For instance, these objects are called *bitangents* when $g = 3$ and *tritangents* when $g = 4$.



(a) Bitangents on the Trott Curve [85].



(b) A tritangent of a curve with three ovals [60].

On the other hand, there is a canonical correspondence between the theta characteristic divisors on $\mathcal{C}$ and the quadratic forms on $\mathrm{Jac}[2](\mathcal{C})$ over $\mathbb{F}_2$ where $\mathrm{Jac}[2](\mathcal{C})$ denotes the 2-torsion points of $\mathrm{Jac}(\mathcal{C})$. The quadratic forms are *labelled* through a combinatorial data which is called an *Aronhold basis*. Section 1.1 recalls a part of the mathematical background which is needed for the algorithm.

Computing such quotient is well known and given by a closed formula for a curve of $g \leq 3$ and hyperelliptic curves of any genus, see [94, 96]. These formulas can be seen as an explicit description of the Torelli map. Indeed, a principally polarized abelian variety can be written as an intersection of explicit quadrics in a projective space [73]. The coefficients of these quadrics are determined by theta constants. These formulas express theta constants in terms of geometry of the curve. In the case of a hyperelliptic curve given by $y^2 = \prod_{i=1}^{2g+2}(x - \alpha_i)$, we have

$$\vartheta[q](\tau)^4 = (2i\pi)^{-2g} \cdot \det(\Omega_1)^2 \cdot \prod_{i,j \in U} (\alpha_i - \alpha_j),$$

where Ω_1 is the first half of a period matrix and U is a set of indices depending on the characteristic $[q]$ [94, Page 218]. This formula, which we call the *absolute Thomae formula*, has then been reproved by [41, 10, 40] using the variational method. A simpler version, which we call the *relative Thomae formula*, expressing the quotient $\vartheta[q](\tau)^8/\vartheta[q'](\tau)^8$ was then achieved in [102, 75, 34] using elementary arguments. Note that this formula, which involves only the roots α_i, is generally sufficient to recover the Jacobian and can moreover be worked out over an arbitrary field [91]. The issue of finding the correct 8th roots of the quotients is considered for $g = 1, 2$ in [26] and can be simply solved over $\mathbb{C}$ by computing the theta contants with a weak precision.

For the non-hyperelliptic curve $\mathcal{C}$ of $g = 3$, for any two even theta characteristics p_1, p_2 we have

$$\left(\frac{\vartheta[p_1](\tau)}{\vartheta[p_2](\tau)}\right)^4 = (-1)^n \cdot \frac{[\beta_1, \beta_2, \beta_3] \cdot [\beta_1, \beta_{12}, \beta_{13}] \cdot [\beta_{12}, \beta_2, \beta_{23}] \cdot [\beta_{13}, \beta_{23}, \beta_3]}{[\beta_{23}, \beta_{13}, \beta_{12}] \cdot [\beta_{23}, \beta_3, \beta_2] \cdot [\beta_3, \beta_{13}, \beta_1] \cdot [\beta_2, \beta_1, \beta_{12}]}, \qquad (\star)$$

where $[\beta_i, \beta_j, \beta_k]$ is the determinant of the coefficients of the equations β_i, β_j and β_k which are certain bitangents labelled via an Aronhold basis [77, Theorem 3.1] and $n = 0, 1$ can be computed depending on p_1, p_2. This formula is called *Weber's formula*. Nevertheless, for any genus $g \geq 3$, the quotient $\left(\frac{\vartheta[p_1](\tau)}{\vartheta[p_2](\tau)}\right)^4$ is expressed as a quotient of determinants of regular sections associated to certain line bundles over $\mathcal{C}$. For explicit computations, we translate this algebraic expression into a quotient which is formed by some functions in certain Riemann-Roch spaces. We show the following theorem and thus have the algorithm.

Theorem. *Let $\tilde{Q}_i^r$ and $\tilde{Q}_i^s$ be the quotients of ternary quadratic forms and A_i's (resp. B_i's) be fixed representatives for the contact points of $\mathcal{C}$ with a specific multitangent for $i = 1, \ldots, g-1$. For any two even theta characteristics p_1, p_2, we have*

$$(-1)^n \cdot \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4}$$
$$= \frac{d_1 \begin{vmatrix} \tilde{Q}_1^s(B_1) & \cdots & \tilde{Q}_{g-1}^s(B_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^s(B_{g-1}) & \cdots & \tilde{Q}_{g-1}^s(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \tilde{Q}_1^r(A_1) & \cdots & \tilde{Q}_{g-1}^s(A_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^r(A_{g-1}) & \cdots & \tilde{Q}_{g-1}^r(A_{g-1}) \end{vmatrix}^2}{d_2 \begin{vmatrix} \tilde{Q}_1^r(B_1) & \cdots & \tilde{Q}_{g-1}^r(B_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^r(B_{g-1}) & \cdots & \tilde{Q}_{g-1}^r(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \tilde{Q}_1^s(A_1) & \cdots & \tilde{Q}_{g-1}^s(A_1) \\ \vdots & & \vdots \\ \tilde{Q}_1^s(A_{g-1}) & \cdots & \tilde{Q}_{g-1}^s(A_{g-1}) \end{vmatrix}^2},$$

where d_1, d_2 are the values of products of linear forms defining certain multitangents at the points A_i and B_i's and $n = 0, 1$ is given purely in terms of p_1, p_2. (For the complete statement, see Theorem 1.2.4.)

In order to apply this algorithm, one needs a complete 2-level structure of genus g. Firstly, we applied the algorithm on an example of a non-hyperelliptic curve of genus 3. In this case, to have an Aronhold basis is enough for the procedure of the algorithm. Indeed, this set gives a model (*Riemann model* [32, Chapter 6]) for the curve, all the equations of 28 bitangents of the curve and an elegant labelling for all the theta characteristic divisors, i.e. gives a complete 2-level structure. In addition, I was able to verify the algorithm via the closed formula of Weber ($\star$).

For higher genus, we focus on the case $g = 4$. We studied Bring's curve. Although we had the equations of all 120 tritangents, we could not overcome the labelling problem efficiently in general. Therefore, we focused on a family of curves which comes from del Pezzo surfaces. Thus we were able to obtain a complete 2-level structure of genus 4. In the second part of Chapter 1, with the motivation of illustrating the algorithm, we shortly explain the geometric structure of del Pezzo surfaces and show how to get a complete 2-level structure for a non-hyperelliptic curve of genus 4. Let $\mathcal{S}$ be a del Pezzo surface of degree 1. The surface $\mathcal{S}$ is the blow up of eight points in general position in $\mathbb{P}^2$. If $\kappa_{\mathcal{S}}$ is the canonical divisor of $\mathcal{S}$, then the linear system $|-2\kappa_{\mathcal{S}}|$ yields a double cover from $\mathcal{S}$ to a quadratic cone in $\mathbb{P}^3$, and the branch curve defines a curve $\mathcal{C}$ of genus 4. The positive point is that there is a 2-1 correspondence between the exceptional divisors of $\mathcal{S}$ and the odd theta characteristic divisors of $\mathcal{C}$ [101]. We compute the equations of all 120 tritangents of $\mathcal{C}$ via computing the equation of the surface by starting from 8 points in $\mathbb{P}^2$ in general position and the exceptional curves of $\mathcal{S}$ by Magma. In this case, note that Aronhold bases come naturally via the configuration of exceptional divisors on $\mathcal{S}$. Indeed, let $\rho : \operatorname{Pic}\mathcal{S} \to \operatorname{Pic}\mathcal{C}$ be the restriction homomorphism from the Picard group of $\mathcal{S}$ to the Picard group of $\mathcal{C}$. We show the following proposition after some observations about the structure of 2-torsion points $\operatorname{Pic}(\mathcal{C})[2]$ of $\operatorname{Pic}(\mathcal{C})$.

Proposition. *Suppose that $E_1, \ldots, E_8$ are the exceptional divisors corresponding to the eight points under the blow up map. Let $v_i = \rho(E_i + \kappa_{\mathcal{S}}) \in \operatorname{Pic}^0(\mathcal{C})$ for $i = 1, \ldots, 8$ and $v_9 = v_1 + \cdots + v_8$. For any odd theta characteristic divisor D of $\mathcal{C}$, the set $\{D + v_i + v_9 \mid i = 1, \ldots, 9\}$ is an Aronhold set.*

This result is obtained by a proposition in the context of quadratic forms, see Proposition 1.1.5. It enables us to have a labelling for all theta characteristic divisors. Hence

we have obtained a complete 2-level structure of $\mathcal{C}$. Section 1.2.2 is an introduction to del Pezzo surfaces of firstly any degree d and then of degree 1. Section 1.2.3 relates the configuration of exceptional divisors of $\mathcal{S}$ with the theta characteristic divisors of $\mathcal{C}$ by focusing on how to find an Aronhold basis.

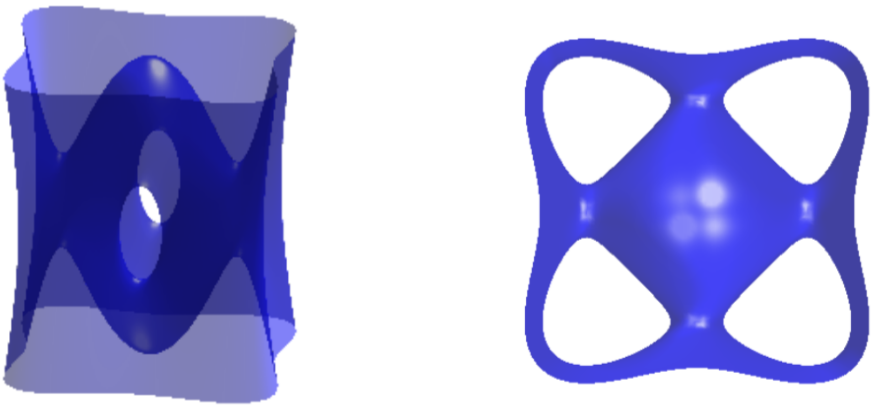


Figure 5: A del Pezzo surface of degree 2 [7].

Hyperelliptic Curve Cryptography

Theta functions arise also in *hyperelliptic curve cryptography* (HECC [25]). Based on remarks in [22], Gaudry [44] shows that scalar multiplication can be accelerated by working on the Kummer variety instead of on the Jacobian of a curve of genus 2. Let $\mathcal{A}$ be an abelian variety. The *Kummer variety* associated to $\mathcal{A}$ is the quotient $\mathcal{K}_{\mathcal{A}} = \mathcal{A}/(-1)$ by the automorphism (-1) acting on $\mathcal{A}$. Consider the Jacobian $\mathrm{Jac}(\mathcal{C})$ of a curve $\mathcal{C}$ of genus 2. Denote $\mathcal{K}_{\mathcal{C}}$ the Kummer variety associated to $\mathrm{Jac}(\mathcal{C})$. It is possible to have a model of $\mathcal{K}_{\mathcal{C}}$ in $\mathbb{P}^3$ by four theta functions with certain characteristics, call them *fundamental theta functions*. The group structure of $\mathrm{Jac}(\mathcal{C})$ endows a pseudo group structure on $\mathcal{K}_{\mathcal{C}}$. Thanks to the pseudo group law and some identities among the fundamental theta functions, we are able to do arithmetic on $\mathcal{K}_{\mathcal{C}}$ by explicit formulas [44, 81]. In the first part of Chapter 2, we present a compact and self-contained text for HECC and *Kummer based HECC* (KHECC) in genus 2 constituting mathematical background.

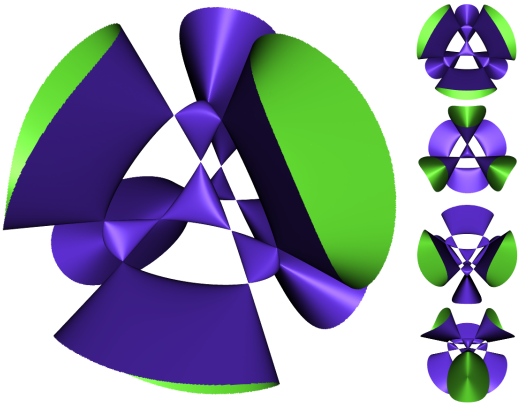


Figure 6: A Kummer surface [85].

Public key cryptography [25, Chapter 1] is a cryptographic system that uses pairs of keys which are public and private. Public keys might be distributed and private keys are only known by the owner. This system originated with Diffie and Helman [31] in 1976. *Elliptic curve cryptography* (ECC) has become a common and standard approach for public key cryptography. The Jacobians of hyperelliptic curves have also been considered for cryptographic objectives as an alternative for elliptic curves in public key cryptography. Indeed, HECC requires smaller finite fields than ECC at a similar security level. However, the number of field-level operations is bigger than in HECC. So the comparison ECC with HECC depends on not only curve parameters, algorithm optimisation but also on the implementation way. Hence, it is also important to analyze them by implementing on hardware platforms such as field programmable gate arrays (FPGAs [25]). KHECC provides promising results for embedded software implementations [81]. Hardware architectures for KHECC based on [81] for scalar multiplication and their FPGA implementations are presented in [42] which is a joint work with Gabriel Gallin and Arnaud Tisserand in *Hardware and Arithmetic for Hyperelliptic Curves Cryptography* (HAH) project [62]. Indeed, I was a member of HAH project and had the mission to provide the mathematical components for the implementation of KCCHE. The joint work studies and evaluates the impact of various architecture parameters on the cost and performances such as type, size and number of units (arithmetic, memory, internal communications); architecture topology; and exploitation of internal parallelism. The architectures are designed for $\mathbb{F}_p$ with a generic prime number p and implemented on different FPGAs. In the second part of Chapter 2, we present results of these FPGA implementations with a comparison by similar works for HECC and ECC in the literature after giving a short description of [81]. I dismiss computer scientific background which is out of my research area. The main part of the work i.e. the engineering, is realised by the team of computer science. Nevertheless, we present a summary of the results after introducing a compact text looking at literature about (KH)ECC from mathematical point of view.

p-rank Computations

This is a joint work with Yara Elias, Burçin Güneş, Rachel Newton, Ekin Ozman, Rachel Pries and Lara Thomas which began at the Women in Numbers Europe 2 workshop in the Lorentz Centre, Leiden [19].

Let p be a prime number and let k be an algebraically closed field of characteristic p. Let A be an abelian variety of dimension g defined over k. The *p-rank* of A is the integer f defined by $\#A[p](k) = p^f$. It is known that $0 \leq f \leq g$. When $f = g$, we say that A (or X) is *ordinary*. Let X be a smooth projective irreducible curve of genus g defined over k. Then the *p-rank of* X is the p-rank of its Jacobian.

Example. *Assume that X is a smooth hyperelliptic curve of genus g given by $y^2 = f(x)$ for a polynomial $f(x) \in k[x]$ having degree $2g+1$ or $2g+2$ which has distinct roots. Let c_s denote the coefficient of x^s in the expansion $f(x)^{\frac{p-1}{2}}$. For $0 \leq l \leq g-1$, let M_l be the $g \times g$ matrix whose ijth entry is $(c_{ip-j})^{p^l}$. The p-rank of X is the rank of $\prod_{i=0}^{g-1} M_{g-1-i}$.*

The p-rank is an invariant for abelian varieties which plays a role to understand the structure of moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g defined over an algebraically closed field k of characteristic p. It induces important stratifications of $\mathcal{A}_g$. If we consider the moduli space $\mathcal{M}_g$ of smooth, connected, projective curves of genus g then the Torelli map $j : \mathcal{M}_g \to \mathcal{A}_g$ allows us to define the analogous stratifications on $\mathcal{M}_g$ by substructures $\mathcal{M}_g^f$ of $\mathcal{M}_g$ where each point corresponds to curves of genus g and p-rank f (see [1]). (For the p-rank stratification of the moduli space of hyperelliptic curves of genus g, see [2].) Because of dimension reasons, this gives a lot of informations when $1 \leq g \leq 3$ and little information when $g \geq 4$. In Chapter 3, we focus on the moduli space $\mathcal{R}_g$ of unramified double covers $\pi \colon Y \to X$ where X is a smooth curve of genus g by studying strata $\mathcal{R}_g^{(f,f')}$ for which X has p-rank f and the Prym variety P_π has p-rank f'.

More precisely, we assume that p is odd from now on and we consider an unramified double cover

$$\pi : Y \longrightarrow X.$$

Then $\mathrm{Jac}(Y)$ is isogenous to $\mathrm{Jac}(X) \oplus P_\pi$ where P_π is the *Prym variety* of π. In this context, P_π is a principally polarized abelian variety of dimension $g-1$. The p-rank f' of P_π satisfies $0 \leq f' \leq g-1$. Since the p-rank is an isogeny invariant, the p-rank of Y equals $f + f'$.

Now the following question arises naturally.

Question. *Suppose that p is an odd prime, and g, f, f' are integers such that $g \geq 2$, $0 \leq f \leq g$, and $0 \leq f' \leq g-1$. Does there exist a curve X defined over k of genus g and p-rank f having an unramified double cover $\pi : Y \longrightarrow X$ such that P_π has p-rank f'?*

The answer to the question is yes for $p \geq 3$ and $0 \leq f \leq g$ under the following restrictions,

- when $g = 2$ [79, Proposition 6.1], unless $p = 3$ and $f = 0, 1$ and $f' = 0$, in which case the answer is no [37, Example 7.1];
- when $g \geq 3$ and $f' = g-1$, as a special case of [79, Theorem 1.1(1)];
- when $g \geq 3$ and $f' = g-2$ (with $f \geq 2$ when $p = 3$), by [79, Theorem 7.1];
- when $p \geq 5$ and $g \geq 4$ and $\frac{g}{2} - 1 \leq f' \leq g-3$, by [79, Corollary 7.3].

We study the first open case of the question, which occurs when X has genus $g = 3$ and P_π has p-rank 0. We focus on the case that X is a smooth plane quartic or, equivalently, that X is non-hyperelliptic. As an application, we verify that the answer to the question is yes when $g = 3$ and $3 \leq p \leq 19$.

Given a genus 2 curve $Z : z^2 = D$ where $D \in k[x]$, it is possible to describe all smooth plane quartic curves X having an unramified double cover $\pi : Y \to X$ whose Prym variety P_π is isomorphic to $\mathrm{Jac}(Z)$. Specifically, the Kummer variety $K = \mathrm{Jac}(Z)/\langle -1 \rangle$ of $\mathrm{Jac}(Z)$ is a quartic surface in $\mathbb{P}^3$. Each smooth plane quartic X having an unramified double cover $\pi : Y \to X$ such that $P_\pi \simeq \mathrm{Jac}(Z)$ arises as the intersection $V \cap K$ for some plane $V \subset \mathbb{P}^3$ [76, 95, 18]. Building on work of Kudo and Harashita [59], we provide a method to determine the Hasse-Witt matrix of X from V and Z in Proposition 3.4.3.

Suppose that $\pi : Y \to X$ is an unramified double cover with $P_\pi \simeq \mathrm{Jac}(Z)$ as in the previous paragraph. In Section 3.5, we first choose $Z : z^2 = x^6 - 1$ and verify in Proposition 3.5.2 that the answer to the question is yes when $(g, f, f') = (3, 3, 0)$ and $p \equiv 5 \bmod 6$.

In the second part of Section 3.5, for an arbitrary smooth curve Z of genus 2, we use commutative algebra to analyze the condition that

$$X \text{ is non-ordinary and } Z \text{ has } p\text{-rank } 0. \qquad (\star\star)$$

In Proposition 3.5.7, we prove that condition $(\star\star)$ is equivalent to the vanishing of 4 homogeneous polynomials of degree $(p+1)(p-1)/2$ in the coefficients on D and the vanishing of one homogeneous polynomial of degree $6(p-1)$ in the coefficients of D and V. As an application, when $p = 3$, we give an explicit characterization of the curves Z and planes V for which $\pi : Y \to X$ satisfies condition $(\star\star)$, see Section 3.5.6.

For the sake of completeness, we present all the following results from our work [19] without their proofs in the last part of Chapter 3. It is an application of the results described above for genus 3 curves in small characteristic to study the p-ranks of Prym varieties of smooth curves of arbitrary genus $g \geq 3$. For this, an inductive method developed in [1] is used. This yields Corollary 3.7.7, which extends [79, Corollary 7.3] for small p and gives the following application.

Corollary. *Let $3 \leq p \leq 19$. The answer to the question is yes, for any $g \geq 2$, under the following conditions on (f, f'),*

1. *If $g = 3r$ and (f, f') is such that $2r \leq f \leq g$ and $r - 1 \leq f' \leq g - 1$;*
2. *If $g = 3r + 2$ and (f, f') is such that $2r \leq f \leq g$ and $r \leq f' \leq g - 1$, (with $f \geq 2r + 2$ when $p = 3$);*
3. *If $g = 3r + 4$ and (f, f') is such that $2r \leq f \leq g$ (with $f \geq 2r + 4$ when $p = 3$) and $r + 1 \leq f' \leq g - 1$.*

All of the existence results for p-ranks described above are proven using a geometric analysis of the p-rank stratification of moduli spaces of curves and their unramified covers. For example, [37, Theorem 2.3] shows that the p-rank f stratum $\mathcal{M}_g^f$ of $\mathcal{M}_g$ is non-empty and each component has dimension $2g - 3 + f$, see also [1, Section 3].

Consider the moduli space $\mathcal{R}_g$. Once we have that $\mathcal{R}_g^{(f,f')}$ is non-empty then we can study its dimension. Suppose that $\mathcal{R}_g^{(f,f')}$ is non-empty. As an application of purity results for the Newton polygon stratification, [79, Proposition 5.2] shows that, if $\mathcal{R}_g^{(f,f')}$ is non-empty, then each of its components has dimension at least $g - 2 + f + f'$.

In fact, the dimension of $\mathcal{R}_g^{(f,f')}$ attains this lower bound in the following cases,

- when $f' = g - 1$, then each component of $\mathcal{R}_g^{(f,f')}$ has dimension $2g - 3 + f$ as a special case of [79, Theorem 1.1(1)];

- when $f' = g - 2$, with $f \geq 2$ when $p = 3$, then each component of $\mathcal{R}_g^{(f,f')}$ has dimension $2g - 4 + f$ [79, Theorem 7.1];
- when $p \geq 5$ and $\frac{g}{2} - 1 \leq f' \leq g - 3$, then at least one component of $\mathcal{R}_g^{(f,f')}$ has dimension $g - 2 + f + f'$ [79, Corollary 7.3].

Theorem 3.7.6, for any prime p, is an inductive result that allows one to leverage information when $g = 3$ about $\mathcal{R}_3^{(f,0)}$ into information about $\mathcal{R}_g^{(f,f')}$ for arbitrarily large g. The final result is Corollary 3.7.7; it proves the existence of unramified double covers $\pi : Y \to X$ with control over the p-rank f of X and the p-rank f' of P_π as long as f is bigger than approximately $2g/3$ and f' is bigger than approximately $g/3$.

Corollary. *If $3 \leq p \leq 19$, the stratum $\mathcal{R}_g^{(f,f')}$ has a (non-empty) component of dimension $g - 2 + f + f'$ for all $g \geq 2$ under the conditions on (f, f') found in the previous corollary.*

Chapter 1

Theta Constants

In this chapter, we aim to give an algorithm to compute the fourth power of the quotient of theta constants associated to a non-hyperelliptic curve of genus $g \geq 3$. To obtain this algorithm, we also discuss how to study these curves combinatorially, algebraically and geometrically by emphasising the link between these perspectives alongside explaining theta functions and constants.

1.1 Background

1.1.1 Quadratic Forms over $\mathbb{F}_2$

In this section, we overview the theory of quadratic forms over $\mathbb{F}_2$ in parallel our requirements for Section 1.2.1. Throughout this section, we skip proofs for most of the statements, since the theory is classically well known. Once for all, we refer to [50] and [32, Section 5.1].

Let $g \geq 1$ be an integer and V be a vector space of dimension $2g$ over $\mathbb{F}_2$. We fix a bilinear, non-degenerate, alternating form $\langle , \rangle$ on V. Since $\operatorname{Char} \mathbb{F}_2 = 2$, there exists a basis $\{e_1, \ldots, e_g, f_1, \ldots, f_g\}$ such that the matrix $\mathcal{M}_g$ associated to the bilinear form $\langle , \rangle$ is

$$\mathcal{M}_g = \begin{pmatrix} 0_g & I_g \\ I_g & 0_g \end{pmatrix},$$

where $0_g, I_g$ are the zero, identity $g \times g$ matrices respectively. In other words,

$$\langle e_i, e_j \rangle = \langle f_i, f_j \rangle = 0 \text{ and } \langle e_i, f_j \rangle = \delta_{ij}$$

for all $i, j \in \{1, \ldots, g\}$. Such a basis is called a *symplectic basis*.

The *symplectic group* $\operatorname{Sp}(V)$ is the group of all $\mathbb{F}_2$-linear isomorphisms $T : V \to V$ with

$$\langle T(v), T(u) \rangle = \langle v, u \rangle.$$

It acts simply transitively on the set of symplectic bases on V. Also, $\operatorname{Sp}(V)$ is generated by the transvections T_u which are defined by

$$T_u(v) = v + \langle v, u \rangle u$$

with $u \neq 0$ in V.

We say that $q : V \to \mathbb{F}_2$ is a *quadratic form* on V if $q(u + v) = q(u) + q(v) + \langle u, v \rangle$ for all $u, v \in V$. Let QV denote the set of all quadratic forms on $(V, \langle , \rangle)$.

The vector space V has an action on QV. Indeed, we define the quadratic form $q+v$ by

$$(q+v)(u) = q(u) + \langle v, u\rangle$$

for any $q \in QV$ and $v \in V$. Since the form $\langle , \rangle$ is nondegenerate, the action is free. The equality $\#V = \#\mathrm{QV}$ implies that the action is also transitive. So, for any two quadratic forms $q, q' \in \mathrm{QV}$, there is a unique vector $v = q + q'$ such that

$$\langle v, u\rangle = q(u) + q'(u).$$

In other words, the space QV is a homogeneous space for V. This implies that the disjoint union

$$V \bigsqcup \mathrm{QV}$$

is an $\mathbb{F}_2$-vector space of dimension $2g+1$. The vector space V is a subspace of codimension 1. Also, the symplectic group acts on QV by

$$q \mapsto T(q),$$

where

$$Tq(T(v)) = q(v).$$

We now define an invariant on quadratic forms which play an important role in the theory of quadratic forms over $\mathbb{F}_2$.

Definition 1.1.1. Let $\{e_1, \ldots, e_g, f_1, \ldots, f_g\}$ be a symplectic basis of $(V, \langle , \rangle)$. We define the *Arf invariant* $a(q)$ of a quadratic form q by

$$a(q) = \sum_{i=1}^{g} q(e_i)q(f_i).$$

A quadratic form q is called *odd* (resp. *even*) if $a(q) = 1$ (resp. $a(q) = 0$). Let QV_- (resp. QV_+) denote the set of all odd (resp. even) quadratic forms.

Although the invariant is defined via symplectic bases, the Arf invariant does not depend on the choice of symplectic basis.

In addition, the action of $\mathrm{Sp}(V)$ has two orbits on QV, namely QV_- and QV_+ which have the cardinalities $2^{g-1}(2^g - 1)$ and $2^{g-1}(2^g + 1)$ respectively.

Quadratic forms in terms of coordinates

We may introduce the quadratic forms also in terms of coordinates. This perspective is useful to study them. For this section, we refer to [77].

Fix a symplectic basis $\{e_1, \ldots, e_g; f_1, \ldots, f_g\}$. We write the linear expression of any vector $w \in V$ as follows

$$w = \lambda_1 e_1 + \cdots + \lambda_g e_g + \mu_1 f_1 + \cdots + \mu_g f_g.$$

For the simplicity, we write $w = (\lambda, \mu)$ where $\lambda = (\lambda_1, \ldots, \lambda_g)$ and $\mu = (\mu_1, \ldots, \mu_g)$ in $\mathbb{F}_2^g$. We define the simplest quadratic form q_0 as

$$q_0(w) = \lambda \cdot \mu, \tag{1.1}$$

where $\cdot$ denotes the usual scalar product of g-tuples. This special quadratic form is central to understand the quadratic forms in terms of coordinates.

If we take any vector $v \in V$ with the coordinates $(\epsilon, \epsilon') = (\epsilon_1, \ldots, \epsilon_g, \epsilon'_1, \ldots, \epsilon'_g)$ then the quadratic form $q := q_0 + v$ acts on V by

$$q(w) = \epsilon \cdot \mu + \epsilon' \cdot \lambda + \lambda \cdot \mu.$$

Let us write $q = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$. We see that

$$\epsilon = (q(e_1), \ldots, q(e_g)), \quad \epsilon' = (q(f_1), \ldots, q(f_g)),$$

and the so Arf invariant of the quadratic form q in coordinates is given as

$$a(q) = \epsilon \cdot \epsilon'.$$

In terms of coordinates, we have

$$\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} + (\lambda, \mu) = \begin{bmatrix} \epsilon + \mu \\ \epsilon' + \lambda \end{bmatrix},$$
$$\begin{bmatrix} \epsilon_1 \\ \epsilon'_1 \end{bmatrix} + \begin{bmatrix} \epsilon_2 \\ \epsilon'_2 \end{bmatrix} + \begin{bmatrix} \epsilon_3 \\ \epsilon'_3 \end{bmatrix} = \begin{bmatrix} \epsilon_1 + \epsilon_2 + \epsilon_3 \\ \epsilon'_1 + \epsilon'_2 + \epsilon'_3 \end{bmatrix},$$

as the sum of a quadratic form and a vector and the sum of three quadratic forms respectively. This implies that

$$a(q + v) = a(q) + q(v), \tag{1.2}$$
$$a(q_1 + q_2 + q_3) = a(q_1) + a(q_2) + a(q_3) + \langle v_1, v_2 \rangle, \tag{1.3}$$

where $v_1 = q_1 + q_2, v_2 = q_1 + q_3$ for any $q, q_1, q_2, q_3 \in \mathrm{QV}$ and $v \in V$.

Aronhold basis

Now, we introduce the notion of Aronhold basis and some basic properties of it. This set enables us to collect all the quadratic forms easily and provides a way to distinguish the odd and even ones.

Let $S = \{q_1, \ldots, q_{2g+1}\}$ be a set of linearly independent vectors of the vector space $V \cup \mathrm{QV}$ where all the vectors lie in QV. Then any vector $q \in V \cup \mathrm{QV}$ can be written as the sum $\sum \alpha_i q_i$ with $\alpha_i = 0, 1 \in \mathbb{Z}$. We define the *length* of q as the sum $\sum \alpha_i$. Denote it $\#q$. So we have $0 \leq \#q \leq 2g + 1$. We remark that if q is in the coset QV then $\#q$ is odd, since the sum of two quadratic forms corresponds to a unique vector in V.

Definition 1.1.2. The set $S = \{q_1, \ldots, q_{2g+1}\}$ is called an *Aronhold basis* if the Arf invariant of any element q only depends on $\#q$ modulo 4.

An Aronhold basis exists. Now, we introduce fundamental sets in V which are closely related with the Aronhold bases, and see how to obtain an Aronhold basis from a fundamental set.

Definition 1.1.3. A set $\{v_1, \ldots, v_{2g+1}\}$ of vectors in V is called a *fundamental set* if

- $\sum_{i=1}^{2g+1} v_i = 0$ (*completeness*),
- $\langle v_i, v_j \rangle = 1$ for all $i \neq j$ (*being azygetic*).

Remark 1.1.4. Any set $\{v_1, \ldots, v_{2g}\}$ satisfying the condition of being azygetic in Definition 1.1.3 can be completed to a fundamental set which is $\{v_1, \ldots, v_{2g}, \sum_{i=1}^{2g} v_i\}$. In addition, note that any $2g$-subset of a fundamental set forms a basis for V.

It is possible to obtain a fundamental set by an Aronhold basis. More concretely, if $\{q_1, \ldots, q_{2g+1}\}$ is an Aronhold basis then $\{q_1 + q_2, \ldots, q_1 + q_{2g+1}\}$ satisfies the condition of being azygetic in Definition 1.1.3. Indeed, for any $2 < i \neq j < 2g + 1$,

$$\langle q_1 + q_i, q_1 + q_j \rangle = a(q_1 + a_i + q_j) + a(q_1) + a(q_i) + a(q_j) = 1$$

since $a(q_1) = a(q_i) = a(q_j) \neq a(q_1 + a_i + q_j)$ which follows from that $\{q_1, \ldots, q_{2g+1}\}$ is an Aronhold basis.

Conversely, we can obtain an Aronhold basis from a fundamental set. Suppose that the set

$$\mathscr{F} := \{v_1, \ldots, v_{2g+1}\}$$

is a fundamental set. Any subset of $\mathscr{F}$ with $2g$ elements forms a basis of V. Also note that $v_j = \sum_{i \neq j}^{2g+1} v_i$ for all $j \in \{1, \ldots, 2g + 1\}$.

Now, let q be any quadratic form. For $\mu \in \{0, 1\}$, consider the set

$$\mathscr{E}_{q,\mu} := \{v_i \in \mathscr{F} \mid q(v_i) = \mu\}.$$

Fix any $\mu \in \{0, 1\}$. We may assume that $\mathscr{E}_{q,\mu} = \{v_1, \ldots, v_k\}$ by reordering $\mathscr{F}$. We set $w := \sum_{i=1}^{k} v_i$.

Proposition 1.1.5. *Under the setting above, if $q_i = q + w + v_i$ for $i = 1, \ldots, 2g + 1$ then the set $\mathcal{A} := \{q_1, \ldots, q_{2g+1}\}$ is an Aronhold basis.*

Proof. First of all, we will show that $\mathcal{A}$ spans $V \sqcup \mathrm{QV}$. Suppose that $v \in V$. Since any $2g$-subset of $\mathscr{F}$ forms a basis, we can write $v = v_{i_1} + \cdots + v_{i_n}$ as a linear combination of vectors in $\mathscr{F}$. Thanks to the completeness property of $\mathscr{F}$, we may assume that n is even. So $v = q_{i_1} + \cdots + q_{i_n}$, since $\mathrm{Char}\, \mathbb{F}_2 = 2$. Now suppose that q' is a quadratic form, then $q + q'$ is a vector $v \in V$. We write $v + w = v_{i_1} + \cdots + v_{i_n}$ as a linear combination of $v_1, \ldots, v_{2g}$. We may assume that n is odd because of the completeness property in Definition 1.1.3. Now, we have

$$q' = \sum_{j=1}^{n} q + w + v_{i_j} = \sum_{j=1}^{n} q_{i_j}.$$

Therefore it forms a basis for $V \cup \mathrm{QV}$ since $\dim V \cup \mathrm{QV} = 2g + 1$.

We need to show that $a(q)$ depends only on $\#q$ modulo 4 for any $q \in \mathrm{QV}$. Firstly, we compute

$$\begin{aligned} a(q_i) &= a(q + w + v_i) \\ &= a(q) + q(w + v_i) \\ &= a(q) + q(w) + q(v_i) + \langle w, v_i \rangle \\ &= \begin{cases} a(q) + q(w) + \mu + k - 1 & \text{if } \ i \in \{1, \ldots, k\} \\ a(q) + q(w) + \mu + 1 + k & \text{otherwise.} \end{cases} \end{aligned}$$

Both cases are equal modulo 2. So we have $a(q_1) = \cdots = a(q_{2g+1})$. We will show that $a(q) = a(q') + 1$ for any $q, q' \in \mathrm{QV}$ with $\#q' = \#q + 2$.

Let $\#q = n$. Write $q = q_{i_1} + \cdots + + q_{i_n}$ and $q' = q_{j_1} + \cdots + + q_{j_{n+2}}$ in terms of quadratic forms in $\mathcal{A}$.

$$\begin{aligned}
a(q) &= a(q_{i_1} + \cdots + + q_{i_n}) \\
&= a(q_{i_1}) + a(q_{i_2}) + a(q_{i_3} + \cdots + q_{i_n}) + \langle q_{i_1} + q_{i_2}, q_{i_1} + q_{i_3} + \cdots + q_{i_n} \rangle \\
&= a(q_{i_1}) + a(q_{i_2}) + a(q_{i_3} + \cdots + q_{i_n}) + \langle v_{i_1} + v_{i_2}, v_{i_1} + v_{i_3} + \cdots + v_{i_n} \rangle \\
&= a(q_{i_1}) + a(q_{i_2}) + \cdots + a(q_{i_n}) \\
&\quad + \langle v_{i_1} + v_{i_2}, v_{i_1} + v_{i_3} + \cdots + v_{i_n} \rangle + \langle v_{i_3} + v_{i_4}, v_{i_3} + v_{i_5} + \cdots + v_{i_n} \rangle \\
&\quad + \cdots + \langle v_{i_{n-2}} + v_{i_{n-1}}, v_{i_{n-2}} + v_{i_n} \rangle \\
&= a(q_{i_1}) + a(q_{i_2}) + \cdots + a(q_{i_n}) + (n-1) + (n-2) + \cdots + 2 + 1 \pmod 2 \\
&= a(q_{i_1}) + a(q_{i_2}) + \cdots + a(q_{i_n}) + \frac{(n-1)}{2} \pmod 2.
\end{aligned}$$

Similarly,

$$a(q') = a(q_{j_1} + \cdots + + q_{j_{n+2}}) = a(q_{j_1}) + a(q_{j_2}) + \cdots + a(q_{j_{n+2}}) + \frac{(n+1)}{2} \pmod 2.$$

Since all the quadratic forms in $\mathcal{A}$ have the same Arf invariant, we have $a(q) = a(q') + 1$. □

Proposition 1.1.6. *Let $\mathcal{A} = \{q_1, \ldots, q_{2g+1}\}$ be an Aronhold basis. For any $i \in \{1, \ldots, 2g+1\}$,*

$$a(q_i) = \begin{cases} 0 & \text{for } g = 0, 1 \pmod 4 \\ 1 & \text{for } g = 2, 3 \pmod 4. \end{cases}$$

Proof. Any quadratic form q can be written uniquely as a linear combination of quadratic forms in $\mathcal{A}$, and $a(q)$ depends only on $\#q$ modulo 4. So if we count the lengths of the quadratic forms which are 1 modulo 4 as follows,

$$\sum_{i=1 \pmod 4}^{2g+1} \binom{2g+1}{i} = \begin{cases} 2^{g-1}(2^g + 1) & \text{for } g = 0, 1 \pmod 4 \\ 2^{g-1}(2^g - 1) & \text{for } g = 2, 3 \pmod 4, \end{cases}$$

then the proposition follows since we have $2^{g-1}(2^g - 1)$ and $2^{g-1}(2^g + 1)$ odd and even quadratic forms respectively. □

Remark 1.1.7. We can determine the Arf invariants of all quadratic forms from their lengths, since we know the Arf invariant of a quadratic form of length 1 for any g.

Labelling

Let $\mathcal{A} = \{q_1, \ldots, q_{2g+1}\}$ be an Aronhold basis. All quadratic forms can be written uniquely as the sum of an odd number of q_i's.

$$\begin{aligned}
&q_i && \text{of length } 1, \\
&q_i + q_j + q_k && \text{of length } 3, \\
&\vdots \\
&\sum_{i=1}^{2g+1} q_i && \text{of length } 2g+1.
\end{aligned}$$

Thanks to Proposition 1.1.6, we can determine whether a quadratic form is even or odd from its length.

In addition, we can label any quadratic form by an odd cardinality subset of $\{1, \dots, 2g+1\}$ of odd cardinality. For an odd number k in $\{1, \dots, 2g+1\}$, the set $I := \{i_1, \dots, i_k\}$ labels the quadratic form $q = \sum_{j=1}^{k} q_{i_j}$ uniquely since the linear expression is unique. We denote q_I the quadratic form q. For our purpose, we are interested in labelling the quadratic forms. But, incidentally, note that any vector in V can be labeled via even cardinality subsets of $\{1, \dots, 2g+1\}$ in the same way as the quadratic forms are labeled.

Let $I_1, \dots, I_k$ be labels for some quadratic forms or vectors in V. Since V is a vector space over $\mathbb{F}_2$, pairs of the same quadratic forms will be cancelled in the sum $q_{I_1} + \cdots + q_{I_k}$. So it is labelled by $I_1 \triangle \dots \triangle I_k$ where $\triangle$ denotes the symmetric difference of set.

Finally, notice that once we fix the Aronhold basis $\mathcal{A}$ the labelling is naturally unique.

Syzygetic Tetrads and Steiner Sets

We introduce being syzygetic for quadratic forms which allows us to group odd quadratic forms. For this section, our reference is [32, Section 5.4].

Definition 1.1.8. A set of three elements q_1, q_2, q_3 in QV is called a *syzygetic triad* (resp. *azygetic triad*) if

$$a(q_1) + a(q_2) + a(q_3) + a(q_1 + q_2 + q_3) = 0 \text{ (resp. } = 1).$$

We remark that a syzygetic triad $\{q_1, q_2, q_3\}$ can be completed into a set of four quadratic forms

$$\{q_1, q_2, q_3, q_1 + q_2 + q_3\}$$

that adds up to zero. Such a set is called *syzygetic tetrad*. By Definition 1.1.8, any 3-subset of this tetrad forms a syzygetic triad, also $a(q_1) = a(q_2) = a(q_3) = a(q_1 + q_2 + q_3)$. We have the following equivalent properties

- $\{q_1, q_2, q_3\}$ is a syzygetic triad,
- $q_1(q_2 + q_3) = a(q_2) + a(q_3)$,
- $\langle q_1 + q_2, q_1 + q_3 \rangle = 0$

for any $q_1, q_2, q_3 \in \mathrm{QV}$. It easily follows from the property 1.2 of the Arf invariant.

