Utrecht University

Faculty of Science

Mathematical Sciences

Supersingular curves of genera four and five in characteristic two

Supervisor:
Prof. dr. Carel Faber

Author:
Dušan Dragutinović

Second reader:
Dr. Valentijn Karemaker

Abstract

Consider the curves of genus $g > 0$ and (principally polarized) abelian varieties of dimension $g > 0$, all defined over a field k of positive characteristic $p > 0$. Denote with $\mathcal{M}_g$ and $\mathcal{A}_g$ respectively their moduli spaces - the spaces that parametrize isomorphism classes of these. The assignment $C \mapsto \mathcal{J}_C$, where a curve of genus g is sent to its Jacobian, that is a principally polarized abelian variety of dimension g, gives rise to the Torelli morphism $\mathcal{M}_g \to \mathcal{A}_g$. An abelian variety A of dimension $g > 0$ is supersingular if it is isogenous to E^g where E is a supersingular elliptic curve over k, that is $E[p](\bar{k}) = \{O\}$. A curve of genus $g > 0$ is supersingular if its Jacobian is supersingular as an abelian variety. There are some invariants used to better understand $\mathcal{M}_g$ and $\mathcal{A}_g$, and in particular, to understand the loci of supersingular curves and principally polarized abelian varieties such as p-rank, Ekedahl-Oort type, and Newton polygon. For $g = 4, 5$, and $p = 2$, we discuss the irreducibility of the supersingular locus $\mathcal{S}_g$ in $\mathcal{A}_g$. Further, we describe a piece of geometry related to the intersection of $\mathcal{S}_4$ with the locus of non-hyperelliptic curves in $\mathcal{M}_4$ in $\mathcal{A}_4$. Lastly, inspired by the paper [49] that (algorithmically) determined all the non-isomorphic curves of genus $g = 4$ defined over a field with two elements, we discuss a similar problem for $g = 5$.

Acknowledgements

First and foremost, I would like to thank my supervisor Carel Faber. His guidance and support in the challenging moments have been precious and irreplaceable to me. I have truly been enjoying the topic he suggested to me and our work on it. Secondly, I would like to thank Valentijn Karemaker, my second reader, for her careful reading and the comments and suggestions.

I am grateful to Utrecht University on the Utrecht Excellence Scholarship for offering me this wonderful experience during these two years. I thank Roelof Bruggeman for a warm welcome on my first group project at the master's studies and some valuable conversations. Furthermore, I thank all the professors I met in the Mastermath program and at Utrecht University. Their expertise had a strong influence on me. I thank Martijn Kool also for his help.

I thank Stevan Gajović and Dušan Joksimović for giving me a lot of advice on living abroad and for pointing me out to Utrecht University in the first place.

I am thankful to Lazar Mitrović for his help in advancing the efficiency of codes for computing non-hyperelliptic non-trigonal curves of genus 5 over $\mathbb{F}_2$ and his general support. Also, I would like to thank Miljan Zarubica and Milan Ogrizović for their unconditional support on my life path.

Finally, I would like to thank my family - Dragana, Darko, and Ana for everything.

Contents

Introduction

An elliptic curve E over a field k of characteristic p is supersingular by definition if the set of geometric points of E, i.e., the $\bar{k}$-points of E with $\bar{k}$ an algebraic closure of k, that are of order p (in the group sense) is empty. A supersingular abelian variety A of dimension g over k is an abelian variety isogenous to E^g for E a supersingular elliptic curve. We say that a curve is supersingular if its Jacobian is. Investigating the supersingular objects will be the main focus of this thesis. Throughout the text, we discuss some standard algebro-geometric results that are relevant for the considered questions to present some of the well-known results as well as some recent ones. Furthermore, we will present some of the conclusions we obtained.

There are several invariants used to describe the parametrizing spaces of principally polarized abelian varieties $\mathcal{A}_g$ of a fixed dimension and curves $\mathcal{M}_g$ of a fixed genus. Some of them are the p-rank, Newton polygon, and the Ekedahl-Oort type. Understanding them is related to understanding the supersingular loci in the mentioned moduli spaces - Supersingular abelian varieties are always of p-rank zero, have the supersingular Newton polygon, and the possibilities for their Ekedahl-Oort type are restricted. For working with the supersingular locus inside $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ for p arbitrary, some theory got developed and a lot of results are known. Here, we are primarily interested in the supersingular locus inside the moduli space $\mathcal{M}_4 = \mathcal{M}_4 \otimes \overline{\mathbb{F}}_2$ of curves of genus four in characteristic two. The main difference when working with curves is that there are no universal tools for answering some of the algebro-geometric questions, such as irreducibility and computing the dimension of the supersingular locus, as well as for deciding, for example, which Ekedahl-Oort types are possible for suspersingular curves.

The problems we considered in this text are inspired by the paper [49]. There, Xarles algorithmically determined a whole set of representatives of non-isomorphic curves of genus four defined over a field with two elements. Working with the obtained data and extracting the relevant information from it, some questions arose regarding the non-hyperelliptic supersingular curves of genus four in characteristic two, but also about the whole supersingular locus in the moduli space of curves of genus four in characteristic two too. There is also a natural question of considering a similar problem as Xarles did for curves of genus five. One of the perks of working in characteristic two is that considering objects defined over the finite field with two elements and using mathematical software for the reasonably demanding computations could lead to getting an intuition of what could happen for all supersingular objects in characteristic two. On the other hand, working in characteristic two is somehow different and requires special attention.

In the first section, we discuss the background. We introduce the notions of abelian varieties and the Jacobians of curves and mention some of their important properties. Then, describing moduli problems in general, we discuss the questions of the existence of $\mathcal{A}_g$ and $\mathcal{M}_g$ and the difference between the types of the possible solutions to the moduli problems.

In section two, we discuss the mentioned invariants used to understand $\mathcal{A}_g$ and $\mathcal{M}_g$ better. We compare the results obtained in the case of each invariant individually and present the important techniques used to work with $\mathcal{A}_g$ and $\mathcal{M}_g$. At the end of the section, we collect some of the relevant results obtained in the preceding years.

The third section contains some information regarding the supersingular locus in $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ for p an arbitrary prime number. We present there some of the tools used to describe this locus, for example, to compute its number of irreducible components via determining certain class numbers and to compute its dimension. After presenting these well-known results, we discuss the irreducibility of the supersingular locus in $\mathcal{A}_4 = \mathcal{A}_4 \otimes \overline{\mathbb{F}}_2$ using mass formulas, and present similar examples for higher g in characteristic two.

In the fourth section, we describe the supersingular locus in $\mathcal{M}_4 = \mathcal{M}_4 \otimes \overline{\mathbb{F}}_2$. For getting the intuition of the geometry occurring over $\overline{\mathbb{F}}_2$, we use Xarles's paper mentioned above. In particular, the data tells us that there is no non-hyperelliptic supersingular curve of genus 4 over $\mathbb{F}_2$ that lies on a quadric cone. Motivated by that, we discuss the intersection of the supersingular locus with the locus of non-hyperelliptic curves lying on a quadric cone over $\overline{\mathbb{F}}_2$.

Lastly, in the fifth section, we discuss the problem of determining the representatives of non-isomorphic curves of genus five over a field with two elements. We do that separately for the hyperelliptic curves, the trigonal curves, and the complete intersections of three quadrics in $\mathbb{P}^4$.

For parts of the arguments we used in proving certain results, we worked in the mathematical software SageMath, and we collect these codes in the appendix. We also used SageMath for the purposes of the final section as well as for getting some examples, and we present them on `https://github.com/DusanDragutinovic/MT_Curves`.

Conventions

We will extensively use the language of algebraic geometry of varieties and schemes and sheaves that can be found in [15], Sections I and II. Taking that into account, we will need to presume the knowledge of some basic notions and constructions.

Let k be any field and $\bar{k}$ its algebraic closure. For us, a **curve** over k is a projective, non-singular algebraic variety over $\bar{k}$ of dimension 1, that is defined by polynomials with coefficients in k; being projective in this situation is equivalent to being complete. Alternatively, a curve over k is a separated scheme of finite type over k, such that $C_{\bar{k}} = C \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\bar{k})$ is an integral and non-singular scheme. The **genus** of a curve C is the number

$$g(C) = \dim_k H^1(C, \mathcal{O}_C).$$

Formally, this is the definition of *geometric genus* of C, which in our setting matches with the arithmetic genus of C. With $\kappa(C)$, we denote the **function field** of C, that is the local ring of C at a generic point using the language of schemes. An important class of curves are hyperelliptic curves, that exist in any genus and over an arbitrary field. We say that a curve C of genus $g \geq 2$ is **hyperelliptic** if there is a morphism $f : C \to \mathbb{P}^1$ of degree 2, that is $[\kappa(C) : \kappa(\mathbb{P}^1)] = 2$.

For any field l that is an extension of k, we define $C(l)$ the **set of l-points of C** to be the set of all morphisms of schemes $\mathrm{Spec}(l) \to C$.

The **divisors** on a curve C for us are elements of form $D = \sum_{i=1}^{N} n_i P_i$ for some $N \in \mathbb{Z}_{>0}, n_i \in \mathbb{Z}$ where $P_i \in C(\bar{k})$ are points on C, i.e., the Weil divisors. The degree of a divisor D is

$$\deg D = \sum_{i=1}^{N} n_i \deg P_i,$$

with $\deg P_i = [\kappa(P_i) : k]$. If $k = \bar{k}$, then $\kappa(P) = k$ for any point $P \in C(\bar{k})$ so $\deg P = 1$. Note that since C is non-singular, $D \mapsto \mathcal{O}_C(D)$ induces an isomorphism between the group of divisors modulo linear equivalence and the group of invertible sheaves modulo isomorphisms; we use the notation $\mathrm{Pic}(C)$ for these groups and call it the **Picard group** of C. Since the sheaf of differentials Ω_C^1 on C is an invertible sheaf on C, there is the linear equivalence class K_C, called the **canonical divisor**, such that $\Omega_C^1 \cong \mathcal{O}(K_C)$.

1 General setting

Here, we set the background of the theory this thesis will discuss. To investigate the supersingular curves and abelian varieties in the next sections, we first need to introduce the notions of abelian varieties, the Jacobians of curves, as well as to at least intuitively understand what the moduli spaces of principally polarized abelian varieties of dimension g and of curves of genus g for some fixed $g \in \mathbb{Z}_{>2}$ are.

1.1 On abelian varieties and Jacobians of curves

As a motivation consider the example that follows. For an elliptic curve E over $\overline{\mathbb{F}}_2$, with $\mathcal{J}_E$ we denote the subgroup of $\operatorname{Pic}(E)$ consisting of the divisors of degree zero.

Example 1.1 (An elliptic curve over $\overline{\mathbb{F}}_2$). *Let $E : y^2 + y = x^3$ be an elliptic curve over $\overline{\mathbb{F}}_2$. To say that E is an elliptic curve is nothing more but to say that it is a 1-pointed curve of genus $g = 1$. Apart from being a curve, it is well-known that E possesses a group structure, and we will show that such structure can be inherited by its Jacobian $\mathcal{J}_E$.*

Let O be an arbitrary point in $E(\overline{\mathbb{F}}_2)$, without loss of generality the point at infinity. Consider the map

$$E(\overline{\mathbb{F}}_2) \to \mathcal{J}_E, P \mapsto [P - O]$$

and let us show that it is a bijection. The Riemann-Roch theorem gives us that for any $D \in \mathcal{J}_E$, if we write K_E for a canonical divisor, we have

$$\dim_{\overline{\mathbb{F}}_2} H^0(E(\overline{\mathbb{F}}_2), D + O) = \dim_{\overline{\mathbb{F}}_2} H^0(E(\overline{\mathbb{F}}_2), K_E - D - O) + 1 - g(E) + \deg(D + O) = 1, \qquad (1)$$

using that $\deg K_E = 2 - 2g(E) = 0 \implies \deg(K_E - D - O) < 0$, *so* $\dim_{\overline{\mathbb{F}}_2} H^0(E(\overline{\mathbb{F}}_2), K_E - D - O) = 0$. *For the surjectivity, consider any $D \in \mathcal{J}_E$ and note that $D + O$ is a divisor of degree 1. The formula (1) gives us that we can change D with some linearly equivalent class, to get that $D + O$ is effective. Thus $D + O = P$ for some $P \in E(\overline{\mathbb{F}}_2)$. For the injectivity, suppose that $P, Q \in E(\overline{\mathbb{F}}_2)$ are two points such that $[P - O] = [Q - O]$ in $\mathcal{J}_E$, i.e., $Q = P + div(f)$ for some $f \in \kappa(E)$. Let $D = P - O$ and get by the previous $H^0(E(\overline{\mathbb{F}}_2), D + O) = \langle 1 \rangle_{\overline{\mathbb{F}}_2}$ since it is 1-dimensional. Since $D + O = P$ and $D + O + div(f) = Q \geq 0$, we obtain $f = c \cdot 1$ for some $c \in \overline{\mathbb{F}}_2$. Hence, $P = Q$.*

By the previous, an elliptic curve is at the same time a curve of genus $g = 1$ and a group. Considering it as a 1-dimensional object with group structure leads to the generalization to the higher-dimensional objects with a group structure that we call the abelian varieties. We discuss them shortly and mention some of the important properties. On the other hand, we will also see a natural way to attach to any curve with higher genus $g \geq 1$ an abelian variety of dimension $g \geq 1$. In this fashion, we will have a unified framework in which we will work.

1.1.1 Abelian varieties

The main reference for this section are Milne's notes [30].

Definition 1. *We say that a **group variety** over a field k is a variety V over k together with morphisms*

$$m : V \times V \to V \text{ (multiplication)}, \quad inv : V \to V \text{ (inverse)},$$

*and an element $e \in V(k)$ such that the structure on $V(\bar{k})$ defined by m and inv is a group structure with identity element $e = e_V$. A group variety A is an **abelian variety** if A is complete.*

We list a few basic properties of abelian varieties below.

- A group variety (and hence an abelian variety) is non-singular.
- The group law on an abelian variety is commutative.
- Every abelian variety is projective.

Even though these properties are fundamental, the proofs of the latter two, as well as some of the claims below, are completely nontrivial and require some technical work. The first property is a consequence of the fact that for any variety, there is an open non-empty subvariety that is non-singular. Using the translates of that subvariety, we can cover the whole variety to see that it is non-singular. It also holds that the set of points $V(R)$ for an arbitrary k-algebra R gets a group structure that depends functorially on R.

Definition 2. *A* ***homomorphism*** *$f : A \to B$ of abelian varieties is a morphism of varieties and also a group homomorphism. We define the* ***kernel*** *of f as $\ker(f) = f^{-1}(e_B)$, with e_B the neutral element of B. Lastly, a homomorphism f is an* ***isogeny*** *if it is surjective and has finite kernel.*

We sum up the equivalent statements of a morphism being an isogeny below.

Proposition 1.2 ([30], Proposition 8.1)**.** *For a morphism $f : A \to B$ of abelian varieties, the following are equivalent:*

1. *f is an isogeny.*
2. *$\dim A = \dim B$ and f is surjective.*
3. *$\dim A = \dim B$ and $\ker(f)$ is a finite group scheme.*
4. *f is a finite, flat and surjective morphism.*

We define the **degree** of an isogeny $f : A \to B$ as the degree of the function field extension $[\kappa(A) : \kappa(B)]$. If $g : B \to C$ is another isogeny, then we have $\deg(g \circ f) = \deg(g)\deg(f)$.