Syzygetic tetrads yield some sets called *Steiner sets* which classify syzygetic tetrads of odd quadratic forms. It is defined as associated to a vector in V.

Definition 1.1.9. For any $v \in V$, we define the *Steiner set*

$$\mathbf{S}_v := \Big\{ \{q, q'\} \mid q, q' \in \mathrm{QV}_- \text{ and } q + q' = v \Big\}.$$

Firstly, notice that $\mathbf{S}_v = \Big\{ \{q, q+v\} \mid \ q, q+v \in \mathrm{QV}_- \Big\}$. We also remark that any two pairs of the same Steiner set form a syzygetic tetrad. Indeed, suppose that $\{q_1, q_2\}$ and $\{q_1', q_2'\}$ are two pairs in the same Steiner set $\mathbf{S}_v$. We take any 3-subset of $\{q_1, q_2, q_1', q_2'\}$, say $\{q_1, q_2, q_1'\}$ without loss of generality. Now,

$$a(q_1 + q_2 + q_1') = a(q_1) + a(q_2) + a(q_1') + \langle q_1 + q_2, q_1 + q_1' \rangle$$

implies that $\langle q_1+q_2, q_1+q_1'\rangle = 0$ since q_1, q_2, q_1', q_2' are odd and $q_1+q_2+q_1'+q_2' = 0$. Therefore, any 3-subset of $\{q_1, q_2, q_1', q_2'\}$ is syzygetic. Conversely, any two pairs of odd quadratic forms in a syzygetic tetrad are in the same Steiner set since such tetrad $\{q_1, q_2, q_3, q_1+q_2+q_3\}$ adds up zero.

Remark 1.1.10. Being syzygetic reflects on the labelling of quadratic forms as follows. Suppose that q_{I_i} is a quadratic form labelled by $I_i \subset \{1, \ldots, 2g+1\}$ for $1 \leq i \leq 4$. Notice that, $\{q_{I_i} \mid i = 1, \ldots, 4\}$ is a syzygetic tetrad if and only if $I_1 \triangle \ldots \triangle I_4 = \emptyset$ since being syzygetic for q_{I_i}'s means that $\sum_{i=1}^{4} q_{I_i} = 0$.

Each Steiner set has $2^{g-2}(2^{g-1}-1)$ pairs of quadratic forms. In addition, there are $2^{2g}-1$ Steiner sets. An important characterization for an odd quadratic form q to belong to $\mathbf{S}_v$ is the equality $q(v) = 0$ holds. It follows from $a(q+v) = a(q) + q(v)$. Also note that

$$\#\mathbf{S}_v \cap \mathbf{S}_{v'} = \begin{cases} 2^{g-1}(2^{g-2}-1) & \langle v, v'\rangle = 0, \\ 2^{g-2}(2^{g-1}-1) & \langle v, v'\rangle \neq 0. \end{cases}$$

We say that $\mathbf{S}_v$ and $\mathbf{S}_{v'}$ are *syzygetic (resp. azygetic)* if $\langle v, v'\rangle = 0$ (resp. $\langle v, v'\rangle = 1$). In addition, the union of the pairwise syzygetic Steiner sets $\mathbf{S}_v$, $\mathbf{S}_{v'}$ and $\mathbf{S}_{v+v'}$ is equal to QV_-.

1.1.2 Theta Functions

In this section, we review some basic notions about theta functions [80] and how to relate them with the Jacobian of a curve.

For an integer $g \geq 1$, let

$$\mathbb{H}_g = \{\tau \in \mathrm{GL}_g(\mathbb{C}) \mid {}^t\tau = \tau,\ \mathrm{Im}\,\tau > 0\}$$

be the *Siegel upper half space*. For any $x \in \mathbb{C}$, let $\boldsymbol{e}(x) = \exp(2i\pi x)$.

Definition 1.1.11. For $\tau \in \mathbb{H}_g$, $z = (z_1, \ldots, z_g) \in \mathbb{C}^g$ and

$$[q] = \begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} \in \mathbb{Z}^g \oplus \mathbb{Z}^g,$$

the function

$$\vartheta[q](z,\tau) = \sum_{n \in \mathbb{Z}^g} \boldsymbol{e}\left(\frac{1}{2}(n+\varepsilon/2)\tau^t(n+\varepsilon/2) + (n+\varepsilon/2)^t(z+\varepsilon'/2)\right)$$

is called the *theta function with characteristic* $[q]$.

This is an analytic function on $\mathbb{C}^g \times \mathbb{H}_g$. If we evaluate $\vartheta[q](z,\tau)$ at $z = 0$ then we get a *theta constant* (*Thetanullwert*) (with characteristic $[q]$), which is denoted by $\vartheta[q](\tau)$. The characteristic $[q]$ is called *even* (resp. *odd*) if $\varepsilon \cdot \varepsilon'$ is even (resp. odd). Since

$$\vartheta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (-z,\tau) = (-1)^{\epsilon\cdot\epsilon'} \cdot \vartheta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (z,\tau), \tag{1.4}$$

the theta function $\vartheta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ is a even (resp. odd) function if and only if $\varepsilon \cdot \varepsilon' = 0$ (resp. $= 1$). In addition, note that a characteristic $[q]$ is odd if and only if the theta constant $\vartheta[q](\tau)$ is identically 0 for all $\tau \in \mathbb{H}_g$. We also have that

$$\vartheta \begin{bmatrix} \epsilon + 2m \\ \epsilon' + 2n \end{bmatrix} (z, \tau) = (-1)^{n \cdot \epsilon} \cdot \vartheta \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} (z, \tau). \tag{1.5}$$

Using the notation of Section 1.1.1, we identify a characteristic $[q]$ modulo 2 with a quadratic form over $\mathbb{F}_2$ which will be denoted by q. The quadratic from q_0 is identified with the characteristic $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$. Conversely, fixing a symplectic basis, if we start with a quadratic form q then we write $q = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ with entries $\{0, 1\}$ in terms of coordinates. We associate $\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ to the characteristic of the theta function $\vartheta \begin{bmatrix} \epsilon + 2m \\ \epsilon' + 2n \end{bmatrix} (z, \tau)$ for all $n, m \in \mathbb{Z}$. The characteristic $\begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ has only an impact on the sign of the theta function because of Equation (1.5). From now on, we only use characteristics with entries $0, 1$.

Now, we introduce the link between the curve and its Jacobian. Let $\mathcal{C}$ be a smooth, irreducible projective curve of genus $g > 0$ over $\mathbb{C}$ and $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_g)$ be a basis of regular differentials. Let $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_{2g})$ be a symplectic basis of $H_1(\mathcal{C}, \mathbb{Z})$ such that the intersection pairing has the matrix

$$\begin{pmatrix} 0_g & I_g \\ I_g & 0_g \end{pmatrix}$$

with I_g and 0_g are the $g \times g$ identity and zero matrices respectively.

With respect to these choices, the period matrix of $\mathcal{C}$ is $\Omega = [\Omega_1, \Omega_2]$ where

$$\Omega_1 = \left(\int_{\delta_i} \omega_j \right)_{1 \leq i \leq g, 1 \leq j \leq g},$$

$$\Omega_2 = \left(\int_{\delta_i} \omega_j \right)_{g+1 \leq i \leq 2g, 1 \leq j \leq g}.$$

We consider a second basis $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_g)$ of regular differentials obtained by $\boldsymbol{\eta} = \Omega_1^{-1} \boldsymbol{\omega}$. The period matrix with respect to this new basis is $[\mathrm{id}, \tau]$ where $\tau = \Omega_1^{-1} \Omega_2 \in \mathbb{H}_g$. This matrix is called the *Riemann matrix*. We let

$$\mathrm{Jac}(\mathcal{C}) = \mathbb{C}^g / (\mathbb{Z}^g + \tau \mathbb{Z}^g).$$

Let us denote

$$e_i = \left(\frac{1}{2} \int_{\delta_i} \eta_j \right)_{1 \leq j \leq g} = (0, \ldots, 0, \frac{1}{2}, 0, \ldots, 0) \in \mathbb{C}^g,$$

and

$$f_i = \left(\frac{1}{2} \int_{\delta_{g+i}} \eta_j \right)_{1 \leq j \leq g} \in \mathbb{C}^g,$$

and

$$v = \sum_{i=1}^{g} \lambda_i e_i + \mu_j f_j = (\lambda, \mu)$$

with $\lambda, \mu \in \mathbb{Z}^g$ for $1 \leq i \leq g$.

Now, we let W be the $\mathbb{Z}$-module generated by $e_1, \ldots, e_g, f_1, \ldots, f_g$, so that

$$\mathrm{Jac}(\mathcal{C})[2] = W/(\mathbb{Z}^g + \tau\mathbb{Z}^g).$$

An element $v \in W$ acts on a theta function. Indeed, if $[q] = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ is a characteristic and $v = (\lambda, \mu) \in W$ then

$$\vartheta[q](z + v, \tau) = \boldsymbol{e}\left(-\frac{1}{4}\mu^t(\epsilon' + \lambda) - \frac{1}{2}\mu^t z - \frac{1}{8}\mu\tau^t\mu\right) \cdot \vartheta\begin{bmatrix} \epsilon + \mu \\ \epsilon' + \lambda \end{bmatrix}(z, \tau). \tag{1.6}$$

Thanks to Equation (1.6), we will write $\big[[q] + v\big] = \begin{bmatrix} \epsilon + \mu \\ \epsilon' + \lambda \end{bmatrix}$. It is possible to see an element of W as a difference of two characteristics.

At the same time, $V = \mathrm{Jac}(\mathcal{C})[2]$ is a vector space over $\mathbb{F}_2$ of $2g$ dimension. The Weil pairing defines a nondegenerate symplectic form on V. We may induce the symplectic basis of V via e_i, f_i's. Now, the theory of quadratic forms on V is coherent with the theta characteristics and (λ, μ) modulo 2. We denote $\bar{v} \in V$ the class of v where the class is identified with the vector $(\lambda \pmod 2, \mu \pmod 2)$. So the quadratic form $q + \bar{v}$ is the quadratic form associated to the theta characteristic $\big[[q] + v\big]$.

1.1.3 Theta Characteristic Divisors

In this section, we introduce theta characteristic divisors of $\mathcal{C}$. Moreover, we explain the link between such divisors and the quadratic forms on $\mathrm{Jac}(\mathcal{C})[2]$ over $\mathbb{F}_2$. For more detailed explanations and results, we refer to [4, Chapter 1].

Let $\mathcal{C}_d$ be the d-fold symmetric product of $\mathcal{C}$ which is identified with the set of effective divisors of degree d. Fix a point Q on $\mathcal{C}$. The *Abel-Jacobi* map is defined by

$$\begin{aligned} u_d : \mathcal{C}_d &\longrightarrow \mathrm{Jac}(\mathcal{C}) \\ D = \sum_i m_i P_i &\longmapsto \sum_i m_i \int_Q^{P_i} (\eta_1, \ldots, \eta_g). \end{aligned}$$

The map depends on the choice of the fixed point Q. Also, the value of the integral depends on the path chosen to integrate, however, $u_d(D)$ is well defined in $\mathrm{Jac}(\mathcal{C})$. It is possible to extend u_d to noneffective divisors of degree d. Abel's theorem [4, Chapter 1] assures that this map is invariant under the linear equivalence between divisors. Denote $\mathrm{Pic}(\mathcal{C})$ the Picard group of $\mathcal{C}$ and $\mathrm{Pic}^d(\mathcal{C})$ the subgroup of the divisor classes of degree d in $\mathrm{Pic}(\mathcal{C})$. By Abel's theorem, u_d leads to a bijection from $\mathrm{Pic}^d(\mathcal{C})$ into $\mathrm{Jac}(\mathcal{C})$. Moreover, it induces an isomorphism between the group $\mathrm{Pic}^0(\mathcal{C})$ of the divisor classes of degree 0 in $\mathrm{Pic}(\mathcal{C})$ and the Jacobian $\mathrm{Jac}(\mathcal{C})$. We keep these identifications in mind when we study theta characteristic divisors in the following part.

The *Riemann Theta function* $\theta(z, \tau)$ of $\mathrm{Jac}(\mathcal{C})$ is the theta function $\vartheta\begin{bmatrix} 0 \\ 0 \end{bmatrix}(z, \tau)$ with the characteristic $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$. Since it is an analytic function on $\mathbb{C}^g \times \mathbb{H}_g$ and quasi periodic with respect to the lattice $\mathbb{Z}^g + \tau\mathbb{Z}^g$ given by $[\mathrm{id}, \tau]$ it defines a divisor Θ of $\mathrm{Jac}(\mathcal{C})$ which is the zero divisor of $\vartheta(z, \tau)$.

We denote $\ell(D)$ the dimension of the Riemann-Roch space of D. The following proposition allows us to relate certain divisors with quadratic forms.

Proposition 1.1.12 (Riemann Singularity Theorem)**.** *Let κ be the canonical divisor of $\mathcal{C}$. There exists a unique divisor class D_0 of degree $g-1$ with $2D_0 \sim \kappa$ and $\ell(D_0)$ is even such that $u_{g-1}(\mathcal{C}_{g-1}) = \Theta + u_{g-1}(D_0)$. Moreover for any $v \in V$, $\mathrm{mult}_v(\Theta) = \ell(D_0 + v)$.*

A divisor (class) D is called a *theta characteristic divisor (class)* if $2D \sim \kappa$. We denote TCh the set of theta characteristic divisors. TCh is nonempty since $\mathrm{Jac}(\mathcal{C})$ is a divisible group.

Remark 1.1.13. Proposition 1.1.12 allows us to have a correspondence between theta characteristic divisors of $\mathcal{C}$ and quadratic forms on $\mathrm{Jac}(\mathcal{C})[2]$ over $\mathbb{F}_2$. Before mentioning this correspondence, we emphasize some points. Firstly, recall that $\theta(z,\tau) = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (z,\tau)$. In addition, Equation (1.6) implies that $\mathrm{mult}_v(\vartheta[q]) = \mathrm{mult}_0(\vartheta[q+v])$ for any characteristic $[q]$ and $v \in \mathrm{Jac}(\mathcal{C})[2]$. In addition, if we let $[q] = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ then it follows from Equation (1.4) that $\vartheta[q]$ is even if and only if $\epsilon \cdot \epsilon' = 0$. So we have $\mathrm{mult}_v(\vartheta[q])$ is even if and only if $\epsilon \cdot \epsilon' = 0$

Firstly, define $q_{D_0}(v) := \ell(D_0 + v) \pmod 2$. Now, if v is given by (λ, μ) with respect to a fixed symplectic basis then by Proposition 1.1.12

$$q_{D_0}(v) = \ell(D_0 + v) \pmod 2 = \mathrm{mult}_v(\Theta) \pmod 2 = \mathrm{mult}_v \left(\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right) \pmod 2 \tag{1.7}$$

$$= \mathrm{mult}_0 \left(\vartheta \begin{bmatrix} \lambda \\ \mu \end{bmatrix} \right) \pmod 2 = \lambda \cdot \mu.$$

So q_{D_0} corresponds to the quadratic form q_0 defined in Equation (1.1). We identify q_{D_0} with q_0. In addition, any theta characteristic divisor D is linearly equivalent to $D_0 + v$ with $v = (\lambda, \mu) \in V$. Indeed, $D - D_0$ is a 2-torsion point of $\mathrm{Jac}(\mathcal{C})$. We can associate D to the quadratic form $q = q_0 + v$. Note that the Arf invariant of q

$$a(q) = a(q_0 + v) = \mathrm{mult}_v(\Theta) \pmod 2$$

since $\mathrm{mult}_v(\Theta)$ is equal to the multiplicity of $\vartheta[q](z,\tau)$ at 0 and the latter has the same parity as q. For any $v \in V$, we have

$$q(v) = a(q + v) + a(q) = \ell(D + v) + \ell(D) \pmod 2.$$

In short, any theta characteristic divisor D defines a quadratic form q_D on V by

$$q_D(v) = \ell(D + v) + \ell(D) \pmod 2.$$

It has Arf invariant $a(q_D) \equiv \ell(D) \pmod 2$. The divisor D_0 corresponds to the quadratic form q_0.

Conversely, any quadratic form q defines a divisor

$$D_q := D_0 + q_0 + q. \tag{1.8}$$

Remark 1.1.14. As we have seen above, there is a one-to-one correspondence between the set of quadratic forms on $\mathrm{Jac}(\mathcal{C})[2]$ and the theta characteristic divisors. Moreover, an odd (resp. even) theta characteristic corresponds to an odd (resp. even) quadratic form. By following Section 1.1, we know that there are $2^{g-1}(2^g + 1)$ (resp. $2^{g-1}(2^g + 1)$) odd (resp. even) quadratic forms. Therefore, we know the number of odd (resp. even) theta characteristic divisors.

1.1.4 Multitangents

We assume that $\mathcal{C}$ is non-hyperelliptic. The basis of regular differentials $\{\omega_1, \ldots, \omega_g\}$ defines the canonical map

$$\begin{aligned} \phi : \mathcal{C} &\to \mathbb{P}^{g-1} \\ P &\mapsto (\omega_1(P) : \ldots : \omega_g(P)). \end{aligned}$$

Let D be a theta characteristic divisor of $\mathcal{C}$. We call D a *vanishing theta characteristic divisor* if $\ell(D) > 1$. Note that $\phi^*(\mathcal{O}_{\mathbb{P}^{g-1}}(1)) = \kappa$. Now, we let H_D be any fixed hyperplane in $\mathbb{P}^{g-1}$ such that $\phi^* H_D \cdot \mathcal{C} \sim 2D$.

Definition 1.1.15. We call such a hyperplane a *multitangent*.

Remark 1.1.16. When $g = 3$, the dimension of the Riemann-Roch space of any theta characteristic divisor is either 0 or 1 because $\mathcal{C}$ is non-hyperelliptic. There are 28 multitangents, in this case these geometrical objects are known as *bitangents*.

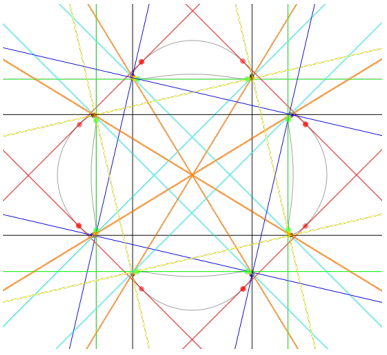


Figure 1.1: 28 bitangents on the Trott curve.

For $g = 4$, first of all, note that $\ell(D) = 0, 1$ or 2 because of Clifford's theorem for divisors [4, Chapter III]. Here multitangents are called *tritangents* in the literature. There are 120 tritangents which correspond to the odd characteristic divisors. To be more specific, the canonical model of $\mathcal{C}$ lies on a smooth quadric if and only if there is not a vanishing theta characteristic divisor. In this case, we have exactly 120 tritangents. Otherwise, C lies on a singular quadric $\mathcal{Q}$, then there is a unique even theta characteristic divisor, call D_{e}. The dimension $\ell(D_{\mathrm{e}}) = 2$. So there is a one dimensional family of tritangents, that pass through the node of $\mathcal{Q}$. The tritangents which correspond to the odd theta characteristic divisors are the ones which do not pass through the node of $\mathcal{Q}$. Note that, such a curve arises from a del Pezzo surface of degree 1 which follows from [71, Theorem 24.4.iii]. In Section 1.2.2, we come back to this subject.

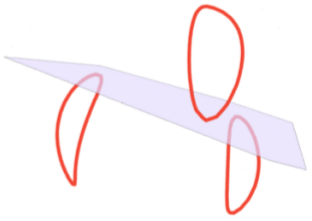


Figure 1.2: A tritangent of a curve.

Remark 1.1.17. Everything aside, if $\mathcal{C}$ is a general curve of genus g, then $\ell(D) = 0, 1$ for any theta characteristic divisor D. So there is a unique hyperplane H_D if D is an odd theta characteristic divisor. For the generality condition, we refer to [51]. In this case, notice that we have exactly $2^{g-1}(2^g - 1)$ multitangents.

In the following proposition, we see the geometric meaning of being syzygetic for quadratic forms corresponding to four theta characteristic divisors. It will be important for us to be able to work out concrete computations in Section 1.2.1.

Proposition 1.1.18. *Suppose that D_1, D_2, D_3, D_4 are four odd theta characteristic divisors corresponding to the quadratic forms q_1, q_2, q_3, q_4 respectively. If q_1, q_2, q_3, q_4 is a syzygetic tetrad then $D_1 + D_2 + D_3 + D_4$ is cut out by a quadric in $\mathbb{P}^{g-1}$.*

Proof. We write $D_i = D_0 + q_0 + q_i$ for $i = 1, \ldots, 4$ by following the correspondence between quadratic forms and theta characteristic divisors above. Because $q_1 + \cdots + q_4 = 0$,

$$\sum_{i=1}^{4} D_i = \sum_{i=1}^{4} (D_0 + q_0 + q_i) \sim 2\kappa.$$

There is a quadric in $\mathbb{P}^{g-1}$ which cuts out $D_1 + D_2 + D_3 + D_4$ since $\phi^*(\mathcal{O}_{\mathbb{P}^{g-1}}(2)) = 2\kappa$. □

Remark 1.1.19. We can construct the Steiner sets by using Proposition 1.1.18 geometrically. For an algorithm of such a construction, we refer to our article [20]. On the other hand, the labelling provides a more efficient way for this construction. In this case, we can verify being syzygetic of given four multitangents on their labels by Remark 1.1.10.

Link between combinatorics, algebra and geometry

We quickly summarize the link between notions which are explained in Section 1.1.1, 1.1.2, 1.1.3 and 1.1.4 in the following figure when $\mathcal{C}$ is general.

$$\left\{ \begin{array}{c} \text{odd theta constants} \\ \text{of } \mathcal{C} \text{ modulo } 2 \end{array} \right\} \iff \left\{ \begin{array}{c} \text{odd quadratic forms } q \\ \text{on } \mathrm{Jac}(\mathcal{C})[2] \end{array} \right\}$$

$$\Updownarrow$$

$$\left\{ \text{multitangents} \right\} \iff \left\{ \begin{array}{c} \text{odd theta characteristic} \\ \text{divisors } D_q \text{ of } \mathcal{C} \end{array} \right\}$$

1.1.5 Line Bundles

In this section, we overview how to associate a line bundle to a given divisor on a variety and how a line bundle on a variety gives a divisor on this variety. We also mention some basic properties of sections over line bundles. For further interests, we refer to the following classical sources [45, Chapter 1], [52].

Basics

Let X be a smooth algebraic variety over a field k. We recall that for any line bundle $\pi : \mathfrak{L} \to X$ of X there is an open cover $\{U_\alpha\}$ of X and there are isomorphisms, called *trivializations*

$$\phi_\alpha : \mathfrak{L}_{U_\alpha} \to U_\alpha \times k$$

of $\mathfrak{L}_{U_\alpha} = \pi^{-1}(U_\alpha)$. Note that ϕ_α induces a linear isomorphism between $\mathfrak{L}_x$ and $\{x\} \times k$ where $\mathfrak{L}_x$ is the fiber $\pi^{-1}(x)$. The composite function

$$\phi_\alpha \circ \phi_\beta^{-1} : (U_\alpha \cap U_\beta) \times k \to (U_\alpha \cap U_\beta) \times k$$

is well defined with

$$\phi_\alpha \circ \phi_\beta^{-1}(x, z) = (x, g_{\alpha\beta}(x)z)$$

for some k-valued function

$$g_{\alpha\beta} : U_\alpha \cap U_\beta \to k^\times.$$

These functions are called the *transition functions*. Conversely, given an open cover $\{U_\alpha\}$ of X and maps $g_{\alpha\beta} : U_\alpha \cap U_\beta \to k^\times$ satisfying some natural compatibility conditions, there is a unique line bundle $\mathfrak{L} \to X$ with transition functions $\{g_{\alpha\beta}\}$. In addition, two collections of transition functions $\{g_{\alpha\beta}\}, \{g'_{\alpha\beta}\}$ define the same line bundle if and only if there is a family of regular functions $\{f_\alpha\}$ such that

$$g'_{\alpha\beta} = \frac{f_\alpha}{f_\beta} g_{\alpha\beta}.$$

If $\mathfrak{L}, \mathfrak{L}'$ are line bundles with transition functions $\{g_{\alpha\beta}\}$,$\{g'_{\alpha\beta}\}$ respectively, then it is possible to define line bundles $\mathfrak{L} \otimes \mathfrak{L}'$ and $\mathfrak{L}^{-1}$ with the transition functions $\{g_{\alpha\beta} g'_{\alpha\beta}\}$ and $\{g_{\alpha\beta}^{-1}\}$ respectively.

Divisors and Line Bundles

Let D be a divisor on X with local defining functions $\{f_\alpha\}$ over some open cover $\{U_\alpha\}$ of X. The line bundle given by the functions

$$\left\{ g_{\alpha\beta} = \frac{f_\alpha}{f_\beta} \right\}$$

is called the *associated line bundle* of D, denoted by $[D]$. We note that

$$[D + D'] = [D] \otimes [D'], \qquad [-D] = [D]^{-1}.$$

A section of a line bundle $\pi : \mathfrak{L} \to X$ is a map

$$s : X \to \mathfrak{L}$$

such that $\pi \circ s = id_X$. A section s of $\mathfrak{L}$ over $\cup_\alpha U_\alpha$ is given by a family of rational functions $\{s_\alpha\}$ on U_α with

$$s_\alpha = g_{\alpha\beta} s_\beta \quad \text{on} \quad U_\alpha \cap U_\beta. \tag{1.9}$$

Conversely, such a family defines a section of $\mathfrak{L}$.

It follows from (1.9) that the divisors $(s_\alpha), (s_\beta)$ are equivalent. So it is possible to define the divisor (s) of a section s of $\mathfrak{L}$ as (s_α) for some α. Note that if a point P is in the zeroes of (s) then it is in the zeroes of (s_α) for all α. So we may define $s(P) = 0$. In addition, the quotient of two sections of $\mathfrak{L}$ is a well defined rational function because of the condition (1.9). Indeed, take any two sections s, s' of $\mathfrak{L}$. Suppose that they are given by the families $\{s_\alpha\}$ and $\{s'_\alpha\}$. The section s/s' is given by the family $\{s_\alpha/s'_\alpha\}$. It is a well defined rational function since $s_\alpha/s'_\alpha = (g_{\alpha\beta}s_\beta)/(g_{\alpha\beta}s'_\beta)$ for any α, β.

If D is a divisor with local defining functions $\{f_\alpha\}$ then they provide a section s_f of $[D]$ with $(s_f) = D$. Conversely, if $\mathfrak{L}$ is a line bundle of X with transition functions $\{g_{\alpha\beta}\}$ then $\mathfrak{L} = [(s)]$ for any global rational section s of $\mathfrak{L}$.

1.2 Computations of Theta Constants

We are finally equipped capably to explain our algorithm for computations of theta constants. Firstly, we focus on the argumentation of developing the algorithm and then we will deal with problems arising from how to obtain an input for the algorithm.

1.2.1 General Algorithm

We describe an algorithm for computing fourth power of quotient even theta constants. The principal idea comes from [77, Remark 1,2], which is based on Weber formula [96] for computing this quotient in terms of bitangents for $g = 3$.

Recall that $\mathcal{C}$ is a non-hyperelliptic curve of genus g with the canonical embedding ϕ into $\mathbb{P}^{g-1}$.

Throughout this section, we fix a Riemann matrix τ associated a normalised regular differentials $\boldsymbol{\eta}$ as introduced in Section 1.1.2. Thus we avoid to write τ in the notation for Theta functions and constants. In addition, fix a theta hyperplane H_{D_q} and also a linear polynomial $\beta_q \in \mathbb{C}[X_1, \ldots, X_g]$ such that H_{D_q} is the hyperplane with equation $\beta_q = 0$.

Let p_1, p_2 be two even quadratic forms. In the Steiner set $\mathbf{S}_{p_1+p_2}$ there are $2^{g-2}(2^{g-1}-1)$ pairs of quadratic forms (see Section 1.1.1). Choose a pair $\{q_1, \overline{q}_1\}$ in $\mathbf{S}_{p_1+p_2}$. So

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

Let $D_{q_1}, D_{\overline{q}_1}$ be the theta characteristics divisors associated to $q_1, \overline{q}_1$. We write

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

where A_i's (respectively B_i's) are the points in the support of multitangent β_{q_1} (respectively $\beta_{\overline{q}_1}$) for $i = 1, \ldots, g-1$.

Let $S = S_1 + \cdots + S_{2g-3}$ be an arbitrary generic effective divisor of degree $2g-3$ on $\mathcal{C}$ and be $\kappa = 2(A_1 + \cdots + A_{g-1})$. By fixing a point P_0 on $\mathcal{C}$, we introduce

$$f_{i,S}(P) := \vartheta[p_i](P + S - \kappa) := \vartheta[p_i]\left(\int_{P_0}^{P} \boldsymbol{\eta} + \sum_{i=1}^{2g-3} \int_{P_0}^{S_i} \boldsymbol{\eta} - 2\sum_{i=1}^{g-1} \int_{P_0}^{A_i} \boldsymbol{\eta}\right).$$

According to Riemann theorem [80, Theorem V.1], $f_{i,S}(P)$ is a regular section of a line bundle over $\mathcal{C}$, and if $f_{i,S}$ is not identically zero then its zero divisor $(f_{i,S})_0$ has degree g and satisfies

$$(f_{i,S})_0 \sim D_0 + (p_i + q_0) + \kappa - S = D_{p_i} + \kappa - S.$$

Since $\ell(\kappa + D_{p_i}) = 2g-2$, we let $\{t_i^{(1)}, \ldots, t_i^{(2g-2)}\}$ be a basis of sections on the line bundle $[\kappa + D_{p_i}]$ (called *Wurzelfunctionen* in Weber's book) which corresponds to a basis of $\mathcal{L}(\kappa + D_{p_i})$. Suppose that $t_i^{(j)}$ is given by family of rational functions $t_{i,\alpha}^{(j)}$ with an open cover $\{U_{i,\alpha}\}_{\alpha \in I}$ of $\mathcal{C}$ for $i = 1, 2$ and $j = 1, \ldots, 2g-2$.

For each $i = 1, 2$, we can find an open cover $\{U_{i,\alpha}\}_\alpha$ of $\mathcal{C}$ such that for each $k = 1, \ldots, 2g-3$ there exists α_k for which S_k is not a pole of $t_{i,\alpha_k}^{(j)}$ for any $j = 1, \ldots, 2g-3$. We define $\chi_{i,S}$ as the family of the following rational functions

$$\chi_{i,S,\alpha}(P) = \begin{vmatrix} t_{i,\alpha}^{(1)}(P) & \cdots & t_{i,\alpha}^{(2g-2)}(P) \\ t_{i,\alpha_1}^{(1)}(S_1) & \cdots & t_{i,\alpha_1}^{(2g-2)}(S_1) \\ \vdots & & \vdots \\ t_{i,\alpha_{2g-3}}^{(1)}(S_{2g-3}) & \cdots & t_{i,\alpha_{2g-3}}^{(2g-2)}(S_{2g-3}) \end{vmatrix}, \quad 1 \le i \le 2, \tag{1.10}$$

on U_α for all α. Therefore, the section $\chi_{i,S}$ belongs to the same line bundle $[\kappa + D_{p_i}]$, since the determinant is a linear combination of $t_{i,\alpha}^{(j)}$'s.

Since $\chi_{i,S}(S_j) = 0$ for $1 \le j \le 2g-3$, we see that $(\chi_{1,S})_0 = S + R_i$ where R_i is an effective divisor of degree g, uniquely defined by $R_i + S \sim \kappa + D_{p_i}$. Now

$$(f_{i,S})_0 \sim D_{p_i} + \kappa - S \sim R_i,$$

so actually $(f_{i,S})_0 = R_i$. Therefore, $(f_{1,S})_0 - (f_{2,S})_0 = R_1 - R_2 = (\chi_{1,S})_0 - (\chi_{2,S})_0$ and there exists a constant λ_S such that

$$\frac{f_{1,S}(P)}{f_{2,S}(P)} = \lambda_S \cdot \frac{\chi_{1,S}(P)}{\chi_{2,S}(P)}.$$

Lemma 1.2.1. *λ_S does not depend on S.*

Proof. One has

$$\frac{f_{1,S}(P)}{f_{2,S}(P)} \cdot \frac{\chi_{2,S}(P)}{\chi_{1,S}(P)} = \lambda_S.$$

We have to prove that the expression on the left side does not depend on the support of $S = S_1 + \cdots + S_{2g-3}$. It is enough to show that $\lambda_S = \lambda_{S'}$ where $S' = S_1' + S_2 + \cdots + S_{2g-3}$ for another generic point S_1'. Note that

$$f_{i,S}(S_1') = \vartheta[p_i](S' - \kappa) = f_{i,S'}(S_1)$$

and $\chi_{i,S}(S_1') = -\chi_{i,S'}(S_1)$. Hence

$$\lambda_S = \frac{f_{1,S}(S_1')}{f_{2,S}(S_1')} \cdot \frac{\chi_{2,S}(S_1')}{\chi_{1,S}(S_1')} = \frac{f_{1,S'}(S_1)}{f_{2,S'}(S_1)} \cdot \frac{\chi_{2,S'}(S_1)}{\chi_{1,S'}(S_1)} = \lambda_{S'}.$$

□

In the sequel we are going to use two particular divisors S and S'.

Lemma 1.2.2. *If* $S = A_2 + \cdots + A_{g-1} + A_1 + \cdots + A_{g-1}$ *then*

$$\frac{f_{1,S}(A_1)^2}{f_{2,S}(A_1)^2} = \frac{\vartheta[p_1](0)^2}{\vartheta[p_2](0)^2}.$$

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

$$\frac{f_{1,S'}(P)^2}{f_{2,S'}(P)^2} = (-1)^{a(q_0+p_1+p_2)} \cdot \frac{f_{2,S}(P)^2}{f_{1,S}(P)^2}.$$

Proof. The first equality is trivial. As for the second, let $[p_1] = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix}$ and

$$(B_1 + \cdots + B_{g-1}) - (A_1 + \cdots + A_{g-1}) \sim D_{\overline{q}_1} - D_1 = [\overline{q}_1] - [q_1] = (\lambda, \mu),$$

so that $[p_2] = [p_1] + [\overline{q}_1] - [q_1] = \begin{bmatrix} \epsilon + \mu \\ \epsilon' + \lambda \end{bmatrix}$ (the choices for the lifts of the quadratic forms are irrelevant because we are going to take squares). Then using (1.6)

$$\begin{aligned} f_{1,S'}(P)^2 &= \vartheta[p_1](P + A_2 + \cdots + A_{g-1} + B_1 + \cdots + B_{g-1} - \kappa)^2 \\ &= \vartheta[p_1](P + A_2 + \cdots + A_{g-1} + B_1 + \cdots + B_{g-1} - \kappa \\ &\quad + (B_1 + \cdots + B_{g-1}) - (A_1 + \cdots + A_{g-1}))^2 \\ &= (-1)^{\mu\cdot(\epsilon'+\lambda)} \cdot c_{\tau,\mu,z} \cdot f_{2,S}(P)^2, \end{aligned}$$

where $z = P + A_2 + \cdots + A_{g-1} + B_1 + \cdots + B_{g-1} - \kappa$, $c_{\tau,\mu,z}$ is a constant depending on τ, μ, z and

$$f_{2,S'}(P)^2 = (-1)^{\mu\cdot\epsilon'} \cdot c_{\tau,\mu,z} \cdot f_{1,S}(P)^2.$$

Hence for the quotient we get

$$\frac{f_{1,S'}(P)^2}{f_{2,S'}(P)^2} = (-1)^{\mu\cdot\lambda} \cdot \frac{f_{2,S}(P)^2}{f_{1,S}(P)^2}.$$

□

From this we get that

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

We denote $\sqrt{q}$ a (fixed) section (*Abelsche Function*) of the line bundle associate to D_q for a quadratic form q. We write $\sqrt{q}(P) = \sqrt[P]{q}$. Let

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

be the sets of $g-1$ many distinct pairs in the Steiner sets $\mathbf{S}_{p_1+q_1}$ and $\mathbf{S}_{p_1+\overline{q}_1}$ respectively. We may choose $g-1$ of them, since a Steiner set contains $2^{g-2}(2^{g-1}-1)$ many pairs of quadratic forms. We can then choose for $t_i^{(1)}, \ldots, t_i^{(2g-2)}$ 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

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

The quotient $\chi_{1,S}(A_1)/\chi_{2,S}(A_1)$ take the indeterminate form $0/0$ so we need first to resolve this ambiguity and then we will express everything in terms of the multitangents. We begin with a divisor $S = S_2 + \cdots + S_{g-1} + A_1 + \cdots + A_{g-1}$. Note that $\sqrt[A_i]{q_1 r_j \overline{r}_j} = 0$, since A_i is in the zeroes of the divisor $\left(\sqrt{q_1 r_j \overline{r}_j}\ \right)$ for $i = 1, \ldots, g-1$ and $j = 1, \ldots, g-1$.

$\chi_{1,S}(P)$

$$= \begin{vmatrix} \sqrt[P]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[P]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[P]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[P]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \sqrt[S_1]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_2]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[S_2]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_2]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[S_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[S_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \sqrt[A_1]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[A_1]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[A_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[A_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \end{vmatrix}$$

$$= \begin{vmatrix} \sqrt[P]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[P]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[P]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[P]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \sqrt[S_2]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_2]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[S_2]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_2]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[S_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[S_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ 0 & \cdots & 0 & \sqrt[A_1]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ 0 & \cdots & 0 & \sqrt[A_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \end{vmatrix}.$$

So

$\chi_{1,S}(P)$

$$= \begin{vmatrix} \sqrt[P]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[P]{q_1 r_{g-1} \overline{r}_{g-1}} \\ \sqrt[S_2]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_2]{q_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[S_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} \end{vmatrix} \begin{vmatrix} \sqrt[A_1]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[A_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \end{vmatrix}$$

$$= c_{1,S} \begin{vmatrix} \sqrt[P]{r_1 \overline{r}_1} & \cdots & \sqrt[P]{r_{g-1} \overline{r}_{g-1}} \\ \sqrt[S_2]{r_1 \overline{r}_1} & \cdots & \sqrt[S_2]{r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[S_{g-1}]{r_1 \overline{r}_1} & \cdots & \sqrt[S_{g-1}]{r_{g-1} \overline{r}_{g-1}} \end{vmatrix} \begin{vmatrix} \sqrt[A_1]{s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[A_{g-1}]{s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{s_{g-1} \overline{s}_{g-1}} \end{vmatrix},$$

where $c_{1,S} = \sqrt[P]{q_1}\ \sqrt[S_2]{q_1} \cdots \sqrt[S_{g-1}]{q_1}\ \sqrt[A_1]{\overline{q}_1} \cdots \sqrt[A_{g-1}]{\overline{q}_1}$.

Similarly, we write down the determinant $\chi_{2,S}(P)$. Also we note that $\sqrt[A_i]{q_1 s_j \overline{s}_j} = 0$ for $i = 1, \ldots, g-1$ and $j = 1, \ldots, g-1$.

$\chi_{2,S}(P)$

$$= \begin{vmatrix} \sqrt[P]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[P]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[P]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[P]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \sqrt[S_2]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_2]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[S_2]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_2]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[S_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[S_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \sqrt[A_1]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[A_1]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[A_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[A_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \end{vmatrix}$$

$$= \begin{vmatrix} \sqrt[P]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[P]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[P]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[P]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \sqrt[S_2]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_2]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[S_2]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_2]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[S_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[S_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[S_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ 0 & \cdots & 0 & \sqrt[A_1]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ 0 & \cdots & 0 & \sqrt[A_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \end{vmatrix}.$$

So

$\chi_{2,S}(P)$

$$= \begin{vmatrix} \sqrt[P]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[P]{q_1 s_{g-1} \overline{s}_{g-1}} \\ \sqrt[S_2]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_2]{q_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[S_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[S_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} \end{vmatrix} \begin{vmatrix} \sqrt[A_1]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[A_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \end{vmatrix}$$

$$= c_{2,S} \begin{vmatrix} \sqrt[P]{s_1 \overline{s}_1} & \cdots & \sqrt[P]{s_{g-1} \overline{s}_{g-1}} \\ \sqrt[S_2]{s_1 \overline{s}_1} & \cdots & \sqrt[S_2]{s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[S_{g-1}]{s_1 \overline{s}_1} & \cdots & \sqrt[S_{g-1}]{s_{g-1} \overline{s}_{g-1}} \end{vmatrix} \begin{vmatrix} \sqrt[A_1]{r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[A_{g-1}]{r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{r_{g-1} \overline{r}_{g-1}} \end{vmatrix},$$

where $c_{2,S} = \sqrt[P]{q_1}\, \sqrt[S_2]{q_1} \cdots \sqrt[S_{g-1}]{q_1}\, \sqrt[A_1]{\overline{q}_1} \cdots \sqrt[A_{g-1}]{\overline{q}_1}$.