Consider the map

$$[n]_A : A \to A, P \mapsto \underbrace{P + \ldots + P}_{n},$$

that is an isogeny of degree $n^{2\dim A}$. If $n = \deg(f)$, then $\ker(f) \subseteq \ker([n]_A)$, and thus we can factor $[n]_A$ as $[n]_A = h \circ f$ for $h : B \to A$ an isogeny. This also shows that the isogeny is an equivalence relation.

For an abelian variety, it turns out that $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ is a finite-dimensional algebra over $\mathbb{Q}$. The investigation of that object is based on decomposing the abelian varieties into some more elementary parts. Using [30], Proposition 12.1, we can decompose an abelian variety A in some simple abelian varieties. We say that an abelian variety is **simple** if it does not have any proper nonzero subvarieties. The mentioned Proposition implies that for any abelian variety A, there are non-isogenous simple abelian varieties A_i and $r_i \in \mathbb{Z}_{>0}$, so that

$$A \sim \prod_{i=1}^{n} A_i^{r_i},$$

and this decomposition is unique up to isogeny.

Example 1.3 (Frobenius morphism)**.** *An important endomorphism on an abelian variety A in positive characteristic p is the* ***Frobenius morphism****. We use [46] as a reference, and give general definitions that we will apply to the cases of our interest.*

For a scheme X of characteristic p, that is all the local rings of X contain $\mathbb{F}_p$, we define the ***absolute Frobenius morphism*** *$F = F_X : X \to X$ by:*

1. *F is the identity on the underlying topological space of X,*

2. *$F^{\#} : \mathcal{O}_X \to \mathcal{O}_X$ is given on sections by $f \mapsto f^p$.*

In the case of an abelian variety A, $F = F_A$ is an isogeny of the degree $p^{\dim A}$. We also cite that there is an isogeny $V = V_A : A \to A$ called the ***absolute Verschiebung morphism*** *so that $V \circ F = [p]$ on A.*

If $\phi : X \to Y$ is a morphism of schemes of chacteristic p, the following diagram is commutative.

$$\begin{tikzcd}
X \arrow[r, "F_X"] \arrow[d, "\phi"] & X \arrow[d, "\phi"] \\
Y \arrow[r, "F_Y"] & Y
\end{tikzcd}$$

When $\pi : X \to S$ is an S-scheme, then the absolute Frobenius on X is not an S-morphism in general. A variation in this case is that we first define the scheme $X^{(p/S)}$ to be the fiber product $X^{(p/S)} = X \times_{F_S, S} S$ so that the following diagram is cartesian

$$\begin{tikzcd}
X^{(p/S)} \arrow[r, "h"] \arrow[d, "\pi^{(p)}"] \arrow[dr, phantom, "\ulcorner", very near start] & X \arrow[d, "\pi"] \\
S \arrow[r, "F_S"] & S
\end{tikzcd},$$

with $\pi^{(p)} : X^{(p/S)} \to S$ a pullback of $\pi : X \to S$ via $F_S : S \to S$. Then, by the universal property of the fiber product and using the morphisms $F_X : X \to X$ and $\pi : X \to S$, we get a unique morphism $F_{X/S} : X \to X^{(p/S)}$ which we call ***the relative Frobenius morphism****. Similarly, there is* ***the relative Verschiebung morphism*** *$V_{X/S} : X^{(p/S)} \to X$ of S-schemes so that $V_{X/S} \circ F_{X/S} = [p]$ on X and $F_{X/S} \circ V_{X/S} = [p]$ on $X^{(p/S)}$.*

Let $a \in A(\bar{k})$ be a $\bar{k}$-point of an abelian variety A, which in particular means that $\kappa(a) \subseteq \bar{k}$. Therefore, we have the isomorphism $A_{\bar{k}} \times \{a\} \overset{\simeq}{\to} A_{\bar{k}}$ and we can define the **translation map** t_a as a composition

$$A_{\bar{k}} \to A_{\bar{k}} \times \{a\} \overset{\iota}{\to} A_{\bar{k}} \times A_{\bar{k}} \overset{m}{\to} A_{\bar{k}},$$

which is on the level of points $p \mapsto m(p, a)$. More general, for $a \in V$, we have $t_a : A_{\kappa(a)} \to A_{\kappa(a)}$, and thus if $a \in A(k)$ we have $t_a : A \to A$. We mention two important properties where the translation maps appear.

- Any morphism (of algebraic varieties) $f : A \to B$ of abelian varieties can be written as a composition of a homomorphism $h : A \to B$ and a translation t_b for some $b \in B(k)$.

- Let $\mathcal{L}$ be an invertible sheaf on an abelian variety A and $a, b \in A(k)$. Then,

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \to t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}$$

is an isomorphism of sheaves (this is the *Theorem of the Square*). Equivalently, after tensoring the previous isomorphism with $\mathcal{L}^{-2}$ and using the commutativity of tensor product since we are working with commutative rings, we get an isomorphism of sheaves that will be useful for further discussions:

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L}^{-1} \to (t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}) \otimes (t_b^*\mathcal{L} \otimes \mathcal{L}^{-1}).$$

Let $\mathcal{L}$ be an invertible sheaf on an abelian variety A. The latter property defines the map $\varphi_{\mathcal{L}}$,

$$\varphi_{\mathcal{L}} : A(k) \to \mathrm{Pic}(A), a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

that is, moreover, a homomorphism. Our wish is to define the *dual variety* of A, that is a variety that naturally comes in pair with A and that can show us some properties of A. For that purpose, consider the group $\mathrm{Pic}^0(A)$ of isomorphism classes of invertible sheaves $\mathcal{L}$ on A such that $t_a^*\mathcal{L} \cong \mathcal{L}$ for any $a \in A(\bar{k})$, or equivalently (we again refer to Milne's notes, [30], V, Section 9) such that $m^*\mathcal{L} \cong p^*\mathcal{L} \otimes q^*\mathcal{L}$ where p, q are two projection morphisms $A \times A \to A$. For an abelian variety A over k, the wish is for the dual variety $A^\vee$ to satisfy $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$ on the level of points. To see why the elements of $\mathrm{Pic}^0(A)$ are nice to be considered, let for a k-scheme S, $f : S \to A, g : S \to A$ be two morphisms and $\mathcal{L} \in \mathrm{Pic}^0(A)$. Then we see that

$$(f+g)^*\mathcal{L} \cong (f,g)^*m^*\mathcal{L} \cong (f,g)^*(p^*\mathcal{L} \otimes q^*\mathcal{L}) \cong f^*\mathcal{L} \otimes g^*\mathcal{L},$$

and in particular, for $S = A$, $n \in \mathbb{Z}$,

$$[n]_A^*\mathcal{L} = (\underbrace{1_A + \ldots + 1_A}_{n})^*\mathcal{L} \cong \mathcal{L}^n.$$

Definition 3. *Consider the pair $(A^\vee, \mathcal{P})$ with $A^\vee$ an abelian variety over k and $\mathcal{P}$ an invertible sheaf on $A \times A^\vee$, that satisfy the universal properties:*

1. *$\mathcal{P}|_{\{0\}\times A^\vee}$ is trivial and for $a \in A^\vee$, $\mathcal{P}|_{A\times\{a\}}$ is an element of $\mathrm{Pic}^0(A_{\kappa(a)})$.*
2. *For T any k-scheme and $\mathcal{L}$ an invertible sheaf on $A \times T$ such that $\mathcal{L}|_{\{0\}\times T}$ is trivial and for $t \in T$, $\mathcal{L}|_{A\times\{t\}}$ is an element of $\mathrm{Pic}^0(A_{\kappa(t)})$, and there is a unique morphism $f : T \to A^\vee$ such that $(1 \times f)^*\mathcal{P} \cong \mathcal{L}$.*

We say that $A^\vee$ is the ***dual variety*** *of A and $\mathcal{P}$ is the* ***Poincaré sheaf****.*

Let us discuss the previous abstract definition and see how it fits in the described wishes. If $K \supseteq k$ is a field, and $T = \mathrm{Spec}(K)$ and $\mathcal{L}$ any invertible sheaf on $A \times \mathrm{Spec}(K) = A_K$, we get that $\mathcal{L}|_{A_K}$ is in $\mathrm{Pic}^0(A_K)$. In other words, we get

$$A^\vee(K) = \mathrm{Pic}^0(A_K)$$

so the correspondence between K-points in $A^\vee$ and sheaves $\mathcal{L}$ as above is one to one. For $K = \bar{k}$ we get $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$. Moreover, $\mathrm{Pic}^0(A_{\bar{k}})$ is parametrized by the family $(\mathcal{P}_a)_{a\in A^\vee(\bar{k})}$, i.e., since any sheaf $\mathcal{L}$ as above corresponds to a unique morphism $f : \mathrm{Spec}(\bar{k}) \to A^\vee$, equivalently to a unique $\bar{k}$-point a_f in $A^\vee$, we see that $\mathcal{P}_{a_f} \cong \mathcal{L}$.

Furthermore, we mention here that for any abelian variety A, the dual variety $A^\vee = (A^\vee, \mathcal{P})$ exists, and the universal properties give us that it is unique.

In addition to the previous, we quote that $A^{\vee\vee} = A$.

Consider a homomorphism $f : A \to B$ of abelian varieties. Let $\mathcal{P}_B$ be the Poincaré sheaf on $B \times B^\vee$. By the universal properties, we get that the invertible sheaf $(f \times 1)^* \mathcal{P}_B$ on $A \times B^\vee$ defines a morphism

$$f^\vee : B^\vee \to A^\vee$$

so that

$$(1 \times f^\vee)^* \mathcal{P}_A \cong (f \times 1)^* \mathcal{P}_B.$$

On the level of points, we can see that $f^\vee$ is the pullback $\mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A)$, and sends the isomorphism classes of invertible sheaves on B to the ones on A. For $f : A \to B$ an isogeny, it follows that $f^\vee$ is an isogeny and moreover, [30], Theorem V.11.1 gives that the exact sequence

$$0 \to \ker(f) \to A \to B \to 0$$

gives rise to the exact sequence

$$0 \to \ker(f)^\vee \to B^\vee \to A^\vee \to 0.$$

Definition 4. *An isogeny $\lambda : A \to A^\vee$ such that $\lambda_{\bar{k}} = \phi_{\mathcal{L}}$ for some ample invertible sheaf $\mathcal{L}$ on $A_{\bar{k}}$ is said to be a **polarization** on A. Its degree is the degree of λ as an isogeny. An abelian variety equipped with polarization is said to be **polarized abelian variety**. If moreover the polarization λ on A is of degree 1, we call the pair (A, λ) the **principally polarized abelian variety**.*

It turns out that taking into account the polarization λ on A leads us to conclusions which guarantee several finiteness properties. Namely, for A an abelian variety we have the following:

- If λ is a polarization on A, the automorphism group of (A, λ) is finite.
- There are only finitely many isomorphism classes of polarized abelian varieties (A, λ) with degree d.
- A has only finitely many direct factors, up to isomorphism.

1.1.2 Jacobian of a curve

Let C be a curve over k of genus g. We saw in Example 1.1, that the elliptic curve E inherits the group structure from the subgroup $\mathcal{J}_E$ of $\mathrm{Pic}(E)$ consisting of divisors of degree zero, so it is considered as an abelian variety. The desire to somehow generalize this and make an abelian variety out of C leads to the definition of the Jacobian varieties. We present the approach based on [30], Chapter VII, with some additions from [15], Section IV.

Consider a connected scheme T over k and an invertible sheaf $\mathcal{L}$ on $C \times T$. Let

$$q : C \times T \to T$$

be the projection on the second coordinate, and say that the degree of an invertible sheaf is the degree of the corresponding divisor. Define

$$P_C^0(T) = \{\mathcal{L} \in \mathrm{Pic}(C \times T) : \deg(\mathcal{L}_t) = 0\} / q^* \mathrm{Pic}(T),$$

and think of elements as families of invertible sheaves of degree 0 on C, parametrized by T modulo trivial families; the justification for the last name is that for any $\mathcal{N} \in \mathrm{Pic}(T)$, it follows that $q^*\mathcal{N} \in \mathrm{Pic}(C \times T), \deg q^*\mathcal{N} = 0$ is trivial on each fiber $C_t = C \times \kappa(t), t \in T$. Note that

$$P_C^0 : \underline{k\text{-Schemes}} \to \underline{\text{AbelianGroups}}$$

is a functor.

Definition 5. *The **Jacobian variety** of C, denoted by $\mathcal{J}_C$, is the unique abelian variety $J = \mathcal{J}_C$ over k, for which there is a natural transformation (morphism of functors) $P_C^0 \to J$ such that $P_C^0(T) \to J(T)$ is an isomorphism whenever $C(T)$ is nonempty.*

As we implicitly assumed, the Jacobian variety always exists; [30], Chapter VII, Theorem 1.1. Purely from the definition, for a field $K \supseteq k$ over which C has a point, we get that

$$\mathrm{Pic}^0(C) = \{\mathcal{L} \in \mathrm{Pic}(C) : \deg(\mathcal{L}) = 0\} = P_C^0(K) \cong \mathcal{J}_C(K),$$

which fulfills the desired properties we wanted out of $\mathcal{J}_C$. See also [46], Chapter VI.

Another approach that can also lead to the definition of the Jacobian variety, and is useful for defining a morphism $C \to \mathcal{J}_C$ is the following.

We say that a pair (S, s) with S a connected k-scheme and $s \in S(k)$, is a **pointed k-scheme**. Further, a **divisorial correspondence** between two pointed k-schemes (S, s) and (T, t) is an invertible sheaf $\mathcal{L}$ on $S \times T$ for which $\mathcal{L}|_{S \times \{t\}}$ and $\mathcal{L}|_{\{s\} \times T}$ are trivial.

Proposition 1.4 ([30], Section VII, Theorem 1.2)**.** *Let C be as above and $p \in C(k)$. Then, there is a divisorial correspondence $\mathcal{M}^P$ between (C, p) and $\mathcal{J}_C$ such that for any divisorial correspondence between (C, p) and a pointed k-scheme (T, t), there is a unique morphism $f : T \to \mathcal{J}(C)$ such that $f(t) = 0$ and $(1 \times f)^*\mathcal{M}^p \cong \mathcal{L}$.*

From the proof of this Proposition in [30], it can be seen that for each $\mathcal{L} \in \mathrm{Pic}(C)$, i.e., for an invertible sheaf on C of degree 0, there is a unique $a \in \mathcal{J}_C(k)$ such that $\mathcal{M}_a \cong \mathcal{L}$ for some $a \in \mathcal{J}_C(k)$.

Let $P \in C(k)$ and let $\mathcal{L}^P$ be the invertible sheaf $\mathcal{O}(\Delta - C \times \{P\} - \{P\} \times C)$ on $C \times C$ with Δ the diagonal in $C \times C$. Using the previous proposition, we obtain a unique morphism

$$f^P : C \to \mathcal{J}_C, \quad \text{such that} \quad f^P(P) = 0,\ (1 \times f^P)^*\mathcal{M}^P \cong \mathcal{L}^P$$

that is moreover a closed immersion. When $C(k) \neq \varnothing$, we may think of $\mathcal{J}_C(k)$ as of $\mathrm{Pic}^0(C)$, and of $f^P : C(k) \to \mathcal{J}_C(k)$ as of $Q \mapsto \mathcal{O}(Q) \otimes \mathcal{O}(P)^{-1} = \mathcal{O}(Q - P)$. In the language of divisors, we have $f^P : Q \mapsto [Q - P]$, with $[Q - P]$ the linear equivalence class of $Q - P$.