We firstly see that $c_{1,S} = c_{2,S}$. We cancel them out in the quotient $\frac{\chi_{1,S}(P)}{\chi_{2,S}(P)}$ then we let $P = A_1$ and $S_i = A_i$ for $i = 2, \ldots, g-1$. So we have $\frac{\chi_{1,S}(A_1)}{\chi_{2,S}(A_1)} = 1$.

Now we have that

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

In order to have $(-1)^{a(q_0+p_1+p_2)} \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4}$, we need to compute $\frac{\chi_{2,S'}(A_1)^2}{\chi_{1,S'}(A_1)^2}$. Notice that $\chi^2_{1,S'}, \chi^2_{2,S'}$ are sections on the same line bundle corresponding to 3κ. So their quotient is a rational function on the curve. All the following computations until we state the main theorem are carried out to find this rational function.

Now, suppose that $S' = A_2 + \cdots + A_{g-1} + B_1 + \cdots + B_{g-1}$. Note that $\sqrt[A_i]{q_1 r_j \overline{r}_j} = 0$, $\sqrt[A_i]{q_1 s_j \overline{s}_j} = 0$ and $\sqrt[B_i]{\overline{q}_1 r_j \overline{r}_j} = 0$, $\sqrt[B_i]{\overline{q}_1 s_j \overline{s}_j} = 0$ for $i = 1, \ldots, g-1$, $j = 1, \ldots, g-1$.

$\chi_{1,S'}(A_1)$

$$= \begin{vmatrix} \sqrt[A_1]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[A_1]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[A_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[A_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \sqrt[B_1]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[B_1]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[B_1]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[B_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[B_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} & \sqrt[B_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[B_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \end{vmatrix}$$

$$= \begin{vmatrix} 0 & \cdots & 0 & \sqrt[A_1]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \vdots & & \vdots & & & \\ 0 & \cdots & 0 & \sqrt[A_{g-1}]{\overline{q}_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 s_{g-1} \overline{s}_{g-1}} \\ \sqrt[B_1]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[B_1]{q_1 r_{g-1} \overline{r}_{g-1}} & 0 & \cdots & 0 \\ \vdots & & \vdots & & & \\ \sqrt[B_{g-1}]{q_1 r_1 \overline{r}_1} & \cdots & \sqrt[B_{g-1}]{q_1 r_{g-1} \overline{r}_{g-1}} & 0 & \cdots & 0 \end{vmatrix}$$

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

where $c_{1,S'} = \sqrt[A_1]{\overline{q}_1} \cdots \sqrt[A_{g-1}]{\overline{q}_1} \sqrt[B_1]{q_1} \cdots \sqrt[A_{g-1}]{q_1}$.

Similarly,

$\chi_{2,S'}(A_1)$

$$= \begin{vmatrix} \sqrt[A_1]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_1]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[A_1]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[A_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[A_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[A_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \sqrt[B_1]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[B_1]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[B_1]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ \sqrt[B_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[B_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} & \sqrt[B_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[B_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \end{vmatrix}$$

$$= \begin{vmatrix} 0 & \cdots & 0 & \sqrt[A_1]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_1]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \vdots & & \vdots & & & \\ 0 & \cdots & 0 & \sqrt[A_{g-1}]{\overline{q}_1 r_1 \overline{r}_1} & \cdots & \sqrt[A_{g-1}]{\overline{q}_1 r_{g-1} \overline{r}_{g-1}} \\ \sqrt[B_1]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[B_1]{q_1 s_{g-1} \overline{s}_{g-1}} & 0 & \cdots & 0 \\ \vdots & & \vdots & & & \\ \sqrt[B_{g-1}]{q_1 s_1 \overline{s}_1} & \cdots & \sqrt[B_{g-1}]{q_1 s_{g-1} \overline{s}_{g-1}} & 0 & \cdots & 0 \end{vmatrix}$$

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

where $c_{2,S'} = \sqrt[A_1]{\overline{q}_1} \cdots \sqrt[A_{g-1}]{\overline{q}_1} \sqrt[B_1]{q_1} \cdots \sqrt[A_{g-1}]{q_1}$.

Since $c_{1,S'} = c_{2,S'}$,

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

In the following part, we reorganize the quotient in order to express it with more elementary functions. For that reason, we complete all the pairs of multitangents appearing in the matrices above to syzygetic tetrads.

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 $i = 1, \ldots, g-1$ in $\mathbf{S}_{p_1+q_1}$ and $\mathbf{S}_{p_1+\overline{q}_1}$ respectively. Then we divide each row of the matrices by one of $\sqrt[S'_i]{r_g \overline{r}_g}$ and $\sqrt[S'_i]{s_g \overline{s}_g}$ with a suitable S'_i for $i = 2, \ldots, 2g-3$ as follows.

$$\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)} = \frac{d_{2,S'}\begin{vmatrix} \frac{\sqrt[B_1]{s_1\overline{s}_1}}{\sqrt[B_1]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[B_1]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[B_1]{s_g\overline{s}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[B_{g-1}]{s_1\overline{s}_1}}{\sqrt[B_{g-1}]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[B_{g-1}]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[B_{g-1}]{s_g\overline{s}_g}} \end{vmatrix} \begin{vmatrix} \frac{\sqrt[A_1]{r_1\overline{r}_1}}{\sqrt[A_1]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[A_1]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[A_1]{r_g\overline{r}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[A_{g-1}]{r_1\overline{r}_1}}{\sqrt[A_{g-1}]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[A_{g-1}]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[A_{g-1}]{r_g\overline{r}_g}} \end{vmatrix}}{d_{1,S'}\begin{vmatrix} \frac{\sqrt[B_1]{r_1\overline{r}_1}}{\sqrt[B_1]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[B_1]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[B_1]{r_g\overline{r}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[B_{g-1}]{r_1\overline{r}_1}}{\sqrt[B_{g-1}]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[B_{g-1}]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[B_{g-1}]{r_g\overline{r}_g}} \end{vmatrix} \begin{vmatrix} \frac{\sqrt[A_1]{s_1\overline{s}_1}}{\sqrt[A_1]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[A_1]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[A_1]{s_g\overline{s}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[A_{g-1}]{s_1\overline{s}_1}}{\sqrt[A_{g-1}]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[A_{g-1}]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[A_{g-1}]{s_g\overline{s}_g}} \end{vmatrix}}, \tag{1.11}$$

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

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

Now, all the entries of the four matrices in Equation (1.11) are associated to quadratic forms making syzygetic tetrads. We will show how to obtain an elementary function by using such a syzygetic tetrad, and we will describe it for one of the aforementioned Steiner sets, namely $\mathbf{S}_{p_1+q_1}$, without loss of generality. We consider a $(g+1)$-subset

$$\left\{\{r_i, \overline{r}_i\} \mid i = 1, \ldots, g+1\right\}$$

of $\mathbf{S}_{p_1+q_1}$. We know that each tetrad in a Steiner set is syzygetic. Suppose that the corresponding odd theta characteristic divisors to $r_i, \overline{r}_i$ are denoted by $D_{r_i}, D_{\overline{r}_i}$ for $i = 1, \ldots, g-1$ respectively. Because of being syzygetic, it follows from Proposition 1.1.18 that

$$D_{r_i} + D_{\overline{r}_i} + D_{r_{g+1}} + D_{\overline{r}_{g+1}}$$

is cut out by a quadric in $\mathbb{P}^{g-1}$ for $i = 1, \ldots, g$. Denote such a quadric $\mathcal{Q}_i^r$ for $i = 1, \ldots, g$.

Remark 1.2.3. A quadric cutting out the divisor $D_{r_i} + D_{\overline{r}_i} + D_{r_{g+1}} + D_{\overline{r}_{g+1}}$ must be in the linear system $|2\kappa - (D_{r_i} + D_{\overline{r}_i} + D_{r_{g+1}} + D_{\overline{r}_{g+1}})|$. The dimension of the linear system is 0 since $D_{r_i}, D_{\overline{r}_i}, D_{r_{g+1}}, D_{\overline{r}_{g+1}}$ form a syzygetic tetrad. So there is a only one such quadric up to multiplicative constant.

Now we have

$$\operatorname{div}\left(\frac{\sqrt{r_i\overline{r}_i}}{\sqrt{r_g\overline{r}_g}}\right) = \operatorname{div}\left(\frac{\mathcal{Q}_i^r}{\mathcal{Q}_g^r}\right).$$

It implies that there is a constant $c_{ig} \in \mathbb{C}$ such that

$$\frac{\sqrt{r_i\overline{r}_i}}{\sqrt{r_g\overline{r}_g}} = c_{ig}\frac{\mathcal{Q}_i^r}{\mathcal{Q}_g^r}. \tag{1.12}$$

By following the argument above, we rewrite $\chi_{2,S'}(A_1)/\chi_{1,S'}(A_1)$ in terms of the corresponding quadrics and take its square. Note that the constants in Equation (1.12) will

appear in the numerator and denominator of the quotient $\chi_{2,S'}(A_1)/\chi_{1,S'}(A_1)$ in the same way, so they will be cancelled out. We do not include them in the following quotient.

$$\left(\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)}\right)^2 = \frac{d_{1,S'}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(B_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(B_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(B_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(A_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_{(g)}^r}(A_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(A_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_g^r}(A_{g-1}) \end{vmatrix}^2}{d_{2,S'}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(B_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_g^r}(B_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(B_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_g^r}(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(A_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(A_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(A_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(A_{g-1}) \end{vmatrix}^2}. \tag{1.13}$$

We give the statement of the result which is obtained above. Recall that β_q is a fixed linear equation of the multitangent H_{D_q} which corresponds to the associated theta characteristic divisor D_q for any quadratic form q.

Theorem 1.2.4. *Let p_1, p_2 be two even quadratic form $p_1+p_2 = q_1+\overline{q}_1$. For $i = 1, \ldots, g-1$, let A_i and B_i be fixed representatives of the contact points of β_{q_1} and $\beta_{\overline{q}_1}$ with the canonical model of $\mathcal{C}$. Consider $g+1$ pairs of quadratic forms*

$$\big\{\{r_i, \overline{r}_i\} \mid i = 1, \ldots, g+1\big\} \text{ and } \big\{\{s_i, \overline{s}_i\} \mid i = 1, \ldots, g+1\big\}$$

in the Steiner sets $\mathbf{S}_{p_1+q_1}$ and $\mathbf{S}_{p_1+\overline{q}_1}$ respectively and Q_i^r and Q_i^s be the aforementioned quadrics for $i = 1, \ldots, g$. Then

$$(-1)^{a(q_0+p_1+p_2)} \cdot \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4} = \frac{d_1 \begin{vmatrix} \mathcal{Q}_1^s(B_1) & \cdots & \mathcal{Q}_{g-1}^s(B_1) \\ \vdots & & \vdots \\ \mathcal{Q}_1^s(B_{g-1}) & \cdots & \mathcal{Q}_{g-1}^s(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \mathcal{Q}_1^r(A_1) & \cdots & \mathcal{Q}_{g-1}^r(A_1) \\ \vdots & & \vdots \\ \mathcal{Q}_1^r(A_{g-1}) & \cdots & \mathcal{Q}_{g-1}^r(A_{g-1}) \end{vmatrix}^2}{d_2 \begin{vmatrix} \mathcal{Q}_1^r(B_1) & \cdots & \mathcal{Q}_{g-1}^r(B_1) \\ \vdots & & \vdots \\ \mathcal{Q}_1^r(B_{g-1}) & \cdots & \mathcal{Q}_{g-1}^r(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \mathcal{Q}_1^s(A_1) & \cdots & \mathcal{Q}_{g-1}^s(A_1) \\ \vdots & & \vdots \\ \mathcal{Q}_1^s(A_{g-1}) & \cdots & \mathcal{Q}_{g-1}^s(A_{g-1}) \end{vmatrix}^2},$$

where q_0 is the quadratic form defined in Equation (1.7) *and*

$$d_1 = \prod_{i=1}^{g-1} (\beta_{r_g}\beta_{\overline{r}_g})(B_i)(1/Q_g^s(B_i))^2 \prod_{i=1}^{g-1} (\beta_{s_g}\beta_{\overline{s}_g})(A_i)(1/Q_g^r(A_i))^2$$

and

$$d_2 = \prod_{i=1}^{g-1} (\beta_{s_g}\beta_{\overline{s}_g})(B_i)(1/Q_g^r(B_i))^2 \prod_{i=1}^{g-1} (\beta_{r_g}\beta_{\overline{r}_g})(A_i)(1/Q_g^s(A_i))^2.$$

Pseudocode

Because of the various identifications in Section 1.1, we will abuse notation and confuse a quadratic form and its corresponding theta characteristic.

Algorithm 1: ThetaConstants

Input:
$\mathcal{C}$, the model of the curve in $\mathbb{P}^{g-1}$ under the canonical embedding,
L_1, the list of fixed equations of the multi-tangents,
L_2, the list of the labels of the equations in L_1 indexed such that the i-th element of L_2 is the label for i-th element of L_1,
$I_{p_1}, I_{p_2} \subset \{1, \ldots, 2g+1\}$, the labels of two even characteristic p_1, p_2 respectively.

Output: $\left(\frac{\vartheta[p_1](\tau)}{\vartheta[p_2](\tau)}\right)^4$.

1: Establish any two labels $I_{q_1}, I_{\overline{q}_1}$ such that $I_{p_1} \triangle I_{p_2} \triangle I_{q_1} \triangle I_{\overline{q}_1} = \emptyset$ where $\triangle$ denotes the symmetric difference of sets. Note that $\{q_1, \overline{q}_1\}$ is a pair of odd quadratic forms in the Steiner set $\mathbf{S}_{p_1+p_2}$.
2: Call the multitangents $\beta_{q_1}, \beta_{\overline{q}_1}$ from L_1 by the indexes of $I_{q_1}, I_{\overline{q}_1}$ in L_2.
3: Compute the tangency points of β_{q_1} and $\beta_{\overline{q}_1}$. Denote them $\{A_1, \ldots, A_{g-1}\}$ and $\{B_1, \ldots, B_{g-1}\}$ respectively.
4: Now compute the Steiner set of $p_1 + q_1$ and $p_1 + \overline{q}_1$ via their labels. Notice that $p_2 + q_1 = p_1 + \overline{q}_1$ and $p_2 + \overline{q}_1 = p_1 + q_1$.
5: Set $\mathbf{S}'_{p_1+q_1}$ and $\mathbf{S}'_{p_1+\overline{q}_1}$ as $g+1$-subsets $\mathbf{S}_{p_1+q_1}$ and $\mathbf{S}_{p_1+\overline{q}_1}$ respectively. i.e Choose $g+1$ pairs of quadratic forms from each of Steiner sets. Denote them $r_i, \overline{r}_i$ and $s_i + \overline{s}_i$ respectively for $i = 1, \ldots, g+1$.
6: Call the multitangents $\beta_{r_i}, \beta_{\overline{r}_i}$ and $\beta_{s_i}, \beta_{\overline{s}_i}$ and compute their contact points with $\mathcal{C}$.
7: Compute d_1 and d_2 defined in Theorem 1.2.4.
8: Now compute the quadrics $\mathcal{Q}^r_i, \mathcal{Q}^r_g$ and $\mathcal{Q}^s_i, \mathcal{Q}^s_g$ for $i = 1, \ldots, g-1$, see Equation (1.12).
9: **return** Compute and return the quotient $\left(\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)}\right)^2$ in Theorem 1.2.4.

As an input of the algorithm, we need the equation of a curve under the canonical embedding, the equations of the multi-tangents and a labelling which is given by an Aronhold basis. This triple is called a *complete* 2*-level structure*. Obtaining such a structure is generally not easy. We can overcome this problem thanks to the geometric structure of a del Pezzo surface of degree 1.

1.2.2 Del Pezzo Surfaces

Firstly, we review basic concepts about del Pezzo surfaces. In this regard, we benefited from several sources such as [32, Chapter 8], [29], [71, Chapter IV].

A complete, smooth surface $\mathcal{S}$ with ample anticanonical divisor $-\kappa_{\mathcal{S}}$ is called *del Pezzo surface*. That is to say, $-n\kappa_{\mathcal{S}}$ is very ample for some positive integer n i.e. there is a closed embedding

$$\rho : S \to \mathbb{P}^m$$

for some $m \geq 0$ such that $(\kappa_{\mathcal{S}}^{-1})^n = \rho^* \mathcal{O}_{\mathbb{P}^m}(1)$. The *degree* d of a del Pezzo surface is defined as the self-intersection $\kappa^2_{\mathcal{S}}$. The degree of a del Pezzo surface is at most 9. The ampleness of $-\kappa_S$ implies the self-intersection κ^2_S is positive(Nakai-Moishezon criterion).

Anticanonical model

For a given del Pezzo surface $\mathcal{S}$, it is possible to have its projective model via the associated *anticanonical model*. For any variety X, if D is a divisor on X then we may construct the graded ring

$$\mathcal{R}(X, D) = \bigoplus_{m \geq 0} \mathcal{L}(mD).$$

In particularly, if $D = -\kappa_X$ then the graded ring is called the anticanonical ring of X.

Theorem 1.2.5. *[58, Theorem III.3.5] If $\mathcal{S}$ be a del Pezzo surface and $\kappa_{\mathcal{S}}^2 \leq 4$ then $\mathcal{S}$ is isomorphic to* $\operatorname{Proj} \mathcal{R}(\mathcal{S}, -\kappa_{\mathcal{S}})$.

The scheme $\operatorname{Proj} \mathcal{R}(\mathcal{S}, -\kappa_{\mathcal{S}})$ is called the *anticanonical model* of $\mathcal{S}$.

Del Pezzo surfaces as blow-ups

In this section, we see the description of a del Pezzo surface $\mathcal{S}$ as a blowup of $\mathbb{P}^2$. This description enables us to classify the exceptional classes in $\operatorname{Pic}(\mathcal{S})$ with exceptional curves of aforementioned blow-up.

Definition 1.2.6. A collection of points of $\mathbb{P}^2$ are said to be in general position if no three of them lie on a line, no six of them lie on a conic and no eight of them lie on a cubic with a singularity at one of the points.

Theorem 1.2.7. *[71, Theorem 24.4]Let $\mathcal{S}$ be a del Pezzo surface of degree d. Then*

(i) $1 \leq d \leq 9$,

(ii) if $d = 9$ then $\mathcal{S}$ is isomorphic to $\mathbb{P}^2$,

(iii) if $d = 8$ then $\mathcal{S}$ isomorphic to either $\mathbb{P}^1 \times \mathbb{P}^1$ or the blow-up of $\mathbb{P}^2$ at a point,

(iv) if $1 \leq d \leq 7$, then $\mathcal{S}$ is isomorphic to the blow-up $\mathbb{P}^2$ at $9 - d$ points in general position.

Conversely, the blow-up of $\mathbb{P}^2$ at $9 - d$ points is a del Pezzo surface if and only if the points are in general position for $1 \leq d \leq 9$.

In the case that $\mathcal{S}$ is isomorphic to the blow-up of $\mathbb{P}^2$ at r many points $P_1 \ldots, P_r$ in general position, we denote it $\operatorname{Bl}_{P_1 \ldots, P_r} \mathbb{P}^2$.

Exceptional curves and the Picard group

An *exceptional curve* E on a projective, smooth surface S is an irreducible curve on X with $E^2 = \kappa_S \cdot E = -1$. The class of an exceptional curve in $\operatorname{Pic}(X)$ is called the *exceptional class*. By the adjunction formula, an exceptional curve is of arithmetic genus 0, therefore it is isomorphic to $\mathbb{P}^1$.

Suppose that $\mathcal{S} = \operatorname{Bl}_{P_1 \ldots, P_r} \mathbb{P}^2$. All the exceptional classes of $\mathcal{S}$ are closely related with the exceptional curves of the blow-up. In addition, the classes of exceptional curves of the blow-up play a fundamental role for the structure of $\operatorname{Pic}(\mathcal{S})$. Indeed, if E_i is the exceptional curve corresponding to P_i and L is the pullback of the class of line in $\mathbb{P}^2$ then

$$\{L, E_1, \ldots, E_r\}$$

forms a basis for $\mathrm{Pic}(\mathcal{S})$. More compactly,

$$\mathrm{Pic}(\mathcal{S}) = \mathbb{Z}L \oplus \mathbb{Z}E_1 \oplus \cdots \oplus \mathbb{Z}E_r.$$

The anticanonical class is given in terms of basis as

$$\kappa_{\mathcal{S}} = -3L + \sum_{i=1}^{r} E_i.$$

Additionally, the intersection theory gives that

$$E_i \cdot E_j = \delta_{ij}, \quad E_i \cdot L = 0, \quad L \cdot L = 1,$$

where δ_{ij} is the Kronecker delta function.

As we have explained above, any divisor class $D \in \mathrm{Pic}(\mathcal{S})$ can be expressed as $aL - \sum_{i=1}^{r} b_i E_i$ in terms of the basis. If D is an exceptional class then we have the following equalities

$$3a - \sum_{i=1}^{r} b_i = 1,$$
$$a^2 - \sum_{i=1}^{r} {b_i}^2 = 1$$

for some integers a, b_i by the definition of an exceptional class. The solutions of these equalities lead to the following proposition.

Proposition 1.2.8. *[71, Theorem 26.1] The exceptional classes of* $\mathrm{Pic}(\mathcal{S})$ *are in the form* $aL - \sum_{i=1}^{r} b_i E_i$ *where* $\{a, b_1 \ldots, b_r\}$ *are obtained by all possible permutations of* b_i *in the following table*

a	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
0	-1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0
2	1	1	1	1	1	0	0	0
3	2	1	1	1	1	1	1	0
4	2	2	2	1	1	1	1	1
5	2	2	2	2	2	2	1	1
6	3	2	2	2	2	2	2	2.

The following theorem mentions the correspondence between the exceptional curves on $\mathcal{S}$ and the classes in $\mathrm{Pic}(\mathcal{S})$ and gives a geometric description of the exceptional curves which will be useful for computational aspects.

Theorem 1.2.9. *[71, Theorem 26.2] Let* $\mathcal{S} = \mathrm{Bl}_{P_1 \ldots, P_r} \mathbb{P}^2$ *be a del Pezzo surface of degree d. The following results hold;*

(i) The image of any exceptional curve on $\mathcal{S}$ *under the blow down map to* $\mathbb{P}^2$ *is in the following type;*

(a) one of the points P_i*,*

(b) a line passing through two of the points P_i,

(c) a conic passing through five of the points P_i,

(d) a cubic passing through seven points P_i such that one of them is double point,

(e) a quartic passing through eight of the points P_i such that three of them are double points,

(f) a quintic passing through eight of the points P_i such that six of them are double points,

(g) a sextic passing through eight of points P_i such that seven of them are double points and one is triple.

For $d = 2$ only (a)-(d), for $d = 3, 4$ only (a)-(c), for $d = 5, 6, 7$ only (a)-(b), for $d = 8$ only (a) hold.

(ii) The number of exceptional curves on $\mathcal{S}$ are given in the following table;

degree	1	2	3	4	5	6	7	8
the number of exceptional curves	240	56	27	16	10	6	3	1

Del Pezzo surfaces of degree 1

From now on, we focus on del Pezzo surfaces of degree 1 which enable us to have not only a curve $\mathcal{C}$ of genus 4 but also a correspondence between the odd theta divisors in $\mathrm{Pic}(\mathcal{C})$ and the exceptional curves in $\mathrm{Pic}(\mathcal{S})$.

Let $\mathcal{S}$ be a del Pezzo surface of degree 1. From now on, $\mathcal{S} = \mathrm{Bl}_{P_1,\dots,P_8}\mathbb{P}^2$ for $P_1, \dots, P_8 \in \mathbb{P}^2$ in general position.

Firstly, we say how to compute the anticanonical model of $\mathcal{S}$. Afterwards, we discuss the linear system $|-2\kappa_{\mathcal{S}}|$ and the Bertini involution in order to see how the curve $\mathcal{C}$ of genus 4 arises. And finally, we reveal the relationship between the odd theta divisors in $\mathrm{Pic}(\mathcal{C})$ and the exceptional divisors in $\mathrm{Pic}(\mathcal{S})$. Furthermore, we see how to label the theta characteristic divisors due to the configuration of the exceptional divisors.

Anticanonical model

Depending on the dimension formula in Equation (**??**), all the dimensions of the following vector spaces are simply known. We may start to compute the anticanonical model [27].

(i) Firstly we choose a basis $\{x, y\}$ of $\mathcal{L}(-\kappa_{\mathcal{S}})$.

(ii) The elements x^2, xy, y^2 are linearly independent in $\mathcal{L}(-2\kappa_{\mathcal{S}})$. So we complete these elements into a basis $\{x^2, xy, y^2, z\}$ of $\mathcal{L}(-2\kappa_{\mathcal{S}})$.

(iii) The elements $x^3, x^2y, xy^2, y^3, xz, yz$ are linearly independent in $\mathcal{L}(-3\kappa_{\mathcal{S}})$, then we choose an element $w \in \mathcal{L}(-3\kappa_{\mathcal{S}})$ to get a basis $\{x^3, x^2y, xy^2, y^3, xz, yz, w\}$ of $\mathcal{L}(-3\kappa_{\mathcal{S}})$.

(iv) The sets $\{x^4, x^3y, x^2y^2, xy^3, y^4, z^2, x^2z, y^2z, xyz, xw, yw\}$ and $\{x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5, xz^2, yz^2, x^3z, y^3z, x^2yz, xy^2z, zw, x^2w, y^2w, xyw\}$ are bases of $\mathcal{L}(-4\kappa_{\mathcal{S}})$ and $\mathcal{L}(-5\kappa_{\mathcal{S}})$ respectively.

(v) The vector space $\mathcal{L}(-6\kappa_{\mathcal{S}})$ is of dimension 22. Then the 23 elements

$$\{x^6, x^5y, x^4y^2, x^3y^3, x^2y^4, xy^5, y^6, z^3, x^2z^2, y^2z^2, xyz^2, x^4z,$$
$$x^3yz, x^2y^2z, xy^3z, y^4z, xzw, yzw, w^2, x^3w, x^2yw, xy^2w, y^3w\}$$

in $\mathcal{L}(-6\kappa_{\mathcal{S}})$ are linearly dependent. Let $h(x, y, z, w)$ be a linear dependence among them.

We suppose that T is the graded algebra $k[x, y, z, w]$ by grading $\deg x = 1$, $\deg y = 1$, $\deg z = 2$ and $\deg w = 3$. Then there is a natural isomorphism between the anticanonical ring $\mathcal{R}(\mathcal{S}, -\kappa_{\mathcal{S}})$ and $T/(h)$ (see [27, Page 1202]). Hence $\mathcal{S}$ can be described as the zero locus of h in $\mathbb{P}(1, 1, 2, 3)$. We may write $h = w^2 + wg(x, y, z) + f(x, y, z)$ where g and f are weighted homogeneous polynomials of degree 3 and 6 respectively. If $\mathrm{Char}\, k \neq 2$ then we may (do) assume $g = 0$ with the change of coordinates $y \mapsto y - g/2$.

Remark 1.2.10. We make the computation of this model of $\mathcal{S}$ by starting from the eight points $P_1, \ldots, P_8$ as follows. Since $-\kappa_{\mathcal{S}}$ is equivalent to $3L - E_1 - \cdots - E_8$ where L is the pullback of the line class in $\mathbb{P}^2$ and E_i is the exceptional class lying above P_i under the blow up map, we look at the space of plane cubics passing through $P_1, \ldots, P_8$ which has dimension 2. By abuse of notation, let $\{x, y\}$ be any basis of this space. Next, we consider the space of plane sextics vanishing doubly on $P_1, \ldots, P_8$ has dimension 4. So there is a sextic z in this space for which $\{x^2, xy, y^2, z\}$ forms a basis. Last, the space of plane nonics vanishing triply on $P_1, \ldots, P_8$ has dimension 7. It is spanned by $\{x^3, x^2y, xy^2, xz, yz, w\}$ for some nonic w. This defines a rational map

$$\begin{array}{rccc} \psi\colon & \mathbb{P}^2 & \longrightarrow & \mathbb{P}(1\colon 1\colon 2\colon 3) \\ & (t_0\colon t_1\colon t_2) & \longmapsto & (x(t_0,t_1,t_2)\colon y(t_0,t_1,t_2)\colon z(t_0,t_1,t_2)\colon w(t_0,t_1,t_2)). \end{array}$$

The Zariski closure of the image $\tilde{\mathcal{S}}$ under this map is a del Pezzo surface of degree 1 [71][Remark 24.4.2] and there is a morphism between $\mathcal{S}$ and $\tilde{\mathcal{S}}$. By abuse of notation, we identify $\mathcal{S}$ with $\tilde{\mathcal{S}}$. After a linear change of coordinates, we have the defining equation of $\mathcal{S}$ in $\mathbb{P}(1, 1, 2, 3)$ as

$$\mathcal{S} : w^2 = z^3 + f_2(x, y)z^2 + f_4(x, y)z + f_6(x, y) \tag{1.14}$$

where $f_i \in k[w, z]$ are homogeneous polynomials of degree d for $d = 0, 2, 4, 6$.

The Bertini involution and linear system $|-2\kappa_{\mathcal{S}}|$

The linear system $|-2\kappa_{\mathcal{S}}|$ defines a double cover $\phi_2 : \mathcal{S} \to \mathbb{P}^3$ onto a cone Q. The map ϕ_2 is called the *antibicanonical map*. Indeed, the basis $\{x^2, xy, y^2, z\}$ of $\mathcal{L}(-2\kappa_{\mathcal{S}})$ determines a two-to-one map ϕ_2 onto the cone $Q = V(t_0t_2 - t_1^2)$ where t_0, t_1, t_2, t_3 are coordinates for $\mathbb{P}^3$. The branch curve $\mathcal{B}$ is a smooth, reduced and irreducible curve of genus 4 which is the intersection of Q with a cubic surface. To be more precise, in the defining equation of $\mathcal{S}$ in Equation (1.14), if we let $F \in k[t_0, t_1, t_2, t_3]$ be the homogenous polynomial of degree 3 corresponding to $f_2(x, y)z^2 + f_4(x, y)z + f_6(x, y)$ under the map $(z^2, zw, w^2, x) \mapsto (t_0, t_1, t_2, t_3)$ then the branch curve $\mathcal{B}$ is given as the zero locus $V(Q, F)$ in $\mathbb{P}^3$ [27].

On the other hand, we consider the map

$$\begin{aligned} \iota : \mathbb{P}(1, 1, 2, 3) &\longrightarrow \mathbb{P}(1, 1, 2, 3) \\ (x : y : z : w) &\mapsto (x : y : z : -w + f). \end{aligned}$$

This map defines an involution ι called *Bertini involution* on the surface S. The fixed locus of ι is a smooth, irreducible, projective curve of genus 4, denote it $\mathcal{C}$. We note that $\phi_2^*(\mathcal{B}) = 2\mathcal{C}$ [29].

We have the following figure

$$\begin{array}{ccccc}
\mathbb{P}^2 & \xrightarrow{\psi} & \mathbb{P}(1:1:2:3) & \supset & X := \overline{\psi(\mathbb{P}^2)} \\
 & & \Big\downarrow{\scriptstyle \pi}\ {\scriptstyle (x:y:z:w)\mapsto(s:t:w)} & & \\
 & & \mathbb{P}(1:1:2) & \supset & \mathcal{B} := \mathrm{BranchCurve}(\pi|_X) \\
 & & \Big\downarrow{\scriptstyle \phi}\ {\scriptstyle (x:y:z)\mapsto(x^2:xy:y^2:z)} & & \Big\downarrow \\
 & & \mathbb{P}^3 & \supset & C
\end{array}$$

Figure 1.3: The del Pezzo surface $\mathcal{S}$ of degree 1 and the branch curve $\mathcal{B}$.

Exceptional divisors and theta characteristic divisors

Let $\rho : \mathrm{Pic}(\mathcal{S}) \to \mathrm{Pic}(\mathcal{C})$ be the restriction homomorphism. Firstly, note that the adjunction formula gives $\kappa_{\mathcal{C}} = -2\rho(\kappa_{\mathcal{S}})$ where $\kappa_{\mathcal{C}}$ is the canonical divisor of $\mathcal{C}$.

Our aim is to see the link between the odd theta characteristic divisors on $\mathcal{C}$ and the exceptional divisors on $\mathcal{S}$.

So we firstly introduce

$$M := \kappa_{\mathcal{S}}^{\perp} = \{D \in \mathrm{Pic}(\mathcal{S}) \mid \kappa_{\mathcal{S}} \cdot D = 0\}. \tag{1.15}$$

It is a $\mathbb{Z}$-module generated by

$$\begin{aligned}
B_1 &:= E_1 - E_2, \\
B_2 &:= E_2 - E_3, \\
&\vdots \\
B_7 &:= E_7 - E_8, \\
B_8 &:= L - E_1 - E_2 - E_3.
\end{aligned}$$

For the structure of $\kappa_{\mathcal{S}}^{\perp}$, we refer to [32, Section 8.2.2].

Proposition 1.2.11. *[101, Section 2] We have the following*

(i) for any $D \in \kappa_{\mathcal{S}}^{\perp}$, $\rho(2D) = 0$,

(ii) if E is an exceptional divisor then $\rho(E)$ is an odd theta characteristic divisor on $\mathcal{C}$,

(iii) $\rho(-\kappa_{\mathcal{S}})$ is an even theta characteristic divisor on $\mathcal{C}$.

The action of the Bertini involution on the exceptional curves is as follows.

Proposition 1.2.12. *[101, Section 2] If E is an exceptional divisor on $\mathcal{S}$ then*

(i) $\iota(E) = -E - 2\kappa_{\mathcal{S}}$,

(ii) $\rho(\iota(E)) = \rho(E)$.

As a corollary, we illustrate the action of ι on the exceptional curves more concretely. Let $I = \{1, \dots, 8\}$. For $n \in \{1, \dots, 8\}$, define $I_{i_1 \dots i_n} := I \setminus \{i_1, \dots, i_n\}$ with $i_k \neq i_l$ for any $k \neq l$. Now, we have the following correspondence

$$E_i \overset{\iota}{\longleftrightarrow} 6L - \sum_{j \in I_i}^{8} 2E_j - 3E_i$$

$$L - E_i - E_j \overset{\iota}{\longleftrightarrow} 5L - \sum_{k \in I_{ij}}^{8} 2E_k - E_i - E_j$$

$$2L - \sum_{l \in I_{ijk}}^{8} E_l \overset{\iota}{\longleftrightarrow} 4L - \sum_{l \in I_{ijk}} E_{i_l} - 2E_i - 2E_j - 2E_k$$

$$3L - 2E_i - \sum_{k \in I_{ij}} E_k \overset{\iota}{\longleftrightarrow} 3L - 2E_j - \sum_{k \in I_{ij}} E_k.$$

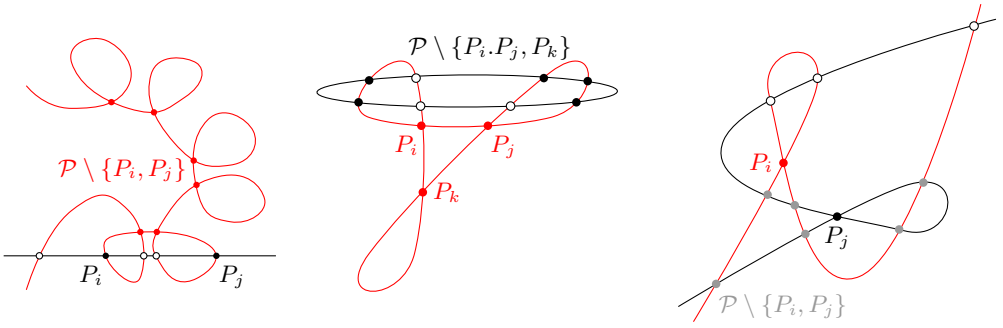


Figure 1.4: Pairs of exceptional curves under the Bertini involution.

Another corollary of Proposition 1.2.12 (ii) is that there is a two-to-one correspondence between the set of exceptional divisors on S and the set of odd theta divisors on $\mathcal{C}$. The preimage of an odd theta characteristic divisor under ρ consists of two exceptional divisors which are conjugate under ι. Let us denote this correspondence

$$\{E, \iota(E)\} \longleftrightarrow D_E. \tag{1.16}$$

Remark 1.2.13. Because of Proposition 1.2.12(i), for any exceptional divisors E we have

$$\rho(\iota(E)) + \rho(E) = \rho(\iota(E) + E) = \rho(-2\kappa_{\mathcal{S}}) = \kappa_{\mathcal{C}}.$$

Since $\mathcal{O}_{\mathbb{P}^3}(1)$ corresponds to $\kappa_{\mathcal{C}}$ under the canonical embedding, $\rho(\iota(E)+E)$ defines a plane in $\mathbb{P}^3$. Moreover, this plane defines a tritangent of $\mathcal{C}$. The equality also hints on how to compute the equations of the tritangents which corresponds to odd theta characteristic divisors by starting from $P_1, \dots, P_8$. Indeed, the preimage of any odd theta characteristic divisor gives a pair of exceptional divisors of $\mathcal{S}$ conjugated under the Bertini involution. All such pairs are mapped to geometric objects given in Theorem 1.2.9(i) under the blow down map. We may compute the zero locus of the union of such pair in $\mathbb{P}^2$ and compute the image in $\mathbb{P}^3$ by passing through $\mathbb{P}(1,1,2,3)$ and $\mathbb{P}(1,1,2)$ under the maps π and ϕ (see Figure 1.3).

We are on our way to get a complete 2-level structure of a genus 4 curve $\mathcal{C}$. Indeed, we are able to compute the canonical model of $\mathcal{C}$ and all the tritangent equations in $\mathbb{P}^3$. In the following section, we obtain an Aronhold basis which provides a labelling for all the theta characteristic divisors (see Section 1.1.1).

1.2.3 Finding an Aronhold basis

Because of Proposition 1.1.5, if we have a fundamental set in $\mathrm{Jac}\,\mathcal{C}[2]$ then we know how to construct an Aronhold basis. The following theorem gives such a fundamental set.

Theorem 1.2.14. *[101, Theorem 2.10] The set* $\{\rho(E_i + \kappa_{\mathcal{S}}) \mid i = 1, \dots, 8\}$ *forms a basis of* $\mathrm{Pic}(\mathcal{C})[2]$ *with* $\langle \rho(E_i + \kappa_{\mathcal{S}}), \rho(E_j + \kappa_{\mathcal{S}}) \rangle = 1$ *if* $i \neq j$ *where* $\langle , \rangle$ *is the Weil pairing. Futhermore, If* M *is defined as in* (1.15) *then the map* $M/2M \to \mathrm{Pic}(\mathcal{C})[2]$ *induced by* ρ *is an isometry with respect to the pairing of intersection number on* M *modulo* 2 *and the Weil pairing* $\langle , \rangle$ *on* $\mathrm{Pic}(\mathcal{C})[2]$.

Remark 1.2.15. By Remark 1.1.4, the set $\{\rho(E_i + \kappa_{\mathcal{S}}) \mid i = 1, \dots, 8\}$ can be completed to a fundamental set in $\mathrm{Jac}(\mathcal{C})[2]$.

Now, we construct an Aronhold basis by following the proof of Proposition 1.1.5.

Consider $\rho(-\kappa_{\mathcal{S}})$. Let the associated quadratic form $q_{\rho(-\kappa_{\mathcal{S}})}$ be the simplest quadratic form defined in Equation (1.7), and denote it by q_0. By following Section 1.1.3, recall that D_q denotes the theta characteristic divisor corresponding to the quadratic form q and

$$D_q = D_{q_0} + q + q_0. \tag{1.17}$$

We denote T_q the corresponding tritangent equation in $\mathbb{P}^3$.

Now, we consider the following 2-torsion elements in $\mathrm{Pic}(\mathcal{C})[2]$

$$\begin{aligned} v_i &:= \rho(E_i + \kappa_{\mathcal{S}}) \text{ for } i = 1, \dots, 8, \\ v_9 &:= \sum_{i=1}^{8} v_i. \end{aligned}$$

By Proposition 1.2.14, the set $\{v_1, \dots, v_9\}$ is a fundamental set in $\mathrm{Jac}(\mathcal{C})[2]$. In order to use Proposition 1.1.5, we observe that

$$\begin{aligned} q_0(v_i) &= \ell(\rho(-\kappa_{\mathcal{S}}) + \rho(E_i + \kappa_{\mathcal{S}})) + \ell(\rho(-\kappa_{\mathcal{S}})) \pmod 2 \\ &= \ell(\rho(E_i)) + \ell(\rho(-\kappa_{\mathcal{S}})) \pmod 2 \\ &= 1 + 0 \pmod 2 \end{aligned}$$

for $i = 1, \dots, 8$ which follows from that $\rho(E_i), \rho(-\kappa_{\mathcal{S}})$ are odd, even respectively. In addition, we can compute $q_0(v_9) = 0$.