To understand $\mathcal{J}_C$ better, we need to introduce the notion of symmetric powers of a curve. Let $r \in \mathbb{Z}_{>0}$ be a positive integer and $\mathbb{S}_r$ the symmetric group of degree r. $\mathbb{S}_r$ acts on C^r by permuting the factors. We say that a morphism $\varphi : C^r \to T$ is a **symmetric morphism** if $\varphi = \varphi \circ \sigma$ for all $\sigma \in \mathbb{S}_r$. It follows that a variety denoted by $C^{(r)}$ and called the ***n*th symmetric power of** C, whose underlying topological space is the quotient $C^r/\mathbb{S}_r$, exists. In this situation, there is also the symmetric morphism $\pi : C^r \to C^{(r)}$ such that any symmetric morphism $\varphi : C^r \to T$ over k factors through π. Furthermore, for affine open subsets $U \subseteq C$, $U^{(r)}$ is an open affine subset of $C^{(r)}$ and it holds that $\mathcal{O}_{C^{(r)}}(U^{(r)}) = \mathcal{O}_{C^r}(U^r)^{\mathbb{S}_r}$.

As before, let $P \in C(k)$ and let $f = f^P$ as introduced above. Consider the map

$$f^r : C^r \to \mathcal{J}_C, (P_1, \dots, P_r) \mapsto f(P_1) + \dots + f(P_r),$$

which is on the level of points

$$(P_1, \dots, P_r) \mapsto [P_1 + \dots + P_r - rP],$$

a complete analogue to the case we considered in Example 1.1. Then f^r is a symmetric morphism, so it induces the morphism $f^{(r)} : C^{(r)} \to \mathcal{J}_C$. Write W^r for the image of $f^{(r)} : C^{(r)} \to \mathcal{J}_C$ that is a closed subvariety as was already mentioned,

$$W^r = f^{(r)}(C^{(r)}) = \underbrace{f(C) + \dots + f(C)}_{r}.$$

It holds that for any $r \leq g$, the morphism $f^{(r)} : C^{(r)} \to W^r$ is a birational morphism, i.e., it is a morphism, and there is an inverse to it as a rational map. When $r = g$, we get that $f^{(g)} : C^{(g)} \to \mathcal{J}_C$ is a surjective birational morphism. Similarly, W^{g-1} is closed subvariety of $\mathcal{J}_C$, birationally equivalent to $C^{(g-1)}$ so of dimension $g - 1$. Hence, $\Theta = W^{g-1}$ is a divisor on $\mathcal{J}_C$. We cite an important theorem that tells us that $\mathcal{J}_C$ is canonically a principally polarized abelian variety via the Θ-divisor.

Theorem 1.5 ([30], Section VII, Theorem 6.6). *The map $\varphi_{\mathcal{O}(\Theta)} : \mathcal{J}_C \to \mathcal{J}_C^\vee$ is an isomorphism.*

At the end of this section, we cite the famous Torelli theorem which gives us that a curve C is uniquely determined by its canonically polarized Jacobian $\mathcal{J}_C$.

Theorem 1.6 ((Torelli's theorem) [30], Section VII, Theorem 12.1). *Let C and C' be curves over an algebraically closed field k, $P \in C(k), P' \in C'(k)$ and let $f : C \to \mathcal{J}_C$, $f' : C' \to \mathcal{J}_{C'}$ be the morphisms $f = f^P$ and $f' = f^{P'}$ defined above. Assume that there is an isomorphism of canonically polarized Jacobians*

$$(\mathcal{J}_C, \lambda) \overset{\cong}{\to} (\mathcal{J}_{C'}, \lambda').$$

Then C and C' are isomorphic.

1.2 On the moduli spaces $\mathcal{A}_g$ and $\mathcal{M}_g$

The moduli spaces we will be mostly interested in throughout this thesis are the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g and the moduli space $\mathcal{M}_g$ of curves of genus g, for $g \in \mathbb{Z}_{>1}$. Roughly speaking, $\mathcal{A}_g$ and $\mathcal{M}_g$ will be objects with some structure (we think of them as varieties) that parametrize isomorphism classes of principally polarized abelian varieties of dimension g and curves of genus g, respectively, satisfying some universal properties.

Following [2], we will here briefly introduce the notions of the coarse and the fine moduli space, and apply that to the cases we are interested in. Lastly, we discuss an alternative to the these notions and define $\mathcal{A}_g$ and $\mathcal{M}_g$ as stacks.

1.2.1 On moduli problems

Let $\mathcal{C}$ be a category whose objects are sets possessing some additional structure, and whose morphisms respect these structures, such that the collection of all morphisms is a set (so-called *small categories*); let $\underline{Set}'$ be a category of (some, perhaps not all) sets and set theoretic maps. Further, consider the covariant functor

$$|\cdot| : \mathcal{C} \to \underline{Set}'$$

that sends objects of $\mathcal{C}$ to their underlying set and satisfies that $\mathrm{Hom}_{\mathcal{C}}(M,N) \to \mathrm{Hom}_{\underline{Set}'}(|M|,|N|)$ is injective. Lastly, we also want that there exists an object P of $\mathcal{C}$ (we write sometimes $P \in \mathcal{C}$) called the *base point object* such that $|P|$ is a point and that there is a canonical bijection

$$\mathrm{Hom}_{\mathcal{C}}(P,M) \overset{\cong}{\to} |M|$$

and for a morphism $f : M \to N$ in C we have that $|f| : |M| \to |N|$ is given by the natural map

$$\mathrm{Hom}_{\mathcal{C}}(P,M) \to \mathrm{Hom}_{\mathcal{C}}(P,N), \psi \mapsto f \circ \psi.$$

Consider $\mathcal{C}$ as above. For a set S and an equivalence relation $\sim_S$ on S we firstly want to solve the *classification problem*, which consists of putting the structure of an object of $\mathcal{C}$ on $S/\sim_S$ in a natural way. We will define two important functors Fam and $\mathcal{F}$ which arise while solving that problem and then introduce the general moduli problem.

Definition 6. *The* ***functor of families of objects of*** *S, denoted by* Fam $: \mathcal{C} \to \underline{Set}'$*, is a contravariant functor that satisfies:*

1. *$P \mapsto S$.*

2. *For all objects T in $\mathcal{C}$ there is an equivalence relation $\sim_T$ on* $\mathrm{Fam}(T)$ *such that for $T = P$ we have that $\sim_T$ equals $\sim_S$.*

3. *For all morphisms $\phi : T_1 \to T_2$ in $\mathcal{C}$, the morphism $\phi^* = \mathrm{Fam}(\phi) : \mathrm{Fam}(T_2) \to \mathrm{Fam}(T_1)$ sends $\sim_{T_2}$-equivalent families to $\sim_{T_1}$-equivalent ones.*

Definition 7. *The* ***functor of equivalence classes of families of objects of*** *S is a contravariant functor $\mathcal{F} : \mathcal{C} \to \underline{Set}'$ such that*

$$\mathcal{F}(T) = \mathrm{Fam}(T)/\sim_T \;\; \textit{and} \;\; \phi^* = \mathcal{F}(\phi) : \mathcal{F}(T_2) \to \mathcal{F}(T_1)$$

for T, T_1, T_2 objects and $\phi : T_1 \to T_2$ a morphism in $\mathcal{C}$.

Note that functor $\mathcal{F}$ is well-defined by the properties of the functor Fam, and $\mathcal{F}(P) = S/\sim_S$. Having the previously introduced notions, we can introduce what the global moduli problems are.

Definition 8. *Suppose that we have $\mathcal{C}$ as above, and that the following data are given: (a) an object X of $\mathcal{C}$, (b) collection of objects S belonging to a category whose objects and morphisms are defined intrinsically in terms of X, (c) an equivalence relation $\sim_S$ on S, and (d) the functor* Fam *of families of objects of S on $\mathcal{C}$ as above. The* ***(global) moduli problem*** $(*)$ *is*

- *to find an object M in $\mathcal{C}$ such that the elements of $|M|$ are in a canonical bijection with the elements of $S/\sim_S$;*

- *to investigate how the properties of families control the structure of M.*

Yoneda's lemma states that for any category $\mathcal{C}$ and X an object in $\mathcal{C}$ the set of natural transformations $\mathrm{Hom}_{\mathcal{C}}(-,X) \to F$ is in natural bijection with $F(X)$. Therefore, if M is a solution to the moduli problem described above, we see that the structure on M is by Yoneda's lemma uniquely determined by the functor $\mathrm{Hom}_{\mathcal{C}}(-,M)$. Recall that a contravariant functor $F : \mathcal{C} \to \underline{Set}'$ is said to be *representable* if for some object X in $\mathcal{C}$ there is a natural equivalence of functors $F \to \mathrm{Hom}_{\mathcal{C}}(-,X)$. In particular, we have that the functor $\mathrm{Hom}_{\mathcal{C}}(-,M)$ is a representable functor.

1.2.2 Fine and coarse moduli spaces

We define the **fine moduli space** to be a solution to the moduli problem $(*)$,

$$M \in \mathcal{C}, \text{ such that } \mathcal{F} \overset{\cong}{\to} \mathrm{Hom}_{\mathcal{C}}(-,M),$$

or more precisely, a pair (M,Φ), which represents the functor $\mathcal{F}$ of equivalence classes of families of objects of S, i.e.

$$\Phi : \mathcal{F} \overset{\cong}{\to} \mathrm{Hom}_{\mathcal{C}}(-,M).$$

Yoneda's lemma gives us that if such a solution M exists, it is unique. In such a situation, we may see that for any object T in $\mathcal{C}$, we have the bijection

$$\mathcal{F}(T) \to \mathrm{Hom}_{\mathcal{C}}(T,M),$$

which uniquely makes the correspondence between all $\sim_T$-equivalent objects of S parametrized by T and all the morphisms $T \to M$.

Further, let us remark how the structure on $S/\sim_S$ corresponds to properties of the families of objects of S. Consider any object $T \in \mathcal{C}$ and a family V on T in $\mathcal{C}$. Any element $t \in |T|$, since $|T| = \mathrm{Hom}_{\mathcal{C}}(P,T)$, defines a morphism $\phi_t : P \to T$ and hence denote $\mathrm{Fam}(\phi_t)(V) = V_t$. Hence, by the definition of fine moduli, the map

$$|T| \to S/\sim_S, \quad t \mapsto V_t/\sim_S$$

gives a unique morphism $T \to M$, which corresponds to $\mathcal{F}(T) = V/\sim_T$.

Even though the previous situation is very satisfying, asking for M to represent the functor $\mathcal{F}$ is demanding, and can lead to having no solution to the described moduli problem.

Another approach is to define the **coarse moduli space** $M = (M,\Phi)$, *with M an object in $\mathcal{C}$ and $\Phi : \mathcal{F} \to \mathrm{Hom}_{\mathcal{C}}(-,M)$ a natural morphism which satisfies:*

- *For P the base-point object in $\mathcal{C}$, the mapping of sets $\Phi(P)$ is bijective.*
- *For any object N in $\mathcal{C}$ and any natural transformation $\Psi : \mathcal{F} \to \mathrm{Hom}_{\mathcal{C}}(-,N)$ there is a unique natural morphism $\Omega : \mathrm{Hom}_{\mathcal{C}}(-,M) \to \mathrm{Hom}_{\mathcal{C}}(-,N)$, such that $\Psi = \Omega \circ \Phi$.*

Similarly as for a fine moduli space, Yoneda's lemma implies that a coarse moduli space for some moduli problem is unique in the cases when exists. By comparing the defining properties, it is not hard to see that a fine moduli space M is also a coarse moduli space. However, as we will see soon, the other implication does not hold necessarily.

Further, the first defining property implies that

$$S/\sim_S = \mathcal{F}(P) \overset{\cong}{\to} \mathrm{Hom}_{\mathcal{C}}(P,M) = |M|,$$

so we can think of structure on $S/\sim_S$ as a structure on M.

1.2.3 The moduli space of curves $\mathcal{M}_g$, $g \geq 2$

Here, we will use the previous theory on a concrete example, namely to define the moduli space $\mathcal{M}_g$ of curves of genus $g \geq 2$, following the approach of [7]. Let k be an algebraically closed field and $g \in \mathbb{Z}_{\geq 2}$. As before, by curves of genus g over k we mean non-singular projective curves of genus $g \geq 2$ over k, (in other words, non-singular projective algebraic varieties of dimension one and genus $g \geq 2$ defined over k). Our wish is to get a variety whose underlying set of points consists of non-isomorphic curves of genus g. Hence, $\mathcal{C}$ from the previous parts will here be the category $\underline{k\text{-Schemes}}$ of k-schemes.

Let S be a k-scheme. A family of curves of genus g over S is a morphism $X \to S$ which is flat, proper over S and whose geometric fibers are curves of genus g. We say that two families $\phi : X \to S, \psi : Y \to S$ over S are equivalent, and write $\sim_S$, if there is an isomorphism $\eta : X \to Y$ such that $\phi = \psi \circ \eta$. This gives a first step in constructing the functors Fam = Fam_g and $\mathcal{F} = \mathcal{F}_g$.

We define

$$\mathrm{Fam}_g(S) = \{\text{Families of curves of genus } g \text{ over } S\},$$

and want to see how two families $\mathrm{Fam}_g(S)$ and $\mathrm{Fam}_g(T)$ relate to each other when there is a morphism $S \to T$.

Let $f : S \to T$ be a k-morphism of two k-schemes. Any family of curves of genus g over T,

$$\phi : X \to T$$

induces a family of curves of genus g over S by

$$f^*\phi : X \times_T S \to S.$$

It is easy to check that then the set theoretic assignment $f^* : \mathrm{Fam}_g(T) \to \mathrm{Fam}_g(S)$ is functorial with respect to families of curves of genus g over T, which gives us a functor

$$\mathrm{Fam}_g : \underline{k\text{-Schemes}} \to \underline{\mathrm{Set}}.$$

Therefore, we get the functor $\mathcal{F}_g : \underline{k\text{-Schemes}} \to \underline{\mathrm{Set}}$:

$$S \mapsto \mathrm{Fam}_g / \sim_S = \{\text{Isomorphism classes of families of curves of genus } g \text{ over } S\},$$

$$(f : S \to T) \mapsto (f^* : (\phi : X \to T)/ \sim_T \to (\mathrm{Fam}_g(f) \circ \phi : X \times_T S \to S)/ \sim_S),$$

where $f^* = [\mathrm{Fam}_g(f)]$ is induced by $\mathrm{Fam}_g(f)$ using that Fam_g respects equivalence classes.

In [11], Theorem 5.1.1 one can find that there exists a coarse moduli space M_g of curves of genus $g \geq 1$, which is a solution the the previously described moduli problem. Deligne and Mumford showed in [6] that M_g is a quasi-projective variety and has dimension $3g - 3$ over k. However, for $g \geq 3$,

- M_g is singular by Popp's [39],
- There is no fine moduli space which is a solution to the previous moduli problem, i.e., the functor $\mathcal{F}_g$ is not representable; one can find a helpful presentation of this in [7], Theorem 4.3.4.

Both non-existence of the fine moduli space of curves over k of genus g and the singularity of the coarse moduli space M_g of curves over k of genus g are consequences of the fact that *there are curves of genus $g \geq 2$ with non-trivial automorphism groups.*

An alternative to the previous is to use a substitution for the desire that the moduli space is a variety or a scheme. Mumford and Deligne in [6] introduced the notion of **stacks**, when they constructed the **Deligne-Mumford stack of stable curves**. Stacks account for the existence of the non-trivial automorphism groups while keeping some of the wanted properties. However, formal presentation of stacks is beyond the scope of this text, and we will here only describe some things from the literature.

Our main references for the following are [6] and [32], Section 1, where we partially used some of the introductory theory from [36].