For $i = 1, \dots, 9$, define $q_i := q_0 + v_i + v_9$. It follows from Proposition 1.1.5 that the set

$$\mathcal{A} = \{q_1, \dots, q_9\}$$

forms an Aronhold basis for the quadratic forms on $\mathrm{Jac}(\mathcal{C})[2]$, in which the basis is formed by even quadratic forms since the genus of $\mathcal{C}$ is 4 because of Proposition 1.1.6. Note that $\sum_{i=1}^{9} q_i = q_0$.

Recall that $\mathcal{S} = \mathrm{Bl}_{P_1, \dots, P_8} \mathbb{P}^2$. In the following part, we see how to realise the labelling (see 1.1.1) which comes from $\mathcal{A}$ in terms of the points $P_1, \dots, P_8$. Therefore, we will have a complete 2-level structure of $\mathcal{C}$.

We know that if you have an odd theta divisor $\rho(E)$ then $\rho(E+\kappa_{\mathcal{S}})$ is a 2-torsion point of $\mathrm{Pic}(\mathcal{C})$. We express $\rho(E+\kappa_{\mathcal{S}})$ as a linear combination of $\rho(E_i+\kappa_S)$'s. Recall that, $I=\{1,\dots,8\}$ and for $n\in\{1,\dots,8\}$, $I_{i_1\dots i_n}=I\setminus\{i_1,\dots,i_n\}$ with $i_k\neq i_l$ for any $k\neq l$.

Proposition 1.2.16. *We have*

(i) $\rho(L-E_i-E_j+\kappa_{\mathcal{S}})=\sum_{k\in I_{ij}}\rho(E_k+\kappa_{\mathcal{S}})$ *for all distinct* $i,j\in I$,

(ii) $\rho\left(2L-\sum\limits_{l\in I_{ijk}}^{8}E_l+\kappa_{\mathcal{S}}\right)=\sum_{l\in I_{ijk}}\rho(E_l+\kappa_{\mathcal{S}})$ *for all distinct* $i,j,k\in I$,

(iii) $\rho\left(3L-2E_i-\sum\limits_{k\in I_{ij}}E_k+\kappa_{\mathcal{S}}\right)=\rho(E_i+\kappa_{\mathcal{S}})+\rho(E_j+\kappa_{\mathcal{S}})$ *for all distinct* $i,j\in I$.

Proof. We have $\left(8L+\sum\limits_{i=1}^{8}3E_i\right)\cdot\kappa_{\mathcal{S}}=0$ where $\kappa_{\mathcal{S}}=-3L+E_1+\cdots+E_8$. It follows from Proposition 1.2.11 that $\rho\left(16L+\sum\limits_{i=1}^{8}6E_i\right)=0$. Now,

$$\begin{aligned}\rho(L-E_i-E_j+\kappa_{\mathcal{S}})-\sum_{\substack{k=1\\k\neq i,j}}^{8}\rho(E_k+\kappa_{\mathcal{S}})&=\rho\left(L-\sum_{i=1}^{8}-5\kappa_{\mathcal{S}}\right)\\&=\rho\left(16L-\sum_{i=1}^{8}6E_i\right)\\&=0.\end{aligned}$$

We have that $\rho(E_i+\kappa_{\mathcal{S}})=\rho(-E_i-\kappa_{\mathcal{S}})$ and $(L+3\kappa_{\mathcal{S}})\cdot\kappa_{\mathcal{S}}=0$. Thus,

$$\begin{aligned}\rho\left(2L-\sum_{\substack{k=1\\i_k\in\{1,\dots,8\}}}^{5}E_{i_k}+\kappa_{\mathcal{S}}\right)-\sum_{\substack{k=1\\i_k\in\{1,\dots,8\}}}^{5}\rho(E_{i_k}+\kappa_{\mathcal{S}})&\\=\rho\left(2L-\sum_{\substack{k=1\\i_k\in\{1,\dots,8\}}}^{5}E_{i_k}\right)+\sum_{\substack{k=1\\i_k\in\{1,\dots,8\}}}^{5}\rho(E_{i_k}+\kappa_{\mathcal{S}})&\\=\rho(2L+6\kappa_{\mathcal{S}})&\\=0.&\end{aligned}$$

We have that $\rho(E_i + \kappa_{\mathcal{S}}) = \rho(-E_i - \kappa_{\mathcal{S}})$ and $\kappa_{\mathcal{S}} = -3L + E_1 + \cdots + E_8$. Thus,

$$\begin{aligned}
&\rho\left(3L - 2E_i - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}}\right) - \rho(E_i + \kappa_{\mathcal{S}}) - \rho(E_j + \kappa_{\mathcal{S}}) \\
&\qquad = \rho\left(3L - 2E_i - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}}\right) + \rho(E_i + \kappa_{\mathcal{S}}) - \rho(E_j + \kappa_{\mathcal{S}}) \\
&\qquad = \rho(3L - E_1 - E_2 - \cdots - E_8 + \kappa_{\mathcal{S}}) \\
&\qquad = 0.
\end{aligned}$$

□

Now, let us write down all the quadratic forms by using $\mathcal{A}$ and figure out the labelling in terms of the indexes of $P_1, \ldots, P_8$. For the following part, recall Theorem 1.2.9 and Remark 1.2.13.

- The quadratic forms q_i are even.
- The quadratic forms of length 3 are odd. Take any $q_{ijk} := q_i + q_j + q_k$ of length 3 for $i, j, k \in \{1, \ldots, 9\}$ then

$$\begin{aligned}
q_{ijk} &= q_i + q_j + q_k \\
&= q_0 + v_i + v_9 + q_0 + v_j + v_9 + q_0 + v_k + v_9 \\
&= q_0 + v_i + v_j + v_k + v_9,
\end{aligned}$$

  where $i \neq j \neq k$. There are two cases.

  – If none of i, j, k is 9 then

$$q_{ijk} = q_0 + \sum_{l\in I_{ijk}} v_l.$$

    where $I_{ijk} = I \setminus \{i, j, k\}$. The corresponding theta characteristic divisor (as in Equation (1.17) is

$$\begin{aligned}
D_{q_{ijk}} &= D_0 + q_{ijk} + q_0 \\
&= D_0 + \sum_{l\in I_{ijk}} v_l \\
&= \rho\left(2L - \sum_{l\in I_{ijk}} E_l\right).
\end{aligned}$$

    by Proposition 1.2.16. So, we actually label the corresponding tritangent via the indexes of the points P_i, P_j, P_k which do not lie on the conic.

    Example 1.2.17. The corresponding odd theta characteristic divisor $D_{q_{123}}$ is $\rho(2L - \sum_{i=4}^{8} E_i)$. The equation of the tritangent arises by a conic passing through $P_4, \ldots, P_8$ which is the image of $2L - \sum_{i=4}^{8} E_i$ under the blown down map. The label is via the indexes of P_1, P_2, P_3 which do not lie on the conic in $\mathbb{P}^2$.

– if one of i, j, k is 9, say k, then

$$q_{ijk} = q_0 + v_i + v_j.$$

It corresponds to the odd theta characteristic divisor

$$\begin{aligned} D_{q_{ij9}} &= D_0 + q_{ij9} + q_0 \\ &= \rho(-\kappa_{\mathcal{S}}) + \rho(E_i + \kappa_S) + \rho(E_j + \kappa_{\mathcal{S}}) \\ &= \rho\left(3L - 2E_i - \sum_{k \in I_{ij}} E_k\right) \end{aligned}$$

by Proposition 1.2.16. We know that $3L - 2E_i - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}}$ maps to a cubic in $\mathbb{P}^2$ that passes through P_k's for $l \in I \setminus \{j\}$ where P_i is a double point under the blow down map. We label the corresponding tritangent via the indexes of the point P_i which is the double point and the point P_j which does not vanish on the cubic. Although we can not distinguish whether i or j in the label $\{i, j, 9\}$ is the index of the double point, it does not cause a problem since $\iota(3L - 2E_i - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}}) = (3L - 2E_j - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}})$ and both of $3L - 2E_i - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}}, 3L - 2E_j - \sum_{k\in I_{ij}} E_k + \kappa_{\mathcal{S}}$ is in the fiber $\rho^{-1}(D_{q_{ij9}})$ by Proposition 1.2.12.

Example 1.2.18. The corresponding theta characteristic divisor $D_{q_{129}}$ is $\rho(3L - 2E_1 - \sum_{i=3}^{8} \rho(E_i + \kappa_{\mathcal{S}}))$. The corresponding tritangent is labelled via the indexes of P_1, P_2 which are the double point and the point that is not on the cubic respectively.

- The quadratic forms of length 5 are even.
- We take any quadratic form $q_{i_1 \dots i_7} := \sum_{n=1}^{7} q_{i_n}$ of length 7 for distinct i_n's in $\{1, \dots, 9\}$. It is odd.
  – If none of i_n's is 9 then

$$\begin{aligned} q_{i_1 \dots i_7} &= \sum_{n=1}^{7} q_{i_n} \\ &= \sum_{n=1}^{7} (q_0 + v_{i_n} + v_9) \\ &= q_0 + v_9 + \sum_{n=1}^{7} v_{i_n} \\ &= q_0 + v_{i_8}. \end{aligned}$$

The corresponding odd theta characteristic divisor $D_{q_{i_1 \dots i_7}}$ is $\rho(E_{i_8})$. The image of E_{i_8} is the point P_{i_8} in $\mathbb{P}^2$. We label the corresponding tritangent via the indexes of $P_{i_1}, \dots, P_{i_7}$ for which the complementary index i_8 in I is the index of the point P_{i_8}.

Example 1.2.19. The odd theta characteristic divisor $D_{q_{1\dots 7}}$ is $\rho(E_8)$. So we label it via the indexes of $P_1, \dots, P_7$.

– if one of i_n's is 9, without loss of generality say $i_7 = 9$, then

$$\begin{aligned} q_{i_1\dots i_7} &= \sum_{n=1}^{7} q_{i_n} \\ &= \sum_{n=1}^{7} (q_0 + v_{i_n} + v_9) \\ &= q_0 + \sum_{n=1}^{6} v_{i_6}. \end{aligned}$$

The corresponding theta characteristic divisor

$$\begin{aligned} D_{q_{i_1\dots i_7}} &= D_0 + q_0 + q_{i_1\dots i_7} \\ &= \rho(-\kappa_{\mathcal{S}}) + \sum_{n=1}^{6} \rho(E_{i_6} + \kappa_{\mathcal{S}}) \\ &= \rho(L - E_i - E_j) \text{ for } i \neq j \in I \setminus \{i_1, \dots, i_6\}. \end{aligned}$$

by Proposition 1.2.16. The image of $L - E_i - E_j$ is a line in $\mathbb{P}^2$ passing through P_i, P_j under the blow down map. The corresponding tritangent is labelled by the indexes of the points $P_{i_1}, \dots, P_{i_6}$ which do not lie on the line. The subset $\{i_1, \dots, i_6\}$ of the label is the complementary set of the indexes of the points lying on the line.

Example 1.2.20. The odd theta characteristic divisor $D_{q_{1\dots 69}}$ is $\rho(L - E_7 - E_8)$. We compute the corresponding tritangent by a line passing through P_8, P_9 in $\mathbb{P}^2$. The tritangent equation is labelled via the indexes of $P_1, \dots, P_6$.

- The quadratic form $q_{12\dots 9} = \sum_{i=1}^{9} q_i$ of length 9 is the unique even form of this length.

1.2.4 Code for the Algorithm

We implement Algorithm 1 in the computational algebra system Magma [12]. The algorithm is available on the `https://turkuozlum.wixsite.com/tocj` in which you find also implemented functions to generate an input for the algorithm which includes a part from algorithms appearing on `https://software.mis.mpg.de`.

Algorithm 1 may return 0/0 if the abelsche functions which are chosen fail to give a basis for certain Riemann-Roch spaces to set the determinant in (1.10). Nevertheless, we can easily detect this phenomenon and try to avoid it by changing abelsche functions. This worked in all cases we have performed. We can not prove that such a solution always exist.

Our problem is based on the following question. Let $\mathcal{C}$ be a non-hyperelliptic curve of genus g. Fix (any) $v \in \mathrm{Pic}(\mathcal{C})[2]$. Let κ be the canonical divisor of $\mathcal{C}$. Can we find a basis of $\mathcal{L}(\kappa + v)$ by the span of the tensor product of the Riemann-Roch spaces $\{\mathcal{L}(D), \mathcal{L}(D + v)\}$ while $D, D + v$ run through the odd and effective divisors?

Table 1.1: Correspondence between exceptional divisors and theta characteristic divisors

$\mathcal{C}$	$\mathcal{S}$	$\mathbb{P}^2$
D_{ijk}	$2L - \sum_{l \in I_{ijk}} E_l$	conic passing through P_l's for $l \in I_{ijk}$
	$4L - \sum_{l \in I_{ijk}} E_l - \sum_{l \in \{i,j,k\}} 2E_l$	quartic passing through all the eight points, where P_i, P_j, P_k are double
D_{ij9}	$3L - 2E_i - \sum_{k \in I_{ij}} E_k$	cubic passing through P_k's for $k \in I_j$, where P_i is double
	$3L - 2E_j - \sum_{k \in I_{ij}} E_k$	cubic passing through P_k's for $k \in I_i$, where P_j is double
$D_{i_1 \dots i_6 i_7}$	E_i for $i \in I \setminus \{i_1, \dots, i_6, i_7\}$	point P_i
	$6L - \sum_{j \in I_i}^{8} 2E_j - 3E_i$ for $i \in I \setminus \{i_1, \dots, i_6, i_7\}$	sextic passing through all the eight points, where P_i is double and the others are triple
$D_{q_{i_1 \dots i_6 9}}$	$L - E_i - E_j$	line passing through P_i, P_j
	$5L - \sum_{k \in I_{ij}}^{8} 2E_k - E_i - E_j$	quintic passing through all the eight points, where each of them are double except P_i, P_j

Chapter 2

(Kummer Based) Hyperelliptic Curve Cryptography

Jacobians of hyperelliptic curves of genus 2 are also considered for cryptographic purposes as well as elliptic curves. Furthermore, not only Jacobians but also Kummer surfaces associated to the Jacobians are taken into the account for certain cryptographic objectives. In particular, they are suitable for protocols for which only scalar multiplication is needed. Scalar multiplication on the Kummer surfaces associated to the Jacobian of a genus 2 curve can be more efficient than the scalar multiplication on the Jacobian itself [44]. In this chapter, we aim to represent a compact text collecting mathematical basics from the literature about hyperelliptic curve cryptography (HECC) and Kummer based HECC (KHECC). We firstly introduce hyperelliptic curves of genus g and how to do arithmetic on themselves, and then we describe Kummer based arithmetic when $g = 2$ with the link between the Kummer surface and the corresponding Jacobian.

The usage of the multiplicative groups in Diffie-Hellmann key exchange scheme is replaced with elliptic curve groups. Elliptic curve groups use base fields of size around 256 bits while multiplicative groups use a size more than 3000 bits to achieve a security level around 128 [9]. The Jacobians of hyperelliptic curves of genus 2 give better performance for high-security [11]. For a security level around 128 bits, hyperelliptic curves of genus 2 use 128 bits base field which produces a group (Jacobian) size around 256 bits. This reduction of the number of bits from genus 1 to genus 2 makes speedup factor around 3 on the base field arithmetic. However, the group operations for genus 2 requires more operations at the level of the base field. The algorithms by Kummer varieties (see Section 2.1.2) making this requirement rise less. So the parameters of the curve, the costs of the algorithms and the implementation play a role for the comparison between ECC and KHECC.

There are many works to reduce the cost of arithmetic operations on the curve in HECC. We may refer to [65], [44], [11] and [81]. Table 2.1 presents some costs for the operations in Elliptic Curve Cryptography (ECC), HECC and KHECC to have a point of view for a comparison in terms of costs of curve level operations.

solution and source	field width (bits)	ADD	DBL
$\mathbb{F}_p$ ECC [8]	l_{ECC}	$3\mathbf{m}+5\mathbf{s}$	$6\mathbf{m}+2\mathbf{s}$
$\mathbb{F}_p$ KECC [8]	l_{ECC}	$9\mathbf{m}+7\mathbf{s}$	
$\mathbb{F}_{2^n}$ HECC [65]	$l_{\text{HECC}} \approx 0.5 l_{\text{ECC}}$	$40\mathbf{m}+4\mathbf{s}$	$38\mathbf{m}+6\mathbf{s}$
$\mathbb{F}_p$ KHECC [81]	$l_{\text{HECC}} \approx 0.5 l_{\text{ECC}}$	$19\mathbf{m}+12\mathbf{s}$	

Table 2.1: Cost per key bit of curve level operations in various HECC solutions, **m** and **s** denote multiplication and square in the field. KECC stands for Kummer based elliptic curve cryptography [61].

KHECC has several advantages such as having smaller finite field size (comparing with ECC); efficient pseudo addition algorithm for the scalar multiplication with a constant time and uniform behaviour against some side channel attacks; large and regular internal parallelism.

I dismiss computer scientific background which is out of my research area. The main part of the work i.e. the engineering is realised by the team of computer science. Nevertheless, we present a summary of the results after introducing a compact text looking at literature about (KH)ECC from the mathematical point of view. At the end of the chapter, we will present some results which are obtained from a hardware design for KHECC. The hardware implementation is based on a software implementation in [81]. We focus on only hardware acceleration for scalar multiplication since this is the main operation in terms of performance, energy consumption and security against side channel attacks (when the scalar is the private key).

2.1 Mathematical Background

An elliptic curve is a hyperelliptic curve of genus 1. Unlike the case of genus 1, in higher genus $g \geq 2$, the points on a hyperelliptic curve do not form a group. However, there is a group structure associated to it. In this section, the aim is to understand the group structure associated to any hyperelliptic curve of genus g, and also how to consider such a group for cryptographic aspects.

2.1.1 Hyperelliptic Curves

Throughout this section, unless otherwise stated, we refer to [72] for most of the statements.

Let K be a field and $\overline{K}$ denote the algebraic closure of K.

Definition 2.1.1. A nonsingular algebraic curve $\mathcal{C}$ of genus $g > 1$ is called a hyperelliptic curve if the function field $K(\mathcal{C})$ is a separable extension of degree 2 of the rational function $x \in K(\mathcal{C})$.

Remark 2.1.2. The function field of $\mathcal{C}$ is the field of fractions of the coordinate ring $K[\mathcal{C}]/I(\mathcal{C})$ where $K[\mathcal{C}] = K[X_1, \ldots, X_n]/I(\mathcal{C})$ for some $n \in \mathbb{N}$ and $I(\mathcal{C})$ is the corresponding prime ideal of $\mathcal{C}$.

Thanks to Riemann-Roch theorem, we have an equation describing a plane affine part of $\mathcal{C}$ [25, Theorem 4.122]

$$\mathcal{C} : y^2 + h(x)y = f(x), \tag{2.1}$$

where

1. $h(x) \in K[x]$ with $\deg h(x) \leq g$,
2. $f(x) \in K[x]$ is a monic polynomial of degree $2g+1$,
3. there is no point over $\overline{K}$ on the curve which satisfies both of the equations

$$2y + h(x) = 0 \quad \text{and} \quad h'(x)y - f'(x) = 0.$$

Remark 2.1.3. Conversely, a projective curve which is birationally isomorphic to an affine curve given by such an Equation (2.1) is a hyperelliptic curve of genus g [25, Theorem 4.122].

We will use then the following definition for hyperelliptic curves of genus g.

Definition 2.1.4. A hyperelliptic curve $\mathcal{C}$ of genus g over K ($g \geq 1$) is the set

$$\{(a,b) \in \overline{K} \times \overline{K} \mid b^2 + h(a)b = f(a)\} \cup \{\infty\}, \tag{2.2}$$

where the *defining equation* $y^2 + h(x)y = f(x)$ satisfies the conditions in (2.1).

The point ∞ is called the point at infinity.

The third condition ensures that the curve is nonsingular. If $\mathrm{Char}(K) \neq 2$ then the change of variables

$$\begin{aligned} x &\mapsto x \\ y &\mapsto \left(y - \frac{h(x)}{2}\right) \end{aligned}$$

transforms the curve to one for which the defining equation is $y^2 = \overline{f}(x)$ where $\overline{f}(x) \in K[x]$. In this case, the third condition is equivalent to $f(x)$ has no repeated root in $\overline{K}$.

The point at infinity lies in the projective plane $\mathbb{P}(K)$. If $g \geq 2$ then it is a singular point in the projective plane.

The *opposite* of a point $P = (a,b)$, denoted $-P$, is $(a, -b - h(a))$. We also define $-\infty := \infty$.

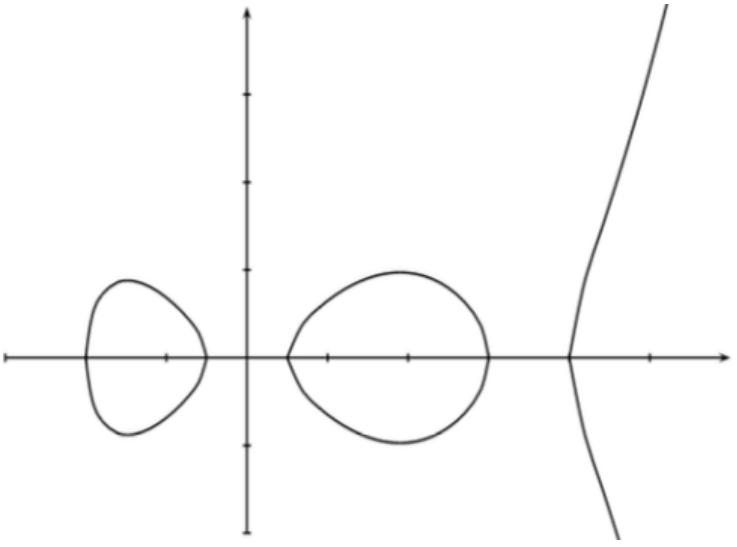


Figure 2.1: A hyperelliptic curve over the field of real numbers.

Let $\mathcal{C}$ be a hyperelliptic curve of genus g over K which is given by Equation (2.1). In order to understand the group structure associated to $\mathcal{C}$, we introduce divisors of $\mathcal{C}$.

A *divisor* is a formal sum of points on $\mathcal{C}$

$$D = \sum_{P \in \mathcal{C}} n_P P \text{ with } n_P \in \mathbb{Z},$$

where only finite number of n_P's are nonzero. The *degree* of D, denoted $\deg D$, is defined as the sum $\sum_{P \in \mathcal{C}} n_p$.

The set $\mathrm{Div}(\mathcal{C})$ of all divisors forms a group under the addition

$$\sum_{P \in \mathcal{C}} n_P P + \sum_{P \in \mathcal{C}} m_P P = \sum_{P \in \mathcal{C}} (n_p + m_P) P.$$

We denote $\mathrm{Div}^0(\mathcal{C})$ the subgroup of $\mathrm{Div}(\mathcal{C})$ consisting all the divisors of degree 0.

In order to define the Jacobian of $\mathcal{C}$, we introduce rational functions of $\mathcal{C}$ and divisors of rational funtions.

Firstly, the *coordinate ring* $K[\mathcal{C}]$ (resp. $\overline{K}[\mathcal{C}]$) of $\mathcal{C}$ over K (resp. $\overline{K}$) is

$$K[x,y]/(y^2 - h(x)y - f(x)) \text{ (resp. } \overline{K}[x,y]/(y^2 - h(x)y - f(x))).$$

An element of $\overline{K}[\mathcal{C}]$ is called a *polynomial function*. Note that each polynomial function $F \in \overline{K}[\mathcal{C}]$ is represented as $F_1(x) - F_2(x)y$ where $F_1, F_2 \in \overline{K}[\mathcal{C}]$ are unique. The field of fractions of the coordinate ring over K (resp. $\overline{K}$) is called the *function field* of $\mathcal{C}$ over K (resp. $\overline{K}$). Denote it by $K(\mathcal{C})$ (resp. $\overline{K}(\mathcal{C})$). An element of $\overline{K}(\mathcal{C})$ is called a *rational function* of $\mathcal{C}$. Let $R \in \overline{K}(\mathcal{C})$, $P \in \mathcal{C}$ and $P \neq \infty$. R is said to be *defined* at P if there exist polynomial functions $F_1, F_2 \in \overline{K}[\mathcal{C}]$ such that $R = F_1/F_2$ and $F_2(P) \neq 0$. Otherwise, we say that R is *not defined* at P. If R is defined at P then the *value* is defined to be $R(P) = F_1(P)/F_2(P)$. Note that the value of R is independent of the choice of F_1, F_2. We say that R has a zero at P if the value of R at P is zero. If it is not defined at P then we say that R has a pole at P, in which case we write $R(P) = \infty$. For any $P \in \mathcal{C}$, there exists a function $U \in \overline{K}(\mathcal{C})$ with $U(P) = 0$ such that for any polynomial function $G \in \overline{K}[\mathcal{C}]^\times$ there is $d \in \mathbb{Z}$ and $V \in \overline{K}(\mathcal{C})$ with $V(P) \neq 0, \infty$ and $G = U^d V$. The integer d does not depend on the choice of U. The function U is called a *uniformizing parameter* for P. The integer d is defined to be the *order* of G at P, denoted as $\mathrm{ord}_P(G)$. We define $\mathrm{ord}_P(R)$ for $R = F_1/F_2 \in \overline{K}(\mathcal{C})$ with $F_1, F_2 \in \overline{K}[\mathcal{C}]$ to be $\mathrm{ord}_P(G_1) - \mathrm{ord}_P(G_2)$.

Remark 2.1.5. It is possible to show that a polynomial function $F \in \overline{K}[\mathcal{C}]^\times$ has a finite number of zeroes and poles. In addition, $\sum_{P \in \mathcal{C}} \mathrm{ord}_P(F) = 0$.

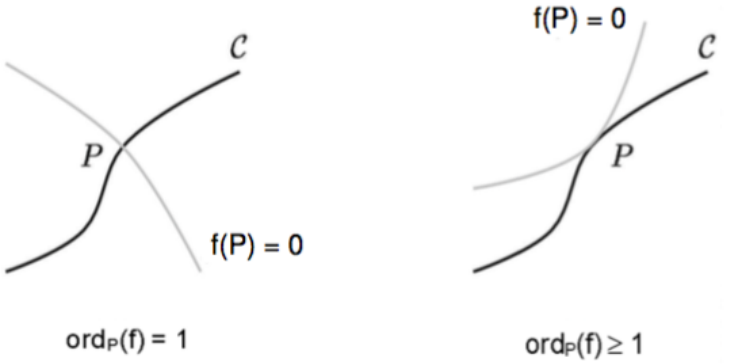


Figure 2.2: Intuitively, multiplicity of a zero [43].

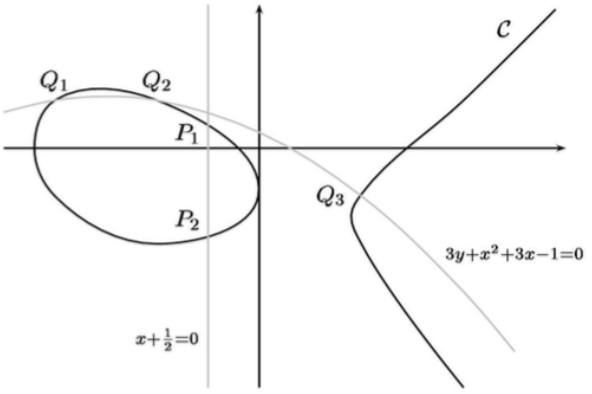


Figure 2.3: An example of rational functions of the curve over $\mathbb{Q}$ by the equation $y^2+xy+2y = x^3+x^2-3x-1$ [43].

For $R \in \overline{K}(\mathcal{C})$, we define the divisor of R, denoted $\mathrm{div}(R)$, to be the sum $\sum_{P\in\mathcal{C}} \mathrm{ord}_P(R)P$ in the light of Remark 2.1.5. Then notice that the degree of the divisor of a rational function is 0.

Remark 2.1.6. It is possible to express $\mathrm{div}(R)$ as a difference of two divisors $\mathrm{div}_0(R)$ and $\mathrm{div}_\infty(R)$ where $\mathrm{div}_0(R)$ corresponds to the intersection of $\mathcal{C}$ with the variety $f = 0$ and similarly $\mathrm{div}_\infty(R)$ corresponds to the intersection of $\mathcal{C}$ with the variety $1/f = 0$.

A divisor D is called *principal* if $D = \mathrm{div}(F)$ for some $F \in K(\mathcal{C})^\times$. The set of all the principal divisors is denoted $\mathrm{Prin}(\mathcal{C})$. It is possible to show that $\mathrm{Prin}(\mathcal{C})$ is a subgroup of $\mathrm{Div}^0(C)$ by noticing $\mathrm{div}(R_1)+\mathrm{div}(R_2) = \mathrm{div}(R_1R_2)$ for $R_1, R_2 \in \overline{K}(\mathcal{C})^\times$.

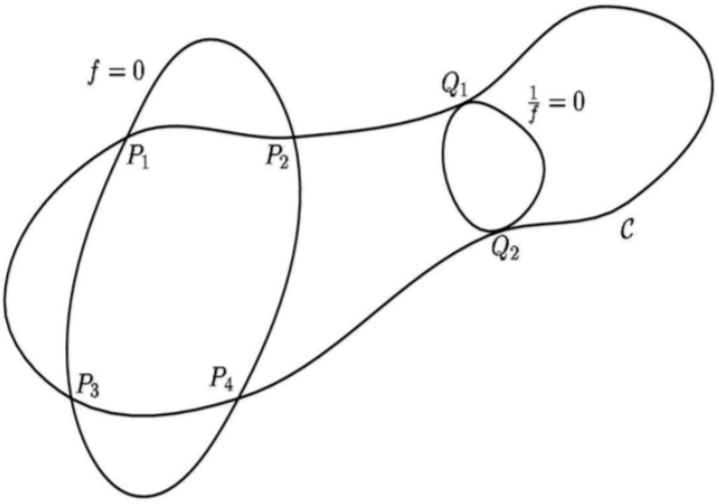


Figure 2.4: An example of a principal divisor $P_1 + P_2 + P_3 + P_4 - 2Q_1 - 2Q_2$ [43].

Definition 2.1.7. The quotient group

$$\mathrm{Jac}(\mathcal{C}) = \mathrm{Div}^0(C)/\,\mathrm{Prin}(\mathcal{C}) \tag{2.3}$$

is called the *Jacobian* of $\mathcal{C}$. If D_1, D_2 are two divisors such that $D_1 - D_2 \in \mathrm{Prin}(\mathcal{C})$ then D_1, D_2 are said to be equivalent. We denote it $D_1 \sim D_2$.

Hence any element of $\mathrm{Jac}(\mathcal{C})$ is an equivalence class of a divisor. By Riemann-Roch theorem, it can be shown that each equivalence class contains a unique *reduced* divisor which is in the form

$$\sum_{i=1}^{r} P_i - r\infty,\ P_i \in \mathcal{C} \setminus \{\infty\},\ r \leq g, \tag{2.4}$$

where $P_i \neq -P_j$ for $i \neq j$.

Example 2.1.8. For $g = 1$, we can take the set of points together with a point at infinity as a group. The group law actually comes from its Jacobian.

For $g = 2$, notice that $r \leq 2$ for a reduced divisor (see (2.4)). We may visualise the group law on the pair of points.

Remark 2.1.9. (Group law on a curve of genus 2). Assume that $g = 2$. Let $D_1 \sim P_1 + P_2 - 2\infty$ and $D_2 \sim Q_1 + Q_2 - 2\infty$. We focus on the general case of divisors for applications. So we may assume P_1, P_2, Q_1, Q_2 are all different and $P_1, P_2 \neq -Q_1, -Q_2$. There is a cubic polynomial passing through P_1, P_2, Q_1, Q_2. Call it $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. (In the case $P_1 = P_2$, we actually take the multiplicity into the account.) Now, we have $y^2 = f(x) = a(x)^2$ by putting $y = a(x)$. Hence $f(x) - a(x)^2$ is a polynomial of degree 6. This polynomial cut the curve at 2 other points, call them $-R_1, -R_2$. So

$$P_1 + P_2 - 2\infty + Q_1 + Q_2 - 2\infty - R_1 - R_2 - 2\infty$$

is a principal divisor. It is equivalent to the identity element of $\mathrm{Jac}(\mathcal{C})$. Once you define $D_3 = R_1 + R_2 - 2\infty$, we see that

$$D_1 + D_2 = D_3.$$

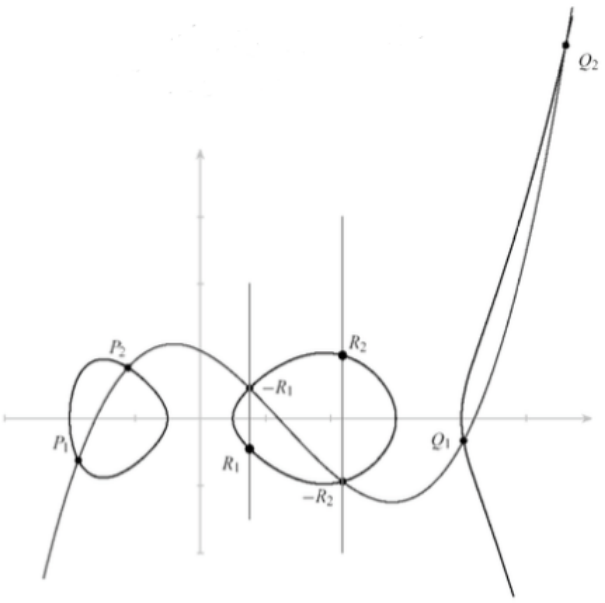


Figure 2.5: Geometric visualisation of the group law when $g = 2$, $(P_1 + P_2) + (Q_1 + Q_2) = R_1 + R_2$ [43].

The following theorem gives a representation of the equivalence classes of $\mathrm{Jac}(\mathcal{C})$ in terms of polynomials over K. This representation is much more convenient for computational aspects.

Theorem 2.1.10 (Mumford's Representation)**.** *Each nontrivial divisor class over K can be uniquely represented by a pair of polynomial $[u(x), v(x)]$ where $u(x), v(x) \in K[x]$ with the following properties,*

1. *$u(x)$ is monic,*
2. *$\deg v(x) < \deg u(x) \leq g$,*
3. *$u(x)$ divides $v(x)^2 + v(x)h(x) - f$.*

Let $\sum_{i=1}^{r} m_i P_i - r\infty$ be a reduced divisor with $m_i \neq 0$ and $P_i \neq -P_j$ for $i \neq j$. Put $P_i = (a_i, b_i)$. Then D is represented by

$$u(x) = \prod_{i=1}^{r} (x - a_i),$$

and if $m_i \neq 1$ then

$$\Big(\frac{\partial}{\partial x}\Big)^j \Big[v(x)^2 + v(x)h(x) - f(x)\Big]_{|_{x=a_i}}, \ 0 \leq j \leq m_i - 1.$$

In other words, we have $u(a_i) = 0$ for $1 \leq i \leq r$ and $v(a_i) = b_i$ with approriate multiplicity. The pair $[u(x), v(x)]$ is called the Mumford's representation of D.

Example 2.1.11. (Mumford's representation of a divisor). Consider the hyperelliptic curve

$$\mathcal{C} : y^2 + (x^2 + x)y = x^5 + x^3 + 1$$

of genus 2 over $\mathbb{F}_{2^5} = \mathbb{F}_2[t]/(t^5 + t^2 + 1)$. Let α be a root of $(t^5 + t^2 + 1)$. Then

$$P_1 = (\alpha^{30}, 0), \quad P_2 = (0, 1)$$

are two points on $\mathcal{C}$. Consider the divisor $D = P_1 + P_2 - 2\infty$. By Theorem 2.1.10, if $u(x) := (x - \alpha^{30})x$ and $v(x) := \alpha x + 1$ then $[u(x), v(x)]$ is the Mumford's representations of D.

Thanks to Cantor and Koblitz [15, 56], the group law can be represented in terms of Mumford's representations. The following algorithm is the initial one in the literature by Cantor. There are two main steps in it. These are addition and reduction. Firstly, the algorithm finds the corresponding Mumford's representation of the sum of two divisors D_1, D_2. This representation is generally not in the reduced form i.e. do not come from a reduced divisor. As a second step, the algorithm reduces the representation which comes from unique reduced divisor in the class of $D_1 + D_2$.

Algorithm 2: `AdditionReduction`

Input: Two divisors D_1, D_2 with the Mumford's representations $[u_1, v_1], [u_2, v_2]$ respectively.

Output: The unique reduced divisor D such that $D \sim D_1 + D_2$.

1: Compute $d_1 = \gcd(u_1, u_2) = e_1u_1 + e_2u_2$
2: Compute $d = \gcd(d_1, v_1 + v_2 + h) = c_1d_1 + c_2(v_1 + v_2 + h)$
3: $s_1 = c_1e_1$, $s_2 = c_1e_2$ and $s_3 = c_2$
4: $u = \frac{u_1u_2}{d^2}$ and $v = \frac{s_1u_1v_2 + s_2u_2v_1 + s_3(v_1v_2 + f)}{d} \mod u$
5: $u' = \frac{f - vh - v^2}{u}$ and $v' = (-h - v) \mod u'$
6: If $\deg u' > g$ then $u = u'$ and $v = v'$ and repeat step 5 until $\deg u' \leq g$
7: $D = [u', v']$
8: **return** D

2.1.2 Kummer Based Arithmetic

In this section, we overview Kummer varieties and how to relate these objects with cryptography.

Let $\mathcal{A}$ be an abelian variety over a field K of dimension g. The Kummer variety $\mathcal{K}$ of dimension g is the variety $\mathcal{A}/\iota$, where ι is the automorphism of $\mathcal{A}$ with $\iota(P) = -P$ for $P \in \mathcal{A}$. We focus on the cases when $\mathcal{A}$ is an elliptic curve or $\mathcal{A}$ is the Jacobian of a hyperelliptic curve of genus 2. Although there is not a group structure on $\mathcal{K}$, there is a way to do scalar multiplication using the *pseudo addition*.

Montgomery Ladder

In this part, we introduce a way to do scalar multiplication in a given group by a method which is called the *Montgomery ladder*. For this section, we refer to [33], [64].

Let G be an additive group and $g \in G$. We want to compute ng for some positive integer n. Write n in the binary expansion $\sum_{i=0}^{k} n_i 2^i$. For $0 \leq j \leq k$, put

$$g_j = \sum_{i=j}^{k} n_i 2^{i-j} g, \ h_j = g_j + g.$$

Then we have

$$g_j = 2g_{j+1} + n_j g = g_{j+1} + h_{j+1} + n_j g - g = 2h_{j+1} + n_j g - 2g.$$

So

$$(g_j, h_j) = \begin{cases} (2g_{j+1}, g_{j+1} + h_{j+1}) \text{ if } n_j = 0 \\ (g_{j+1} + h_{j+1}, 2h_{j+1}) \text{ if } n_j = 1 \text{ for } 1 \leq j \leq k-1. \end{cases}$$

Notice that $g_0 = ng$ and $g_k = n_k g$.

Algorithm 3: `ScalarMultiplication`

Input: $g, (n_k \dots n_0)_2$ which is the binary expansion of n.
Output: $g' = ng$

1: $f_0 = 1$, $f_1 = g$.
2: **for** $i = k$ **to** 0 **do**
3: **if** $n_i = 0$ **then**
4: $f_1 = f_0 + f_1, f_0 = 2f_0$.
5: **else**
6: $f_0 = f_0 + f_1, f_1 = 2f_1$.
7: **end if**
8: **end for**
9: **return** f_0

The first step always compute the pair $(g, 2g)$ since n_k is always 1. We can avoid this step, by putting $f_0 = g$ and $f_1 = 2g$.

Example 2.1.12. Consider $n = 5$. Then the binary expansion $(n_2 n_1 n_0)$ is $(101)_2$. We start with the pair $(0, g)$. Then we compute $(g, 2g)$ since $n_2 = 1$. And we compute $(2g, 3g)$ in the step of $n_1 = 0$. As the last step with $n_0 = 1$, we compute $(5g, 6g)$. Finally, we return $5g$.

The case of dimension 1

We firstly consider Kummer varieties of dimension 1 to discuss the pseudo addition. For this section, we refer to [33]. Let K be a field. An abelian variety of dimension 1 is an elliptic curve $\mathcal{E}$. The Kummer variety $\mathcal{K}_\mathcal{E}$ of $\mathcal{E}$, known as the Kummer line obtained by identifying the opposite points of $\mathcal{E}$. The way of doing arithmetic on $\mathcal{K}$ enables us to avoid to do computations of the second coordinate of points lying on $\mathcal{E}$ which is given in the Weierstrass form.

Let $\overline{P}, \overline{Q} \in \mathcal{K}_\mathcal{E}$ such that $\{P, -P\}$ and $\{Q, -Q\}$ are the corresponding points lying on $\mathcal{E}$ respectively. To define $\overline{P} + \overline{Q}$, there are two natural candidates $\overline{P+Q}$ and $\overline{P-Q}$. However, $\overline{P} + \overline{Q}$ is not well defined with any choice among $\overline{P+Q}$ and $\overline{P-Q}$. So the *pseudo addition* takes $\overline{P}, \overline{Q}$ and one of $\overline{P+Q}, \overline{P-Q}$, say $\overline{R}$, and then it gives $\overline{S} \in \mathcal{K}_\mathcal{E}$

which is one of $\overline{P+Q}, \overline{P-Q}$ with $\overline{S} \neq \overline{R}$. Note that, it is possible to define $2\overline{P}$ since it easy to distinguish $2P$ and the identity element of $\mathcal{E}$. The pseudo addition provides the scalar multiplication on $\mathcal{K}$. Indeed, suppose that we know $\overline{P}, n\overline{P}, (n+1)\overline{P}$, then we are able to compute not only the double of these points but also $(2n+1)\overline{P}$ since we have the substraction $\overline{P}$ of $(n+1)\overline{P}, n\overline{P}$.

We refer to [68], [78] for the recovery of the point on $\mathcal{E}$ which corresponds to a given point on Kummer line of $\mathcal{E}$.

The case of dimension 2

Now, we focus on the case of dimension 2. Although the way to do scalar multiplication for this case is similar to the case of dimension 1, we use different notation than the case of elliptic curves since we prefer to adhere to the notation appearing in [44].

We firstly describe Kummer varieties of dimension 2, namely Kummer surfaces, and then we mention the link between the Kummer surfaces and the Jacobians of hyperelliptic curves of genus 2.

Let $\mathbb{H}_2$ be the Siegel upper half plane and $\vartheta[q](\mathbf{z}, \tau)$ be the theta function with characteristic $[q]$ on $\mathbb{C}^2 \times \mathbb{H}_2$ (see Definition 1.1.11). For basic properties of Theta functions with characteristic, see Section 1.1.2. Now fix $\tau \in \mathbb{H}_2$. For our purpose, we focus on the ones which are given by the characteristics from the set $\{0, \frac{1}{2}\}^2 \oplus \{0, \frac{1}{2}\}^2$. There are sixteen many of them such that ten of them are even and the remaning six of them are odd. Let $\vartheta_i(\mathbf{z})$ denote the odd and even ones for $1 \leq i \leq 10$ and $11 \leq i \leq 16$ respectively. Also, ϑ_i denotes the Theta constant associated to $\vartheta_i(\mathbf{z})$. For the construction of a Kummer surface and arithmetic on it, we need four many theta functions

$$\vartheta_1(\mathbf{z}) = \vartheta \begin{bmatrix} (0,0) \\ (0,0) \end{bmatrix} (\mathbf{z}, \tau),$$
$$\vartheta_2(\mathbf{z}) = \vartheta \begin{bmatrix} (0,0) \\ (\frac{1}{2},0) \end{bmatrix} (\mathbf{z}, \tau),$$
$$\vartheta_3(\mathbf{z}) = \vartheta \begin{bmatrix} (0,0) \\ (0,\frac{1}{2}) \end{bmatrix} (\mathbf{z}, \tau),$$
$$\vartheta_4(\mathbf{z}) = \vartheta \begin{bmatrix} (0,0) \\ (\frac{1}{2},\frac{1}{2}) \end{bmatrix} (\mathbf{z}, \tau).$$

Put

$$a^2 = \vartheta_1(0)^2, b^2 = \vartheta_2(0)^2, c^2 = \vartheta_3(0)^2, d^2 = \vartheta_4(0)^2. \tag{2.5}$$

Definition 2.1.13. The zero locus of the image of

$$\varphi : \mathbb{C}^2 \to \mathbb{P}^3(\mathbb{C}) \tag{2.6}$$
$$\mathbf{z} \mapsto (\vartheta_1(\mathbf{z})^2, \vartheta_2(\mathbf{z})^2, \vartheta_3(\mathbf{z})^2, \vartheta_4(\mathbf{z})^2) \tag{2.7}$$

is called the Kummer surface $\mathcal{K}(\tau)$ associated to τ. We denote it $\mathcal{K}$ simply.

Note that $(\vartheta_1(\mathbf{z}), \vartheta_2(\mathbf{z}), \vartheta_3(\mathbf{z}), \vartheta_4(\mathbf{z})) \neq (0,0,0,0)$ for any $\mathbf{z} \in \mathbb{C}^2$. In addition, φ can be defined from the abelian variety $\mathbb{C}^2/\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$ because

$$\vartheta \begin{bmatrix} 0 \\ b \end{bmatrix} (\mathbf{z} + \tau m + n) = \exp(-2i\pi^t b \cdot m - i\pi^t m \tau m - 2i\pi^t m \cdot \mathbf{z}) \vartheta \begin{bmatrix} 0 \\ b \end{bmatrix} (\mathbf{z})$$

for all $\mathbf{z} \in \mathbb{C}^2$, for all $b \in \{0, \frac{1}{2}\}$ and for all $m, n \in \mathbb{Z}^2 \times \mathbb{Z}^2$ [74, page 123].

Remark 2.1.14. By Lefschetz Theorem [26, Theorem 3.1.10], $\mathcal{K}$ is the image of the induced embedding of φ from $\mathbb{C}^2/\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2/\sim$ where $\sim$ is the equivalence relation such that $\mathbf{z} \sim -\mathbf{z}$.

Since ϑ_i is even for $1 \leq i \leq 4$, $\varphi(\mathbf{z}) = \varphi(-\mathbf{z})$ for $\mathbf{z} \in \mathbb{C}^2$. So φ does not carry the group law on $\mathbb{C}^2/\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$ to $\mathcal{K}$. Once we have the four coordinates of $\varphi(\mathbf{z})$ for some $\mathbf{z} \in \mathbb{C}^2$, it is possible to compute the coordinates of $\varphi(2\mathbf{z})$ by relations among fundamental theta functions [26, Property 3.2.3]. On the other hand, we do not have good candidate to define $\varphi(\mathbf{z}_1) + \varphi(\mathbf{z}_2)$ among $\varphi(\mathbf{z}_1 + \mathbf{z}_2)$, $\varphi(\mathbf{z}_1 - \mathbf{z}_2)$ since $\{\mathbf{z}_1, -\mathbf{z}_1\}$ and $\{\mathbf{z}_2, -\mathbf{z}_2\}$ are the preimages of $\varphi(\mathbf{z}_1)$ and $\varphi(\mathbf{z}_2)$ respectively. In order to do arithmetic on $\mathcal{K}$, we try to deduce $\varphi(\mathbf{z}_1) + \varphi(\mathbf{z}_2)$ from $\varphi(\mathbf{z}_1 + \mathbf{z}_2)$, $\varphi(\mathbf{z}_1 - \mathbf{z}_2)$. We will present the algorithms for the scalar multiplication after introducing a projective model of $\mathcal{K}$. The algorithms are obtained by relations among fundamental theta functions [26, Property 3.2.3, 3.2.4].

Because of applicational motivations for operations on Kummer varieties, we need an algebraic equation of the variety. Thanks to some relations among Theta constants [26, Property 3.1.13], it is possible to have a projective model of $\mathcal{K}$ in $\mathbb{P}^3$ which is given by the following equation

$$E'XYZT - \left(\left(X^2 + Y^2 + Z^2 + T^2\right) - F\left(XT + YZ\right) - G\left(XZ + YT\right) - H\left(XY + ZT\right)\right)^2 = 0,$$

where

$$A = a^2 + b^2 + c^2 + d^2, \quad B = a^2 + b^2 - c^2 - d^2,$$
$$C = a^2 - b^2 + c^2 - d^2, \quad D = a^2 - b^2 - c^2 + d^2,$$

$$E' = \frac{ABCD}{(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2)},$$

$$F = \frac{a^4 - b^4 - c^4 + d^4}{a^2d^2 - b^2c^2}, \quad G = \frac{a^4 - b^4 + c^4 - d^4}{a^2c^2 - b^2d^2}, \quad H = \frac{a^4 + b^4 - c^4 - d^4}{a^2b^2 - c^2d^2},$$

thanks to the Riemann equations [26, Proposition 3.1.13] among the fundamental Theta functions.

Remark 2.1.15. Let τ be the period matrix (see Section 1.1.2) of a hyperelliptic curve $\mathcal{C}$ of genus 2, then $\mathrm{Jac}(\mathcal{C}) \cong \mathbb{C}^2/\mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$ [4, Page 18]. In this case, the Kummer surface which is given with τ is the one corresponding to $\mathcal{C}$. We remark also that products of two Theta constants vanish (e.g. $a^2b^2 - b^2d^2 = \vartheta_5(0)^2\vartheta_6(0)^2$) if $\mathrm{Jac}(\mathcal{C})$ is a product of two elliptic curves which implies vanishing denominators F, G, H. We may avoid it by avoiding such abelian varieties [44].

We refer to [44] for the algorithms named as `DoubleKummer`, `PseudoAddKummer` and `ScalarMultiplication`.

Firstly, we present the algorithm for doubling of a point on $\mathcal{K}$.

Algorithm 4: `DoubleKummer`

Input: A point $P = (X, Y, Z, T)$ on $\mathcal{K}$.
Output: The point $2P$ on $\mathcal{K}$.

1: $X' = (X + Y + Z + T)^2/A$
2: $Y' = (X + Y - Z - T)^2/B$
3: $Z' = (X - Y + Z - T)^2/C$
4: $T' = (X - Y - Z + T)^2/D$
5: $X_2 = (X' + Y' + Z' + T')/a^2$
6: $Y_2 = (X' + Y' - Z' - T')/b^2$
7: $Z_2 = (X' - Y' + Z' - T')/c^2$
8: $T_2 = (X' - Y' - Z' + T')/d^2$
9: **return** (X_2, Y_2, Z_2, T_2)

The following algorithm is the implementation of the pseudo addition on $\mathcal{K}$.

Algorithm 5: `PseudoAddKummer`

Input: Two points $P = (X, Y, Z, T)$ and $Q = (\underline{X}, \underline{Y}, \underline{Z}, \underline{T})$ on $\mathcal{K}$ and $R = (\overline{X}, \overline{Y}, \overline{Z}, \overline{T}) = P - Q$, with $\overline{XYZT} \neq 0$.
Output: The point $P + Q = (X, Y, Z, T)$.

1: $X' = (X + Y + Z + T) \times (\underline{X} + \underline{Y} + \underline{Z} + \underline{T})/A$
2: $Y' = (X + Y - Z - T) \times (\underline{X} + \underline{Y} - \underline{Z} - \underline{T})/B$
3: $Z' = (X - Y + Z - T) \times (\underline{X} - \underline{Y} + \underline{Z} - \underline{T})/C$
4: $T' = (X - Y - Z + T) \times (\underline{X} - \underline{Y} - \underline{Z} + \underline{T})/C$
5: $X = (X' + Y' + Z' + T')/\overline{X}$
6: $Y = (X' + Y' - Z' - T')/\overline{Y}$
7: $Z = (X' - Y' + Z' - T')/\overline{Z}$
8: $T = (X' - Y' - Z' + T')/\overline{T}$
9: **return** (X, Y, Z, T)

The following algorithm proceeds the scalar algorithm by composing the pseudo addition algorithm with the Montgomery ladder algorithm (see Section 2.1.2).

Algorithm 6: `ScalarMultiplication` which is the combination of the Montgomery ladder (see Algorithm 3) and the pseudo addition.

Input: A point P on $\mathcal{K}$ with no zero coordinate and an integer $n > 1$.
Output: The point nP on $\mathcal{K}$.

1: If $n = 2$ then return `DoubleKummer`(P).
2: Let $n_0 n_1 \dots n_k$ be the binary expansion of n where n_0 is the most significant bit.
3: $P_m = P$; $P_p =$ `DoubleKummer`(P)
4: For i from 1 to k do

(a) $Q =$ `PseudoAddKummer`(P_p, P_m, P)

(b) If n_i equals 1 then

(i) $P_p =$ `DoubleKummer`(P_p)

(ii) $P_m = Q$

(c) else

(i) $P_m =$ `DoubleKummer`(P_m)

(ii) $P_p = Q$

5: **return** P_m

Back and Forth between $\mathcal{K}$ and $\mathcal{C}$ in genus 2

We focus on the relation between $\mathcal{K}$ and the curve $\mathcal{C}$ associated to $\mathcal{K}$ in the Rosenhain form. The Rosenhain model for the curve $\mathcal{C}$ is

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu),$$

where λ, μ, ν can be computed in terms of the fundamental Theta constants as follows

$$\lambda = \frac{a^2c^2}{b^2d^2},\ \mu = \frac{c^2(AB+CD)}{d^2AB-CD},\ \nu = \frac{a^2(AB+CD)}{b^2(AB-CD)}.$$

On the other hand, by setting $d^2 = 1$, we can compute the squared fundamental Theta constants

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\quad b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\nu-\mu)}},\quad a^2 = b^2c^2\frac{\nu}{\mu}$$

to obtain the associated $\mathcal{K}$ from a Rosenhain form with λ, μ, ν of a hyperelliptic curve of genus 2.

From now on, consider $\mathcal{K}$ to be $\mathrm{Jac}(\mathcal{C})/ < \iota >$ (see Remark 2.1.14) where $\mathcal{C}$ is given in the Rosenhain form with λ, μ, ν and ι is the involution with $\iota(P) = -P$ for $P \in \mathcal{C}$. We denote $\overline{D}$ the image of an element $D \in \mathrm{Jac}(\mathcal{C})$ on $\mathcal{K}$ and identify the elements of $\mathrm{Jac}(\mathcal{C})$ with their Mumford's representations. In the following part, we see to go back and forth between $\mathcal{K}$ and $\mathcal{C}$.

The following algorithm [23, Algorithm 1] is the implementation of finding the image of a divisor in $\mathrm{Jac}(\mathcal{C})$ on $\mathcal{K}$.

Algorithm 7: `JacobianToKummer`

Input: An element $D \in \mathrm{Jac}(\mathcal{C})$.
Output: The image $\overline{D}$ of D on $\mathcal{K}$.

if $D = 0$ **then**
  $\overline{D} = (a^2 : b^2 : c^2 : d^2)$
else
  if $D =< x - u, v >$ **then**
    $(t_1, t_2, t_3, t_4) = (u - 1, u - \lambda, u - \mu, u - \nu)$
    $\overline{D} = (a^2 t_1 t_3 : b t_2 t_4 : c t_1 t_4 : d t_2 t_3)$
  else
    $(D =< x^2 + a_1 x + a_0, b_1 x + b_0 >)$
    $(t_1, t_2, t_3) = (a_1 + \lambda, a_1 + 1, b_0^2)$
    $(t_4, t_5) = (a_0 \times (a_0 - \mu) \times (t_1 + \nu), a_0 \times (a_0 - \lambda\nu) \times (t_2 + \mu))$
    $(t_6, t_7) = (a_0 \times (a_0 - \nu) \times (t_1 + \mu), a_0 \times (a_0 - \lambda\nu) \times (t_2 + \nu))$
    $\overline{D} = (a t_4 + t_3 : b t_5 + t_3 : c t_6 + t_3 : d t_7 + t_3)$
  end if
end if
return $\overline{D}$

Additionally, it is possible to recover the corresponding Mumford's representations associated to the Rosenhain model for a given point on $\mathcal{K}$. The formulas for the corresponding Mumford's representation are obtained by [75, Theorem IIIa.7.6]. For the complete expressions for the formulas, we refer to [11, Section 5.3]. Suppose that $(X : Y : Z : T) \in \mathcal{K}$. There are two divisors mapping to $(X : Y : Z : T)$ which are opposite to each other. Call them D and $-D$. Write $D =< x^2 + u_1 x + u_0, v_1 x + v_0 >$, and then $-D =< x^2 + u_1 x + u_0, -v_1 x - v_0 >$. Now,

$$u_0 = \frac{u_{00}X + u_{01}Y + u_{02}Z + u_{03}T}{w_0 X + w_1 Y + w_2 Z + w_3 T}, \quad u_1 = \frac{u_{10}X + u_{01}Y + u_{12}Z + u_{13}T}{w_0 X + w_1 Y + w_2 Z + w_3 T} - u_0 - 1,$$

where

$$\begin{aligned}
u_{00} &= -\vartheta_1^2\vartheta_3^2\vartheta_8^2\vartheta_5^2\vartheta_9^2, & u_{10} &= -\vartheta_7^2\vartheta_9^2\vartheta_5^2\vartheta_8^2, & w_0 &= -\vartheta_2^2\vartheta_4^2\vartheta_{10}^2\vartheta_6^2\vartheta_7^2,\\
u_{01} &= -\vartheta_1^2\vartheta_3^2\vartheta_8^2\vartheta_6^2\vartheta_7^2, & u_{11} &= -\vartheta_7^2\vartheta_9^2\vartheta_5^2\vartheta_{10}^2, & w_1 &= -\vartheta_2^2\vartheta_4^2\vartheta_{10}^2\vartheta_5^2\vartheta_9^2,\\
u_{02} &= -\vartheta_1^2\vartheta_3^2\vartheta_8^2\vartheta_5^2\vartheta_7^2, & u_{12} &= -\vartheta_7^2\vartheta_9^2\vartheta_5^2\vartheta_8^2, & w_2 &= -\vartheta_2^2\vartheta_4^2\vartheta_{10}^2\vartheta_6^2\vartheta_9^2,\\
u_{03} &= -\vartheta_1^2\vartheta_3^2\vartheta_8^2\vartheta_6^2\vartheta_9^2, & u_{13} &= -\vartheta_7^2\vartheta_9^2\vartheta_5^2\vartheta_{10}^2, & w_3 &= -\vartheta_2^2\vartheta_4^2\vartheta_{10}^2\vartheta_5^2\vartheta_7^2.
\end{aligned}$$

On the other hand

$$\begin{aligned}
v_0 &= \sqrt{l\frac{\vartheta_8^2\vartheta_3^4\vartheta_1^4\vartheta_{14}^2(\mathbf{z})}{(\vartheta_{16}^2(\mathbf{z})bd\vartheta_{10})^2}},\\
v_1 &= \frac{u_0^3 - u_0^2(u_1^2 + u_1 + (u_1 + 1)(\lambda + \mu + \nu) + \lambda\mu + \nu\lambda + \nu\mu) + u_0\lambda\mu\nu + u_1 v_0^2}{2v_0 u_0},
\end{aligned}$$

where

$$l = -\Bigg(\vartheta_{12}^2(\mathbf{z})\vartheta_7^2(\mathbf{z})bc\vartheta_9^4(\mathbf{z}) + \vartheta_{11}^2(\mathbf{z})\vartheta_9^2(\mathbf{z})ad\vartheta_7^4(\mathbf{z}) + 2abcd(XZ+YT)$$
$$+ (X^2+Y^2+Z^2+T^2 - F(XT+YZ) - G(XZ+YT) - H(XY+ZT))\frac{ac+bd}{E}\Bigg).$$

Note that the sequence of the characteristics $\left[[q_j] \mid j \in \{5,\dots,10,11,12,14,16\}\right]$ which is used in the formulas is the sequence

$$\left[\begin{bmatrix}(\frac{1}{2},0)\\(0,0)\end{bmatrix}, \begin{bmatrix}(\frac{1}{2},0)\\(0,\frac{1}{2})\end{bmatrix}, \begin{bmatrix}(0,\frac{1}{2})\\(0,0)\end{bmatrix}, \begin{bmatrix}(\frac{1}{2},\frac{1}{2})\\(0,0)\end{bmatrix}, \begin{bmatrix}(0,\frac{1}{2})\\(\frac{1}{2},0)\end{bmatrix},\right.$$
$$\left.\begin{bmatrix}(\frac{1}{2},\frac{1}{2})\\(\frac{1}{2},\frac{1}{2})\end{bmatrix}, \begin{bmatrix}(0,\frac{1}{2})\\(0,\frac{1}{2})\end{bmatrix}, \begin{bmatrix}(0,\frac{1}{2})\\(\frac{1}{2},\frac{1}{2})\end{bmatrix}, \begin{bmatrix}(\frac{1}{2},\frac{1}{2})\\(\frac{1}{2},0)\end{bmatrix}, \begin{bmatrix}(\frac{1}{2},\frac{1}{2})\\(0,\frac{1}{2})\end{bmatrix}\right].$$

Remark 2.1.16. (Finite fields). In order to apply the algorithms on the Kummer surfaces, we need to be sure that these make sense over $\mathbb{F}_q$. For this, we need to find a curve $\overline{\mathcal{C}}$ over a number field $\mathbb{K}$ and a prime ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_{\mathbb{K}}$ with the residue field $\mathbb{F}_q$ such that $\overline{\mathcal{C}}$ and $\mathrm{Jac}(\overline{\mathcal{C}})$ have good reduction modulo $\mathfrak{p}$ and $\overline{\mathcal{C}}$ reduces to $\mathcal{C}$ [44, Section 5.1].

2.2 Hardware Implementation

Hardware implementation provides a fast way of encrypting and/or signing messages. It also allows parallelism which may increase performance significantly. To design an hardware architecture for KHECC by studying and evaluating the impact of architecture parameters on the cost and performance is an objective of HAH (Hardware and Arithmetic for Hyperelliptic Curves Cryptography) project [62].

2.2.1 Software Implementation

Firstly, we describe a part of the work [81] of embedded software implementations in which the potential of genus-2 hyperelliptic curves is analysed for key exchange and signatures on the 8-bit AVR ATmega architecture and 32-bit ARM Cortex-M0 processor. Their implementation for Diffie-Hellmann key exchange scheme improves the application of Kummer surfaces of hyperelliptic curve cryptography which is described in Section 2.1.2. They work over the finite field $\mathbb{F}_p$ where $p = 2^{127}-1$. Note that p is a Mersenne prime, which provides fast modular reduction algorithms. The Kummer surface $\mathcal{K}_{\mathcal{C}}$ is constructed by the (squared) theta constants by

$$a^2 := -11, \quad b^2 := 22, \quad c^2 := 19, \quad d^2 := 3.$$

where $\mathcal{C}$ is the corresponding hyperelliptic curve given in the Rosenhain form. Let $\overline{P} := (X_P : Y_P : Z_P : T_P)$ be a point on $\mathcal{K}_{\mathcal{C}}$. For the scalar multiplication $k\overline{P}$ for a scalar k, they let the scalar size be 256-bits. Due to advantages of the Montgomery Ladder 2.1.2, it is used for the scalar multiplication algorithm which is called `cryptoscalarmult`.

The algorithm `xDBLADD` is the main operation in ML. It modifies and combines the pseudo addition and doubling algorithms (see the algorithms 4,5). The scalar multiplication computes a couple of points at each iteration level of the algorithm `xDBLADD` by starting

with $(a^2 : b^2 : c^2 : d^2)$ and $(X_P : Y_P : Z_P : T_P)$. More precisely, at the iteration of i-th step in the scalar multiplication algorithm,

$$(l\overline{P}, (l+1)\overline{P})$$

is computed with $l = \sum_{j=i}^{\beta-1} m_j 2^{\beta-1-i}$. Finally, the algorithm produces $(k\overline{P}, (k+1)\overline{P})$. The execution of the algorithm `xDBLADD` is uniform and in a constant time.

We present the algorithms `cryptoscalarmult` and `xDBLADD` to give a complete description. For this, we need three operations in $\mathbb{P}^3$ and the pseudo addition algorithm `xADD`.

Let

$$\mathcal{M} : \mathbb{P}^3 \times \mathbb{P}^3 \to \mathbb{P}^3,$$

where

$$\mathcal{M}((x_1 : y_1 : z_1 : t_1), (x_2 : y_2 : z_2 : t_2)) = (x_1x_2 : y_1y_2 : z_1z_2 : t_1t_2).$$

Let $\mathcal{H}$ be the Hadamard transform

$$\mathcal{H} : \mathbb{P}^3 \to \mathbb{P}^3$$

such that

$$\mathcal{H}((x : y : z : t)) = (x' : y' : z' : t') \text{ where } \begin{cases} x' = x + y + z + t, \\ y' = x + y - z - t, \\ z' = x - y + z - t, \\ t' = x - y - z + t. \end{cases}$$

Algorithm 8 implements the pseudo addition. Algorithm 9 combines doubling on $\mathcal{K}_\mathcal{C}$ with the pseudo addition. Finally, the algorithm `cryptoscalarmult` is an implementation of the ML on $\mathcal{K}_\mathcal{C}$.

Algorithm 8: `xADD`

Input: A triple $(\overline{P}, \overline{Q}, \overline{P-Q})$ of points on $\mathcal{K}_\mathcal{C}$ for some P, Q in $\mathrm{Jac}(\mathcal{C})$ where $\overline{P-Q} = (X : Y : Z : T)$.
Output: $\overline{P+Q} \in \mathcal{K}_\mathcal{C}$.
1: $(V_1, V_2) = (\mathcal{H}(\overline{P}), \mathcal{H}(\overline{Q}))$
2: $V_1 = \mathcal{M}(V_1, V_2)$
3: $V_1 = \mathcal{M}(V_1, (1/A : 1/B : 1/C : 1/D))$
4: $V_1 = \mathcal{H}(V_1)$
5: $V_1 = \mathcal{M}(V_1, V_1)$
6: $(C_1, C_2) = (Z \times T, X \times Y)$
7: $V_2 = \mathcal{M}((C_1 : C_2 : C_3 : C_4), (Y : X : T : Z))$
8: **return** $\mathcal{M}(V_1, V_2)$

Remark 2.2.1. The steps (5) and (6) of Algorithm 8 computes $(YZT : XZT : XYT : XYZ)$. This point projectively equivalent to $(1/X : 1/Y : 1/Z : 1/T)$ (if none of X, Y, Z, T is nonzero). In Algorithm 10, the third argument of the pseudo addition is fixed. It makes sense to precompute $(1/X : 1/Y : 1/Z : 1/T)$ by scaling it by X. So $(1 : X/Y : X/Z : X/T)$ can be stored which is the *wrapped* form of $\overline{P-Q} = (X : Y : Z : T)$.

Algorithm 9: `xDBLADD`

Input: A triple $(\overline{P}, \overline{Q}, (X/Y, X/Z, Z/T))$ in $\mathcal{K}_{\mathcal{C}}^2 \times \mathbb{F}_p$ for some P, Q in $\mathrm{Jac}(\mathcal{C})$ with $\overline{P-Q} = (X : Y : Z : T)$.
Output: $(2\overline{P}, \overline{P+Q}) \in \mathcal{K}_{\mathcal{C}}^2$.
1: $(V_1, V_2) = (\mathcal{M}(\overline{P}, \overline{P}), \mathcal{M}(\overline{Q}, \overline{Q}))$
2: $(V_1, V_2) = (\mathcal{H}(V_1), \mathcal{H}(V_2))$
3: $(V_1, V_2) = (\mathcal{M}(V_1, V_1), \mathcal{M}(V_1, V_1))$
4: $(V_1, V_2) = (\mathcal{M}(V_1, (1/A : 1/B : 1/C : 1/D)), \mathcal{M}(V_2, (1/A : 1/B : 1/C : 1/D))$
5: $(V_1, V_2) = (\mathcal{H}(V_1), \mathcal{H}(V_2))$
6: **return** $(\mathcal{M}(V_1, (1/a^2 : 1/b^2 : 1/c^2 : 1/d^2)), \mathcal{M}(V_2, (1 : X/Y : X/Z : X/T)))$

If `CSWAP` is a constant-time conditional swap routine such that

$$\texttt{CSWAP}(b, (V_1, V_2)) = \begin{cases} (V_1, V_2) \text{ if } b = 0 \\ (V_2, V_1) \text{ if } b = 1 \end{cases} \tag{2.8}$$

then we have Algorithm 10.

Algorithm 10: `cryptoscalarmult`

Input: A tuple $(m = \sum_{i=0}^{\beta-1} m_i 2^i, (X/Y, X/Z, Z/T)$ in $[0, 2^\beta) \times \mathbb{F}_q^3$ for some $\overline{P}$ in $\mathcal{K}_{\mathcal{C}}$ with $\overline{P} = (X : Y : Z : T)$ where $(X/Y, X/Z, Z/T)$ is the wrapped form of $\overline{P}$.
Output: $(m\overline{P}, (m+1)\overline{P+Q}) \in \mathcal{K}_{\mathcal{C}}^2$.
1: $V_1 = (a^2 : b^2 : c^2 : d^2)$
2: $V_2 = \overline{P}$
3: **for** $i = 250$ **to** 0 **do**
4: $\quad (V_1, V_2) = \texttt{CSWAP}(m_i, (V_1, V_2))$
5: $\quad \texttt{xDBLADD}(V_1, V_2, (X/Y, X/Z, Z/T))$
6: $\quad \texttt{CSWAP}(m_i, (V_1, V_2))$
7: **end for**
8: **return** (V_1, V_2)

In order to avoid branching in the procedure combining the Montgomery ladder with pseudo addition and doubling, `cryptoscalarmult` uses the routine `CSWAP` which is swapping V_1, V_2 depending on the bits at the each of iteration level. This method makes Algorithm 10 uniform and constant-time.

2.2.2 Results

These results come from a joint work with Gabriel Gallin and Arnaud Tisserand under HAH (Hardware and Arithmetic for Hyperelliptic Curves Cryptography) project [62]. In this thesis, we depose computer scientific background which is out of our research area. Nevertheless, we present a summary of the results after introducing a compact text looking through the literature about (KH)ECC from the mathematical point of view.

We aim KHECC on generic finite fields. We suggest to use the parameters a^2, b^2, c^2, d^2 (fundamental theta constants) from [44] for the construction of the Kummer variety. We present results of 4 selected hardware architectures in various configurations of hardware architectures on several FPGAs such as Virtex 4 VLX100 (V4), Virtex 5 LX110T (V5)

and Spartan 6 SLX75 (S6). We denote the architectures A_i for $i = 1, \ldots, 4$. The first design A_1 is small and basic one embedding the minimum number of units, A_2 is designed similarly with A_1 by optimising `CSWAP` (2.8) unit in A_1. The architecture A_3 embeds more units for arithmetic operations (at the level of the field). The design of A_4 is a cluster of parallel units for both arithmetic operations and data memory operations. The sources in the hardware accelerators are arithmetic units for field level operations (addition, subtraction and multiplication in $\mathbb{F}_p$ with a generic prime p), memory unit(s) for storing intermediate values (elements in $\mathbb{F}_p$ for the coordinates of the points on the Kummer variety $\mathcal{K}_\mathcal{C}$, parameters and constants for the construction of $\mathcal{K}_\mathcal{C}$), an internal communication system for data transfer between the units, a control unit based on a microcode running the architecture. Table 2.2 summarizes the FPGA implementation results. For the comparison of the results with some ECC and HECC solutions, we present the Table 2.3 and 2.4.

For more detailed architectural information, we refer to our article [42]. This work is the first hardware implementation of scalar multiplication in KHECC for 128-bit security level. Several architectures with different amount of internal parallelism have been optimised and fully implemented on 3 different FPGAs. The results give similar speed with the best curve based solutions for embedded systems by using almost a half size area.

archi	w [bit]	target	logic slices	DSP blocks	RAM blocks	freq. [MHz]	time [ms]
A_2	34	V4	1121	11	4	330	0.56
A_3	136		3660	22	9	285	0.42
A_4	34		2158	22	7	324	0.44
A_2	34	V5	541	11	4	360	0.51
A_3	136		1594	22	9	348	0.34
A_4	34		1013	22	7	358	0.40
A_2	34	S6	381	11	4	293	0.63
A_3	136		1131	22	9	225	0.53
A_4	34		758	22	7	262	0.54

Table 2.2: FPGA implementations results. Note that we do not include A_1 into the table since A_2 is an improved version of A_1.

ref.	year	target	n	LUT	FF	logic slices	RAM blocks	freq. [MHz]	time [ms]
[5]	2006	Virtex 2 Pro	83	20999	n.a.	11296	n.a.	166	0.5
[38]	2008	XC2V4000	83	n.a.	n.a.	2316	6	125	0.31
[55]	2004	XC2V4000	89	8451	2178	4995	1	54	1.02
		XC2V4000	89	16459	4437	9950	0	57	0.44
[87]	2006	Virtex 2 Pro	83	n.a.	n.a.	2446	1*	100	0.99
		Virtex 2 Pro	83	n.a.	n.a.	6586	3*	100	0.42
[90]	2016	Virtex 2	83	n.a.	n.a.	5734	n.a.	145	0.3
		XC5V240	83	n.a.	n.a.	5086	n.a.	175	0.29
[99]	2004	Virtex 2 Pro	81	n.a.	n.a.	4039	1	57	0.79
		Virtex 2 Pro	81	n.a.	n.a.	7737	0	61	0.39
		XC2V4000	81	n.a.	n.a.	3955	1	54	0.83
		XC2V4000	81	n.a.	n.a.	7785	n.a.	57	0.42
[35]	2007	XC2V8000	113	n.a.	n.a.	25271	n.a.	45	2.03

Table 2.3: FPGA implementation results for HECC solutions over $\mathbb{F}_{2^n}$. (The values with an upper star are estimated numbers of RAM blocks.)

ref.	year	target	n	LUT	FF	logic slices	DSP blocks	RAM blocks	freq. [MHz]	time [ms]
[3]	2014	XCV6FX760	NIST-256	32900	n.a.	11200	289	128	100	0.4
[49]	2008	XC4VFX12	NIST-256	2589	2028	1715	32	11	490	0.5
		XC4VFX12	NIST-256	34896	32430	24574	512	176	375	0.04
[63]	2012	XC4VFX12	GEN-256	n.a.	n.a.	2901	14	n.a.	227	1.09
		XC5VLX110	GEN-256	n.a.	n.a.	3657	10	n.a.	263	0.86
[70]	2013	XC4VLX100	GEN-256	5740	4876	4655	37	11	250	0.44
		XC5LX110T	GEN-256	4177	4792	1725	37	10	291	0.38

Table 2.4: FPGA implementation results for ECC solutions over $\mathbb{F}_p$ and 128-bit security level.

Chapter 3

p-Rank Computations

3.1 Motivation

Let p be a prime number and let k be an algebraically closed field of characteristic p. Let A be an abelian variety of dimension g defined over k. The *p-rank* of A is the integer f_A defined by $\#A[p](k) = p^{f_A}$. It is known that $0 \leq f_A \leq g$. Let X be a smooth projective connected curve of genus g defined over k. Then the p-rank of X is the p-rank of its Jacobian. An equivalent definition is that f_A equals the maximal integer m such that there exists an unramified $(\mathbb{Z}/p\mathbb{Z})^m$-Galois cover $X' \to X$. When $f_A = g$, we say that A (or X) is *ordinary*.

The p-rank of a curve X equals the stable rank of the Frobenius map on $\mathrm{H}^1(X, \mathcal{O}_X)$, and thus can be determined from its Hasse-Witt or Cartier-Manin matrix (see subsections 3.2.1-3.2.3). Given a prime p and integers g and f with $0 \leq f \leq g$, a result of Faber and Van der Geer [37, Theorem 2.3] implies that there exists a curve over $\overline{\mathbb{F}}_p$ of genus g and p-rank f.

We assume that p is odd from now on. Consider an unramified double cover

$$\pi : Y \longrightarrow X.$$

Then $\mathrm{Jac}(Y)$ is isogenous to $\mathrm{Jac}(X) \oplus P_\pi$ where P_π is the *Prym variety* of π. In this context, P_π is a principally polarized abelian variety of dimension $g-1$. The p-rank f' of P_π satisfies $0 \leq f' \leq g-1$. Since the p-rank is an isogeny invariant, the p-rank of Y equals $f + f'$ where f is the p-rank of X.

Now the following question arises naturally.

Question 3.1.1. Suppose that p is an odd prime, and g, f, f' are integers such that $g \geq 2$, $0 \leq f \leq g$, and $0 \leq f' \leq g-1$. Does there exist a curve X defined over $\overline{\mathbb{F}}_p$ of genus g and p-rank f having an unramified double cover $\pi : Y \longrightarrow X$ such that P_π has p-rank f'?

Table 3.1 presents the cases for which the answer to Question 3.1.1 is yes.

In this chapter, we study an open case of Question 3.1.1, which occurs when X has genus $g = 3$ and P_π has p-rank 0. We focus on the case that X is a smooth plane quartic or, equivalently, that X is not hyperelliptic.

3.2 Background

In this section, we introduce some definitions and background material.

g, genus	f', p-rank of P_π	f, p-rank of X	p, prime	reference
$g=2$	$0 \le f' \le g-1$	$0 \le f \le g$	$p>3$	[79, Proposition 6.1]
	$f'=1$	$f=2$	$p=3$	[37, Example 7.1]
$g \ge 3$	$f'=g-1$	$0 \le f \le g$	$p \ge 3$	[79, Theorem 1.1(1)]
	$f'=g-2$	$0 \le f \le g$	$p>3$	[79, Theorem 7.1]
		$2 \le f \le g$	$p=3$	[79, Theorem 7.1]
$g \le 4$	$g/2-1 \le f' \le g-3$	$0 \le f \le g$	$p \ge 5$	[79, Corollary 7.3]

Table 3.1: p-rank of unramified double cover $\pi : Y \to X$.

Let k be an algebraically closed field of characteristic $p > 0$. Unless stated otherwise, every curve is a smooth projective connected k-curve. Suppose that C is a curve of genus $g \ge 1$.

3.2.1 The Cartier-Manin matrix

Let L be the function field of C/k. Since k is perfect, there exists a separating variable $x \in L \setminus k$ such that $L/k(x)$ is algebraic and separable. It follows that $L = L^p(x)$ and hence every element $z \in L$ can be written uniquely in the form

$$z = z_0^p + z_1^p x + \cdots + z_{p-1}^p x^{p-1}$$

with $z_0, \ldots, z_{p-1} \in L$. The *Cartier operator* $\mathscr{C}$ is defined on differentials of the first kind by

$$\mathscr{C}((z_0^p + z_1^p x + \cdots + z_{p-1}^p x^{p-1})dx) = z_{p-1}dx.$$

The Cartier operator is $\frac{1}{p}$-linear, meaning that $\mathscr{C}(a^p\omega_1 + b^p\omega_2) = a\mathscr{C}(\omega_1) + b\mathscr{C}(\omega_2)$ for all $a, b \in L$ and all $\omega_1, \omega_2 \in \Omega^1(L)$. It is independent of the choice of separating variable and hence gives a well-defined map on the k-vector space of regular differentials on C,

$$\mathscr{C} : \mathrm{H}^0(C, \Omega^1_C) \to \mathrm{H}^0(C, \Omega^1_C).$$

Definition 3.2.1. Let $\omega_1, \ldots, \omega_g$ be a k-basis for $\mathrm{H}^0(C, \Omega^1_C)$. Write $\mathscr{C}(\omega_j) = \sum_{i=1}^g c_{ij}\omega_i$ with $c_{ij} \in k$. The Cartier-Manin matrix of C with respect to the basis $\omega_1, \ldots, \omega_g$ is the matrix $(c_{ij}^p)_{i,j}$.

Remark 3.2.2. The Cartier-Manin matrix depends on the choice of basis. Let $\omega'_1, \ldots, \omega'_g$ be another k-basis for $\mathrm{H}^0(C, \Omega^1_C)$ and let $T = (t_{ij})$ be the change of basis matrix so that $\omega_j = \sum_{i=1}^g t_{ij}\omega'_i$. Then the Cartier-Manin matrix with respect to the basis $\omega'_1, \ldots, \omega'_g$ is $T^{(p)}(c_{ij}^p)T^{-1}$, where $T^{(p)}$ denotes the matrix obtained from T by taking the pth power of each of its entries.

The Cartier-Manin matrix of a hyperelliptic curve

Let p be odd and let Z be a hyperelliptic curve of genus g. Then Z has an equation of the form $y^2 = f(x)$ for a separable polynomial $f(x) \in k[x]$ having degree $2g+1$ or $2g+2$. Write $\omega_i = \frac{x^{i-1}}{y}dx$, so that $\{\omega_1, \ldots, \omega_g\}$ is a basis for $\mathrm{H}^0(Z, \Omega^1_Z)$.

Proposition 3.2.3. *(Yui) [100, Proposition 2.1] Let c_s denote the coefficient of x^s in the expansion of $f(x)^{(p-1)/2}$. Then the Cartier-Manin matrix of Z is $A_0 = (c_{ip-j})_{i,j}$.*

3.2.2 The Hasse-Witt matrix

The *(absolute) Frobenius* F of C is the morphism of schemes given by the identity on the underlying topological space and $f \mapsto f^p$ on $\mathcal{O}_C$. We write F^* for the induced endomorphism of $\mathrm{H}^1(C, \mathcal{O}_C)$. It is a p-linear map, meaning that $F^*(\lambda\xi) = \lambda^p F^*\xi$ for all $\lambda \in k$ and all $\xi \in \mathrm{H}^1(C, \mathcal{O}_C)$.

Proposition 3.2.4. *[89, Proposition 9] Serre duality gives a perfect pairing*

$$\langle\ ,\ \rangle : \mathrm{H}^1(C, \mathcal{O}_C) \times \mathrm{H}^0(C, \Omega^1_C) \to k$$

such that

$$\langle F^*\xi, \omega\rangle = \langle \xi, \mathscr{C}\omega\rangle^p$$

for all $\xi \in \mathrm{H}^1(C, \mathcal{O}_C)$ *and all* $\omega \in \mathrm{H}^0(C, \Omega^1_C)$.

Definition 3.2.5. Let $\xi_1, \ldots \xi_g$ be a k-basis of $\mathrm{H}^1(C, \mathcal{O}_C)$. Write $F^*(\xi_j) = \sum_{i=1}^g a_{ij}\xi_i$ with $a_{ij} \in k$. The Hasse-Witt matrix of C with respect to the basis $\xi_1, \ldots \xi_g$ is the matrix $(a_{ij})_{i,j}$.