Definition 9. *For any scheme S and fixed $g \geq 2$, we say that a* ***stable curve*** *of genus g over S is a proper flat morphism $\pi : C \to S$, whose geometric fibers are reduced, connected schemes C_s of dimension one such that:*

1. *C_s has at worst nodal sinuglarities, i.e., it is either non-singular or its singularities are ordinary double points;*
2. *If P is a non-singular rational component of C_s, i.e., P is of genus 0, then P meets other components of C_s in at least three distinct points; and*
3. $\dim H^1(C_s, \mathcal{O}_{C_s}) = g$.

We are interested in cases when S is $\operatorname{Spec}(k)$ for a field k. Moreover, we assume here for simplicity that k is algebraically closed.

To a stable curve C over k, we associate the *dual graph* as in the following definition.

Definition 10. *Let C be a stable curve over k. An undirected graph Γ is the* ***dual graph*** *of C if it satisfies:*

- *Vertices of Γ correspond (bijectively) to the irreducible components of C;*
- *Edges of Γ represent the set of singular points of C; extremities of an edge are the vertices corresponding to the components on which that singular point lie (they can be loops too).*

Denote with $\overline{\mathcal{M}_g}$ the Deligne-Mumford stack of stable curves of genus g. It contains the moduli stack $\mathcal{M}_g$ of non-singular curves of genus g as an open substack. We will call $\mathcal{M}_g$ the **moduli space of curves of genus** g and $\overline{\mathcal{M}_g}$ the **Deligne-Mumford compactification of** $\mathcal{M}_g$. Lastly, let M_g, be the *underlying coarse variety* of $\mathcal{M}_g$ that we introduced before.

In [6], Deligne and Mumford show that $\overline{\mathcal{M}_g}$, for $g \geq 2$, is a complete, connected and non-singular Deligne-Mumford stack of dimension $3g-3$. Furthermore, $\mathcal{M}_g$ is open and dense inside $\overline{\mathcal{M}_g}$, so in particular we have

$$\dim \mathcal{M}_g = 3g - 3.$$

The complement $\overline{\mathcal{M}_g} - \mathcal{M}_g$ is a divisor whose irreducible components we denote by

$$\Delta_0,\ \Delta_1, \dots,\ \Delta_{\lfloor \frac{g}{2} \rfloor},$$

and briefly describe. Namely, we cite that Δ_0 is such that there is its non-empty open part parametrizing the irreducible curves with a single node, while Δ_i for $0 \leq i \leq \lfloor g/2 \rfloor$ have non-empty open parts that parametrize curves with exactly two irreducible components which genera are i and $g - i$.

We say that a stable curve C over (algebraically closed) k of genus $g \geq 2$ is of **compact type** if its dual graph is a tree, their irreducible components are non-singular, and the sum of genera summing over all irreducible components is g. Denote the substack of $\overline{\mathcal{M}_g}$ consisting of curves of compact type by $\mathcal{M}_g^{ct}$, and its underlying coarse moduli with M_g^{ct}. It turns out that $\mathcal{M}_g^{ct} \subseteq \overline{\mathcal{M}_g}$ is precisely the complement of the prime divisor Δ_0.

Moreover, it holds that the Jacobian of a stable curve C is a principally polarized abelian variety if and only if C is of compact type. In that situation, if $C_1, \ldots, C_j, C_{j+1}, \ldots, C_n$ are all irreducible components of a curve of compact type C, with C_i non-rational, i.e. of genus at least 1, for $1 \leq i \leq j$, and C_i rational for $j < i \leq n$, then the Jacobian of C as an abelian variety equals

$$\mathcal{J}_C = \prod_{i=1}^{j} \mathcal{J}_{C_i}. \tag{2}$$

In other words, $\mathcal{J}_C$ is the product of the Jacobians of the irreducible components of C; recall that the Jacobian of a projective line is a point, so that the Jacobians of the rational components of C do not occur in (2).

1.2.4 The moduli space of principally polarized abelian varieties $\mathcal{A}_g$, $g \geq 2$

Similarly to the case of curves, there are the Deligne-Mumford stack $\mathcal{A}_g$ of principally polarized abelian varieties, and the underlying coarse moduli space A_g.

Attaching to a curve C its Jacobian $\mathcal{J}_C$, results in the **Torelli morphism**, a representable morphism $\tau : \mathcal{M}_g \to \mathcal{A}_g$, between two algebraic stacks. In [32], Section 1.3, we find that the same things happen with

$$\tau : \mathcal{M}_g^{ct} \to \mathcal{A}_g,$$

which we also call the Torelli morphism and is defined in a similar fashion.

This can also be done on the level of coarse moduli spaces, where the Torelli morphism gives rise to

$$\tau : M_g^{ct} \to A_g.$$

The image of M_g^{ct} in A_g is called the **Torelli locus** in A_g, while the image of M_g in A_g is the **open Torelli locus**. It turns out that the open Torelli locus is open and dense in the Torelli locus.

2 Supersingular abelian varieties and curves

Having introduced the background in the previous section, we are in the situation to define the main objects of interest, the supersingular abelian varieties, and the supersingular curves. In order to investigate them, we discuss some invariants of abelian varieties and curves used to better understand the geometry of $\mathcal{A}_g$ and $\mathcal{M}_g$.

2.1 Invariants of abelian varieties

Let A be a principally polarized abelian variety of dimension g defined over some field k, with $\mathbb{F}_p \subseteq k \subseteq \overline{\mathbb{F}}_p$. Here, we define several invariants that have been used while working with abelian varieties, and in particular, while working with Jacobians of curves. Later, we will be most interested in the cases $p = 2$ and $g \in \{4, 5\}$, but for the purpose of having the universal theory, we will work with the general case. Our main resources for these topics are [41], [8] and [51].

Definition 11. *Let E be an arbitrary elliptic curve over $\overline{\mathbb{F}}_p$ with $E[p](\overline{\mathbb{F}}_p) = \{O\}$. We say that A is a **supersingular abelian variety** if it is isogenous to E^g, i.e., if*

$$A \sim \underbrace{E \times \ldots \times E}_{g};$$

*we say that a curve C is supersingular if its Jacobian is. Similarly, the abelian variety A is **superspecial** if it is isomorphic to E^g, i.e.,*

$$A \cong \underbrace{E \times \ldots \times E}_{g};$$

similarly to the supersingular case, a curve C is superspecial if $\mathcal{J}_C$ is.

Note that being superspecial implies being supersingular. However, the other implication does not necessatily hold.

2.1.1 p-rank, a-number and Newton polygon of abelian varieties

The first important invariants we define are the *p-rank* and the *a-number* of A.

Definition 12. *The **p-rank** of A equals p-rank$(A) = f$, where $f, 0 \leq f \leq g$ is the integer such that*

$$\#A[p](\overline{\mathbb{F}}_p) = p^f.$$

An alternative definition that we will not use here is

$$p\text{-rank}(A) = \dim \operatorname{Hom}_{\mathbb{F}_p}(\mu_p, A),$$

with $\mu_p = \operatorname{Spec}(\overline{\mathbb{F}}_p[x]/(x^p - 1))$ the kernel of the Frobenius morphism on the multiplicative group $\mathbb{G}_m$.

Definition 13. *We define the **a-number** of A as*

$$a(A) = \dim \operatorname{Hom}_{\overline{\mathbb{F}}_p}(\alpha_p, A),$$

where $\alpha_p = \operatorname{Spec}(\overline{\mathbb{F}}_p[x]/(x^p))$ is the kernel of the Frobenius morphism on the additive group $\mathbb{G}_a$.

It holds that g-dimensional A is superspecial if and only if $a(A) = g$; see [35], Theorem 2. We will later see some equivalent definitions of the a-number of abelian varieties that will be more useful in concrete situations.

The p-rank and the a-number of the abelian variety A are connected via the well-known relations

$$0 \leq p\text{-rank}(A) \leq g, \quad 1 \leq a(A) + p\text{-rank}(A) \leq g.$$

Furthermore,

$$p\text{-rank}(A_1 \times A_2) = p\text{-rank}(A_1) + p\text{-rank}(A_2), \quad a(A_1 \times A_2) = a(A_1) + a(A_2),$$

for any two abelian varieties A_1 and A_2 over k.

The Newton polygon of an abelian variety is the invariant used in practice to determine whether the abelian variety is supersingular. We will define it in the case when k is a finite extension of $\mathbb{F}_p$ and we will only mention the definition for the general case. Let A be an abelian variety over $k = \mathbb{F}_q$ with $q = p^r$ of dimension g.

Let $h_A(t) \in \mathbb{Z}[t]$ be the characteristic polynomial of the Frobenius morphism on A. The **L-polynomial** of A is defined via $h_A(t) = t^{2g}L(A/\mathbb{F}_q, t^{-1})$, and it factors over $\mathbb{C}$ as

$$L(A/\mathbb{F}_q, t) = \prod_{i=1}^{2g}(1 - \alpha_i t),$$

with $\alpha_i \in \mathbb{C}, |\alpha_i| = \sqrt{q}$; see for example [29].

If $L(A/\mathbb{F}_q, t) = \sum_{i=0}^{2g} a_i t^i$, denote with v_i the p-adic value of the coefficients a_i, $v_i = \max\{n : p^n | a_i\}$ or if $a_i = 0, v_i = +\infty$. The **Newton polygon** of A is the lower convex hull of the points $(i, v_i/r)$ for $i \in \{0, 1, \ldots, 2g\}$. Therefore, Newton polygons are piecewise linear functions on the interval $[0, 2g]$, starting at $(0,0)$ and ending at $(2g, g)$, so that the coordinates of the break points are integers. They are symmetric in the following sense: if (i, j) is a break point of the Newton polygon N, then $(2g - i, g - i + j)$ is also a break point of N, or equivalently, if the slope λ appears in N with multiplicity m, then the slope $1 - \lambda$ also appears with the same multiplicity in N.

We say that the Newton polygon that is the straight line from $(0,0)$ to $(2g, g)$, i.e., that has only the slopes $1/2$, is the **supersingular Newton polygon**, while the **ordinary Newton polygon** is the polygon consisting of two lines, the one from $(0,0)$ to $(g, 0)$ and the one from $(g, 0)$ to $(2g, g)$, i.e., whose slopes are only 0 and 1.

It holds that an abelian variety A over $\mathbb{F}_q = \mathbb{F}_{p^r}$ of dimension g is supersingular if and only if its Newton polygon is. Furthermore, we have that the Newton polygon is an isogeny invariant, which follows from, for example [29]. Similarly as for previous invariants, the Newton polygon of a curve C of genus g over $\mathbb{F}_q = \mathbb{F}_{p^r}$ is the Newton polygon of its Jacobian variety.

For a curve C over $k = \mathbb{F}_q, q = p^r$ of genus g, we have a useful way of computing its Newton polygon that is based on computing the number of points over a few finite extensions of $\mathbb{F}_q$.

The **zeta function** of C is

$$Z(C/\mathbb{F}_q, t) = \exp\left(\sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n})\frac{t^n}{n}\right).$$

The (proven) Weil conjecture for curves implies that there is a polynomial $L(C/\mathbb{F}_q, t) \in \mathbb{Z}[t]$ of degree $2g$, such that

$$Z(C/\mathbb{F}_q, t) = \frac{L(C/\mathbb{F}_q, t)}{(1-t)(1-qt)}.$$

The notation we used to denote this polynomial is not by accident, namely, this is precisely the L-polynomial of $\mathcal{J}_C$. Now, using the obtained L-polynomial $L(C/\mathbb{F}_q,t) = \sum_{i=0}^{2g} a_i t^i$, we can proceed as before, and define the Newton polygon of C in the same manner as the lower convex hull of the set of points $(i, v_i/r), 0 \leq i \leq 2g$ with v_i the p-adic value of a_i.

Example 2.1. *Consider the elliptic curve $E : y^2 + y = x^3$ defined over $\mathbb{F}_2$ from Example 1.1. Then E is a supersingular curve, and we will see that using three possible definitions in the case of elliptic curves: via 2-rank, being superspecial, and by computing its Newton polygon.*

First, using Silverman's [44], Group Law III.2.3, if $P = (x_P, y_P) \neq O$, on E with $x_P, y_P \in \overline{\mathbb{F}}_2$ is of order two, then $(x_P, y_P) = (x_P, y_P + 1)$ which is not possible, so the 2-rank of E is zero. Secondly, using

$$1 \leq a(E) + 2\text{-rank}(E) \leq 1,$$

we see that E has a-number $1 = g(E)$, and thus is superspecial. Lastly, using [44], Theorem V.2.3.1, and $\#C(\mathbb{F}_2) = 3$, the characteristic polynomial of E equals

$$h_E(t) = t^2 - (2 + 1 - \#C(\mathbb{F}_2))t + 2 = t^2 + 2,$$

so

$$L(E/\mathbb{F}_2, t) = 1 + 2t^2.$$

Therefore, its Newton polygon is a line from $(0,0)$ to $(2,1)$, thus with a unique slope $1/2$.

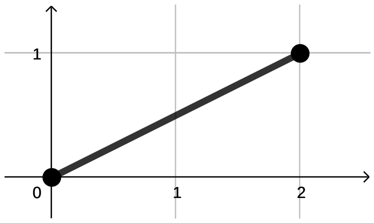

Figure 1: Newton polygon of $E : y^2 + y = x^3$ over $\mathbb{F}_2$

Note that there are two eligible Newton polygons in the case of elliptic curves; namely, the supersingular and the ordinary one.

If we left out the condition that k is a finite field, we sketch the definition of the Newton polygon of an abelian variety A as follows. Consider for $n \in \mathbb{Z}_{>0}$ the kernels $A[p^n]$ of morphisms $[p^n] : A \to A$, and define the **p-divisible group** of A, $A[p^\infty] = \varinjlim A[p^n]$. Over $k = \bar{k}$, the Dieudonné-Manin theory gives a unique (up to so-called *isogeny of p-divisible groups*) classification of $A[p^\infty]$ as

$$A[p^\infty] \sim \oplus_{\lambda = \frac{d}{c+d}} G_{c,d}^{m_\lambda},$$

where $c, d \in \mathbb{Z}_{\geq 0}, \gcd(c,d) = 1$, and $G_{c,d}$ are *simple p-divisible groups over k of codimension c and dimension d.* We define the Newton polygon of A in this case as the multi-set of the slopes λ, that uniquely form a lower convex hull from $(0,0)$ to $(2g, g)$. In particular, A is supersingular if

$$A[p^\infty] \sim G_{1,1}^g.$$

Even though the notions of being supersingular, superspecial and of p-rank zero coincide for elliptic curves, as we saw in the concrete example, these conditions differ for $g \geq 3$. For example [41], Proposition 3.1, tells us that, in general, a principally polarized abelian variety A of dimension g satisfies

$$A \text{ superspecial } \implies A \text{ supersingular } \implies p\text{-rank}(A) = 0.$$

However, we cite that for $g \geq 2$ being supersingular does not imply being superspecial; note that isogeny between two abelian varieties is "weaker" that an isomorphism between them.

The p-rank of an abelian varieties A can alternatively be defined using the Dieudonné-Manin classification as the multiplicity of the slope 0 in the Newton polygon. Since there is always a principally polarized abelian variety of dimension g with slopes $1/g$ and $(g-1)/g$, which will follow from the theorem on stratification of the moduli space of principally polarized abelian varieties of dimension g by the Newton polygons given in Section 2.2.2, we see that for $g \geq 3$, possessing p-rank zero does not imply being supersingular.

2.1.2 Ekedahl-Oort type

To define the Ekedahl-Oort type of an abelian variety A we firstly need to introduce the *first de Rham cohomology*; for presenting this, we combine [9] and [51].

For an arbitrary scheme X, let $\mathcal{U} = \{U_i : i \in I\}$ be an arbitrary open affine cover of X, and $\mathcal{F}$ a sheaf of abelian groups on X. Let us denote with $C^\bullet(\mathcal{U}, \mathcal{F})$ the Čech complex of abelian groups, and for ease of notation, let $C^i = C^i(\mathcal{U}, \mathcal{O}_X)$. Let

$$Z^1_{dR}(\mathcal{U}) = \{(f,\omega) \in C^1 \times C^0 : f_{|U_i \cap U_k} = f_{|U_i \cap U_j} + f_{|U_j \cap U_k}, \mathrm{d}f_{|U_i \cap U_j} = \omega_{|U_i} - \omega_{|U_j}, \mathrm{d}\omega_{|U_i} = 0\},$$

$$B^1_{dR}(\mathcal{U}) = \{(f,\omega) \in C^1 \times C^0 : g \in C^0, f_{|U_i \cap U_j} = g_{|U_i} - g_{|U_j}, \omega_{|U_i} = \mathrm{d}g_{|U_i}\}.$$

We define the **first de Rham cohomology** of X as $H^1_{dR}(X) = H^1_{dR}(\mathcal{U})$ (it does not depend on the choice of covering) by

$$H^1_{dR}(\mathcal{U}) = Z^1_{dR}(\mathcal{U}) / B^1_{dR}(\mathcal{U}).$$

If we go back to the case when $X = A$ is an abelian variety, the (relative) Verschiebung morphism $V_{A/k}$ induces the k-linear map

$$V^*_{A/k} : H^1_{dR}(A) \to H^1_{dR}(A^{(p/k)}).$$

Using that $H^1_{dR}(A)$ and $H^1_{dR}(A^{(p/k)})$ are in particular the same, only with a different k-action, instead of $V^*_{A/k}$, we can consider the **Veschiebung operator**

$$V : H^1_{dR}(A) \to H^1_{dR}(A)$$

that is a p^{-1}-linear map, i.e., $V(cf) = c^{1/p}V(f)$ for $c \in k, f \in H^1_{dR}(A)$. Similarly, we have the p-linear **Frobenius operator** $F : H^1_{dR}(A) \to H^1_{dR}(A)$. Also, the properties $[p]_A = V_{A/k} \circ F_{A/k}$ and $[p]_{A^{(p/k)}} = F_{A/k} \circ V_{A/k}$ imply that

$$VF = FV = 0.$$

There is a symplectic form $\langle -, - \rangle$ on $H^1_{dR}(A)$, such that, after ignoring $p^{\pm 1}$-linearity as described above, for any $\omega, \eta \in H^1_{dR}(A)$ it holds

$$\langle V(\omega), \eta \rangle = \langle \omega, F(\eta) \rangle\,;$$

for example, see [51], page 22. If we denote by $H^{\perp}$ the orthogonal complement of a subspace H of $H^1_{dR}(A)$, we see that

$$(V(H))^{\perp} = F^{-1}(H^{\perp}),$$

so in particular, we have

$$V(H^1_{dR}(A)) = H^0(A,\Omega^1_A) = F^{-1}(0), \text{ and } F(H^1_{dR}(A)) = V^{-1}(0).$$

In the case when A is the Jacobian of a curve C, things are much nicer, and we can see them more explicitly. For that purpose, we use the *Cartier operator* and the *Hasse-Witt* matrix.

Definition 14. *Let C be a curve over $k = \overline{\mathbb{F}}_p$ of genus g. Let x be a separating variable of $\kappa(C)$ the function field of C, that is an element in $\kappa(C) - \kappa(C)^p$, which forms a p-basis of $\kappa(C)$ over $\kappa(C)^p$, so that we can write any function $z \in \kappa(C)$ in a unique way as*

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

*for some $z_0, z_1, \ldots, z_{p-1} \in \kappa(C)$. We define the **Cartier operator** $\mathcal{C}$ on $H^0(C,\Omega^1_C)$ as*

$$\mathcal{C}(z\mathrm{d}x) = z_{p-1}\mathrm{d}x.$$

*For a given basis $\{\omega_1, \ldots, \omega_g\}$ of $H^0(C,\Omega^1_C)$, let $\omega = \sum_{i=1}^{g} h_{i,j}\omega_i$ with $h_{i,j} \in k$. The **Hasse-Witt matrix** $HW(C)$ of C is then defined as*

$$HW(C) = (h^p_{i,j})_{1\leq i,j\leq g}.$$

Later, in Section 4.3, we will discuss more thoroughly some important properties of the Cartier operator and connections to the previously introduced invariants.

In [23], Proposition 3.1, we find that there is a *Hodge-de-Rham short exact sequence*

$$0 \to H^0(C,\Omega^1_C) \xrightarrow{\iota} H^1_{dR}(C) \xrightarrow{\gamma} H^1(C,\mathcal{O}_C) \to 0. \tag{3}$$

The map ι is defined by $\iota : \omega \mapsto (0,\omega)$, where, formally, the second coordinate of $(0,\omega)$ is $\omega_i = \omega|_{U_i}$ on affine open subsets of C. The other homomorphism γ sends the cohomology class of (ϕ,ω) to the cohomology class of ϕ. It follows that these maps are well-defined from the definition of $H^1_{dR}(C)$ and the fact that the coboundary conditions on $H^1_{dR}(C)$ and $H^1(C,\mathcal{O}_C)$ are compatible.

The Frobenius operator F and the Verschiebung operator V on $H^1_{dR}(C)$ are defined as

$$F(f,\omega) = (f^p,0) \quad \text{and} \quad V(f,\omega) = (0,\mathcal{C}(\omega)). \tag{4}$$

Using this description, we can see that $\ker F = H^0(C,\Omega^1_C)$ which then equals $V(H^1_{dR}(C))$ by the existence of the mentioned symplectic form $\langle -,- \rangle$. Further, the Verschiebung operator V restricted to $H^0(C,\Omega^1_C) \subseteq H^1_{dR}(C)$ coincides with the Cartier operator $\mathcal{C}$.

Let $A = (A,\lambda)$ be a principally polarized variety of dimension g and write $G = H^1_{dR}(A)$. The **final filtration** is the filtration stable under V and F^{-1},

$$0 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_g = V(G) \subseteq \ldots \subseteq G_{2g} = G,$$

which also satisfies $\dim(G_i) = i$ and $G_i^{\perp} = G_{2g-i}, i \in \{1, \ldots, 2g\}$. To such a filtration, we associate **final type** v, that is the increasing surjective map

$$v : \{0, 1, \ldots, 2g\} \to \{0, 1, \ldots, g\},$$

such that $V(G_i) = G_{v(i)}$.

We mention that the final filtration is not unique, but the final type is! The properties of V and F give

$$v(2g - i) = v(i) - i + g, \text{ for } 0 \leq i \leq g.$$

As a remark, by saying that v is an increasing surjective map as above, in particular, we get that

$$v(i) \leq v(i+1) \leq v(i) + 1, \quad 0 \leq i < g.$$

For a given final type v on A, we define the **Ekedahl-Oort** type of A, as the n-tuple $\mu = [\mu_1, \ldots, \mu_n]$ with $0 \leq n \leq g$ and $\mu_1 > \mu_2 > \ldots > \mu_n > 0$, so that

$$\mu_j = \#\{i : 1 \leq i \leq g, v(i) + j \leq i\}.$$

Note that $\mu = \varnothing$ is also a valid option. The combinatorial objects μ are also called **Young diagrams**, and we will use this terminology when we consider them without mentioning a specific (principally polarized) abelian variety. Note that giving the final type v is equivalent to giving a Young diagram μ associated with v.

Let us now see how the Ekedahl-Oort type of an abelian variety is connected to its p-rank and a-number. If a principally polarized abelian variety A of dimension g has Ekedahl-Oort type μ with corresponding final type v, in [37] we find that p-rank$(A) = f$, where $f \in \{0, 1, \ldots, g\}$ is the integer with the property

$$v(f) = f = v(f+1).$$

Furthermore, the a-number of A equals

$$a(A) = g - v(g) = g - \dim V(H^0(A, \Omega_A^1)).$$

In the language of Young diagrams, if $\mu = [\mu_1, \ldots, \mu_n]$ for $0 \leq n \leq g$ and $\mu_1 > \mu_2 > \ldots > \mu_n > 0$, we can translate the previous to

$$a(A) = n, \quad \text{ and } p\text{-rank}(A) = g - \mu_1.$$

For a curve C of genus g we thus have that

$$a(C) = g - \dim \mathcal{C}(H^0(C, \Omega_C^1)) = g - \operatorname{rank}(\mathcal{C}).$$

Also, it holds that

$$p\text{-rank}(C) = \operatorname{rank}(\mathcal{C}^g);$$

see for example [45], Section 3. In particular, we find that a principally polarized abelian variety is superspecial if and only if $\operatorname{rank}(\mathcal{C}) = 0$ and that it is of p-rank zero if and only if $\operatorname{rank}(\mathcal{C}^g) = 0$.

2.2 Stratifications of $\mathcal{A}_g$ and $\mathcal{M}_g$ and some results

Let $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ be the moduli space (stack) of principally polarized abelian varieties in characteristic p of dimension g, and $\mathcal{M}_g = \mathcal{M}_g \otimes \overline{\mathbb{F}}_p$ be the moduli space (stack) of curves in characteristic p of genus g. Recall that the mapping $C \mapsto \mathcal{J}_C$ that to a curve associates its Jacobian induces the *Torelli morphism*

$$\tau : \mathcal{M}_g \to \mathcal{A}_g.$$

In this section, we will introduce some invariants useful for better understanding the geometries of $\mathcal{A}_g$ and $\mathcal{M}_g$. They define the stratifications of $\mathcal{A}_g$ by p-rank, Newton polygon and Ekedahl-Oort type. Using the Torelli morphism, we transfer them to $\mathcal{M}_g$.

For the stratification by Newton polygons, we combine [3] and [8], while for the Ekedahl-Oort stratification, we use [37], [51].

2.2.1 Stratification by p-rank

For $f \in \{0, 1, \dots, g\}$, let $V_f \subseteq \mathcal{A}_g$ be the locus of principally polarized abelian varieties with p-rank less than or equal to f. Using the theory of Dieudonné modules, Norman and Oort in [34], gave us that each V_f is closed, non-empty and pure of codimension $g - f$, i.e., for any irreducible component Z of V_f, it holds that

$$\dim Z = \frac{g(g+1)}{2} - g + f.$$

In the case of curves, we have a similar result. The moduli spaces $\mathcal{M}_g$ and $\overline{\mathcal{M}}_g$ can also be stratified by p-rank into $\mathcal{M}_g^f$ and $\overline{\mathcal{M}}_g^f$ that are the loci whose points correspond to curves, and stable curves respectively, of genus g and p-rank equal to f, as $\mathcal{M}_g = \cup \mathcal{M}_g^f$, where $\mathcal{M}_g^f$ are locally closed. It is known by [1], Lemma 3.2 that $\mathcal{M}_g^f$ are open and dense in the locus $\overline{\mathcal{M}}_g^f$ of stable curves whose points are of genus g and p-rank f. Let $V_f(\overline{\mathcal{M}}_g) = \cup_{0 \le e \le f} \overline{\mathcal{M}}_g^e$ be the locus of stable curves with p-rank less or equal to f in $\overline{\mathcal{M}}_g$. Discussing the completeness and codimensions of some components of $V_r(\overline{\mathcal{M}}_g)$ via induction on r, Faber and van der Geer show in [10], Theorem 2.3 that the locus $V_f(\overline{\mathcal{M}}_g)$ is pure of codimension $g - f$ in $\overline{\mathcal{M}}_g$. In other words, for any irreducible component $Z \subseteq V(\overline{\mathcal{M}}_g)$, it holds that

$$\dim Z = 2g - 3 + f.$$

Since supersingular principally polarized abelian varieties, and in particular curves (i.e., their Jacobians), have p-rank 0, we will mainly be interested in the p-rank 0 loci in $\mathcal{A}_g$ and $\mathcal{M}_g$.

2.2.2 Stratification by Newton polygons

Consider the *eligible Newton polygons of dimension* g, that are the ones starting at $(0, 0)$ and $(2g, g)$, where if the slope λ occurs in it precisely m times, then the slope $1 - \lambda$ occurs in it with the same multiplicity. On the set of all eligible Newton polygons of dimension g, there is a partial ordering $\le$. For two such Newton polygons N and N', we write $N \le N'$ if N' lies on or completely above N, and naturally, $N < N'$ if $N \le N'$ and $N \ne N'$. Note that the supersingular Newton polygon is the greatest element of the partially ordered set of eligible Newton polygons of dimension g, while the ordinary Newton polygon is its smallest element. It is not hard to show

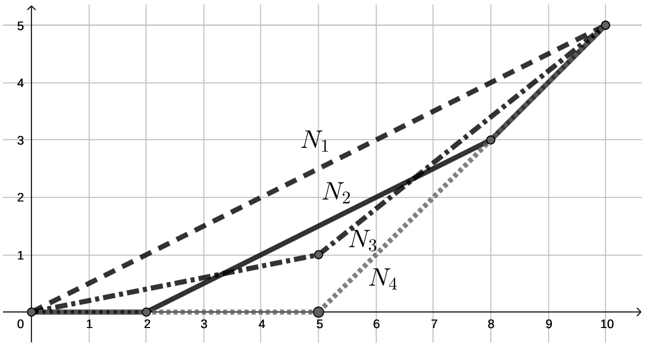

Figure 2: Some Newton polygons: N_1 - dashed, N_2 - solid, N_3 - dashdotted, N_4 - gray and dotted

that any two maximal chains of the introduced poset with the same endpoints have the same length.

In Figure 2, $N_i, i \in \{1,2,3,4\}$ are some eligible Newton polygons of dimension $g = 5$. The Newton polygon N_1 is the one with the slopes $[\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}]$, so the *supersingular Newton polygon*, while N_4 is the *ordinary Newton polygon*, the one with slopes $[0,0,0,0,0,1,1,1,1,1]$. N_2 has slopes $[0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1]$ and lastly, the Newton polygon N_3 has slopes $[\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5}]$. We can see that $N_4 \leq N_2 \leq N_1$ and $N_4 \leq N_3 \leq N_1$, but also that we cannot compare N_2 and N_3.

Consider in $\mathcal{A}_g$ the locus of principally polarized abelian varieties of dimension g whose Newton polygons $NP(A)$ satisfy $N \leq NP(A)$, denoted by $W_N = W_N(\mathcal{A}_g)$, where N is a fixed eligible Newton polygon of dimension g. The sets W_N are closed in $\mathcal{A}_g$ by Grothendieck and Katz, see [22], Theorem 2.3.1. Using the theory of the Dieudonné crystals (related to the theory of Dieudonné modules applied to working with $\mathcal{A}_g$), de Jong and Oort shown in [5], Theorem 4.1 the celebrated *De Jong-Oort's Purity Theorem*, that the Newton polygon stratification jumps purely in codimension 1. If we use the terminology from [8], and say that the **elevation** of an eligible Newton polygon N in dimension g is the number of lattice points (i,j) with $1 \leq i \leq g, j \geq 0$, then every irreducible component of the stratum W_N has codimension equal to the elevation of N.

For the supersingular Newton polygon N, we say that W_N is the **supersingular locus** in $\mathcal{A}_g$, and use the notation $\mathcal{S}_g = \mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ for it. In Section 3, we will discuss some properties of $\mathcal{S}_g$.