Remark 3.2.6. The Hasse-Witt matrix depends on the choice of basis. Let $\xi'_1, \ldots, \xi'_g$ be another k-basis for $\mathrm{H}^1(C, \mathcal{O}_C)$ and let $S = (s_{ij})$ be the change of basis matrix so that $\xi'_j = \sum_{i=1}^g s_{ij}\xi_i$. Then the Hasse-Witt matrix with respect to the basis $\xi'_1, \ldots, \xi'_g$ is $S^{-1}(a_{ij})S^{(p)}$, where $S^{(p)}$ denotes the matrix obtained from S by taking the pth power of each of its entries.

Remark 3.2.7. If the basis $\xi_1, \ldots \xi_g$ of $\mathrm{H}^1(C, \mathcal{O}_C)$ is the dual basis for the basis $\omega_1, \ldots, \omega_g$ of $\mathrm{H}^0(C, \Omega^1_C)$, then the Hasse-Witt matrix is the transpose of the Cartier-Manin matrix.

3.2.3 The p-rank

We recall that If A is an abelian variety of dimension g over k, its p-rank is the number f_A such that $\#A[p](k) = p^{f_A}$. If C is a curve of genus g over k, its p-rank is the p-rank of $\mathrm{Jac}(C)$. We write f_A (resp. f_C) for the p-rank of A (resp. C).

Here is another definition of the p-rank. The k-vector space $\mathrm{H}^1(C, \mathcal{O}_C)$ has a direct sum decomposition into F^*-stable subspaces as

$$\mathrm{H}^1(C, \mathcal{O}_C) = \mathrm{H}^1(C, \mathcal{O}_C)_s \oplus \mathrm{H}^1(C, \mathcal{O}_C)_n$$

where F^* is bijective on $\mathrm{H}^1(C, \mathcal{O}_C)_s$ and nilpotent on $\mathrm{H}^1(C, \mathcal{O}_C)_n$. The dimension of $\mathrm{H}^1(C, \mathcal{O}_C)_s$ is equal to the rank of the composition of F^* with itself g times, and this rank is called the *stable* rank of Frobenius on $\mathrm{H}^1(C, \mathcal{O}_C)$.

Proposition 3.2.8. *The p-rank of C is equal to the stable rank of the Frobenius endomorphism $F^* : \mathrm{H}^1(C, \mathcal{O}_C) \to \mathrm{H}^1(C, \mathcal{O}_C)$.*

Proof. See [89]. □

The p-rank of the Jacobian of C can be determined from either the Cartier-Manin or Hasse-Witt matrix. For a matrix M, we write $M^{(p^i)}$ for the matrix obtained from M by raising each of its entries to the power p^i.

Proposition 3.2.9. *Let C be a curve of genus g with Hasse-Witt matrix H and Cartier-Manin matrix M. Then the p-rank of C is*

$$f_C = \mathrm{rk}(HH^{(p)} \ldots H^{(p^{g-1})}) = \mathrm{rk}(M^{(p^{g-1})} \ldots M^{(p)}M).$$

Proof. The first equality follows from Proposition 3.2.4 and the fact that Frobenius is p-linear. The second equality is a consequence of Serre duality, see Proposition 3.2.8. □

Remark 3.2.10. Notice that C is ordinary, i.e. p-rank of C is g. Proposition 3.2.9 implies that

$$\mathrm{rk}(M^{(p^{g-1})} \dots M^{(p)} M) = g$$

where M is the Cartier-Manin matrix, i.e. the determinant $|(M^{(p^{g-1})} \dots M^{(p)} M)|$ is nonzero. On the other hand,

$$|(M^{(p^{g-1})} \dots M^{(p)} M)| \neq 0 \text{ if and only if } |M| \neq 0,$$

since determinant is a multiplicative map. Hence, it is enough to show that $|M| \neq 0$ to see that $\mathrm{Jac}(C)$ is ordinary.

3.2.4 Prym varieties

Suppose that p is odd. If X is a curve of genus g defined over k, then $\mathrm{Jac}(X)$ is a principally polarized abelian variety of dimension g. There is a bijection between 2-torsion points on $\mathrm{Jac}(X)$ and unramified double covers $\pi : Y \to X$. Without further comment, we require that Y is connected, which is equivalent to the 2-torsion point being non-trivial. Also, we note that Y is smooth if X is smooth.

Let $\pi : Y \to X$ be an unramified double cover of X. By the Riemann-Hurwitz formula, Y has genus $2g-1$. Also Jac(X) is isogenous to a sub-abelian variety of $\mathrm{Jac}(Y)$. Let σ be the endomorphism of $\mathrm{Jac}(Y)$ induced by the involution generating $\mathrm{Gal}(Y/X)$. The *Prym variety* P_π is the connected component containing 0 in the kernel of the map $\pi^* : \mathrm{Jac}(Y) \to \mathrm{Jac}(X)$. It is also the image of the map $1-\sigma$ in $\mathrm{Jac}(Y)$. In other words,

$$P_\pi = \mathrm{Im}(1-\sigma) = \mathrm{Ker}(1+\sigma)^0.$$

The canonical principal polarization of $\mathrm{Jac}(Y)$ induces a principal polarization on P_π. Finally, $\mathrm{Jac}(Y)$ is isogenous to $\mathrm{Jac}(X) \oplus P_\pi$.

3.2.5 Moduli spaces

Throughout this chapter, we consider

- $\mathcal{M}_g$ the moduli space of curves of genus g over k,
- $\mathcal{A}_g$ the moduli space of principally polarized abelian varieties of dimension g over k,
- $\mathcal{R}_g$ the moduli space whose points represent unramified double covers $\pi : Y \to X$ over k, where X is a curve of genus g,
- $\mathcal{R}_g^{(f,f')}$ the stratum of $\mathcal{R}_g$ representing points where X has p-rank f and P_π has p-rank f'.

3.3 Hasse-Witt matrices of genus 3 curves and their Prym varieties

We continue to work over an algebraically closed field k of characteristic $p > 2$. Suppose $\pi : Y \to X$ is an unramified double cover of a non-hyperelliptic smooth curve of genus 3. In [14], Bruin describes the equations for X and P_π in terms of quadratic forms. We describe

the Hasse-Witt matrices of X and P_π in terms of the quadratic forms, using results of Stöhr and Voloch in [92] and Yui in [100]. As an application, we answer Question 3.1.1 affirmatively when $3 \leq p \leq 19$ and $g = 3$ in Proposition 3.3.4.

A smooth curve X of genus 3 which is not hyperelliptic is isomorphic to a smooth plane quartic.

Lemma 3.3.1. *[14, Bruin] Suppose $\pi : Y \to X$ is an unramified double cover of a smooth plane quartic curve. Then there exist quadratic forms $Q_1, Q_2, Q_3 \in k[u, v, w]$ such that $X \subset \mathbb{P}^2$ is given by the equation*

$$X : Q_1(u, v, w)Q_3(u, v, w) = Q_2(u, v, w)^2, \tag{3.1}$$

$Y \subset \mathbb{P}^4$ is given by the equations

$$Y : Q_1(u, v, w) = r^2,\ Q_2(u, v, w) = rs,\ Q_3(u, v, w) = s^2, \tag{3.2}$$

and the Prym variety P_π is isomorphic to $\mathrm{Jac}(Z)$ for the smooth genus 2 curve Z with equation

$$Z : z^2 = D(x) := -\det(M_1 + 2xM_2 + x^2M_3), \tag{3.3}$$

where M_i is the symmetric 3×3 matrix such that

$$(u, v, w)M_i(u, v, w)^T = Q_i(u, v, w).$$

Conversely, if $Q_1, Q_2, Q_3 \in k[u, v, w]$ are quadratic forms such that (3.1) defines a smooth plane quartic X, then the equations above give an unramified double cover $\pi : Y \to X$ and a smooth genus 2 curve Z such that $P_\pi \simeq \mathrm{Jac}(Z)$.

Proof. This is proven in [14, Theorem 5.1(4)]. The fact that Z is smooth when X is smooth can be found in [14, Section 5, Case 4]. □

3.3.1 Hasse-Witt matrices

Lemma 3.3.2. *Let $\pi : Y \to X$ be an unramified double cover of a smooth plane quartic curve and suppose $P_\pi = \mathrm{Jac}(Z)$. Let $Q_1, Q_2, Q_3 \in k[u, v, w]$ be quadratic forms as in Lemma 3.3.1, and let $D(x) \in k[x]$ be defined as in Lemma 3.3.1(3.3).*

1. *Let*
$$q(u, v) = Q_2(u, v, 1)^2 - Q_1(u, v, 1)Q_3(u, v, 1).$$
Let $a_{i,j}$ be the values in k such that $q(u, v)^{p-1} = \sum_{i,j} a_{i,j}u^i v^j$. Then the Hasse-Witt matrix of X is
$$H_X = \begin{pmatrix} a_{p-1,p-1} & a_{2p-1,p-1} & a_{p-1,2p-1} \\ a_{p-2,p-1} & a_{2p-2,p-1} & a_{p-2,2p-1} \\ a_{p-1,p-2} & a_{2p-1,p-2} & a_{p-1,2p-2} \end{pmatrix}.$$

2. *Let $b_i \in k$ be the values in k such that $D(x)^{(p-1)/2} = \sum_i b_i x^i$. Then the Hasse-Witt matrix of Z is*
$$H_Z = \begin{pmatrix} b_{p-1} & b_{2p-1} \\ b_{p-2} & b_{2p-2} \end{pmatrix}.$$

Remark 3.3.3. In Lemma 3.3.2(1), the Hasse-Witt matrix is taken with respect to the basis of $\mathrm{H}^1(X, \mathcal{O}_X)$ given by the dual of the basis $\frac{du}{q_v}$, $u\frac{du}{q_v}$, $v\frac{du}{q_v}$ of $\mathrm{H}^0(X, \Omega^1_X)$. In Lemma 3.3.2(2), the Hasse-Witt matrix is taken with respect to the basis of $\mathrm{H}^1(Z, \mathcal{O}_Z)$ given by the dual of the basis $\frac{dx}{z}, x\frac{dx}{z}$ of $\mathrm{H}^0(Z, \Omega^1_Z)$.

Proof. 1. Let $\omega_1, \ldots, \omega_g$ be a basis for $\mathrm{H}^0(X, \Omega_X)$ and suppose that the action of the Cartier operator is given by

$$\mathscr{C}(\omega_i) = \sum_{j=1}^{g} c_{ij}\omega_j. \tag{3.4}$$

By Definition 3.2.1 and Remark 3.2.7, the Hasse-Witt matrix with respect to the dual basis is the matrix (c_{ij}^p).

The result [92, Theorem 1.1] of Stöhr and Voloch yields the following information in (3.5) and (3.6) about the action of the Cartier operator on the smooth plane curve X, with affine equation $q(u, v) = 0$. Consider the partial derivative operator $\nabla = \frac{\partial^{2p-2}}{\partial u^{p-1}\partial v^{p-1}}$. Then for any $h \in k(u, v)$,

$$\mathscr{C}\left(h\frac{du}{q_v}\right) = \left(\nabla(q^{p-1}h)\right)^{\frac{1}{p}} \frac{du}{q_v}. \tag{3.5}$$

Also, if $\alpha_{i,j} \in k$, then

$$\nabla\left(\sum_{i,j} \alpha_{i,j}u^i v^j\right) = \sum_{i,j} \alpha_{ip+p-1,jp+p-1}u^{ip}v^{jp}. \tag{3.6}$$

Write $\omega_i = h_i(u, v)\frac{du}{q_v}$. By (3.5) and (3.4),

$$\nabla(q^{p-1}h_i) = \sum_j c_{ij}^p h_j^p. \tag{3.7}$$

In this case, a basis for $H^0(X, \Omega_X^1)$ is $\omega_1 = \frac{du}{q_v}, \omega_2 = u\frac{du}{q_v}, \omega_3 = v\frac{du}{q_v}$. By definition, $q(u, v)^{p-1} = \sum_{i,j} a_{i,j}u^i v^j$. By (3.7) and (3.6) we have

$$\nabla(q^{p-1}) = \sum_{i,j} a_{ip+p-1,jp+p-1}u^{ip}v^{jp} = c_{11}^p + c_{12}^p u^p + c_{13}^p v^p$$

where c_{11}, c_{12}, c_{13} are the entries in the first row of the Hasse-Witt matrix. Note that $\deg(q) = 4$, so $\deg(q^{p-1}) = 4(p-1)$ and hence $\deg(\nabla(q^{p-1})) \leq 2(p-1)$. Therefore, the coefficient of $u^{ip}v^{jp}$ in $\nabla(q^{p-1})$ is zero unless $i + j \leq 1$. Equating the nonzero coefficients gives $c_{11} = a_{p-1,p-1}, c_{12} = a_{2p-1,p-1}$ and $c_{13} = a_{p-1,2p-1}$.

Similarly, for the other two rows in the Hasse-Witt matrix,

$$\nabla(q^{p-1}u) = \sum_{i,j} a_{ip+p-1,jp+p-1}u^{ip+1}v^{jp} = c_{21}^p + c_{22}^p u^p + c_{23}^p v^p,$$

and

$$\nabla(q^{p-1}v) = \sum_{i,j} a_{ip+p-1,jp+p-1}u^{ip}v^{jp+1} = c_{31}^p + c_{32}^p u^p + c_{33}^p v^p.$$

2. Note that Z is smooth since X is smooth by [14, Section 5, Case 4]. The result follows from [13, Lemma 5.1]. Alternatively, the matrix H_Z is the transpose of the Cartier-Manin matrix for Z from [100, Proposition 3.2.3].

□

3.3.2 The p-ranks of X and Z

By Proposition 3.2.9, the p-rank $f = f_X$ of X is the rank of $H_X H_X^{(p)} H_X^{(p^2)}$ and the p-rank $f' = f_Z$ of Z is the rank of $H_Z H_Z^{(p)}$.

Proposition 3.3.4. *Let $3 \leq p \leq 19$. For each pair (f, f') such that $0 \leq f \leq 3$ and $0 \leq f' \leq 2$, there exists an unramified double cover $\pi : Y \to X$ such that X is a smooth curve of genus 3 and p-rank f and P_π has p-rank f'; in other words, $\mathcal{R}_3^{(f,f')}$ is non empty when $3 \leq p \leq 19$.*

Proof. The result holds (without any restriction on p) when $f' = 2$ or $f' = 1$ by [79, Proposition 6.4], as long as $(f, f') \neq (0,1), (1,1)$ when $p = 3$. To complete the proof, we provide an example below in each case when $f' = 0$ (and when $p = 3$ and $(f, f') = (0,1), (1,1)$). These examples were found with a computational search, using Lemma 3.3.2. □

In the examples below, we give the equations of the curves X, Z along with the coefficients of the quadratic forms that lead to these curves in the following format

$$[q_{111}, q_{112}, q_{122}, q_{113}, q_{123}, q_{133}, q_{211}, q_{222}, q_{233}, q_{311}, q_{312}, q_{322}, q_{313}, q_{323}, q_{333}],$$

where:

- $Q_1 = q_{111}u^2 + q_{112}uv + q_{122}v^2 + q_{113}uw + q_{123}vw + q_{133}w^2$;
- $Q_2 = q_{211}u^2 + q_{222}v^2 + q_{233}w^2$;
- $Q_3 = q_{311}u^2 + q_{312}uv + q_{322}v^2 + q_{313}uw + q_{323}vw + q_{333}w^2$.

Example 3.3.5. $p = 3$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 2u^4 + 2u^3v + u^3 + 2u^2v^2 + u^2v + 2u^2 + 2uv^3 + uv^2 + uv + 2u + v^3 + v^2 + 2v + 1$
	$Z : 2x^5 + x^4 + 2x^2 + x + z^2 + 1$
	$[q_{ijk}] = [2,0,2,0,0,1,1,1,1,0,1,2,2,2,2]$
$(2,0)$	$X : 2u^4 + u^3v + 2u^3 + u^2v + 2uv^3 + uv^2 + 2v^3 + 2v^2 + 2$
	$Z : x^6 + 2x^5 + 2x^4 + x^2 + x + z^2$
	$[q_{ijk}] = [1,0,2,0,0,0,1,1,1,0,1,2,2,1,2]$
$(1,0)$	$X : 2u^4 + 2u^3 + 2u^2v + 2u^2 + uv^2 + 2uv + x + 2v^4 + v^3 + v + 2$
	$Z : 2x^6 + 2x^5 + z^2 + 1$
	$[q_{ijk}] = [2,0,0,1,1,1,1,1,1,0,0,1,1,1,0]$
$(0,0)$	$X : 2u^4 + 2u^3 + 2u^2v + 2u^2 + 2uv^2 + u + v^4 + 2v^3 + v + 1$
	$Z : 2x^6 + x + z^2 + 1$
	$[q_{ijk}] = [2,0,2,0,0,1,1,1,1,0,0,1,1,1,2]$
$(1,1)$	$Z : 2x^6 + 2x^4 + x + y^2$
	$X : 2x^4 + x^2y^2 + x^2 + xy^3 + xy^2 + 2xy + 2x + 2y^4 + y^3 + 2y$
	$[q_{ijk}] = [0,0,1,0,0,2,1,1,1,0,1,0,1,1,2]$
$(0,1)$	$Z : 2x^6 + 2x^3 + 2x^2 + x + y^2 + 1$
	$X : 2x^4 + 2x^3y + 2x^3 + 2x^2 + xy^3 + xy^2 + 2xy + 2x + y^2 + 2$
	$[q_{ijk}] = [2,0,1,0,0,2,1,0,0,0,1,0,1,0,1]$

Example 3.3.6. $p = 5$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 4u^4 + 3u^3 + 4u^2v^2 + u^2v + 3uv^2 + 4u + v^3 + 3v^2 + 3v$
	$Z : 4x^6 + x^3 + 2x + z^2 + 3$
	$q_{ijk} = [1,0,1,0,0,3,1,1,0,0,0,1,3,1,0]$
$(2,0)$	$X : 4u^4 + 3u^3 + 4u^2v^2 + u^2v + 3uv^2 + u + v^3 + 2v^2 + 2v$
	$Z : 4x^6 + 4x^3 + 3x + z^2 + 2$
	$[q_{ijk}] = [1,0,1,0,0,2,1,1,0,0,0,1,3,1,0]$
$(1,0)$	$X : 4u^4 + 3u^2v^2 + 3u^2v + 2u^2 + 4uv^2 + uv + 2u + 4v^4 + 4v^3 + 4v^2 + 3$
	$Z : 2x^5 + x^3 + 2x^2 + 2x + z^2 + 2$
	$[q_{ijk}] = [3,4,4,4,4,3,1,1,1,0,0,0,0,1,3]$
$(0,0)$	$X : 4u^4 + 3u^2v^2 + 3u^2v + 2u^2 + 4uv^2 + 3uv + 3v + 4v^4 + 4v^3 + v + 2$
	$Z : 2x^5 + 2x^2 + 2x + z^2 + 2$
	$[q_{ijk}] = [3,4,4,1,0,1,1,1,1,0,0,0,0,1,3]$

Example 3.3.7. $p = 7$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 6u^4 + 5u^2v^2 + 3u^2v + 6u^2 + 6v^4 + v^3 + 3v^2 + v + 4$
	$Z : 6x^5 + 6x^3 + z^2 + 4$
	$[q_{ijk}] = [1,0,5,0,0,5,1,1,1,0,0,0,0,3,1]$
$(2,0)$	$X : 6u^4 + 5u^2v^2 + 2u^2v + 2u^2 + 6v^4 + 4v^3 + 6v^2 + 6$
	$Z : 5x^5 + x^4 + 4x^3 + 6x^2 + 4x + z^2$
	$[q_{ijk}] = [1,0,2,0,0,0,1,1,1,0,0,0,0,2,4]$
$(1,0)$	$X : 6u^4 + 5u^2v^2 + 2u^2v + u^2 + 6v^4 + 5v^2 + 4v + 5$
	$Z : 6x^5 + 6x^4 + x^2 + x + z^2$
	$[q_{ijk}] = [3,0,0,0,0,6,1,1,1,0,0,0,0,3,1]$
$(0,0)$	$X : 6u^4 + u^2v^2 + 4u^2 + 3v^4 + 6v^2 + 6$
	$Z : 4x^5 + 4x^4 + 3x^2 + 3x + z^2$
	$[q_{ijk}] = [3,0,4,0,0,0,1,1,1,0,0,1,0,0,2]$

Example 3.3.8. $p = 11$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 10u^4 + 9u^2v^2 + 5u^2v + 2u^2 + 10v^4 + 10v^3 + 4v^2 + 4v + 6$
	$Z : 9x^5 + 4x^4 + x^3 + 7x^2 + 8x + z^2 + 3$
	$[q_{ijk}] = [8,0,5,0,0,2,1,1,0,0,0,0,0,2,3]$
$(2,0)$	$X : 10u^4 + 9u^2v^2 + 9u^2v + 9u^2 + 10v^4 + v^3 + v^2 + 7v + 7$
	$Z : 9x^5 + 9x^4 + 9x^3 + 2x^2 + 2x + z^2 + 1$
	$[q_{ijk}] = [10,0,6,0,0,9,1,1,0,0,0,0,0,2,2]$
$(1,0)$	$X : 10u^4 + 9u^2v^2 + 9u^2v + 8u^2 + 10v^4 + 3v^3 + 10v^2 + 4v + 6$
	$Z : 9x^5 + 2x^4 + 3x^3 + 9x^2 + 2x + z^2 + 8$
	$[q_{ijk}] = [10,0,7,0,0,2,1,1,0,0,0,0,0,2,3]$
$(0,0)$	$X : 10u^4 + 9u^2v^2 + 3u^2v + 5u^2 + 10v^4 + 9v^3 + 8v^2 + 4v + 1$
	$Z : 9x^5 + 8x^4 + 9x^3 + 3x^2 + 10x + z^2 + 8$
	$[q_{ijk}] = [7,0,10,0,0,2,1,1,1,0,0,0,0,2,1]$

Example 3.3.9. $p = 13$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 12u^4 + 11u^2v^2 + 6u^2v + 11u^2 + 12v^4 + 12v^3 + 11v^2 + 3v + 12$
	$Z : 11x^5 + 10x^4 + 8x^3 + 3x^2 + 11x + z^2 + 1$
	$[q_{ijk}] = [3, 0, 6, 0, 0, 8, 1, 1, 1, 0, 0, 0, 2, 0]$
$(2,0)$	$X : 12u^4 + 11u^2v^2 + 2u^2v + 4u^2 + 12v^4 + 11v^3 + 5v^2 + 11v + 6$
	$Z : 11x^5 + 10x^4 + 8x^3 + 3x^2 + 11x + z^2 + 1$
	$[q_{ijk}] = [1, 0, 12, 0, 0, 12, 1, 1, 1, 0, 0, 0, 2, 6]$
$(1,0)$	$X : 12u^4 + 11u^2v^2 + 9u^2v + 9u^2 + 12v^4 + 7v^3 + 8v^2 + 4v + 1$
	$Z : 11x^5 + 7x^4 + 11x^3 + 6x^2 + 5x + z^2 + 1$
	$[q_{ijk}] = [2, 0, 3, 0, 0, 11, 1, 1, 1, 0, 0, 0, 0, 11, 12]$
$(0,0)$	$X : 12u^4 + 11u^2v^2 + 9u^2v + 7u^2 + 12v^4 + 8v^3 + 6v^2 + 12v + 11$
	$Z : 6x^5 + 5x^4 + 3x^3 + 6x^2 + 6x + z^2 + 6$
	$[q_{ijk}] = [9, 0, 8, 0, 0, 12, 1, 1, 1, 0, 0, 0, 0, 1, 1]$

Example 3.3.10. $p = 17$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 16u^4 + 15u^2v^2 + 15u^2 + 16v^4 + 5v^3 + 7v^2 + 6v + 3$
	$Z : 4x^5 + 8x^4 + 9x^3 + 9x^2 + x + z^2$
	$[q_{ijk}] = [0, 0, 13, 0, 0, 2, 1, 1, 1, 0, 0, 0, 0, 3, 2]$
$(2,0)$	$X : 16u^4 + 15u^2v^2 + 10u^2v + u^2 + 16v^4 + 3v^3 + 4v^2 + 16$
	$Z : 4x^5 + 8x^4 + 9x^3 + 9x^2 + x + z^2$
	$[q_{ijk}] = [9, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 3, 6]$
$(1,0)$	$X : 16u^4 + 15u^2v^2 + 10u^2v + 3u^2 + 16v^4 + 4v^3 + 14v + 6$
	$Z : 4x^5 + 7x^4 + 5x^3 + 10x^2 + 9x + z^2 + 5$
	$[q_{ijk}] = [9, 0, 7, 0, 0, 16, 1, 1, 1, 0, 0, 0, 0, 3, 10]$
$(0,0)$	$X : 16u^4 + 15u^2v^2 + 6u^2v + 15u^2 + 16v^4 + 9v^3 + 15v^2 + 15v + 16$
	$Z : 8x^5 + 7x^4 + 8x^3 + x^2 + 14x + z^2 + 11$
	$[q_{ijk}] = [6, 0, 9, 0, 0, 15, 1, 1, 1, 0, 0, 0, 0, 1, 0]$

Example 3.3.11. $p = 19$

(f, f')	$X, Z, [q_{ijk}]$
$(3,0)$	$X : 18u^4 + 17u^2v^2 + 9u^2v + 3u^2 + 18v^4 + 5v^3 + 5v^2 + 18$
	$Z : 5x^5 + 11x^4 + 13x^3 + 8x^2 + 10x + z^2$
	$[q_{ijk}] = [3, 0, 8, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 3, 8]$
$(2,0)$	$X : 18u^4 + 17u^2v^2 + 12u^2v + 18u^2 + 18v^4 + 18v^3 + 9v^2 + 18$
	$Z : 5x^5 + 11x^4 + 13x^3 + 8x^2 + 10x + z^2$
	$[q_{ijk}] = [4, 0, 6, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 3, 5]$
$(1,0)$	$X : 18u^4 + 17u^2v^2 + 5u^2v + 18u^2 + 18v^4 + 6v^3 + 3v^2 + 6v + 4$
	$Z : 17x^5 + x^4 + x^3 + 18x^2 + 10x + z^2 + 13$
	$[q_{ijk}] = [12, 0, 3, 0, 0, 3, 1, 1, 1, 0, 0, 0, 0, 2, 8]$
$(0,0)$	$X : 18u^4 + 17u^2v^2 + 17u^2v + 4u^2 + 18v^4 + v^3 + 14v^2 + 12v + 1$
	$Z : 16x^5 + 9x^4 + 14x^3 + 10x^2 + 8x + z^2 + 3$
	$[q_{ijk}] = [11, 0, 4, 0, 0, 10, 1, 1, 1, 0, 0, 0, 0, 5, 4]$

Remark 3.3.12. Since k is an algebraically closed field of odd characteristic p, it is possible to diagonalize the quadratic form Q_2 and take its coefficients to be 0 or 1. Even so, the complicated nature of the entries of H_X and H_Z makes it difficult to analyze the p-ranks algebraically.

The entries of H_X are quite complicated even in terms of the coefficients of $q(u, v) = Q_2(u, v, 1)^2 - Q_1(u, v, 1)Q_3(u, v, 1)$. For example, if $p = 3$ and $q(u, v) = \sum_{i,j} b_{ij}u^i v^j$, then the upper left entry of H_X is $2b_{00}b_{22} + 2b_{01}b_{21} + 2b_{02}b_{20} + 2b_{10}b_{12} + b_{11}^2$.

Similarly, even the equation for $Z : z^2 = D(x)$ is rather complicated in terms of the coefficients of Q_1 and Q_3.

3.4 The Hasse-Witt matrix of a smooth plane quartic defined as an intersection in $\mathbb{P}^3$

In this section, we determine the Hasse-Witt matrix of a curve C of genus 3 defined as the intersection of a plane and degree 4 hypersurface in $\mathbb{P}^3$. We use this result in Section 3.5 to determine the Hasse-Witt matrix of each smooth plane quartic X which has an unramified double cover $\pi : Y \to X$ such that P_π is isomorphic to a fixed abelian surface.

As before, let k be an algebraically closed field of characteristic $p > 2$. Following [59], let C/k be a curve in $\mathbb{P}^3 = \mathrm{Proj}(k[x, y, z, w])$ defined by $v = h = 0$ for homogeneous polynomials $v, h \in k[x, y, z, w]$ with $\gcd(v, h) = 1$. Let r and s denote the degrees of v and h respectively. Let C^p denote the curve in $\mathbb{P}^3$ defined by $v^p = h^p = 0$. For $n \in \mathbb{Z}$, let $\mathcal{O}_{\mathbb{P}^3}(n)$ denote the nth tensor power of Serre's twisting sheaf.

Lemma 3.4.1. *[59, Lemma 3.1.3] The following diagram is commutative with exact rows, where the composite map $\mathrm{H}^1(C, \mathcal{O}_C) \to \mathrm{H}^1(C, \mathcal{O}_C)$ is induced by the Frobenius morphism on C and the map F_1 is the Frobenius morphism on $\mathbb{P}^3$.*

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^1(C, \mathcal{O}_C) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r-s)) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r)) \oplus \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-s)) \\
 & & \downarrow & & \downarrow{\scriptstyle F_1^*} & & \downarrow \\
0 & \longrightarrow & \mathrm{H}^1(C^p, \mathcal{O}_{C^p}) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}((-r-s)p)) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-rp)) \oplus \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-sp)) \\
 & & \downarrow & & \downarrow{\scriptstyle (vh)^{p-1}} & & \downarrow \\
0 & \longrightarrow & \mathrm{H}^1(C, \mathcal{O}_C) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r-s)) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r)) \oplus \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-s))
\end{array}$$

Proof. This is an excerpt from the diagram immediately preceding [59, Proposition 3.1.4]. □

For $t \in \mathbb{Z}_{>0}$, the k-vector space $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-t))$ has basis

$$\{x^{k_1} y^{k_2} z^{k_3} w^{k_4} : (k_1, k_2, k_3, k_4) \in (\mathbb{Z}_{<0})^4, k_1 + k_2 + k_3 + k_4 = -t\}.$$

Lemma 3.4.2. *Suppose that $r \leq 3$. Then the following diagram is commutative with exact rows, where the map F is the Frobenius morphism on C and the map F_1 is the Frobenius morphism on $\mathbb{P}^3$.*

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^1(C, \mathcal{O}_C) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r-s)) & \xrightarrow{v} & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-s)) \\
 & & {\scriptstyle F^*}\downarrow & & \downarrow{\scriptstyle (vh)^{p-1}F_1^*} & & \downarrow \\
0 & \longrightarrow & \mathrm{H}^1(C, \mathcal{O}_C) & \longrightarrow & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r-s)) & \xrightarrow{v} & \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-s))
\end{array} \tag{3.8}$$

Proof. This follows immediately from Lemma 3.4.1 and the fact that $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-r)) = 0$ for $r \leq 3$. □

For $i, j \in \mathbb{Z}$, set $\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$.

Set $t = 5$ and let

$$S_{-5} = \{(k_1, k_2, k_3, k_4) \in (\mathbb{Z}_{<0})^4, k_1 + k_2 + k_3 + k_4 = -5\}.$$

Write $S_{-5} = \{(k_1^{(i)}, k_2^{(i)}, k_3^{(i)}, k_4^{(i)})\}_{1 \le i \le 4}$, where $k_j^{(i)} = -1 - \delta_{ij}$ for $1 \le i, j \le 4$.

Proposition 3.4.3. *Let v and h be homogeneous polynomials in $k[x, y, z, w]$ with $\gcd(v, h) = 1$. Suppose that $r = \deg(v) = 1$ and $s = \deg(h) = 4$. Write $v = a_1x + a_2y + a_3z + a_4w$ and fix t, with $1 \le t \le 4$, such that $a_t \neq 0$. Let C/k be the curve in $\mathbb{P}^3 = \mathrm{Proj}(k[x, y, z, w])$ defined by $v = h = 0$.*

Write $(vh)^{p-1} = \sum c_{i_1,i_2,i_3,i_4} x^{i_1} y^{i_2} z^{i_3} w^{i_4}$. For $1 \le i, j \le 4$, write

$$\gamma_{i,j} = c_{p(1+\delta_{1j})-(1+\delta_{1i}),\ p(1+\delta_{2j})-(1+\delta_{2i}),\ p(1+\delta_{3j})-(1+\delta_{3i}),\ p(1+\delta_{4j})-(1+\delta_{4i})}.$$

Then the Hasse-Witt matrix of C is given by

$$\mathrm{HW}_C = (a_t^{p-1}\gamma_{i,j} - a_j^p a_t^{-1}\gamma_{i,t})_{1 \le i,j \le 4, i \neq t, j \neq t}.$$

Let $t = 4$ and $a_4 = 1$ and write $a = a_1$, $b = a_2$ and $c = a_3$.

Then the matrix HW_C in Proposition 3.4.3 equals $\mathrm{HW}_C = (h_{i,j})$ where

$$\begin{aligned}
h_{1,1} &= c_{2p-2,p-1,p-1,p-1} - a^p c_{p-2,p-1,p-1,2p-1},\\
h_{1,2} &= c_{p-2,2p-1,p-1,p-1} - b^p c_{p-2,p-1,p-1,2p-1},\\
h_{1,3} &= c_{p-2,p-1,2p-1,p-1} - c^p c_{p-2,p-1,p-1,2p-1},\\
h_{2,1} &= c_{2p-1,p-2,p-1,p-1} - a^p c_{p-1,p-2,p-1,2p-1},\\
h_{2,2} &= c_{p-1,2p-2,p-1,p-1} - b^p c_{p-1,p-2,p-1,2p-1},\\
h_{2,3} &= c_{p-1,p-2,2p-1,p-1} - c^p c_{p-1,p-2,p-1,2p-1},\\
h_{3,1} &= c_{2p-1,p-1,p-2,p-1} - a^p c_{p-1,p-1,p-2,2p-1},\\
h_{3,2} &= c_{p-1,2p-1,p-2,p-1} - b^p c_{p-1,p-1,p-2,2p-1},\\
h_{3,3} &= c_{p-1,p-1,2p-2,p-1} - c^p c_{p-1,p-1,p-2,2p-1}.
\end{aligned}$$

Proof. Consider the multiplication-by-v map $[\times v] : \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5)) \to \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-4))$. By Lemma 3.4.2, computing the matrix of F^* is equivalent to computing the matrix of $(vh)^{p-1}F_1^*$ on the kernel of $[\times v]$.

First, we compute the matrix of $(vh)^{p-1}F_1^*$ on all of $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5))$. The k-vector space $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5))$ is 4-dimensional with basis

$$\{x^{k_1}y^{k_2}z^{k_3}w^{k_4} : (k_1, k_2, k_3, k_4) \in S_{-5}\}.$$

Explicitly, a basis is given by

$$e_1 = x^{-2}y^{-1}z^{-1}w^{-1}, e_2 = x^{-1}y^{-2}z^{-1}w^{-1}, e_3 = x^{-1}y^{-1}z^{-2}w^{-1}, e_4 = x^{-1}y^{-1}z^{-1}w^{-2}.$$

As in the proof of [59, Proposition 3.1.4], for each $j \in \{1, \ldots, 4\}$, then

$$\begin{aligned}
(vh)^{p-1}F_1^*(e_j) &= (vh)^{p-1}F_1^*(x^{k_1^{(j)}}y^{k_2^{(j)}}z^{k_3^{(j)}}w^{k_4^{(j)}})\\
&= (vh)^{p-1}x^{pk_1^{(j)}}y^{pk_2^{(j)}}z^{pk_3^{(j)}}w^{pk_4^{(j)}}\\
&= \sum c_{i_1,i_2,i_3,i_4} x^{i_1+pk_1^{(j)}}y^{i_2+pk_2^{(j)}}z^{i_3+pk_3^{(j)}}w^{i_4+pk_4^{(j)}}\\
&= \sum_{i=1}^{4} c_{k_1^{(i)}-pk_1^{(j)},k_2^{(i)}-pk_2^{(j)},k_3^{(i)}-pk_3^{(j)},k_4^{(i)}-pk_4^{(j)}} x^{k_1^{(i)}}y^{k_2^{(i)}}z^{k_3^{(i)}}w^{k_4^{(i)}}\\
&= \sum_{i=1}^{4} \gamma_{i,j}e_i.
\end{aligned}$$

Explicitly, the following 4-by-4 matrix H_0 represents the map $(vh)^{p-1}F_1^*$ on $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5))$, with respect to the basis e_1, e_2, e_3, e_4:

$$H_0 = \begin{pmatrix} c_{2p-2,p-1,p-1,p-1} & c_{p-2,2p-1,p-1,p-1} & c_{p-2,p-1,2p-1,p-1} & c_{p-2,p-1,p-1,2p-1} \\ c_{2p-1,p-2,p-1,p-1} & c_{p-1,2p-2,p-1,p-1} & c_{p-1,p-2,2p-1,p-1} & c_{p-1,p-2,p-1,2p-1} \\ c_{2p-1,p-1,p-2,p-1} & c_{p-1,2p-1,p-2,p-1} & c_{p-1,p-1,2p-2,p-1} & c_{p-1,p-1,p-2,2p-1} \\ c_{2p-1,p-1,p-1,p-2} & c_{p-1,2p-1,p-1,p-2} & c_{p-1,p-1,2p-1,p-2} & c_{p-1,p-1,p-1,2p-2} \end{pmatrix}. \quad (3.9)$$

Now we calculate the 3-by-3 matrix representing the restriction of $(vh)^{p-1}F_1^*$ to the kernel of $[\times v]$ on $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5))$. First, note that if $\ell \in \mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-5))$ is in $\mathrm{Ker}([\times v])$, then $(vh)^{p-1}F_1^*(\ell)$ is also in $\mathrm{Ker}([\times v])$, by the commutativity of (3.8).

The k-vector space $\mathrm{H}^3(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(-4))$ is 1-dimensional with basis element $\lambda = x^{-1}y^{-1}z^{-1}w^{-1}$. Note that $v \cdot e_i = a_i\lambda$. Thus $\mathrm{Ker}([\times v]) = \{\sum_{i=1}^4 c_i e_i \mid \sum_{i=1}^4 a_i c_i = 0\}$. For $1 \le i, j \le 4$, write $\beta_j^{(i)} = a_i e_j - a_j e_i$. If $a_t \neq 0$, then $\mathrm{Ker}([\times v])$ has basis $\{\beta_j^{(t)}\}_{1\le j\le 4, j\neq t}$. It follows that

$$\begin{aligned} (vh)^{p-1}F_1^*(\beta_j^{(t)}) &= a_t^p (vh)^{p-1}F_1^*(e_j) - a_j^p (vh)^{p-1}F_1^*(e_t) \\ &= a_t^p \sum_{i=1}^4 \gamma_{i,j} e_i - a_j^p \sum_{i=1}^4 \gamma_{i,t} e_i \\ &= \sum_{i=1}^4 (a_t^p \gamma_{i,j} - a_j^p \gamma_{i,t}) e_i. \end{aligned} \quad (3.10)$$

The commutativity of the diagram (3.8) shows that $(vh)^{p-1}F_1^*(\beta_j^{(t)})$ is in $\mathrm{Ker}([\times v])$. Therefore, there are coefficients $\lambda_{i,j} \in k$ such that for $j \neq t$,

$$\begin{aligned} (vh)^{p-1}F_1^*(\beta_j^{(t)}) &= \sum_{1\le i\le 4, i\neq t} \lambda_{i,j} \beta_i^{(t)} \\ &= \sum_{1\le i\le 4, i\neq t} \lambda_{i,j} (a_t e_i - a_i e_t). \end{aligned} \quad (3.11)$$

Comparing the coefficients of e_i for $i \neq t$ in (3.10) and (3.11), we see that

$$\lambda_{i,j} = a_t^{-1}(a_t^p \gamma_{i,j} - a_j^p \gamma_{i,t}).$$

This completes the proof of Proposition 3.4.3. □

3.5 The fiber of the Prym map when $g = 3$

In Section 3.3, we used a description from [14] of an unramified double cover $\pi : Y \to X$ of a plane quartic curve X and its Prym variety P_π in terms of quadratic forms. We then calculated the Hasse-Witt matrices of X and P_π and produced examples where X and P_π have specified p-ranks for small primes p. However, since the entries of the Hasse-Witt matrices are very complicated, it is not clear how to apply this method for arbitrarily large primes p.

In the current section, we describe an alternative method in which we start with a smooth curve Z of genus 2 over k and construct smooth plane quartic curves X having an unramified double cover $\pi : Y \to X$ such that $P_\pi \simeq \mathrm{Jac}(Z)$. The advantage of this alternative method is that it allows us to prove an existence result for infinitely many primes. In particular, in Proposition 3.5.2, we prove that if $p \equiv 5 \bmod 6$, then there exists

a smooth curve X defined over $\overline{\mathbb{F}}_p$ with genus 3 and p-rank 3 having an unramified double cover $\pi : Y \longrightarrow X$ such that P_π has p-rank 0.