Denote by $W_N^0 = W_N^0(\mathcal{A}_g)$ the locally closed locus in $\mathcal{A}_g$ of (principally polarized) abelian varieties whose Newton polygon equals N. Chai and Oort in [4] found that if N is not a supersingular Newton polygon, then both W_N and W_N^0 are geometrically irreducible, and moreover

$$\bigcup_{N' < N} W_{N'}^0 \subseteq \left(W_N^0\right)^{Zar},$$

where $\left(W_N^0\right)^{\mathrm{Zar}}$ is the closure of W_N^0 in $\mathcal{A}_g$. The Purity Theorem implies that for each eligible Newton polygon N of dimension g, the stratum W_N^0 of $\mathcal{A}_g$ defined by N is nonempty and of codimension equal to the elevation of N.

When it comes to curves and to $\mathcal{M}_g$ (the moduli space of curves of genus $g > 0$ over $\overline{\mathbb{F}}_p$), for a Newton polygon N, we can similarly introduce sets $W_N^0(\mathcal{M}_g)$ and $W_N(\mathcal{M}_g)$, as the subsets of $\mathcal{M}_g$ whose points corresponds to curves with Newton polygon equal, and respectively less than or equal to N. The supersingular locus in $\mathcal{M}_g$ is the locus of points corresponding to the supersingular curves.

Alternatively, we may think of these loci in $\mathcal{A}_g$, as of the intersections of the image of $\mathcal{M}_g$ in $\mathcal{A}_g$ with W_N, W_N^0 and $\mathcal{S}_g$ respectively. However, in general, even though W_N, W_N^0 and $\mathcal{S}_g$ are to some extent understood, we cannot say that for their intersections with the open Torelli locus.

2.2.3 Stratification by Ekedahl-Oort type

Let us denote by Z_μ the locus in $\mathcal{A}_g$ consisting of principally polarized abelian varieties of dimension g with Ekedahl-Oort type μ.

For any Young type μ, [37] gives us that the sets Z_μ are locally closed and that they define the *Ekedahl-Oort stratification* of the moduli space $\mathcal{A}_g$. Furthermore, if $\mu = [\mu_1, \dots, \mu_n]$, then the stratum Z_μ has codimension $\sum_{i=1}^n \mu_i$ in $\mathcal{A}_g$.

Consider the set of all Young diagrams in dimension g. Using the constraints we have on the final type v: $v(i) \le v(i+1) \le v(i)+1$ and $v(2g-i) = v(i) - i + g$ for $0 \le i < g$, we see that the choice of the first g "jumps" on the values of $v(i), 0 \le i \le 2g$ determines the complete type μ. Therefore, there are 2^g eligible Young diagrams of dimension g, and they define 2^g strata in the Ekedahl-Oort stratification. Note that further for any μ, from their codimension in $\mathcal{A}_g$, the sets Z_μ are also nonempty. One only needs to check the diagram $\mu = [g, g-1, \dots, 2, 1]$, which corresponds to the non-empty set of superspecial principally polarized abelian varieties. Note also that the diagram $\mu = \varnothing$ defines the largest Ekedahl-Oort stratum in $\mathcal{A}_g$, the ordinary one - we can actually see that it matches with the loci of principally polarized abelian varieties of dimension g with p-rank equal to g, or ones with the ordinary Newton polygon. The first conclusion is by the fact for $\mu = [\mu_1, \dots, \mu_n]$, $p\text{-rank}(A) = g - \mu_1$, and the second one by the characterization of the p-rank of principally polarized abelian varieties of dimension g with fixed Newton polygon N, as the number of slopes 0 in N.

On the set of Young diagrams in dimension g, there is a partial order, that we will (again) denote by $\le$, introduced as

$$\mu = [\mu_1, \dots, \mu_n] \le \nu = [\nu_1, \dots, \nu_m]$$

if $n \le m$ and for all $i \in \{1, 2, \dots, n\}$ it holds that $\mu_i \le \nu_i$. Writing $\overline{Z_\mu}$ for the Zariski closure of Z_μ in $\mathcal{A}_g$ we have

$$\mu \le \nu \implies \overline{Z_\nu} \subseteq \overline{Z_\mu} \text{ in } \mathcal{A}_g.$$

Lastly, we mention [4], Theorem 4.8, a result by Chai and Oort giving a conditions when the Ekedahl-Oort stratum is completely contained in the supersingular locus.

Lemma 2.2 ([4], Theorem 4.8). *Let v be the final type associated to the Young diagram. Then*

$$v\left(\left\lfloor \frac{g+1}{2} \right\rfloor\right) = 0 \implies Z_\mu \subseteq \mathcal{S}_g.$$

2.3 Supersingular curves

Let $g > 0$. Most of the results regarding the supersingular objects are known in terms of abelian varieties, for which, our key reference is the book [27] by Li and Oort.

The supersingular locus $\mathcal{S}_g = \mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ in $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ is of dimension $\lfloor g^2/4 \rfloor$ and the number of its irreducible components can be described using certain class numbers as we will see in Section 3. Also, the generic point of each irreducible component of $\mathcal{S}_g$ has a-number 1, and moreover, if by $\mathcal{S}_g(a \geq 2)$ we denote the closed subset of points of $\mathcal{S}_g$ whose points correspond to the abelian varieties A with $a(A) \geq 2$, then for $g \geq 1$, any irreducible component of $\mathcal{S}_g(a \geq 2)$ is of codimension 1 in $\mathcal{S}_g$. One of the key ingredients in obtaining these results is the use of the theory of Dieudonné modules, which we already referred to a few times while presenting some of the results known in the context of abelian varieties. However, diving into that theory was out of our scope.

We aim to investigate the supersingular curves and to do that in characteristic two. We first mention some differences appearing when working with supersingular curves instead of supersingular principally-polarized abelian varieties and then present some of the relevant results regarding the locus of supersingular curves.

We saw in Section 2.2.1 that the p-rank stratification of $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ and of $\mathcal{M}_g = \mathcal{M}_g \otimes \overline{\mathbb{F}}_p$ behave relatively similarly. However, we are not able to say that for the Newton polygons nor the Ekedahl-Oort types.

Consider any maximal chain of Newton polygons $\{N_i : i \in I\}$ between the supersingular and the ordinary Newton polygon. By the Purity Theorem, it is of length

$$\delta_g = \frac{g(g+1)}{2} - \left\lfloor \frac{g^2}{4} \right\rfloor,$$

and, after relabeling the indices, it defines a stratification $\{W_{N_i} : 0 \leq i \leq \delta_g\}$ of $\mathcal{A}_g$,

$$\mathcal{S}_g = W_{N_0} \subseteq W_{N_1} \subseteq \ldots \subseteq W_{N_{\delta_g}} = \mathcal{A}_g,$$

so that W_{N_i} is of codimension 1 in $W_{N_{i+1}}$. However, we cannot claim the same in the case of $\mathcal{M}_g$, see [38], Expectation 8.5.4 and [41], Section 5.3. Namely, if we take for example $\delta_g > 3g-3$, which happens for $g > 9$, we see that the properties of $\{W_{N_i}(\mathcal{M}_g) : 0 \leq i \leq \delta_g\}$ are not analogous to those previously described. Since $\delta_g > \dim \mathcal{M}_g$, some of the $W_{N_i}(\mathcal{M}_g)$ for $0 \leq i \leq \delta_g$ need to be of the same dimension, which may lead to the fact that some of the $W_N^0(\mathcal{M}_g)$ is empty. In other words, for a fixed Newton polygon N, it can happen that there is no curve whose Newton polygon is N.

In particular, we cannot say much about the supersingular locus in $\mathcal{M}_g$ and we do not even now whether is it empty for some g and p. Heuristically, the dimension of $\mathcal{S}_g$ is a half of the dimension of $\mathcal{A}_g$ and they both grow quadratically, while the dimension of $\mathcal{M}_g$ grows only linearly. When $p = 2$, we will shortly mention the result by van der Geer and van der Vlugt giving us that the supersingular locus is non-empty, and moreover giving us (only) the lower bound for the dimension of the supersingular locus in $\mathcal{M}_g$. However, the question of the irreducibility of this locus, or the number of irreducible components is still unanswered, as well as the question of computing its exact dimension.

Similarly, even though for any Young diagram $\mu = [\mu_1, \ldots, \mu_n]$, the locus Z_μ is of codimension $\sum_{i=1}^n \mu_i$ in $\mathcal{A}_g$, the same conclusion does not apply in general for the locus Z_μ in $\mathcal{M}_g$. There are some partial results, out of which we will mention in the end of this section the one resembling the conclusion for abelian varieties in the case of hyperelliptic curves and characteristic 3.

What seems to be much more approachable while working with curves is the use of the Cartier operator and the computation of the Ekedahl-Oort type of the curves. In particular, we will see in Section 4 that for genus 4 curves over $\overline{\mathbb{F}}_2$, there are some restrictions for the possible a-numbers.

2.3.1 Some relevant results

One of the starting points regarding supersingular curves in characteristic two is the paper [47], where van der Geer and van der Vlugt, for any $g \in \mathbb{Z}_{>0}$ constructed a class of supersingular curves of genus g that are defined over $\overline{\mathbb{F}}_2$. In particular, that showed that in characteristic two, there is a supersingular curve for any possible genus $g > 0$. We use the notation GV_g to denote the locus of supersingular curves in genus g they considered, and describe it below.

Let $\mathcal{R}_h^* = \{\sum_{i=0}^h a_i x^{2^i} : a_i \in \overline{\mathbb{F}}_2, a_h \neq 0\}$ be a $\overline{\mathbb{F}}_2$-vector space of 2-linearized polynomials and let

$$g = 2^{s_1} \cdot (1 + 2 + \ldots + 2^{r_1}) + \ldots + 2^{s_t} \cdot (1 + 2 + \ldots + 2^{r_t})$$

be a unique representation of $g \in \mathbb{Z}_{\geq 0}$ with $s_i, r_i \in \mathbb{Z}_{\geq 0}$ such that $s_i + r_i + 2 \leq r_{i+1}$ for $i \in \{1, \ldots, t-1\}$. If we denote $u_i = s_i + 1 - \sum_{j=1}^{i-1}(r_j + 1)$ for $i \in \{1, \ldots, t\}$, then one of the construction of the class GV_g is as follows. Let further $L_i \subseteq \mathcal{R}_{u_i}^*$ be a $\overline{\mathbb{F}}_2$-vector space of dimension $\dim_{\overline{\mathbb{F}}_2} L_i = r_i + 1$, and let $\mathcal{L} = \bigoplus_{i=1}^t x \cdot L_i$. If $f_1, \ldots, f_n$ form a $\overline{\mathbb{F}}_2$-basis for $\mathcal{L}$, define

$$C_{f_k} : y^2 + y = x \cdot f_k$$

and take $\phi_k : C_{f_k} \to \mathbb{P}^1$ to be morphisms defined on function fields as inclusion $\overline{\mathbb{F}}_2(x) \subseteq \overline{\mathbb{F}}_2(x, y)$. Then the curve $C^{\mathcal{L}}$ defined as a normalization of the fiber product

$$C_{f_1} \times \ldots \times C_{f_n},$$

with respect to the maps ϕ_k, is a supersingular curve of genus g. Choosing a different basis for $\mathcal{L}$ results in a curve that is $\overline{\mathbb{F}}_2(x)$-isomorphic to $C^{\mathcal{L}}$.

The authors also determined completely when the curves defined in this fashion are isomorphic. Firstly, they showed that for $R = \sum_{i=0}^h a_i x^{2^i}, R' = \sum_{i=0}^h a_i' x^{2^i} \in \mathcal{R}_h^*$ for some $h \geq 2$, the curves $C_R : y^2 + y = x \cdot R, C_{R'} : y^2 + y = x \cdot R'$ are isomorphic if and only if there is some $\rho \in \overline{\mathbb{F}}_2$ such that for all $i = 1, \ldots, h$, it holds that $a_i' = \rho^{2^i + 1} a_i$. Using that and choosing the basis elements f_k for $\mathcal{L}$ whose coefficient for x is zero, they obtained that $C^{\mathcal{L}}$ is isomorphic over $\overline{\mathbb{F}}_2$ with $C^{\mathcal{L}'}$ is and only if $\mathcal{L} \cong \mathcal{L}'$ as $\overline{\mathbb{F}}_2$-vector spaces via an isomorphism of the form $x \mapsto \rho x$ for some $\rho \in \overline{\mathbb{F}}_2^*$. Using this, they showed that for $g \neq 2$, the dimension of the supersingular locus in the coarse moduli space M_g is greater than or equal to

$$\sum_{i=1}^t (r_i + 1) u_i - 1.$$

In case $g = 3$ for $p > 0$ a prime number, both the moduli space of curves $\mathcal{M}_3 = \mathcal{M}_3 \otimes \overline{\mathbb{F}}_p$ and the moduli space of principally polarized abelian varieties $\mathcal{A}_3 = \mathcal{A}_3 \otimes \overline{\mathbb{F}}_p$ have dimension

$$\dim \mathcal{M}_3 = 3 \cdot 3 - 3 = 6 = \frac{3 \cdot (3 + 1)}{2} = \dim \mathcal{A}_3,$$

while the supersingular locus $\mathcal{S}_3 = \mathcal{S}_3 \otimes \overline{\mathbb{F}}_p$ has dimension 3. In [36], Oort explored the intersection of the supersingular locus $\mathcal{S}_3$ with the locus of hyperelliptic curves of compact type of genus $g = 3$ over $\overline{\mathbb{F}}_p$, that is of dimension 5. He showed that every component of this intersection, i.e., of the locus of (the image in $\mathcal{A}_3$ of the) supersingular hyperelliptic curves of compact type of genus $g = 3$ over $\overline{\mathbb{F}}_p$ has dimension 1.

In particular, for $p = 2$, he constructed a curve of genus $g = 3$ over $\overline{\mathbb{F}}_2$ that is non-hyperelliptic and supersingular, as well as a curve of compact type that is supersingular hyperelliptic. Then, using class number formula computations (that we will meet in Section 3) for the result that $\mathcal{S}_3 \otimes \overline{\mathbb{F}}_2$ is irreducible, the mentioned result that the locus of supersingular hyperelliptic curves of compact type of genus $g = 3$ over $\overline{\mathbb{F}}_2$ is of dimension 1 follows by a dimension argument. However, it turns out that in the case $p = 2$, there is no supersingular hyperelliptic (irreducible) curve. This is concluded by inspecting what the possibilities are for an automorphism group of a Jacobian of a supersingular hyperelliptic (irreducible) curve of genus $g = 3$, and by arguing that none of those can exist.

From van der Geer and van der Vlugt's construction, we extract that for $g = 4$, the locus GV_4 of non-isomorphic supersingular curves of genus $g = 4$ defined over $\overline{\mathbb{F}}_2$ consists of curves that can be represented in the form

$$y^2 + y = x^9 + c_5x^5 + c_3x^3,$$

with $c_3, c_5 \in \overline{\mathbb{F}}_2$ arbitrary.

Moreover, in [43], using so-called *2-adic box analysis* for obtaining lower bound for the first slopes of the Newton polygons of curves, Scholten and Zhu concluded that the locus of hyperelliptic supersingular curves of genus $g = 4$ over $\overline{\mathbb{F}}_2$ precisely equals the locus GV_4. In other words, a hyperelliptic curve of genus $g = 4$ over $\overline{\mathbb{F}}_2$ is supersingular if and only if it is isomorphic to one with affine equation $y^2 + y = x^9 + c_5x^5 + c_3x^3$, for some $c_3, c_5 \in \overline{\mathbb{F}}_2$. This completely describes supersingular hyperelliptic curves and is the reason why we will be interested in this thesis in considering non-hyperelliptic supersingular curves of genus $g = 4$ over $\overline{\mathbb{F}}_2$.

Lastly, let us mention some relevant results for curves of genus 4, that discuss characteristics other than two.

In [25], the authors showed the existence of a supersingular curve of genus 4 in any characteristic $p > 0$ by considering the *Howe curves*, the curves obtained as desingularizations of some fiber products of elliptic curves over $\mathbb{P}^1$.