Here is an outline of the section. In Section 3.5.1, we review a result of Verra that describes the geometry of the fibers of the Prym map $\mathcal{R}_3 \to \mathcal{A}_2$. In Section 3.5.2, we work with an explicit construction of the curves represented by points in the irreducible 3-dimensional component of the fiber above $\mathrm{Jac}(Z)$. These curves occur as the intersection in $\mathbb{P}^3$ of a plane and the Kummer surface of $\mathrm{Jac}(Z)$. They are smooth plane curves X having an unramified double cover $\pi : Y \to X$ such that $P_\pi \simeq \mathrm{Jac}(Z)$. In Section 3.5.3, we describe the determinant of the Hasse-Witt matrix of X. The main application when $p \equiv 5 \bmod 6$ is in Section 3.5.4.

In Section 3.5.5, we use commutative algebra to characterize when X is non-ordinary (under conditions on the p-rank of Z). In Section 3.5.6, we fix $p = 3$ and apply the results of the section to a 1-dimensional family of genus 2 curves Z with 3-rank 0. This allows us to deduce information about the locus of planes V for which X is non-ordinary and the geometry of the corresponding moduli space $\mathcal{R}_3^{(2,0)}$.

3.5.1 Review of work of Verra

Let A be a principally polarized abelian surface. Let $\mathcal{A}_2$ be the moduli space of principally polarized abelian surfaces. Let s be the point of $\mathcal{A}_2$ representing A. We would like to consider the fiber of the Prym map $Pr_3 : \mathcal{R}_3 \to \mathcal{A}_2$ over s. (More precisely, let $\tilde{\mathcal{A}}_2$ denote the smooth toroidal compactification of $\mathcal{A}_2$ and $\bar{\mathcal{R}}_3$ the compactification of $\mathcal{R}_3$ and consider the fiber of $\bar{Pr}_3 : \bar{\mathcal{R}}_3 \to \tilde{\mathcal{A}}_2$ over s.)

Following [95, Section 2], let $\Theta \subset A$ be a symmetric theta divisor. Suppose that $\mathrm{Aut}(\Theta) \simeq \mathbb{Z}/2$. Under this mild condition on s, Verra proves in [95, Corollary 4.1] that $\bar{Pr}_3^{-1}(s)$ is a blow-up of $\mathbb{P}^3$. Moreover, $\bar{Pr}_3^{-1}(s)$ has one irreducible component N_s of dimension 3 and three components of dimension 2. By [95, (3.14)-(3.16), page 442], the latter represent unramified double covers of hyperelliptic or singular curves whose Prym is isomorphic to A. The generic point of N_s represents an unramified double cover $\pi : Y \to X$ where X is a smooth plane quartic and $P_\pi \simeq A$. We briefly review the results of Verra in more detail below.

The linear system $|2\Theta|$ has dimension 3 and is thus isomorphic to $\mathbb{P}^3$. Every element $\tilde{C}$ in the linear system is a curve of arithmetic genus 5 with an involution. The linear system is base point free and its generic element is a smooth irreducible curve. For each $\tilde{C} \in |2\Theta|$, there is a morphism $\psi : A \to (\mathbb{P}^3)^\wedge$, where the wedge in superscript indicates taking the dual space. Let $K = \psi(A)$. Then $\deg(\psi) = 2$ if and only if $A = \mathrm{Jac}(Z)$ for some smooth irreducible curve Z of genus 2; (if not, then $\deg(\psi) = 4$). If $\deg(\psi) = 2$, then K is the Kummer quartic surface of A.

By [95, page 438], this yields a map $\phi : \mathbb{P}^3 - T \to \bar{Pr}_3^{-1}(s)$. Here T denotes the set of $\tilde{C}$ which are not stable. By [95, (2.1)], $T = B \cap K^\wedge$. Note that $K^\wedge \subset ((\mathbb{P}^3)^\wedge)^\wedge \simeq \mathbb{P}^3$ is birational to K. Here B denotes the union of B_τ where τ is a 2-torsion point of A and B_τ denotes the set of $\tilde{C}$ in the linear system $|2\Theta|$ such that $\tilde{C}$ contains τ.

3.5.2 Explicit version of the fiber of the Prym map

Let Z be a smooth curve of genus 2. The results of [95] give a way to find all smooth plane quartics X having an unramified double cover $\pi : Y \to X$ such that $P_\pi \simeq \mathrm{Jac}(Z)$. This is discussed in [14, Section 7], where Bruin shows how to recover a model of the form $X : Q_1 Q_3 = (Q_2)^2$ from a smooth plane section X of the Kummer surface K.

Consider the Kummer surface

$$K = \mathrm{Jac}(Z)/\langle -1\rangle \subset \mathbb{P}^3$$

associated to Z, namely the quotient of $\mathrm{Jac}(Z)$ by the Kummer involution. It is a quartic surface, with 16 singularities corresponding to $\mathrm{Jac}(Z)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{2g}$. Let $\phi : \mathrm{Jac}(Z) \longrightarrow K$ be the degree 2 quotient map.

For a sufficiently general plane $V \subseteq \mathbb{P}^3$, the intersection

$$X = V \cap K$$

is a smooth quartic plane curve. This implies that X does not contain any of the branch points of ϕ. Thus the restriction of ϕ to $Y = \phi^{-1}(X)$ is an unramified double cover $\pi : Y \to X$. Since Y is in $|2\Theta|$, the Prym variety P_π is isomorphic to $\mathrm{Jac}(Z)$, as seen on [6, page 616]. Conversely, by Verra's result, if $\mathrm{Jac}(Z)$ is isomorphic to the Prym variety of an unramified double cover $\pi : Y \to X$, with X a smooth plane quartic, then X is isomorphic to a planar section of K and Y is its preimage in $\mathrm{Jac}(Z)$.

The Kummer surface

Suppose that Z is a smooth curve of genus 2 with affine equation $Z : z^2 = D(x) := \sum_{i=0}^{6} d_i x^i$. Consider the Kummer surface $K = \mathrm{Jac}(Z)/\langle -1\rangle$ associated to Z, which is a quartic surface in $\mathbb{P}^3$. In this section, we write down the equation of K as found in [18, Chapter 3, Section 1].

There is a map $\phi : \mathrm{Jac}(Z) \to K$ defined as follows. A generic divisor of degree 2 on Z has the form $(x_1, z_1) + (x_2, z_2)$. Let Z_∞ be the divisor above $x = \infty$. Then

$$\begin{aligned} \phi\colon \mathrm{Jac}(Z) &\to K \\ [(x_1, z_1) + (x_2, z_2) - Z_\infty] &\mapsto [1 : x_1 + x_2 : x_1x_2 : \beta_0], \end{aligned}$$

where $\beta_0 = (F_0(x_1, x_2) - 2z_1z_2)/(x_1 - x_2)^2$ and $F_0(x_1, x_2)$ equals

$$2d_0+d_1(x_1+x_2)+2d_2x_1x_2+d_3(x_1+x_2)x_1x_2+2d_4(x_1x_2)^2+d_5(x_1+x_2)(x_1x_2)^2+2d_6(x_1x_2)^3.$$

The map ϕ realizes $\mathrm{Jac}(Z)$ as a double cover of K that ramifies precisely at $\mathrm{Jac}(Z)[2]$. It maps the 16 points of order 2 of $\mathrm{Jac}(Z)$ to the 16 singularities of K.

Let $X_1, \ldots, X_4$ denote the coordinates on $\mathbb{P}^3$. By [18, (3.1.8)], a projective model of the Kummer surface K in $\mathbb{P}^3$ is the zero locus of the following equation,

$$\kappa(X_1, X_2, X_3, X_4) = K_2X_4^2 + K_1X_4 + K_0 \tag{3.12}$$

with

$$\begin{aligned} K_2 &= X_2^2 - 4X_1X_3 \\ K_1 &= -2(2d_0X_1^3 + d_1X_1^2X_2 + 2d_2X_1^2X_3 + d_3X_1X_2X_3 + 2d_4X_1X_3^2 + d_5X_2X_3^2 + 2d_6X_3^3) \\ K_0 &= (d_1^2 - 4d_0d_2)X_1^4 - 4d_0d_3X_1^3X_2 - 2d_1d_3X_1^3X_3 - 4d_0d_4X_1^2X_2^2 \\ &\quad +4(d_0d_5 - d_1d_4)X_1^2X_2X_3 + (d_3^2 + 2d_1d_5 - 4d_2d_4 - 4d_0d_6)X_1^2X_3^2 - 4d_0d_5X_1X_2^3 \\ &\quad +4(2d_0d_6 - d_1d_5)X_1X_2^2X_3 + 4(d_1d_6 - d_2d_5)X_1X_2X_3^2 - 2d_3d_5X_1X_3^3 - 4d_0d_6X_2^4 \\ &\quad -4d_1d_6X_2^3X_3 - 4d_2d_6X_2^2X_3^2 - 4d_3d_6X_2X_3^3 + (d_5^2 - 4d_4d_6)X_3^4, \end{aligned}$$

where $d_0, \ldots, d_6$ are the coefficients of $D(x)$ in the equation for Z.

This model of the Kummer surface K in $\mathbb{P}^3$ arises from a projective model of $\mathrm{Jac}(Z)$ in $\mathbb{P}^{15}$; explicit calculations are thus more efficient on the Kummer surface. Alternatively, by combining a few Frobenius identities of theta characteristic functions, one can derive another projective model of K parametrized by four theta constants [76, Section 7, Chapter IIIa].

Plane quartics as planar sections of the Kummer surface

Let K be the Kummer surface from (3.12). For a plane $V \subset \mathbb{P}^3$, consider the curve

$$X = V \cap K.$$

If X is smooth, then it has genus 3 and the pullback of $\mathrm{Jac}(Z) \to K$ to X yields an unramified double cover $\pi : Y \to X$ such that the Prym variety P_π is isomorphic to $\mathrm{Jac}(Z)$.

Let $V = V_{a,b,c,d}$ be a plane defined over k by

$$V : \ v(X_1, X_2, X_3, X_4) = aX_1 + bX_2 + cX_3 + dX_4 = 0. \tag{3.13}$$

The point $(0 : 0 : 0 : 1)$ is a singular point of the Kummer surface. For planes V which avoid the singularities of K, it is no restriction to take $d = 1$.

3.5.3 The Hasse-Witt matrix of X

In Section 3.4, we determined the Hasse-Witt matrix for a curve X given as the intersection of a plane and quartic surface in $\mathbb{P}^3$. Recall that $X = V \cap K \subset \mathbb{P}^3$ where $K : \kappa = 0$ and $V : v = 0$ are defined in (3.12) and (3.13). Recall that c_{i_1,i_2,i_3,i_4} is the coefficient of $X_1^{i_1}X_2^{i_2}X_3^{i_3}X_4^{i_4}$ in $(v\kappa)^{p-1}$. In other words,

$$(v\kappa)^{p-1} = \sum_{i_1+i_2+i_3+i_4=5(p-1)} c_{i_1,i_2,i_3,i_4} X_1^{i_1} X_2^{i_2} X_3^{i_3} X_4^{i_4}.$$

Proposition 3.4.3 describes the Hasse-Witt matrix H_X of X in terms of the coefficients c_{i_1,i_2,i_3,i_4} and a, b, c, d.

Lemma 3.5.1. *Setting $d = 1$, then the coefficients of H_X are each homogeneous of degree $2(p-1)$ in $a, b, c, d_0, \ldots, d_6$.*

Proof. First, note that the equation κ in (3.12) for K is homogeneous of degree 2 in $d_0, \ldots, d_6, X_4$. This is because $K_2X_4^2$, K_1X_4, and K_0 are each homogeneous of degree 2 in $d_0, \ldots, d_6, X_4$. Also, the equation v for V is homogeneous of degree 1 in a, b, c, X_4. Thus $(\kappa v)^{p-1}$ is homogeneous of degree $3(p-1)$ in $a, b, c, d_0, \ldots, d_6, X_4$. The coefficients of the 4×4 matrix H_0 from (3.9) are coefficients of $(\kappa v)^{p-1}$.

We now determine information about the coefficients of the Hasse-Witt matrix H_X. Set $d = 1$. Let U be the 3×3 matrix obtained by removing the 4th row and 4th column of H_0. Let $C = [c_{p-2,p-1,p-1,2p-1}, c_{p-1,p-2,p-1,2p-1}, c_{p-1,p-1,p-2,2p-1}]^T$. By Proposition 3.4.3, $H_X = U - C[a^p, b^p, c^p]$. The coefficients of U are of the form c_{i_1,i_2,i_3,i_4} with $i_4 = p-1$; thus they are each homogeneous of degree $2(p-1)$ in $a, b, c, d_0, \ldots, d_6$. The coefficients of C are of the form c_{i_1,i_2,i_3,i_4} with $i_4 = 2p-1$; thus they are each homogeneous of degree $p-2$ in $a, b, c, d_0, \ldots, d_6$. Thus each coefficient of $H_X = U - C[a^p, b^p, c^p]$ is homogeneous of degree $2(p-1)$ in $a, b, c, d_0, \ldots, d_6$. □

3.5.4 An existence result for each $p \equiv 5 \bmod 6$

Proposition 3.5.2. *If $p \equiv 5 \bmod 6$, then there exists a smooth curve X defined over $\overline{\mathbb{F}}_p$ with genus 3 and 3-rank 3 having an unramified double cover $\pi : Y \longrightarrow X$ such that P_π has 3-rank 0. More generally, $R_3^{(3,0)}$ is non-empty of dimension 4 for each prime $p \equiv 5 \bmod 6$.*

Proof. Consider the genus 2 curve $Z : z^2 = x^6 - 1$; it is superspecial, and thus has p-rank 0, when $p \equiv 5 \bmod 6$ [53, Proposition 1.11]. The Kummer surface K in $\mathbb{P}^3$ is the zero locus of

$$\kappa(X_1, X_2, X_3, X_4) = K_2 X_4^2 + K_1 X_4 + K_0 \tag{3.14}$$

with

$$\begin{aligned} K_2 &= X_2^2 - 4X_1X_3 \\ K_1 &= 4X_1^3 - 4X_3^3 \\ K_0 &= 4X_1^2X_3^2 - 8X_1X_2^2X_3 + 4X_2^4. \end{aligned}$$

So

$$\kappa = X_2^2X_4^2 - 4X_1X_3X_4^2 + 4X_1^3X_4 - 4X_3^3X_4 + 4X_1^2X_3^2 - 8X_1X_2^2X_3 + 4X_2^4.$$

Let $v = aX_1 + bX_2 + cX_3 + X_4$ (so $d = 1$). Let c_{i_1,i_2,i_3,i_4} be the coefficient of $X_1^{i_1}X_2^{i_2}X_3^{i_3}X_4^{i_4}$ in $(\kappa v)^{p-1}$. By Proposition 3.4.3, the Hasse-Witt matrix H_X of $X = V \cap K$ is the matrix $(h_{i,j})_{1 \le i,j \le 3}$ where

$$\begin{aligned} h_{1,1} &= c_{2p-2,p-1,p-1,p-1} - a^p c_{p-2,p-1,p-1,2p-1}, \\ h_{1,2} &= c_{p-2,2p-1,p-1,p-1} - b^p c_{p-2,p-1,p-1,2p-1}, \\ h_{1,3} &= c_{p-2,p-1,2p-1,p-1} - c^p c_{p-2,p-1,p-1,2p-1}, \\ h_{2,1} &= c_{2p-1,p-2,p-1,p-1} - a^p c_{p-1,p-2,p-1,2p-1}, \\ h_{2,2} &= c_{p-1,2p-2,p-1,p-1} - b^p c_{p-1,p-2,p-1,2p-1}, \\ h_{2,3} &= c_{p-1,p-2,2p-1,p-1} - c^p c_{p-1,p-2,p-1,2p-1}, \\ h_{3,1} &= c_{2p-1,p-1,p-2,p-1} - a^p c_{p-1,p-1,p-2,2p-1}, \\ h_{3,2} &= c_{p-1,2p-1,p-2,p-1} - b^p c_{p-1,p-1,p-2,2p-1}, \\ h_{3,3} &= c_{p-1,p-1,2p-2,p-1} - c^p c_{p-1,p-1,p-2,2p-1}. \end{aligned}$$

By Lemma 3.5.3 (below), when $p \equiv 5 \bmod 6$, then the determinant of H_X has degree $4(p-1)$ when considered as a polynomial in b. In particular, $\det(H_X)$ is a non-zero polynomial in a, b, c. The condition that X is singular is a non-zero polynomial condition in a, b, c. Therefore, there exists a triple $(a, b, c) \in \overline{\mathbb{F}}_p^3$ such that X is smooth and $\det(H_X) \neq 0$. This implies that X is ordinary, with p-rank 3, and the unramified double cover $\pi : Y \to X$ has the property that $P_\pi \simeq \mathrm{Jac}(Z)$ has p-rank 0. Thus $R_3^{(3,0)}$ is non-empty. The dimension result follows from [79, Proposition 5.2]. □

We remark that a result similar to Proposition 3.5.2 may be true when $p \equiv 5, 7 \bmod 8$ with $Z : z^2 = x^5 - x$ or when $p \equiv 2, 3, 4 \bmod 5$ with $Z : z^2 = x^5 - 1$.

The next lemma provides the cornerstone of the proof of Proposition 3.5.2.

Lemma 3.5.3. *Let $p \equiv 5 \bmod 6$ and let X be as in the proof of Proposition 3.5.2. When considered as a polynomial in b, the determinant of H_X has degree $4(p-1)$.*

Proof. When considered as a polynomial in b, the coefficient c_{i_1,i_2,i_3,i_4} of $X_1^{i_1}X_2^{i_2}X_3^{i_3}X_4^{i_4}$ in $(\kappa v)^{p-1}$ has degree at most $p-1$. Any occurrence of b comes from the term bX_2 in v, so c_{i_1,i_2,i_3,i_4} has degree at most i_2 in b.

Note that κ has degree 2 in X_4, so κ^{p-1} has degree $2p-2$ in X_4. Any monomial in κ^{p-1} not divisible by X_2 arises as the product

$$(-4X_1X_3X_4^2)^{m_1}(4X_1^3X_4)^{m_2}(-4X_3^3X_4)^{m_3}(4X_1^2X_3^2)^{m_4} \tag{3.15}$$

for some $m_1, m_2, m_3, m_4 \in \mathbb{Z}_{\ge 0}$ with $m_1 + m_2 + m_3 + m_4 = p - 1$.

Claim 1: When considered as a polynomial in b, any term of the form $c_{i_1,p-1,i_3,2p-1}$ has degree at most $p-2$.

Proof of Claim 1: Any occurrence of b^{p-1} in $(\kappa v)^{p-1}$ comes from $\kappa^{p-1}(bX_2)^{p-1}$. The coefficient of $X_1^{i_1}X_3^{i_3}X_4^{2p-1}$ in κ^{p-1} is zero because κ^{p-1} has degree $2p-2$ in X_4.

By Claim 1, in the middle column of H_X, the top and bottom entries,

$$c_{p-2,2p-1,p-1,p-1} - b^p c_{p-2,p-1,p-1,2p-1} \text{ and } c_{p-1,2p-1,p-2,p-1} - b^p c_{p-1,p-1,p-2,2p-1},$$

have degrees at most $2p-2$ in b. We consider the six terms in the expansion of $\det(H_X)$. The four terms that do not contain the central coefficient of H_X have degrees at most $2p-2+p-1+p-2 = 4p-5$. It remains to consider the product of the diagonal coefficients, and the product of the antidiagonal coefficients. We show that the former has degree at most $4p-6$ and the latter has degree $4p-4$ as polynomials in b.

Claim 2: When considered as a polynomial in b, each of the two terms $c_{k(p-1),p-1,\ell(p-1),p-1}$ for $(k,\ell) \in \{(1,2),(2,1)\}$ has degree at most $p-2$.

Proof of Claim 2: We must show that the coefficient of $X_1^{k(p-1)}X_3^{\ell(p-1)}X_4^{p-1}$ in κ^{p-1} is zero. Since X_2 does not divide this monomial, it appears as a product as in (3.15). In order to attain the desired powers of X_1 and X_3, we must have

$$m_1 + 3m_2 + 2m_4 = k(p-1)$$

and

$$m_1 + 3m_3 + 2m_4 = \ell(p-1).$$

Subtracting the two equations gives $3(m_2 - m_3) = \pm(p-1)$. But $3 \nmid (p-1)$ since $p \equiv 5 \bmod 6$. So the coefficient of $X_1^{k(p-1)}X_3^{\ell(p-1)}X_4^{p-1}$ in κ^{p-1} is zero, as required.

Combining Claims 1 and 2 shows that the product of the diagonal entries of H_X has degree at most $p-2+2p-2+p-2 = 4p-6$ in b. Finally, we show that the product of the antidiagonal entries has degree $4p-4$ when considered as a polynomial in b.

Claim 3: When considered as polynomials in b, the following terms have degree $p-1$:

$$(1)\ c_{p-2,p-1,2p-1,p-1} \text{ and } (2)\ c_{2p-1,p-1,p-2,p-1}.$$

Proof of Claim 3: For (1), any occurrence of b^{p-1} in $(\kappa v)^{p-1}$ comes from $\kappa^{p-1}(bX_2)^{p-1}$. Hence we must show that the coefficient of $X_1^{p-2}X_3^{2p-1}X_4^{p-1}$ in κ^{p-1} is nonzero. Since X_2 does not divide this monomial, it arises as a product as in (3.15). In order to attain the desired power of X_4, we must have

$$2m_1 + m_2 + m_3 = p-1,$$

whereby $m_1 = m_4$. In order to attain the desired powers of X_1 and X_3, we must have

$$\begin{aligned} m_1 + 3m_2 + 2m_4 = 3(m_1+m_2) &= p-2 \\ &\text{and} \\ m_1 + 3m_3 + 2m_4 = 3(m_1+m_3) &= 2p-1. \end{aligned}$$

So m_1 determines m_2, m_3, m_4. Write $p = 6k + 5$ for some integer k, so $m_2 = 2k + 1 - m_1$ and $m_3 = 4k + 3 - m_1$. The coefficient of $b^{p-1}X_1^{p-2}X_2^{p-1}X_3^{2p-1}X_4^{p-1}$ in $c_{p-2,p-1,2p-1,p-1}$ is

$$\sum_{m_1+m_2+m_3+m_4=p-1} \frac{(p-1)!}{m_1!m_2!m_3!m_4!}(-4)^{m_1}4^{2k+1-m_1}(-4)^{4k+3-m_1}4^{m_1}$$
$$= (-1)^{4k+3}4^{p-1} \sum_{m_1+m_2+m_3+m_4=p-1} \frac{(p-1)!}{m_1!m_2!m_3!m_4!}.$$

Note that

$$\sum_{m_1+m_2+m_3+m_4=p-1} \frac{(p-1)!}{m_1!m_2!m_3!m_4!} = 4^{p-1}.$$

Therefore, the coefficient of $b^{p-1}X_1^{p-2}X_2^{p-1}X_3^{2p-1}X_4^{p-1}$ is the nonzero number

$$(-1)^{4k+3}4^{p-1}4^{p-1} = -4^{2p-2}.$$

For (2), consider the coefficient of b^{p-1} in $c_{2p-1,p-1,p-2,p-1}$. By the same strategy as above:

$$m_1 = m_4;$$
$$3m_1 + 3m_2 = 2p - 1 = 12k + 9;$$
$$3m_1 + 3m_3 = p - 2 = 6k + 3.$$

So, the coefficient of $b^{p-1}X_1^{2p-1}X_2^{p-1}X_3^{p-2}X_4^{p-1}$ in $c_{2p-1,p-1,p-2,p-1}$ is the nonzero number

$$\sum_{m_1+m_2+m_3+m_4=p-1} \frac{(p-1)!}{m_1!m_2!m_3!m_4!}(-4)^{m_1}4^{4k+3-m_1}(-4)^{2k+1-m_1}4^{m_1}$$
$$= (-1)^{2k+1}4^{p-1} \sum_{m_1+m_2+m_3+m_4=p-1} \frac{(p-1)!}{m_1!m_2!m_3!m_4!} = -4^{2p-2}.$$

Claim 4: When considered as a polynomial in b, the term $c_{p-1,p-2,p-1,2p-1}$ has degree $p - 2$.

Proof of Claim 4: Consider the coefficient of b^{p-2} in $c_{p-1,p-2,p-1,2p-1}$. Since κ^{p-1} has degree $2p - 2$ in X_4, any occurrence of $b^{p-2}X_1^{p-1}X_2^{p-2}X_3^{p-1}X_4^{2p-1}$ in $(\kappa v)^{p-1}$ comes from choosing the monomial bX_2 in $p - 2$ factors v of v^{p-1}, and X_4 in the remaining one. There are $p - 1$ ways of doing so.

Now we compute the coefficient of $X_1^{p-1}X_3^{p-1}X_4^{2p-2}$ in κ^{p-1}. A monomial divisible by X_2 cannot be chosen in a factor κ of κ^{p-1}. Therefore, to obtain the exponent $2p - 2$ of X_4, we need to pick the monomial $-4X_1X_3X_4^2$ in each factor κ of κ^{p-1}. Hence, the coefficient of $b^{p-2}X_1^{p-1}X_2^{p-2}X_3^{p-1}X_4^{2p-1}$ in $c_{p-1,p-2,p-1,2p-1}$ is $(p-1)(-4)^{p-1}$, which is not zero.

By the claims, the leading power of b arises in the product of the antidiagonal entries and has degree $p - 1 + p + p - 2 + p - 1 = 4p - 4$. □

3.5.5 The condition that X is non-ordinary

In this subsection, Z is an arbitrary smooth curve of genus 2 and $X = K \cap V$ with Hasse-Witt matrix H_X as in Section 3.5.3.

The condition that X is non-ordinary

The curve X is non-ordinary if and only if $\det(H_X)$ is non-zero.

Proposition 3.5.4. *Setting $d = 1$, then $\det(H_X)$ is non-zero and homogeneous of degree $6(p-1)$ in $a, b, c, d_0, \ldots, d_6$.*

Proof. By Lemma 3.5.1, each coefficient of the 3×3 matrix H_X is homogeneous of degree $2(p-1)$ in these variables. Thus it suffices to prove that $\det(H_X)$ is non-zero. We expect that this can be proven algebraically, but to avoid long computations we continue with the following theoretical argument. If $\det(H_X)$ is identically 0, then a generic point of $\mathcal{R}_3 = \Pi^{-1}(\mathcal{M}_3)$ would represent an unramified double cover $\pi : Y \to X$ such that X is non-ordinary; this is false. □

We apply a fractional linear transformation to x in order to reduce the number of variables defining Z, while preserving the degree of $\det(H_X)$ and its homogeneous property. Without loss of generality, we can suppose that no Weierstrass point of Z lies over $x = \infty$ and that 3 of the Weierstrass points are rational and lie over $x = 0, 1, -1$; (over a non-algebraically closed field, this may only be true after a finite extension). Then,

$$\begin{aligned} Z : z^2 &= D(x) := (x^3 - x)(A_0x^3 + Ax^2 + Bx + C) && (3.16)\\ &= A_0x^6 + Ax^5 + (B - A_0)x^4 + (C - A)x^3 - Bx^2 - Cx. && (3.17) \end{aligned}$$

Note that $A_0 \neq 0$ by the hypothesis at ∞ and $C \neq 0$ since Z is smooth.

The condition that X is non-ordinary and Z has p-rank 1

As in (3.16), write $Z : z^2 = D(x) := (x^3 - x)(A_0x^3 + Ax^2 + Bx + C)$. The curve Z is not ordinary if and only if $\det(H_Z) = 0$

Lemma 3.5.5. *Then $\det(H_X)$ does not vanish identically under the polynomial condition $\det(H_Z) = 0$, which is homogeneous of degree $p - 1$ in A_0, A, B, C.*

Proof. Since $D(x)$ is linear in A_0, A, B, C, the entries of the Hasse-Witt matrix H_Z are homogeneous of degree $(p-1)/2$ so $\det(H_Z)$ is homogeneous of degree $p - 1$.

For the non-vanishing claim, it suffices to show that X is typically ordinary when Z has p-rank 1. This follows from the fact that each component of $\mathcal{R}_3^{(3,1)}$ has dimension 5, while each component of $\mathcal{R}_3^{(2,1)}$ has dimension 4, which is a special case of [79, Theorem 7.1]. □

For example, when $p = 3$ and $(A_0, A, B, C, a, b, c) = (1, 0, 1, 2t, 0, 1, 1)$ with $t \in \mathbb{F}_9$ a root of $t^2 - t - 1$ then $f = 1$ and $f' = 1$ and the curve X is smooth.

The condition that X is non-ordinary and Z has p-rank 0

Lemma 3.5.6. *The curve Z is not ordinary under a polynomial condition on A_0, A, B, C which is homogeneous of degree $p - 1$. The curve Z has p-rank 0 under 4 polynomial conditions on A_0, A, B, C which are each homogeneous of degree $(p + 1)(p - 1)/2$.*

Proof. The curve Z has p-rank 0 if and only if $H_Z H_Z^{(p)} = [0]$. The entries of $H_Z^{(p)}$ are homogeneous of degree $p(p-1)/2$, so the entries of $H_Z H_Z^{(p)}$ are homogeneous of degree $(p + 1)(p - 1)/2$. □

Proposition 3.5.7. *Let Z be a genus 2 curve with equation $z^2 = (x^3 - x)(A_0x^3 + Ax^2 + Bx + C)$. Let V be a plane with equation $aX_1 + bX_2 + cX_3 + X_4$. Let $X = V \cap K$ and consider the unramified double cover $\pi : Y \to X$ given by the restriction of $\phi : \mathrm{Jac}(Z) \to K$. Then the condition that X is non-ordinary and Z has p-rank 0 is given by the vanishing of 4 homogeneous polynomials of degree $(p+1)(p-1)/2$ in A_0, A, B, C and the vanishing of one homogeneous polynomial $\det(H_X)$ of degree $6(p-1)$ in a, b, c, A_0, A, B, C.*

Proof. The curve X is non-ordinary if and only if $\det(H_X)$ vanishes. By Proposition 3.5.4, $\det(H_X)$ is homogeneous of degree $6(p-1)$ in a, b, c and the coefficients of $D(x)$, which are linear in A_0, A, B, C. The curve Z has p-rank 0 under the conditions in Lemma 3.5.6. □

We expect that the answer to Question 3.1.1 is yes for all odd p when $g = 3$, $f = 2, 3$, and $f' = 0$. We now rephrase the question in those cases to a question in commutative algebra.

Question 3.5.8. For all odd primes p, is there a plane V for which $\det(H_X)$ does not vanish identically under the 4 conditions when $H_Z H_Z^{(p)} = [0]$? Is there a plane V for which $\det(H_X)$ does vanish for some Z such that $H_Z H_Z^{(p)} = [0]$?

The difficulty in showing that $\det(H_X)$ does not vanish identically when Z has p-rank 0 is that we do not know much about the variety of the ideal generated by the 4 polynomial conditions when $H_Z H_Z^{(p)} = [0]$ or the behavior of the derivatives of $\det(H_X)$ with respect to the variables a, b, c.

Example: when $p = 3$

Write $Z : z^2 = D(x) = (x^3 - x)(A_0x^3 + Ax^2 + Bx + C)$. Then

$$H_Z = \begin{pmatrix} -B & A \\ -C & B - A_0 \end{pmatrix}.$$

The 4 entries of $H_Z H_Z^{(3)}$ are:

$$B^4 - AC^3,\ C(B^3 - C^2(B - A_0)),\ A((B - A_0)^3 - BA^2), -CA^3 + (B - A_0)^4.$$

Recall that $C \neq 0$ since Z is smooth. If Z has 3-rank 0 then if any of $A, B, B - A_0$ are zero then all of them are zero, which implies $A_0 = 0$, which contradicts the hypothesis at ∞. Thus $AB(B - A_0) \neq 0$ when Z has 3-rank 0. One can check that $H_Z H_Z^{(3)} = [0]$ if and only if

$$B^4 - AC^3 = 0, B^3 - C^2(B - A_0) = 0.$$

Write

$$(v\kappa)^2 = \sum_{i_1+i_2+i_3+i_4=10} c_{i_1,i_2,i_3,i_4} X_1^{i_1} X_2^{i_2} X_3^{i_3} X_4^{i_4},$$

and assume that $d = 1$. Then the Hasse-Witt matrix H_X is given by

$$\begin{pmatrix} c_{4,2,2,2} - a^3 c_{1,2,2,5} & c_{1,5,2,2} - b^3 c_{1,2,2,5} & c_{1,2,5,2} - c^3 c_{1,2,2,5} \\ c_{5,1,2,2} - a^3 c_{2,1,2,5} & c_{2,4,2,2} - b^3 c_{2,1,2,5} & c_{2,1,5,2} - c^3 c_{2,1,2,5} \\ c_{5,2,1,2} - a^3 c_{2,2,1,5} & c_{2,5,1,2} - b^3 c_{2,2,1,5} & c_{2,2,4,2} - c^3 c_{2,2,1,5} \end{pmatrix} \tag{3.18}$$

By Proposition 3.2.9, the 3-rank of X is the stable rank of H_X, which is the rank of $H_X H_X^{(3)} H_X^{(3^2)}$. The entries of H_X are homogeneous of degree 4 and $\det(H_X)$ is homogeneous of degree 12 in a, b, c, A_0, A, B, C.

Example: Genus 3 curves having Pryms of 3-rank 1 when $p = 3$

In Example 3.3.5, we showed that $\mathcal{R}_3^{(1,1)}$ and $\mathcal{R}_3^{(0,1)}$ are non-empty when $p = 3$, by finding curves X of 3-rank 1 or 0 having an unramified double cover $\pi : Y \to X$ such that P_π has 3-rank 1. Here we give a second proof of this using the methods of this section.

For $t, u \in k$ with $t \neq u$, consider the genus 2 curve

$$Z_{t,u} : z^2 = D(x) := x^6 + x^3 + 1 + x(x^3 + 1)(tx + u) = x^6 + tx^5 + ux^4 + x^3 + tx^2 + ux + 1.$$

One can check that $Z_{t,u}$ is smooth if $t \neq u$ and $Z_{t,u}$ has 3-rank 1 for $t \neq \pm u$.

Example 3.5.9. Let $p = 3$. Consider the plane quartic $X = V \cap K$ where K is the Kummer surface of $\mathrm{Jac}(Z_{t,u})$ and $V \subset \mathbb{P}^3$ is a plane. Then X has an unramified double cover $\pi : Y \to X$ such that $P_\pi \simeq Z_{t,u}$ has p-rank 1.

1. If $V : -X_2 + X_3 + X_4 = 0$ and $t = 1$, $u = 0$, then X is smooth with 3-rank $f = 1$.
2. If $V : -X_1 - X_2 + X_4 = 0$ and $t = 0$, $u = 1$, then X is smooth with 3-rank $f = 0$.

3.5.6 The moduli space of genus 3 curves having Pryms of 3-rank 0 when $p = 3$

In this section, we fix $p = 3$. In Section 3.5.6, we parametrize $\mathcal{M}_2^0$ (the 3-rank 0 stratum of $\mathcal{M}_2$) by a 1-parameter family of curves of genus 2 and 3-rank 0. Let α be the name of this parameter. In Section 3.5.6, we then analyze $\det(H_X)$ as V and α vary. This allows us to prove some information about the locus of the parameter space where X is non-ordinary. This implicitly provides geometric information about $\mathcal{R}_3^{(2,0)}$.

A family of genus 2 curves with 3-rank 0 when $p = 3$

For $\alpha \in k - \{0, 1, -1\}$, define

$$Z_\alpha : \ z^2 = A(x)B(x),$$

where

$$A(x) = x^3 - \alpha x^2 + \alpha x + (\alpha + 1), \text{ and } \ B(x) = (x - \alpha)(x - (\alpha + 1))(\alpha x + (\alpha + 1)).$$

The importance of the next lemma is that it shows that $\mathrm{Jac}(Z_\alpha)$ parametrizes the 3-rank 0 stratum of $\mathcal{A}_2$, which is irreducible of dimension 1 when $p = 3$.

Lemma 3.5.10. *When $p = 3$, then the family $\{Z_\alpha\}_\alpha$ is a non-isotrivial family of smooth curves of genus 2 and 3-rank 0.*

Proof. For $\alpha \in k - \{0, 1, -1\}$, the polynomial $A(x)B(x)$ has no repeated roots, hence the curve Z_α is smooth and of genus 2. If Z_α is isomorphic to Z_β for $\alpha, \beta \in k - \{0, 1, -1\}$ then they have the same absolute Igusa invariants j_1, j_2, j_3 [54]. Using SageMath [30], we find that the absolute Igusa invariants of Z_α are:

$$\begin{aligned} j_1 &= -\frac{(\alpha - 1)^6}{\alpha(\alpha + 1)^2}, \\ j_2 &= -\frac{(\alpha - 1)^6}{\alpha(\alpha + 1)^2}, \\ j_3 &= \frac{(\alpha - 1)^2(\alpha^2 - \alpha - 1)^2}{\alpha^2}. \end{aligned}$$

In particular, the absolute Igusa invariants are non-constant functions of α, hence the family $\{Z_\alpha\}_\alpha$ is non-isotrivial.

By Proposition 3.2.3, the Cartier-Manin matrix M of Z_α is

$$\begin{pmatrix} (\alpha+1)^3 & -(\alpha+1)^4 \\ 1 & -(\alpha+1) \end{pmatrix}$$

so the matrix $M^{(3)}M$ is

$$\begin{pmatrix} (\alpha+1)^9 & -(\alpha+1)^{12} \\ 1 & -(\alpha+1)^3 \end{pmatrix} \begin{pmatrix} (\alpha+1)^3 & -(\alpha+1)^4 \\ 1 & -(\alpha+1) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

so Z_α has 3-rank $f' = 0$ by Proposition 3.2.9. □

The locus of the parameter space where X is non-ordinary when $p = 3$

Now, we compute the equation of the Kummer surface K_α of Z_α and choose a plane $V = V_{a,b,c,d}$ to obtain the smooth plane quartic $X_V^\alpha = K_\alpha \cap V$. Our goal is to find information about the 3-rank $f = f_V^\alpha$ of X_V^α as V and α vary. To do this, we determine the Hasse-Witt matrix $H := H_{X_V^\alpha}$ of X_V^α as in (3.18).

Proposition 3.5.11. *For a generic choice of plane V, the curve X_V^α is ordinary for all but finitely many α and has 3-rank 2 for at least one and at most finitely many α.*

Proof. When $d = 1$, the value of the 3-rank of X_V^α is determined by polynomial conditions in a, b, c and α. In particular, X_V^α has 3-rank 3 if and only if the determinant of H_V^α is non-zero. So the first statement can be proven by checking, for a fixed plane V and fixed parameter α, whether $\det(H_V^\alpha) \neq 0$. The second statement can be proven by checking, for a fixed plane V, whether $\det(H_V^\alpha) = 0$ under a polynomial condition on α and whether there exists one value of α satisfying that polynomial condition for which X_V^α is smooth and has 3-rank 2.

Thus both statements follow from the next claim.

Claim: For the plane $V : -X_2 + X_4 = 0$, the curve X_V^α is ordinary for all but finitely many $\alpha \in k - \{0, 1, -1\}$, and X_V^α has 3-rank 2 for a non-zero finite number of $\alpha \in k$.

Proof of claim: When $V : -X_2 + X_4 = 0$, the Hasse-Witt matrix H of X_V^α is

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

where

$$\begin{aligned}
a_{11} &= \alpha^{13} - \alpha^{11} - \alpha^{10} + \alpha^9 + \alpha^7 + \alpha^6 - \alpha^3 - \alpha^2 - 1, \\
a_{12} &= -\alpha^7 - \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha, \\
a_{13} &= \alpha^{10} + \alpha^9 + \alpha^7 - \alpha^6 + \alpha^5 - \alpha^4, \\
a_{21} &= -\alpha^{16} - \alpha^{13} + \alpha^{11} + \alpha^9 + \alpha^8 + \alpha^7 - \alpha^5 + \alpha^4 - \alpha^3 - \alpha^2, \\
a_{22} &= \alpha^{13} + \alpha^9 + \alpha^8 + \alpha^7 - \alpha^6 - \alpha^4 - \alpha^3 - \alpha^2 - \alpha - 1, \\
a_{23} &= -\alpha^{13} + \alpha^{10} + \alpha^9 - \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 - \alpha^2 - \alpha - 1, \\
a_{31} &= \alpha^{13} + \alpha^{12} - \alpha^9 + \alpha^8 + \alpha^7 + \alpha^6 - \alpha^5 + \alpha^2 + \alpha, \\
a_{32} &= \alpha^{10} - \alpha^8 + \alpha^7 + \alpha^5 - \alpha^4 - \alpha^3 - \alpha^2 - \alpha - 1, \\
a_{33} &= \alpha^{12} - \alpha^{10} + \alpha^6 + \alpha^5 - \alpha^4 - \alpha - 1.
\end{aligned}$$

The determinant Det_H of H is

$$\mathrm{Det}_H = \alpha^3(\alpha+1)^4(\alpha-1)^5(\alpha^3+\alpha^2+\alpha-1)(\alpha^5+\alpha^4+\alpha^3+\alpha^2-\alpha+1)$$
$$(\alpha^5-\alpha^4+\alpha^3+\alpha^2+\alpha+1)(\alpha^6-\alpha^4+\alpha^3-\alpha+1)(\alpha^7+\alpha^5+\alpha-1).$$

For each $\alpha \in k - \{0, 1, -1\}$ which is not a root of Det_H, the Hasse-Witt matrix is invertible and so X_V^α is ordinary. For $\alpha \in k$ satisfying $\alpha^3+\alpha^2+\alpha-1=0$, a computation in SageMath [30] shows that X_V^α is smooth and the matrix $HH^{(3)}H^{(3^2)}$ has rank 2. Therefore, for these values of α, X_V^α has 3-rank 2 by Proposition 3.2.9.