By discussing the Cartier operator on curves, in [42] Re gave some bounds for the a-number of curves in terms of the genus and the characteristic in which a curve is defined. Also, by considering a special class of curves that are certain cyclic covers of the projective line, in [28], the authors showed the existence of some supersingular curves of genus $4 \leq g \leq 11$ depending on the characteristic. We will discuss and use some of these results in Section 4.

Furthermore, in [50], Zhou discussed the Ekedahl-Oort type in the moduli space $\mathcal{M}_4$. By considering a special class of curves, there it is showed that for any prime $p \equiv \pm 2 \mod 5$ the locus $Z_{[4,2]}$ of curves with Ekedahl-Oort type $[4, 2]$ in $\mathcal{M}_4 \otimes \overline{\mathbb{F}}_p$ is nonempty, while for $p > 2$ and $p \equiv \pm 2 \mod 5$, $Z_{[4,3]}$ is nonempty. In particular, the last fact implies that for p odd and $p \equiv \pm 2 \mod 5$, the supersingular locus in $\mathcal{M}_4 \otimes \overline{\mathbb{F}}_p$ is nonempty by Lemma 2.2. Also, for $p = 3$, it was shown that for a Young diagram $\mu = [\mu_1, \ldots, \mu_n]$, the intersection Z_μ with the hyperelliptic locus $\mathcal{H}_4$ is empty if $\mu \geq [3, 2, 1]$, and otherwise, of (the expected) codimension $\sum_{i=1}^{n} \mu_i$ in $\mathcal{H}_g$.

3 Class numbers and number of the irreducible components of $S_g \subseteq A_g$ over $\overline{\mathbb{F}}_2$.

A basic question that arises while investigating (the geometry of) supersingular abelian varieties is whether we can tell something about the irreducibility of the supersingular locus $\mathcal{S}_g$ in the moduli space of principally polarized abelian varieties $\mathcal{A}_g$, or generally, about its number of irreducible components. Oort, Katsura, Ibukiyama, and Li connected the problem of counting the number of these components with the problem of computing certain class numbers. In [19], Ibukiyama, Katsura and Oort firstly did that for $g = 2$, and then in [21], Katsura and Oort considered $g = 3$. Finally, in [27], Section 4, Li and Oort generalized results of the previous papers and obtained a conclusion for arbitrary g. Here, we first present some of the general theory from [27] together with some introductory examples. Using mass formulas and the results from lower g, we discuss the case $g = 4$ and show that $\mathcal{S}_4$ is irreducible in $\mathcal{A}_4$. Lastly, we shortly discuss the irreducibility questions for some small genera g.

As for example in [13], Section 1, for $a, b \in \mathbb{Q}^*$, the **quaternion algebra** $B = (a, b)_{\mathbb{Q}}$ over $\mathbb{Q}$ is a 4-dimensional $\mathbb{Q}$-algebra

$$(a, b)_{\mathbb{Q}} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

with i, j some of its elements, satisfying $i^2 = a, j^2 = b$ and $ij = -ji$. We usually write $k = ij$ and in addition, we say that B is definite if $a, b < 0$.

For a quaternion $q = x + yi + zj + wk \in (a, b)_{\mathbb{Q}}$, we introduce its **conjugate** $\bar{q}$ as

$$\bar{q} = x - yi - zj - wk,$$

and its **norm**

$$N(q) = q\bar{q} = x^2 - ay^2 - bz^2 + abw^2 \in \mathbb{Q}.$$

The main example is when $a = b = -1$. Then in $(-1, -1)_{\mathbb{Q}}$ it follows that $i^2 = j^2 = -1$, $ij = -ji$ and for $q = x + yi + zj + wk$ with $x, y, z, w \in \mathbb{Q}$, we have $N(q) = x^2 + y^2 + z^2 + w^2$.

We say that $(a, b)_{\mathbb{Q}}$ is **split** if it is isomorphic to $M_2(\mathbb{Q})$ as $\mathbb{Q}$-algebra, and for any finite place p of $\mathbb{Q}$ (so the equivalence class of a non-archimedean absolute value or valuation), we say that $(a, b)_{\mathbb{Q}}$ is **split at** p if it is, after tensoring with $\mathbb{Q}_p$, isomorphic to $M_2(\mathbb{Q}_p)$ as a $\mathbb{Q}_p$-algebra.

An **order** $\mathcal{O}$ of a finite-dimensional $\mathbb{Q}$-algebra B is a subring of B which spans B over $\mathbb{Q}$ and is a $\mathbb{Z}$-lattice in B. For any $n \in \mathbb{Z}_{>0}$, B a finite-dimensional $\mathbb{Q}$-algebra and $\mathcal{O}$ a maximal order of B^n, we say that a $\mathbb{Z}$-module L in B^n is a **left $\mathcal{O}$-lattice** in B^n if it is a left $\mathcal{O}$-module as well as a $\mathbb{Z}$-lattice in B^n.

As a motivation for the definitions that follow, we mention that for every prime $p \in \mathbb{Z}_{>0}$ there is an elliptic curve E over $\mathbb{F}_p$ such that its relative Frobenius $F : E \to E^{(p)}$ is such that $F^2 + p = 0$. Such an elliptic curve always exists, and it is in fact supersingular; this follows from the Hasse bound and some of the equivalent statements of being supersingular and by the Eichler-Deuring mass formula; see [44], Exercise V.5.8 and Exercise V.5.9. Moreover, for $\mathcal{O}_E = \mathrm{End}(E \otimes \overline{\mathbb{F}}_p) = \mathrm{End}(E \otimes \mathbb{F}_{p^2})$ it holds that $\mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_E) = 4$, and $B_E = \mathrm{End}^0(E \otimes \overline{\mathbb{F}}_p) = \mathrm{End}^0(E \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Q} = Q_{\infty,p}$ is a quaternion algebra that is split at all primes $l \neq p$, and $\mathcal{O}_E$ is a maximal order in B_E.

Let $p \in \mathbb{Z}_{>0}$ be an arbitrary prime number. Let B be the definite quaternion algebra defined over the field of rational numbers $\mathbb{Q}$ that is split at all prime numbers $l \neq p$, i.e., it is of discriminant

p, and let $\mathcal{O}$ be a maximal order of B. For any $g \in \mathbb{Z}_{>0}$, if L is a (left) $\mathcal{O}$-lattice in $B^{\oplus g}$, we have that it is of the form $\mathcal{O}^{\oplus g} m_L$ with $m_L \in \mathrm{GL}_g(B)$.

We define **the group of similitudes** G by

$$G = \{h \in M_g(B) : h\bar{h}^t = n(h)\mathrm{Id}_g \text{ for some } n(h) \in \mathbb{Q}^*\}.$$

We say that two $\mathcal{O}$-lattices L_1 and L_2 in $B^{\oplus g}$ are **globally equivalent** and write $L_1 \approx L_2$ if there is some $h \in G$ for which $L_1 = L_2 h$. Similarly, if we write $B_l = B \otimes_{\mathbb{Q}} \mathbb{Q}_l, \mathcal{O}_l = \mathcal{O}_l \otimes_{\mathbb{Q}} \mathbb{Q}_l$ and $L_l = L \otimes_{\mathbb{Q}} \mathbb{Q}_l$ for any prime number $l \in \mathbb{Z}_{>0}$, we define locally the group of similitudes

$$G_l = \{h \in M_g(B_l) : h\bar{h}^t = n(h)\mathrm{Id}_g \text{ for some } n(h) \in \mathbb{Q}_l^*\},$$

and we say that any two $\mathcal{O}_l$-lattices $L_{1,l}$ and $L_{2,l}$ are equivalent locally at l, and write $L_{1,l} \sim L_{2,l}$ if $L_{1,l} = L_{2,l} h$ for some $h \in G_l$.

Lastly, for g even, let us denote by N_p the $\mathcal{O}_p$-lattice in $B_p^{\oplus g}$ defined by

$$N_p = \mathcal{O}_p^{\oplus g} \begin{pmatrix} \mathrm{Id}_k & \\ & \pi \mathrm{Id}_k \end{pmatrix} \xi, \tag{5}$$

with π a prime element of $\mathcal{O}_p$ and $\xi \in \mathrm{GL}_g(B_p)$ such that $\xi\bar{\xi}^t = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$.

The **principal genus** $\mathcal{L}_g(p,1)$ **of the (hermitian) space** $B^{\oplus g}$ is the set of all $\mathcal{O}$-lattices L of $B^{\oplus g}$ which are locally at all prime numbers $l \in \mathbb{Z}_{>0}$ equivalent to $\mathcal{O}_l^{\oplus g}$, i.e., $L_l \sim \mathcal{O}_l^{\oplus g}$ for all primes $l \in \mathbb{Z}_{>0}$. We further call the number of global equivalence classes in $\mathcal{L}_g(p,1)$ **the class number of the principal genus**, and write $H_g(p,1) = \#(\mathcal{L}_g(p,1)/\approx)$. Similarly, we define the **non-principal genus** $\mathcal{L}_g(1,p)$, the set of $\mathcal{O}$-lattices L such that $L_l \sim \mathcal{O}_l^{\oplus g}$ for all prime numbers $l \in \mathbb{Z}_{>0}, l \neq p$ and $L_p \sim N_p$, and we call $H_g(1,p)$ **the class number of the non-principal genus**, the number of global equivalence classes in that genus $H_g(1,p) = \#(\mathcal{L}_g(1,p)/\approx)$.

In terms of the previously introduced notions, we can get a piece of information on the supersingular locus in the moduli space of the principally polarized abelian varieties. Namely, we will see in Theorem 3.2 that the number of irreducible components of $\mathcal{S}_g = \mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ equals $H_g(p,1)$ if the genus g is odd or $H_g(1,p)$ when g is even.

Example 3.1. *In the case we will be mostly interested in, when B is the quaternion algebra over $\mathbb{Q}$ with discriminant $p = 2$, we have*

$$B = (-1,-1)_{\mathbb{Q}} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

with $k = ij, i^2 = j^2 = -1$ and $ij = -ji$, and

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}.$$

Additionally, for $g = 4$ we have $N_2 = \mathcal{O}_2^{\oplus 4} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \pi & \\ & & & \pi \end{pmatrix}\xi$, where $\xi \in \mathrm{GL}_4(B_2)$ is such that $\xi\bar{\xi}^t = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}$, and for computing $\#\{$irreducible components of $\mathcal{S}_4\}$, we are interested in computing $\#(\mathcal{L}_4(1,2)/\approx)$, i.e., in finding non-equivalent left $\mathcal{O}$-lattices L in $B^{\oplus 4}$ such that $L_l \sim \mathcal{O}_l^{\oplus 4}$ for all primes $l \neq 2$ and $L_2 \sim N_2$. When $g = 5$, we are interested in $L \in \mathcal{L}_5(2,1)$, i.e., the ones for which $L_l \sim \mathcal{O}_l^{\oplus 5}$ for all prime l.

3.1 The supersingular locus $\mathcal{S}_g = \mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ in $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$

Here, we will make a brief summary of the theory used in [27] to describe the supersingular locus $\mathcal{S}_g = \mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ in $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$. We also consult the material from [20].

Fix a supersingular elliptic curve E over $\mathbb{F}_p$ to be as in the motivation from Section 3 and F, V its relative Frobenius and Verschiebung morphism. Let K be any field containing $\mathbb{F}_p$ and k an algebraically closed field such that $K \subseteq k$. Furthermore, let η be a polarization of $E^g \times K = E^g \times_{\operatorname{Spec}(\mathbb{F}_p)} \operatorname{Spec}(K)$ such that $\ker(\eta) = E^g[F^{g-1}] \times K$, which exists for any $K \supseteq \mathbb{F}_{p^2}$; see [27], Section 3.6. Recall that the supersingular abelian varieties X are the ones with $X \times k \sim E^g \times k$, while the superspecial abelian varieties are the ones with $X \times k \cong E^g \times k$.

For $g \geq 2$ and X an arbitrary supersingular abelian variety of dimension g over K, we cite [27], Lemma 1.8, that there always exists a superspecial abelian variety Y and a K-isogeny

$$\rho : Y \to X,$$

called a minimal isogeny. The construction of such an isogeny is done inductively, by considering certain quotients, and it motivates the following definition.

Let S be a K-scheme and η as above. A **polarized flag type quotient** (PFTQ) over S with respect to η is a chain of polarized varieties $(Y_i, \lambda_i), 0 \leq i < g$ over S:

$$(Y_\bullet, \rho_\bullet) : (Y_{g-1}, \lambda_{g-1}) \xrightarrow{\rho_{g-1}} (Y_{g-2}, \lambda_{g-2}) \xrightarrow{\rho_{g-2}} \dots \xrightarrow{\rho_1} (Y_0, \lambda_0),$$

such that

1. $Y_{g-1} = E^g \times S$, $\lambda_{g-1} = \eta \times id_S$
2. ρ_i are isogenies compatible with polarizations, i.e., $\rho_i^\vee \circ \lambda_{i-1} \circ \rho_i = \lambda_i$ for $1 \leq i < g$,
3. $\ker(\rho_i)$ is an α-group of α-rank i, $1 \leq i < g$, i.e., $\ker(\rho_i)$ is locally isomorphic to $\underbrace{\alpha_p \times \dots \alpha_p}_{i} \times S$,
4. $\ker(\lambda_i) \subseteq \ker(F^{i-j} \circ V^j)$ for all $j \in \{0, 1, \dots, \lfloor i/2 \rfloor\}$.

If moreover

$$\ker(Y_{g-1} \to Y_i) = \ker(Y_{g-1} \to Y_0) \cap Y_{g-1}[F^{g-1-i}]$$

for all $1 \leq i < g$ we call it a **rigid PFTQ**.

For an arbitrary polarization η of $E^g \times K$ such that $\ker(\eta) = E^g[F^{g-1}]$, by [27], Lemma 3.8, there is a projective space $\mathcal{P}'_{g,\eta}$ over K that represents the functor

$$\underline{K\text{-Schemes}} \to \underline{Sets},$$

$$S \mapsto \{\text{rigid PFTQs over } S \text{ with repect to } \eta\} / \cong .$$

Moreover, by [27], Proposition 4.3, $\mathcal{P}'_{g,\eta}$ is non-singular, and geometrically integral of dimension

$$\dim_k \mathcal{P}'_{g,\eta} = \left\lfloor \frac{g^2}{4} \right\rfloor.$$

Let Λ be a set of representatives of polarizations η, with $\ker(\eta) = E^g[F^{g-1}]$ of $E^g \times \overline{\mathbb{F}}_p$ up to isomorphism, where

$$\eta_1 \cong \eta_2 \Longleftrightarrow \phi^\vee \eta_1 \phi = \eta_2 \text{ for some } \phi \in \operatorname{Aut}(E^g \times \overline{\mathbb{F}}_p).$$

Using [27], Proposition 4.1, which says that for any principally polarized supersingular abelian variety (X, λ) of dimension g over $\overline{\mathbb{F}}_p$ there are finitely many, but at least one, rigid PFTQs with respect to some $\eta \in \Lambda$, $(Y_\bullet, \rho_\bullet)$ over $\overline{\mathbb{F}}_p$ such that $(Y_0, \lambda_0) \cong (X, \lambda)$, there is a finite and surjective morphism

$$\Psi : \coprod_{\eta \in \Lambda} \mathcal{P}'_{g,\eta} \to \mathcal{S}_g \otimes \overline{\mathbb{F}}_p. \tag{6}$$

Therefore, understanding the structure of $\mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ can be understood by understanding $\Psi(\mathcal{P}'_{g,\eta})$ for $\eta \in \Lambda$. It turns out that Ψ induces a one-to-one correspondence between the set Λ and the set of irreducible components of $\mathcal{S}_g \otimes \overline{\mathbb{F}}_p$. After presenting the theorem describing the main properties of the supersingular locus $\mathcal{S}_g$ based on the use of (6), we will try to give an insight into the connections between $\#\Lambda$ and the class numbers mentioned in the introduction.