□

Proposition 3.5.11 does not eliminate the possibility that there exists a plane V such that $\det(H_V^\alpha) = 0$ for all α.

Proposition 3.5.12. *For a generic choice of $\alpha \in k$, the curve X_V^α is ordinary for a generic choice of V and has 3-rank 2 under a codimension 1 condition on V.*

Proof. The first statement already follows from Proposition 3.5.11. The second statement can be proven by checking, for fixed $\alpha \in k$, whether $\det(H_V^\alpha) = 0$ under a polynomial condition on a, b, c and whether there exists one possibility for a, b, c satisfying that polynomial condition for which X_V^α is smooth and has 3-rank 2.

Let $\alpha \in \mathbb{F}_9$ be fixed to be a root of the polynomial t^2+2t+2. If $d=1$, the Hasse-Witt matrix $H = (a_{ij})_{i,j}$ of X_V^α, for arbitrary a, b, c, is given by :

$$\begin{aligned}
a_{11} &= a^3c + b^2 + ac + (\alpha+1)(a^3 - bc + a) + (\alpha-1)(ab-b) - \alpha c^2\\
a_{12} &= b^3c + (\alpha+1)b^3\\
a_{13} &= c^4 - ac + (\alpha+1)c^2(c-1) + (-\alpha+1)b^2 + -\alpha(ab+bc)\\
a_{21} &= a^3b - ab + (-\alpha-1)(a^3+ac+c) + (-\alpha+1)(a^2+c^2+a-bc)\\
a_{22} &= b^4 + (-\alpha-1)b^3 - \alpha c^2 + \alpha b\\
a_{23} &= bc^3 + (-\alpha-1)c^3 + \alpha(a^2 - ac + bc + c^2) + (\alpha-1)ab\\
a_{31} &= a^4 - a^2 + (-\alpha+1) + (\alpha+1)(a^3 - ab - b) + (-\alpha+1)(b^2 - bc - c) + \alpha ac\\
a_{32} &= ab^3 + (\alpha+1)b^3 + \alpha bc\\
a_{33} &= ac^3 + a^2 + (\alpha+1)(c^3 + ac - c) - \alpha(b^2 + bc + ab).
\end{aligned}$$

Then one can check that $\det(H)$ is non-vanishing in a, b, c. Also, when $(a, b, c) = (2, 0, 2)$, then one can check that the curve X_V^α is smooth with 3-rank 2. □

We note that Proposition 3.5.12 does not eliminate the possibility that there exists $\alpha \in k$ such that $\det(H_V^\alpha) = 0$ for all planes V.

3.6 Points on the Kummer surface

Suppose that Z is a supersingular curve of genus 2 defined over a finite field $\mathbb{F}_q$ of characteristic p. This section contains a result about the number of $\mathbb{F}_q$-points on the Kummer surface K of $\mathrm{Jac}(Z)$. The material in this section is probably well known to experts but we could not find it in the literature. The connection between this section and the rest of the paper is found in Question 3.6.4 below: if $X = V \cap K$ for some plane V and if p divides $\#X(\mathbb{F}_q)$, then the p-rank of X is at least 1.

Let Z be a genus 2 curve over $\mathbb{F}_q$. Suppose that Z has equation $z^2 = D(x)$ and define a quadratic twist W of Z by $\lambda z^2 = D(x)$ for $\lambda \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$. The isomorphism class of W does not depend on the choice of non-square element λ.

Lemma 3.6.1. *Let Z be a genus 2 curve over $\mathbb{F}_q$ and let W be its quadratic twist. Let $K = \mathrm{Jac}(Z)/\langle -1\rangle$. Then*

$$|K(\mathbb{F}_q)| = (|\mathrm{Jac}(Z)(\mathbb{F}_q)| + |\mathrm{Jac}(W)(\mathbb{F}_q)|)/2.$$

Proof. The degree 2 cover $\phi : \mathrm{Jac}(Z) \to K$ is defined over $\mathbb{F}_q$. Let $\psi : \mathrm{Jac}(Z) \to \mathrm{Jac}(W)$ be the isomorphism of abelian varieties over $\mathbb{F}_{q^2}$ induced by the isomorphism of the underlying curves given by $(x, z) \mapsto (x, \sqrt{\lambda}z)$. Let τ be a generator for $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. Then $\tau\psi\tau^{-1} = -\psi$.

Let $P \in K(\mathbb{F}_q)$. Write $\phi^{-1}(P) = \{Q, -Q\}$. Since $P \in K(\mathbb{F}_q)$ and ϕ is defined over $\mathbb{F}_q$, then $\{\sigma(Q), -\sigma(Q)\} = \{Q, -Q\}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Therefore, Q is defined over $\mathbb{F}_{q^2}$ and either $\tau(Q) = Q$, whereby $Q \in \mathrm{Jac}(Z)(\mathbb{F}_q)$, or $\tau(Q) = -Q$, whereby $\psi(Q) \in \mathrm{Jac}(W)(\mathbb{F}_q)$. The points $P \in K(\mathbb{F}_q)$ for which $\phi^{-1}(P) = \{Q, -Q\}$ with $Q = -Q$ are precisely those for which $Q \in \mathrm{Jac}(Z)(\mathbb{F}_q)$ and $\psi(Q) \in \mathrm{Jac}(W)(\mathbb{F}_q)$. Therefore, every point in $K(\mathbb{F}_q)$ is counted twice in $|\mathrm{Jac}(Z)(\mathbb{F}_q)| + |\mathrm{Jac}(W)(\mathbb{F}_q)|$. □

The zeta function of a genus 2 curve $Z/\mathbb{F}_q$ is

$$\mathcal{Z}(T) = \exp\left(\sum_{k\geq 1} \frac{|Z(\mathbb{F}_{q^k})|}{k} T^k\right) = \frac{L_{Z/\mathbb{F}_q}(T)}{(1-T)(1-qT)},$$

where $L_{Z/\mathbb{F}_q}(T) = 1 + a_1T + a_2T^2 + qa_1T^3 + q^2T^4 = \prod_{i=1}^{4}(1 - \alpha_i T)$ with $\alpha_1\alpha_3 = \alpha_2\alpha_4 = q$.

Lemma 3.6.2. *Let Z be a genus 2 curve over $\mathbb{F}_q$, let $A = \mathrm{Jac}(Z)$ and let $K = A/\langle -1\rangle$. Then*

$$|\mathrm{Jac}(Z)(\mathbb{F}_q)| = 1 + a_1 + a_2 + a_1q + q^2$$

and

$$|K(\mathbb{F}_q)| = 1 + a_2 + q^2$$

where the a_i are the coefficients of $L_{Z/\mathbb{F}_q}(T)$ as defined above.

Proof. The second statement follows from the first, using Lemma 3.6.1 and the fact that if $W/\mathbb{F}_q$ is the quadratic twist of Z, then $L_{W/\mathbb{F}_q}(T) = L_{Z/\mathbb{F}_q}(-T) = 1 - a_1T + a_2T^2 - qa_1T^3 + q^2T^4$.

For the first statement, note that

$$|\mathrm{Jac}(Z)(\mathbb{F}_q)| = \frac{|Z(\mathbb{F}_q)|^2 + |Z(\mathbb{F}_{q^2})|}{2} - q. \tag{3.19}$$

Equating the coefficients of T and T^2 in

$$\frac{L_{Z/\mathbb{F}_q}(T)}{(1-T)(1-qT)} = \exp\left(\sum_{k\geq 1} \frac{|Z(\mathbb{F}_{q^k})|}{k} T^k\right)$$

gives $a_1 = |Z(\mathbb{F}_q)| - (q+1)$ and $a_2 = \frac{1}{2}|Z(\mathbb{F}_q)|^2 + \frac{1}{2}|Z(\mathbb{F}_{q^2})| - (q+1)|Z(\mathbb{F}_q)| + q$. The result now follows from (3.19). □

Corollary 3.6.3. *Let Z be a supersingular genus 2 curve over $\mathbb{F}_q$, let $A = \mathrm{Jac}(Z)$ and let $K = A/\langle -1\rangle$. Then*

$$|K(\mathbb{F}_q)| \equiv 1 \bmod q.$$

Proof. If Z is supersingular then $q \mid a_2$. The result now follows. □

Question 3.6.4. Suppose Z is supersingular. Does there exist a plane $V \subset \mathbb{P}^3$ defined over $\mathbb{F}_q$ such that p divides $\#X(\mathbb{F}_q)$ where $X = V \cap K$? If so, then the p-rank of X is at least 1.

3.7 Results for arbitrary g

In this section, when $3 \leq p \leq 19$, we use the results from Section 3.3 about genus 3 curves in characteristic p to verify the existence of smooth curves X of arbitrary genus $g \geq 3$ having an unramified double cover whose Prym has small p-rank. Specifically, we work inductively to study the dimension of certain moduli strata $\mathcal{R}_g^{(f,f')}$ for $g \geq 3$ in characteristic p with $3 \leq p \leq 19$. The reader is strongly advised to read [79] before reading this section.

A highlight of this approach is that X is smooth and we can control its p-rank f. Indeed, the original proof of [98], found in [6, Section 2], shows that $\bar{\mathcal{R}}_g^{(f'+1,f')}$ is non-empty for each $g \geq 2$ and $0 \leq f' \leq g-1$; in other words, there is a *singular* curve of genus g and p-rank $f'+1$ with an unramified double cover π such that P_π has p-rank f'. We omit the details of this argument.

In this section, the word *component* means irreducible component. Although the phrasing is slightly redundant, we emphasize that a component of a given dimension is *non-empty* because this property of the component is the most difficult to prove and is sufficient to yield the existence applications.

3.7.1 Increasing the p-rank of the Prym variety

The next result allows us to use geometric information about $\mathcal{R}_g^{(f,f')}$ to deduce geometric information about $\mathcal{R}_g^{(f,F')}$ when $f' \leq F' \leq g-1$.

Proposition 3.7.1. *[79, Proposition 5.2] Let $g \geq 3$. Suppose that $\mathcal{R}_g^{(f,f')}$ is non-empty and has a component of dimension $g-2+f+f'$ in characteristic p. Then $\mathcal{R}_g^{(f,F')}$ is non-empty and has a component of dimension $g-2+f+F'$ in characteristic p for each F' such that $f' \leq F' \leq g-1$.*

3.7.2 Background on boundary of $\mathcal{R}_g$

The strategy used in [79] is to use unramified double covers of *singular* curves of given genus and p-rank to produce unramified double covers of *smooth* curves of the same genus and p-rank, with control over the p-rank of the Prym variety. This strategy must be implemented very precisely because, in general, the p-rank of both the curve and the Prym will increase when deforming X away from the boundary. In fact, there are situations where this is guaranteed to happen.

This section contains background about p-ranks of unramified double covers of singular curves. Let $\bar{\mathcal{R}}_g$ be the compactification of $\mathcal{R}_g$ as defined and analyzed in [21, Section 1.4]. The points of $\bar{\mathcal{R}}_g \backslash \mathcal{R}_g$ represent unramified double covers of singular stable curves of genus g.

Let $\bar{\mathcal{R}}_{g;1} = \bar{\mathcal{R}}_g \times_{\bar{\mathcal{M}}_g} \bar{\mathcal{M}}_{g;1}$ be the moduli space whose points represent unramified double covers $\pi : Y \to X$ together with marked points $y \in Y$ and $x \in X$ such that $\pi(y) = x$, as in [79, Section 2.3]. Adding a marking increases the dimension of the moduli space by 1. By [79, Lemma 2.1], there is a surjective morphism $\psi_R : \bar{\mathcal{R}}_{g;1} \to \bar{\mathcal{R}}_g$ whose fibers are irreducible.

Suppose that $g = g_1 + g_2$, with $g_i \geq 1$. We recall some material about the boundary divisor $\Delta_{g_1:g_2}[\bar{\mathcal{R}}_g]$ from [21, Section 1.4]. This boundary divisor is the image of the clutching map

$$\kappa_{g_1:g_2} : \bar{\mathcal{R}}_{g_1;1} \times \bar{\mathcal{R}}_{g_2;1} \to \bar{\mathcal{R}}_g,$$

defined on a generic point as follows. Let τ_1 be a point of $\bar{\mathcal{R}}_{g_1;1}$ representing $(\pi_1 : C_1' \to C_1, x_1' \mapsto x_1)$ and let τ_2 be a point of $\bar{\mathcal{R}}_{g_2;1}$ representing $(\pi_2 : C_2' \to C_2, x_2' \mapsto x_2)$. Let X

be the curve with components C_1 and C_2, formed by identifying x_1 and x_2 in an ordinary double point. Let Y be the curve with components C_1' and C_2', formed by identifying x_1' and x_2' (resp. $x_1'' = \sigma(x_1')$ and $x_2'' = \sigma(x_2')$) in an ordinary double point. Then $\kappa_{g_1:g_2}(\tau_1, \tau_2)$ is the point representing the unramified double cover $Y \to X$. This is illustrated in Figure 3.1.

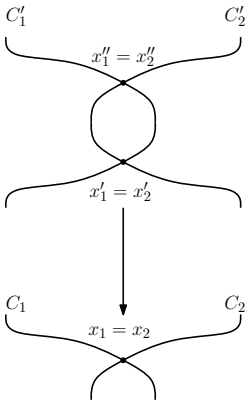


Figure 3.1: $\Delta_{g_1:g_2}$

In [79, Section 3.4.1], the authors analyze the p-rank stratification of this boundary divisor. By [79, Lemmas 3.6-3.7], the clutching morphism restricts to the following:

$$\kappa_{g_1:g_2} : \mathcal{R}_{g_1;1}^{(f_1,f_1')} \times \mathcal{R}_{g_2;1}^{(f_2,f_2')} \to \Delta_{g_1:g_2}[\bar{\mathcal{R}}_g^{(f_1+f_2,f_1'+f_2'+1)}]. \tag{3.20}$$

The following lemma is useful in the inductive arguments in Section 3.7.5.

Lemma 3.7.2. *Suppose that $S_i \subset \mathcal{R}_{g_i}^{(f_i,f_i')}$ has dimension d_i for $i = 1, 2$. Then the dimension of*

$$\mathcal{K} = \kappa_{g_1:g_2}(\psi_R^{-1}(S_1) \times \psi_R^{-1}(S_2))$$

is $d_1 + d_2 + 2$. Furthermore, if S_i is a component of $\mathcal{R}_{g_i}^{(f_i,f_i')}$ for $i = 1, 2$, then $\mathcal{K}$ is contained in a component of $\bar{\mathcal{R}}_g^{(f_1+f_2,f_1'+f_2'+1)}$ whose dimension is at most $d_1 + d_2 + 3$.

3.7.3 Some extra results when $p = 3$

The $p = 3$ case is guaranteed to be more difficult, because $\mathcal{R}_2^{(0,0)}$ and $\mathcal{R}_2^{(1,0)}$ are empty in that case [37, Section 7.1]. In other words, when $p = 3$, if $\pi : Y \to X$ is an unramified double cover of a genus 2 curve such that P_π is non-ordinary, then X is ordinary. This is the key reason why there are extra hypotheses when $p = 3$ in [79, Propositions 6.1, 6.4, Theorem 7.2].

We now have the extra information that all pairs (f, f') occur when $p = 3$ and $g = 3$. In this section, we use this to confirm that the extra hypotheses when $p = 3$ can be removed from most of the results of [79, Sections 6 and 7]. This will allow us to work more uniformly for odd p in the next section.

Let $\tilde{\mathcal{A}}_{g-1}$ denote the toroidal compactification of $\mathcal{A}_{g-1}$. Let $\tilde{\mathcal{A}}_{g-1}^{f'}$ denote the p-rank f' stratum of $\tilde{\mathcal{A}}_{g-1}$. Let $V_g^{f'} = \bar{Pr}_g^{-1}(\tilde{\mathcal{A}}_{g-1}^{f'}) \cap \mathcal{R}_g$,

The next result about the p-rank stratification of $R_3^{(f,1)}$ is true for all $p \geq 5$ by [79, Proposition 6.4].

Lemma 3.7.3. *The result [79, Proposition 6.4] does not require the hypothesis $f \neq 0, 1$ when $p = 3$. In other words, if $p = 3$ and $0 \leq f \leq 3$, then $\Pi^{-1}(\mathcal{M}_3^f)$ is irreducible and $\mathcal{R}_3^{(f,1)} = \Pi^{-1}(\mathcal{M}_3^f) \cap V_3^1$ is non-empty with dimension $2 + f$.*

The next result about non-ordinary Prym varieties is true for all $p \geq 5$ by [79, Theorem 7.1]. We say that P_π is almost ordinary if its p-rank satisfies $f' = g - 2$.

Lemma 3.7.4. *The result [79, Theorem 7.1] does not require the hypothesis $f \geq 2$ when $p = 3$ and $g \geq 3$. In other words, if $p = 3$, $g \geq 3$, and $0 \leq f \leq g$, then $\mathcal{R}_g^{(f,g-2)}$ is non-empty and each of its components has dimension $2g - 4 + f$. More generally, let S be a component of $\mathcal{M}_g^f$, then the locus of points of $\Pi^{-1}(S)$ representing unramified double covers for which the Prym variety P_π is almost ordinary is non-empty and codimension 1 in $\Pi^{-1}(S)$.*

The hypothesis $p \geq 5$ also appears in [79, Corollary 7.3], because a key point of the proof is that $\mathcal{R}_2^{(1,0)}$ and $\mathcal{R}_2^{(0,0)}$ are non-empty, which is false when $p = 3$. We generalize [79, Corollary 7.3] to include the case $p = 3$ in Section 3.7.5.

3.7.4 A dimension result

The following result is also needed in Section 3.7.5.

Proposition 3.7.5. *Let $3 \leq p \leq 19$. Then $\mathcal{R}_3^{(3,0)}$ contains a component of dimension 4 and $\mathcal{R}_3^{(2,0)}$ contains a component of dimension 3.*

3.7.5 Final result

In this section, in characteristic $3 \leq p \leq 19$, we verify the existence of unramified double covers $\pi : Y \to X$ where X has genus g and p-rank f and P_π has p-rank f', for arbitrary g as long as f is bigger than approximately $2g/3$ and f' is bigger than approximately $g/3$. This is most interesting when either $\frac{g}{3} \leq f' < \frac{g}{2} - 1$ or $p = 3$ because [79, Corollary 7.2] resolves the case when $\frac{g}{2} - 1 \leq f' \leq g - 1$ with no conditions on g and f when $p \geq 5$.

We first include an inductive result which holds for any odd prime p. This strengthens [79, Theorem 7.2].

Theorem 3.7.6. *Let f_0 be such that $\mathcal{R}_3^{(f_1,0)}$ has a (non-empty) component of dimension $1 + f_1$ in characteristic p for each f_1 such that $f_0 \leq f_1 \leq 3$.*

Let $g \geq 2$ and write $g = 3r + 2s$ for integers $r, s \geq 0$. Suppose that $rf_0 \leq f \leq g$ (with $f \geq rf_0 + 2s$ when $p = 3$) and $r + s - 1 \leq f' \leq g - 1$.

Then $\mathcal{R}_g^{(f,f')}$ has a (non-empty) component of dimension $g - 2 + f + f'$ in characteristic p.

Corollary 3.7.7. *Let $f_0 = 2$ and $3 \leq p \leq 19$. Let $g \geq 2$ and write $g = 3r + 2s$ for integers $r, s \geq 0$. Suppose that $2r \leq f \leq g$ (with $f \geq 2r + 2s$ when $p = 3$) and $r + s - 1 \leq f' \leq g - 1$.*

Then $\mathcal{R}_g^{(f,f')}$ has a (non-empty) component of dimension $g - 2 + f + f'$ in characteristic p.

In particular, this holds in the following situations:

1. *If $g = 3r$ and (f, f') is such that $2r \leq f \leq g$ and $r - 1 \leq f' \leq g - 1$;*
2. *If $g = 3r + 2$ and (f, f') is such that $2r \leq f \leq g$ and $r \leq f' \leq g - 1$, (with $f \geq 2r + 2$ when $p = 3$);*

3. *If* $g = 3r + 4$ *and* (f, f') *is such that* $2r \leq f \leq g$ *(with* $f \geq 2r + 4$ *when* $p = 3$*) and* $r + 1 \leq f' \leq g - 1$.

Conclusion

Computations of Theta Constants

We aim to compute certain power of the quotient of theta constants of a non-hyperelliptic curve $\mathcal{C}$ of genus g with motivation originated from Weber's formula which is expressing such a power in terms of bitangents of $\mathcal{C}$ when $g = 3$. Although we could not obtain a similar formula for curves of genus strictly bigger than 3 due to complicated geometric and combinatorial structure of the curve, we were able to find a way to compute them algorithmically and algebraically (heuristically). Nevertheless, we have the following question left. Let κ be the canonical divisor. For any fixed $v \in \mathrm{Pic}(\mathcal{C})[2]$, can we find a basis of $\mathcal{L}(\kappa + v)$ by the span of the tensor product of the Riemann-Roch spaces $\{\mathcal{L}(D), \mathcal{L}(D + v)\}$ while $D, D + v$ run through the odd and effective divisors?

On the other hand, one of the challenges of this part is to obtain a 2-level structure of $\mathcal{C}$. We achieved solving this problem in a particular case when $\mathcal{C}$ is a non-hyperelliptic curve of genus 4 by using the algebraic and geometric structure of del Pezzo surfaces. Labelling all the theta characteristic divisors is an important part of getting the structure and is generally difficult. One can overcome it via computations in terms of theta characteristics and 2-torsion points in $\mathrm{Pic}(\mathcal{C})$ but this way is inconvenient. One further direction would be to study the labelling problem in terms of extrinsic geometric data for a generic curve of genus $g \geq 4$.

In order to experiment the algorithm, we work out the rich geometric structure of curves of genus 4. This gave some ways to certain questions. One of such motivating problems is the reconstruction of the curve from its multitangents. This problem goes back to Aronhold and Coble. They provided formulas for non-hyperelliptic curves of genus 3 to recover the curve from its 7 bitangents corresponding to an Aronhold basis [24, 32]. Recently, several directions have shown up such as working on weakening the condition of being labelled for the bitangents [17, 66], also a generalization of the result to higher genus [16] and abelian varieties [46, 47]. However, even for genus 4, the results are not effective. Finally, Lehavi gave an effective result for generic curves of genus 4 [67]. In a joint work with Avinash Kulkarni, Yue Ren and Mahsa Sayyary Namin, we give several algorithms related to non-hyperelliptic curves of genus 4, including an implementation of the effective result of Lehavi by extending his result. Another problem is an appropriate generalisation of the bitangent matrix for a non-hyperelliptic curve of genus 3 [28] to the case of genus 4.

Kummer Based Hyperelliptic Curve Cryptography

Our work [42] is the first hardware implementation of Kummer-based HECC solution for 128-bit security level. Several architectures with different amount of internal parallelism have been optimised and fully implemented on 3 different FPGAs. The obtained results lead to similar speed than the best curve based solutions for embedded systems but with

an area almost divided by 2 (-40% for DSP and RAM blocks and -60% for logic slices). The results were obtained with generic prime fields and fully programmable architectures.

p-rank Computations

We have shown that $\mathcal{R}_3^{(2,0)}$ has dimension 3 for $3 \leq p \leq 19$; more specifically, that there is a 3-dimensional family of smooth plane quartics X with p-rank 2 having an unramified double cover $\pi : Y \to X$ such that P_π has p-rank 0 for $3 \leq p \leq 19$. We expect this to be true for all odd primes p but were only able to prove it computationally for $3 \leq p \leq 19$.

Bibliography

[1] J. D. Achter and R. Pries. Monodromy of the p-rank strata of the moduli space of curves. *International Mathematics Research Notices. IMRN*, 2008:rnn053, 2008.

[2] J. D. Achter and R. Pries. The p-rank strata of the moduli space of hyperelliptic curves. *Advances in Mathematics*, 227(5):1846–1872, 2011.

[3] H. Alrimeih and D. N. Rakhmatov. Fast and flexible hardware support for ECC over multiple standard prime fields. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 22:2661–2674, 2014.

[4] E. Arbarello, M. Cornalba, P. Griffiths, and J. D. Harris. *Geometry of Algebraic Curves*, volume 1 of *267*. Springer-Verlag, New York, 1 edition, 1985.

[5] L. Batina, N. Mentens, B. Preneel, and I. Verbauwhede. Flexible hardware architectures for curve-based cryptography. In *IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, pages 4839–4842. IEEE, 2006.

[6] A. Beauville. Prym varieties: a survey. In *Theta functions–Bowdoin 1987*, volume 49 of *Proceedings Symposia Pure Applied Mathematics*, pages 607–620. American Mathematical Society, Providence, RI, 1989.

[7] O. Bergvall. *Cohomology of arrangements and moduli spaces*. PhD thesis, Stockholm University, 2016.

[8] D. J. Bernstein and T. Lange. Explicit-formulas database. `https://hyperelliptic.org/EFD/`.

[9] D. J. Bernstein and T. Lange. Hyper-and-elliptic-curve cryptography. *LMS Journal of Computation and Mathematics*, 17(A):181–202, 2014.

[10] O. Bolza. The partial differential equations for the hyperelliptic θ- and σ-functions. *American Journal of Mathematics*, 21(2):107–125, 1899.

[11] J. W. Bos, C. Costello, H. Hisil, and K. Lauter. Fast cryptography in genus 2. *Journal of Cryptology*, 29(1):28–60, 2016.

[12] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[13] I. Bouw. The p-rank of ramified covers of curves. *Compositio Mathematica*, 126(3):295–322, 2001.

[14] N. Bruin. The arithmetic of Prym varieties in genus 3. *Compositio Mathematica*, 144(2):317–338, 2008.

[15] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48(177):95–101, 1987.

[16] L. Caporaso and E. Sernesi. Characterizing curves by their odd Theta-characteristics. *Journal für die reine und angewandte Mathematik*, 2003:101–135, 2002.

[17] L. Caporaso and E. Sernesi. Recovering plane curves from their bitangents. *Journal of Algebraic Geometry*, 12(2):225–244, 2003.

[18] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, New York, 1996.

[19] T. O. Celik, Y. Elias, B. Güneş, R. Newton, E. Ozman, R. Pries, and L. Thomas. Non-ordinary curves with a Prym variety of low p-rank. In *Women in Numbers Europe II*, pages 117–158. Springer International Publishing, 2018.

[20] T. O. Celik, A. Kulkarni, Y. Ren, and M. Sayyary Namin. Tritangents and their space sextics. arXiv:1805.11702.

[21] A. Chiodo, D. Eisenbud, G. Farkas, and F. Schreyer. Syzygies of torsion bundles and the geometry of the level ℓ modular variety over $\overline{\mathcal{M}}_g$. *Inventiones Mathematicae*, 194(1):73–118, 2013.

[22] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385 – 434, 1986.

[23] P. N. Chung, C. Costello, and B. Smith. Fast, uniform scalar multiplication for genus 2 Jacobians with fast Kummers. In *Selected Areas in Cryptography – SAC 2016*, pages 465–481. Springer International Publishing, 2017.

[24] A. B. Coble. *Algebraic Geometry and Theta Functions*. American Mathematical Society, 1961.

[25] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2006.

[26] R. Cosset. *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*. PhD thesis, Nancy 1, 2011.

[27] P. Cragnolini and P. A. Oliverio. Lines on del Pezzo surfaces with in characteristic $\neq 2$. *Communications in Algebra*, 27(3):1197–1206, 1999.

[28] F. Dalla Piazza, A. Fiorentino, and R. Salvati Manni. Plane quartics: the universal matrix of bitangents. *Israel Journal of Mathematics*, 217:111–138, 2017.

[29] M. Demazure. Surfaces de del Pezzo. In *Séminaire sur les Singularités des Surfaces*, pages 23–69. Springer, Berlin, Heidelberg, 1980.

[30] The Sage Developers. *SageMath, the Sage Mathematics Software System*, 2017. `http://www.sagemath.org`.

[31] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 2006.

[32] I. V. Dolgachev. *Classical Algebraic Geometry: A Modern View*. Cambridge University Press, 2012.

[33] S. Duquesne. Montgomery scalar multiplication for genus 2 curves. In *6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004, Proceedings*, volume 3076, pages 153–168. Springer-Verlag, Berlin, Heidelberg, 2004.

[34] A. Eisenmann and H. M. Farkas. An elementary proof of Thomae's formulae. *Online Journal of Analytic Combinatorics [electronic only]*, 3, 2008.

[35] G. Elias, A. Miri, and T. H. Yeap. On efficient implementation of FPGA-based hyperelliptic curve cryptosystems. *Computers and Electrical Engineering*, 33(5):349 – 366, 2007. Security of Computers and Networks.

[36] V. Z. Enolski and T. Grava. Thomae type formulae for singular $\mathbb{Z}_N$ curves. *Letters in Mathematical Physics*, 76(2):187–214, 2006.

[37] C. Faber and G. van der Geer. Complete subvarieties of moduli spaces and the Prym map. *Journal für die reine und angewandte Mathematik*, 573:117–137, 2004.

[38] J. Fan, L. Batina, and I. Verbauwhede. HECC goes embedded: An area-efficient implementation of HECC. In *Selected Areas in Cryptography*, pages 387–400. Springer, Berlin, Heidelberg, 2009.

[39] H. Farkas, S. Grushevsky, and R. Salvati Manni. An explicit solution to the weak Schottky problem. `https://arxiv.org/abs/1710.02938`, 2017.

[40] J. Fay. *On the Riemann-Jacobi Formula*. 2]: [Nachrichten der Akademie der Wissenschaften in Göttingen. Vandenhoeck & Ruprecht, 1979.

[41] L. I. Fuchs. Über die Form der Argumente der Thetafunction und über die Bestimmung von $\vartheta(0, 0...0)$ als Function der Klassenmoduln. *Journal für die reine und angewandte Mathematik*, 73:305–324, 1871.

[42] G. Gallin, T. O. Celik, and A. Tisserand. Architecture level optimizations for Kummer based HECC on FPGAs. In *IndoCrypt 2017 - 18th International Conference on Cryptology in India*, volume 10698 of *International Conference in Cryptology in India : Progress in Cryptology – INDOCRYPT 2017*, pages 44–64. Springer, 2017.

[43] P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie*. PhD thesis, L'École Polytechnique, 2000.

[44] P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007.

[45] P. Griffiths and J. Harris. *Principles of Algebraic Geometry*. Wiley-Interscience, 1978.

[46] S. Grushevsky and R. Salvati Manni. Gradients of odd theta functions. *Journal für die reine und angewandte Mathematik*, 2004(573):45–59, 2006.

[47] S. Grushevsky and R. Salvati Manni. Theta functions of arbitrary order and their derivatives. *Journal für die reine und angewandte Mathematik*, 2006(590):31–43, 2006.

[48] J. Guàrdia. On the Torelli problem and Jacobian Nullwerte in genus three. *The Michigan Mathematical Journal*, 60(1):51–65, 2011.

[49] T. Güneysu and C. Paar. Ultra high performance ECC over NIST primes on commercial FPGAs. In *Cryptographic Hardware and Embedded Systems – CHES 2008*, pages 62–78. Springer, Berlin, Heidelberg, 2008.

[50] B. H. Gross and J. Harris. On some geometric constructions related to theta characteristics. In *Contributions to Automorphic Forms, Geometry, and Number*. Johns Hopkins University Press, 2004.

[51] J. Harris. Theta-characteristics on algebraic curves. *Transactions of the American Mathematical Society*, 271(2):611–638, 1982.

[52] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, Heidelberg, 1977.

[53] T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Mathematica*, 57(2):127–152, 1986.

[54] J. I. Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics, Second Series*, 72:612–649, 1960.

[55] H. Kim, T. Wollinger, Y. Choi, K. Chung, and C. Paar. Hyperelliptic curve coprocessors on a FPGA. In *Information Security Applications*, pages 360–374. Springer, Berlin, Heidelberg, 2005.

[56] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989.

[57] S. Koizumi. Remarks on Takase's paper "a generalization of Rosenhain's normal form with an application". *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 73(1):12–13, 1997.

[58] J. Kollar. *Rational Curves on Algebraic Varieties*, volume 32. Springer-Verlag, Berlin, Heidelberg, 1 edition, 1996.

[59] M. Kudo and S. Harashita. Superspecial curves of genus 4 in small characteristic. *Finite Fields and Their Applications*, 45:131–169, 2017.

[60] A. Kulkarni, Y. Ren, M. Sayyary Namin, and B. Sturmfels. Real space sextics and their tritangents. `https://arxiv.org/abs/1712.06274`, to appear in the Proceedings of ISSAC 2018, 2017.

[61] P. L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48:243–243, 1987.

[62] Labex COMIN Labs. Hardware and arithmetic for hyperelliptic curves cryptography. `https://h-a-h.cominlabs.u-bretagneloire.fr`.

[63] J. Y. Lai, Y. S. Wang, and C. T. Huang. High-performance architecture for elliptic curve cryptography over prime fields on FPGAs. *Interdisciplinary Information Sciences*, 18(2):167–173, 2012.

[64] T. Lange. Montgomery addition for genus two curves. In *Algorithmic Number Theory*, volume 3076, pages 309–317. Springer, Berlin, Heidelberg, 2004.

[65] T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 15(5):295–328, 2005.

[66] D. Lehavi. Any smooth plane quartic can be reconstructed from its bitangents. *Israel Journal of Mathematics*, 146(1):371–379, 2005.

[67] D. Lehavi. Effective reconstruction of generic genus 4 curves from their theta hyperplanes. *International Mathematics Research Notices*, 2015(19):9472–9485, 2015.

[68] J. López and R. Dahab. Fast multiplication on elliptic curves over GF($2m$) without precomputation. In *Cryptographic Hardware and Embedded Systems*, pages 316–327. Springer, Berlin, Heidelberg, 1999.

[69] D. Lubicz and D. Robert. Arithmetic on abelian and Kummer varieties. *Finite Fields and Their Applications*, 39:130 – 158, 2016.

[70] Y. Ma, Z. Liu, W. Pan, and J. Jing. A high-speed elliptic curve cryptographic processor for generic curves over GF(p). In *Revised Selected Papers on Selected Areas in Cryptography – SAC 2013 - Volume 8282*, pages 421–437. Springer-Verlag, New York, 2014.

[71] Yu. I. Manin. *Cubic forms; Algebra, Geometry, Arithmetic.* Elsevier, 2 edition, 1989.

[72] A. J. Menezes, Y. Wu, and R. J. Zuccherato. An elementary introduction to hyperelliptic curves. In *Algebraic Aspects of Cryptography.* Springer-Verlag, Berlin, Heidelberg, 1998.

[73] D. Mumford. On the equations defining abelian varieties. I. *Inventiones mathematicae*, 1:287–354, 1966.

[74] D. Mumford. *Tata Lectures on Theta I*, volume 28. Birkhäuser Basel, 1 edition, 1983.

[75] D. Mumford. *Tata Lectures on Theta II.* Birkhäuser Basel, 2007.

[76] D. Mumford. *Tata Lectures on Theta II.* Modern Birkhäuser Classics, 2007.

[77] E. Nart and C. Ritzenthaler. A new proof of a Thomae-like formula for non hyperelliptic genus 3 curves. In *Arithmetic, geometry, cryptography and coding theory*, volume 686 of *Contemporary Mathematics*, pages 137–155. American Mathematical Society, 2017.

[78] K. Okeya and K. Sakurai. Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve. In *Cryptographic Hardware and Embedded Systems — CHES 2001*, pages 126–141. Springer, Berlin, Heidelberg, 2001.

[79] E. Ozman and R. Pries. On the existence of ordinary and almost ordinary Prym varieties. to appear in Asian Journal of Math, 2017. http://arxiv.org/abs/1502.05959.

[80] H. E. Rauch and H. M. Farkas. *Theta functions with applications to Riemann surfaces.* Baltimore : Williams & Wilkins, 1974.

[81] J. Renes, P. Schwabe, B. Smith, and L. Batina. μKummer: efficient hyperelliptic signatures and key exchange on microcontrollers. In *Cryptographic Hardware and Embedded Systems – CHES 2016*, volume 9813 of *Cryptographic Hardware and Embedded Systems – CHES 2016*, page 20. IACR, Springer-Verlag, 2016.

[82] B. Riemann. Theorie der Abel'schen Functionen. *Journal für die reine und angewandte Mathematik*, 54:101–155, 1857.

[83] B. Riemann. Über das Verschwinden der ϑ-Functionen. *Journal für die reine und angewandte Mathematik*, 65:161–172, 1866.

[84] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic Number Theory Symposium (ANTS)*, 2004.

[85] C. Rocchini. Claudio Rocchini's Home Page. `http://www.rockini.name`.

[86] G. Rosenhain. Abhandlung über die Functionen zweier Variabler mit vier Perioden. *Ostwald's Klassiker der Exacten Wissenschaften*, 65, 1895.

[87] K. Sakiyama, L. Batina, B. Preneel, and I. Verbauwhede. Superscalar coprocessor for high-speed curve-based cryptography. In *Cryptographic Hardware and Embedded Systems - CHES 2006*, pages 415–429. Springer, Berlin, Heidelberg, 2006.

[88] R. Salvati Manni. Modular varieties with level 2 theta structure. *American Journal of Mathematics*, 116(6):1489–1511, 1994.

[89] J. P. Serre. Sur la topologie des variétés algébriques en caractéristique p. In *Symposium internacional de topología algebraica*, pages 24–53. Universidad Nacional Autónoma de México and UNESCO, 1958.

[90] A. Sghaier, C. Massoud, M. Zeghid, and M. Machhout. Flexible hardware implementation of hyperelliptic curves cryptosystem. *International Journal of Computer Science and Information Security*, 14(4):1, 2016.

[91] N. Shepherd-Barron. Thomae's formulae for non-hyperelliptic curves and spinorial square roots of theta-constants on the moduli space of curves. `https://arxiv.org/abs/0802.3014`, 2008.

[92] K. O. Stöhr and J. F. Voloch. A formula for the Cartier operator on plane algebraic curves. *Journal für die reine und angewandte Mathematik*, 377:49–64, 1987.

[93] K. Takase. A generalization of Rosenhain's normal form for hyperelliptic curves with an application. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 72(7):162–165, 1996.

[94] J. Thomae. Beitrag zur Bestimmung von $\vartheta(0, 0, ...0)$ durch die Klassenmoduln algebraischer Funktionen. *Journal für die reine und angewandte Mathematik*, 71:201–222, 1870.

[95] A. Verra. The fibre of the Prym map in genus three. *Mathematische Annalen*, 276(3):433–448, 1987.

[96] H. Weber. *Theorie der Abel'schen Funktionen vom Geschlecht 3.* 1876.

[97] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(435-458), 2003.

[98] W. Wirtinger. *Untersuchungen über Thetafunctionen*. B. G. Teubner, Leipzig, 1895.

[99] T. Wollinger. *Software and hardware implementation of hyperelliptic curve cryptosystems*. PhD thesis, Ruhr University Bochum, 2004.

[100] N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *Journal of Algebra*, 52(2):378–410, 1978.

[101] Yu. G. Zarhin. Del Pezzo surfaces of degree 1 and Jacobians. *Mathematische Annalen*, 340(2):407–435, 2008.

[102] O. Zariski. On hyperelliptic ϑ-functions with rational characteristics. *American Journal of Mathematics*, 50(3):315–344, 1928.

Abstract

Algebraic curves are central objects in algebraic geometry. In this thesis, we consider these objects from different angles in algebraic geometry such as computational algebraic geometry and arithmetic geometry. In the first chapter, we study non-hyperelliptic curves of genus g and their Jacobians linked via theta characteristic divisors. Such divisors provide extrinsic geometric properties which allow us to compute theta constants. In the second chapter, we focus on hyperelliptic curves of genus 2 and the associated Kummer surface with a cryptographic motivation. In the third and final chapter, we examine unramified double covers of non-hyperelliptic curves of genus g to obtain information about the p-rank.

Résumé

Les courbes algébriques sont des objets centraux de la géométrie algébrique. Dans cette thèse, nous étudions ces objets sous différents angles de la géométrie algébrique tels que la géométrie algébrique effective et la géométrie arithmétique. Dans le premier chapitre, nous étudions les courbes non-hyperelliptiques de genre g et leurs jacobiennes liées par l'intermédiaire de diviseurs thêta caractéristiques. Ces derniers contiennent des propriétés géométriques extrinsèques qui permettent de calculer les constantes thêta. Dans le deuxième chapitre, nous nous concentrons sur les courbes hyperelliptiques de genre 2 et leur surface de Kummer associée avec une motivation cryptographique. Dans le troisième et dernier chapitre, nous étudions les revêtements doubles non-ramifiés des courbes non-hyperelliptiques de genre g pour obtenir des informations sur le p-rang.