Theorem 3.2 ([27], Theorem 4.9)**.** *Let $p \in \mathbb{Z}_{>0}$ be a prime number and let $g \in \mathbb{Z}_{>0}$. The supersingular locus $\mathcal{S}_g = \mathcal{S}_g \otimes \overline{\mathbb{F}}_p$ in $\mathcal{A}_g = \mathcal{A}_g \otimes \overline{\mathbb{F}}_p$ has dimension $\left\lfloor \frac{g^2}{4} \right\rfloor$. Furthermore, it holds that*

$$\#\{\textit{irreducible components of } \mathcal{S}_g\} = \begin{cases} H_g(p,1) & \textit{if } g \textit{ is odd} \\ H_g(1,p) & \textit{if } g \textit{ is even} \end{cases}$$

The key ingredient of the proof is that for any $\eta \in \Lambda$, $\Psi(\mathcal{P}'_{g,\eta}) = (X, \lambda)$ is a *supergeneral abelian variety*, that is a supersingular (principally polarized) abelian variety with $a(X) = 1$. For such (X, λ), the rigid PFTQ over $\overline{\mathbb{F}}_p$ satisfies

$$\ker(\lambda_{g-1}) = \ker(F^{g-1} : Y_{g-1} \to Y_{g-1}) = Y_{g-1}[F^{g-1}],$$

or in other words $\ker(\eta) = E^g[F^{g-1}]$. Now, since for $g = 2m+1$, $E^{g-1}[F^{g-1}] \subseteq E^g[p^m]$ and using that $\deg F^{g-1} = \deg[p^m]$, we actually get

$$\ker(\eta) = E^g[p^m], \quad \text{if } g = 2m+1 \text{ is odd}$$

and similarly, we obtain

$$\ker(\eta) = E^g[p^m F], \quad \text{if } g = 2m+2 \text{ is even.}$$

Therefore, using [27], Corollary 4.8 which gives us:

- The number of equivalence classes of polarization η of $E^g \otimes \overline{\mathbb{F}}_p$ such that $\ker(\eta) = \ker([p^n])$ is equal to $H_g(p,1)$, and
- The number of equivalence classes of polarization η of $E^g \otimes \overline{\mathbb{F}}_p$ such that $\ker(F^{2n+1}) \subseteq \ker(\eta)$ and $\#(\ker(\eta)) = p^{2(ng + \lfloor (g+1)/2 \rfloor)}$, for any $n \in \mathbb{Z}_{>0}$, is equal to $H_g(1,p)$,

we get the desired conclusion

$$\#\Lambda = \begin{cases} H_g(p,1) & \text{if } g \text{ is odd} \\ H_g(1,p) & \text{if } g \text{ is even} \end{cases}$$

The mentioned Corollary is obtained in [27] using the following lemma. We will not present its whole proof, and our focus will be on showing the explicit relation between computing the number of irreducible components, polarizations and certain lattices.

Lemma 3.3 ([19], Theorem 2.10, and [27], Proposition 4.7)**.** *The following results hold.*

1. *The class number $H_g(p,1)$ is equal to the number of equivalence classes of principal polarizations of $A = E^g \otimes \mathbb{F}_p$ up to isomorphism of A.*

2. *The class number $H_g(1,p)$ is equal to the number of equivalence classes of polarization η of $E^g \otimes \overline{\mathbb{F}}_p$ with $\ker(F) \subseteq \ker(\eta)$ and $\deg(\eta) = p^{\lfloor (g+1)/2 \rfloor}$.*

Sketch of a proof for part 1. For $E = E \otimes \overline{\mathbb{F}}_p$, denote $A = E^g$ and $\mathcal{O} = \mathrm{End}(E)$, $B = \mathcal{O} \otimes \mathbb{Q}$, and let

$$D = E^{g-1} \times \{0\} + E^{g-2} \times \{0\} \times E + \ldots + \{0\} \times E^{g-1}$$

be a divisor on A. By [33], page 60, we have that D is ample if and only if the set of $\overline{\mathbb{F}}_p$-points P on A such that $\tau_P^* D = D$ is finite, for τ_P the translation as in Section 1, using the equivalence of the divisors and invertible sheaves. Therefore, D defines a polarization φ_D, for which in [19] it is stated that it is principal.

Note that for divisors $H \in \mathrm{Pic}^0(A)$ we have $\varphi_H = 0$, so the mapping

$$\mathrm{Pic}(A)/\mathrm{Pic}^0(A) \to \mathrm{Hom}(A, A^\vee)$$

is injective. The group $NS(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ is called the *Néron-Severi group.* We say that $\gamma \in \mathrm{GL}_g(A)$ is *positive definite* and write $\gamma > 0$ if for all $y \in B^n$, it holds that $y\gamma\bar{y}^t > 0$. The mapping

$$NS(A) \to \mathrm{End}(A) = M_g(\mathcal{O}), H \mapsto \varphi_D^{-1} \circ \varphi_H$$

induces by [19], Proposition 2.8 a bijection between the set of principal polarizations on A and the set $S = \{\gamma \in \mathrm{GL}_g(\mathcal{O}) : \gamma = \bar{\gamma}^t > 0\}$. Then [19], Lemma 2.3, gives that any $\mathcal{O}$-lattice $L = \mathcal{O}^g x$, $x \in GL_g(B)$ is in $\mathcal{L}_g(p,1)$ if and only if there are some $\gamma \in \mathrm{GL}_g(\mathcal{O}), n \in \mathbb{Q}_{>0}$ such that $\gamma = \bar{\gamma}^t$ and $x\bar{x} = n\gamma$.

Consider the mapping from the set of principal polarizations on A to $\mathcal{L}_g(p,1)$, induced by $NS(A) \to \mathcal{L}_g(p,1)$. We should show that taking equivalence classes from these define the bijection. On one hand, for any automorphism γ of A and $H_1, H_2 \in NS(A)$, we have that $\gamma^* H_1 = H_2$ if and only if

$$(\varphi_D^{-1}\gamma^\vee\varphi_D)(\varphi_D^{-1}\varphi_{H_1})\gamma = \varphi_D^{-1}\varphi_{H_2}.$$

On the other hand, [27], Lemma 2.5, gives us that two lattices $L_1 = \mathcal{O}^g x_1$ with $x_1\bar{x_1}^t = n_1\gamma_1, \gamma_1 \in \mathrm{GL}_g(\mathcal{O}), n_1 \in \mathbb{Q}_{>0}$ and $L_2 = \mathcal{O}^g x_2$ with $x_2\bar{x_2}^t = n_2\gamma_2, \gamma_2 \in \mathrm{GL}_g(\mathcal{O}), n_2 \in \mathbb{Q}_{>0}$ are globally equivalent if and only if for some $n \in \mathbb{Q}_{>0}, \gamma \in \mathrm{GL}_n(\mathcal{O})$ it holds that

$$\bar{\gamma}^t\gamma_1\gamma = n\gamma_2.$$

We have $\gamma_1 = \varphi_D^{-1}\varphi_{H_1}$ and $\gamma_2 = \varphi_D^{-1}\varphi_{H_2}$, so $\gamma = \bar{\gamma}^t = \varphi_D^{-1}\gamma^\vee\varphi_D$ should give the result. □

3.2 Mass formulas and irreducibility of $\mathcal{S}_4 = \mathcal{S}_4 \otimes \overline{\mathbb{F}}_2$ in $\mathcal{A}_4 = \mathcal{A}_4 \otimes \overline{\mathbb{F}}_2$

In addition to the previously introduced notions, for fixed prime number p, an even $g > 0$, B a quaternion algebra of discriminant p over $\mathbb{Q}$, and $\mathcal{O} \subseteq B$ a maximal order in B as before, let us define the group G_l^* for any prime number l by

$$G_l^* = \{h \in M_g(B_l) : h \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \bar{h}^t = n(h) \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}, \text{ for some } n(h) \in \mathbb{Q}_l^*\}.$$

If $\xi \in \mathrm{GL}_g(B_l)$ is such that $\xi\bar{\xi}^t = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$, then the mapping $h \mapsto \xi h \xi^{-1}$ induces a group isomorphism between G_l and G_l^*.

The local conditions defining $\mathcal{L}_g(1,p)$ give that an arbitrary $\mathcal{O}$-lattice $L \in \mathcal{L}_g(1,p)$ introduced above should be written in a simpler form using G_p^*. Namely, in [17], Part III, we find that an $\mathcal{O}$-lattice L in $B^{\oplus g}$ is in $\mathcal{L}_g(1,p)$ if for all $l \neq p$ we have

$$L_l = \mathcal{O}^{\oplus g} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \end{pmatrix} h_l = (\underbrace{\mathcal{O}_l, \dots, \mathcal{O}_l}_{g}) h_l$$

for some $h_l \in G_l^*$, and

$$L_p = \mathcal{O}^{\oplus g} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \pi & \\ & & & \ddots \end{pmatrix} h_p = (\underbrace{\mathcal{O}_p, \dots, \mathcal{O}_p}_{g/2}, \underbrace{\pi\mathcal{O}_l, \dots, \pi\mathcal{O}_l}_{g/2}) h_p$$

for some $h_p \in G_p^*$, where π is a prime element of $\mathcal{O}_p$. Using that the matrices of the form

$$\begin{pmatrix} 1 & & & & & & \\ & & & & & 1 & \\ & & & & 1 & & \\ & & & \iddots & & & \\ & & 1 & & & & \\ & 1 & & & & & \\ & & & & & & 1 \end{pmatrix}$$

belong to G_p^* for the appropriate dimensions, we see that the second condition can also be interpreted as $L_p = (\overbrace{\underbrace{\mathcal{O}_p, \pi\mathcal{O}_p}_{2}, \dots, \underbrace{\mathcal{O}_p, \pi\mathcal{O}_p}_{2}}^{g}) h_p$ for some $h_p \in G_p^*$.

It is known by Hashimoto and Ibukiyama, [17], Part II and by Ibukiyama, Katsura and Oort, [19], Remark 2.17, that the locus of supersingular abelian varieties of dimension $g = 2$ over $\overline{\mathbb{F}}_2$ is irreducible, i.e., that $H_2(1,2) = 1$. Thinking in terms of lattices, this gives us a unique (up to global equivalence) lattice $L = \mathcal{O}^{\oplus 2} m_L \in \mathcal{L}_2(1,2)$, for some $m_L \in \mathrm{GL}_2(B)$. We will decide whether the supersingular locus in $\mathcal{A}_4$ is irreducible by applying the known results in the case $g = 2$ for the case $g = 4$, and therefore, let us denote by $G_{g=2}$ and $G_{g=4}$ the groups of similitudes G of the corresponding dimensions $g = 2$ and $g = 4$ respectively, and for prime numbers $p \in \mathbb{Z}_{>0}$ similarly $G_{p,g=2}, G_{p,g=4}$ for the local groups of similitudes G_p, and $G^*_{p,g=2}, G^*_{p,g=4}$ for the groups G_p^*. Note that for any prime p and $h \in M_g(B_p)$ we have

$$\left(\begin{array}{c|c} h & \\ \hline & h \end{array}\right)\begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}\left(\begin{array}{c|c} \bar{h}^t & \\ \hline & \bar{h}^t \end{array}\right) = \left(\begin{array}{c|c} & h\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\bar{h}^t \\ \hline h\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\bar{h}^t & \end{array}\right),$$

and thus $h \in G^*_{g=2,p}$ implies that $\left(\begin{array}{c|c} h & \\ \hline & h \end{array}\right) \in G^*_{g=4,p}$.

Let $\hat{L}$ be the $\mathcal{O}$-lattice in $B^{\oplus 4}$ defined by $\hat{L} = \mathcal{O}^{\oplus 4}\left(\begin{array}{c|c} m_L & \\ \hline & m_L \end{array}\right)$. Since locally at any prime $p \neq 2$, $L_p \sim \mathcal{O}_p^{\oplus 2}$ we have that $\hat{L}_p \sim (\mathcal{O}_2, \mathcal{O}_2, \mathcal{O}_2, \mathcal{O}_2)$ and similarly, for $p = 2$, we have $\hat{L}_2 \sim (\mathcal{O}_2, \pi\mathcal{O}_2, \mathcal{O}_2, \pi\mathcal{O}_2)$. Therefore, $\hat{L} \in \mathcal{L}_4(1,2)$. The aim is to check whether $\hat{L}$ is the unique element of $\mathcal{L}_4(1,2)$ up to equivalence.

For any $g \in \mathbb{Z}_{>0}$ and prime $p \in \mathbb{Z}_{>0}$, let us for an $\mathcal{O}$-lattice Λ in $B^{\oplus g}$ define its automorphism group $\mathrm{Aut}(\Lambda) = \{h \in G : \Lambda = \Lambda h\}$. Further, let us define the **mass of the non-principal genus** $\mathcal{L}_g(1,p)$ by

$$\mathrm{Mass}(\mathcal{L}_g(1,p)) = \sum_{\Lambda \in \mathcal{L}_g(1,p)/\approx} \frac{1}{|\mathrm{Aut}(\Lambda)|}.$$

Note that there are precisely $H_g(1,p)$ summands in the previous formula.

Theorem 3.4 ([14], Proposition 3.5.3; [20] Theorem 2.4)**.** *Let $g \in \mathbb{Z}_{>0}$ be an even integer and let $p \in \mathbb{Z}_{>0}$ by any prime number. Then*

$$\mathrm{Mass}(\mathcal{L}_g(1,p)) = \frac{(-1)^{g(g+1)/2}}{2}\prod_{i=1}^{g}\zeta(1-2i)\prod_{i=1}^{g/2}(p^{4i-2}-1),$$

where ζ is the Riemann zeta function.

If we take a look at the table of the first few values of the Riemann zeta function $\zeta(-1) = -\frac{1}{12}, \zeta(-3) = \frac{1}{120}, \zeta(-5) = -\frac{1}{252}$ and $\zeta(-7) = \frac{1}{240}$ occurring in the special case we are interested in, when $p = 2$ and $g = 2$ or $g = 4$, we get

$$\mathrm{Mass}(\mathcal{L}_2(1,2)) = \frac{1}{1920}, \quad \mathrm{Mass}(\mathcal{L}_4(1,2)) = \frac{1}{2 \cdot 1920^2}. \tag{7}$$

Now, if we show that $|\mathrm{Aut}(\hat{L})| = 2 \cdot 1920^2$, we will immediately get that the locus $\mathcal{S}_4$ is irreducible in $\mathcal{A}_4$. Recall that $H_2(1,2) = 1$ and $L \in \mathcal{L}_2(1,2)$, and see that (7) gives us $|\mathrm{Aut}(L)| = 1920$. Moreover, in [18], Section 2, this group $\Gamma_2 = \mathrm{Aut}(L)$ is explicitly given as $m^{-1}\mathrm{GL}_2(\mathcal{O})m \cap G_{g=2}$ where $m = \begin{pmatrix} 1 & -1 \\ 0 & r \end{pmatrix}$ with $r = i - k$, and consists of the elements of the following forms

$$\begin{pmatrix} ar^{-1} & -aa_0r^{-1} \\ ar^{-1} & aa_0r^{-1} \end{pmatrix}, \quad \begin{pmatrix} ar^{-1} & aa_0r^{-1} \\ -ar^{-1} & aa_0r^{-1} \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & aa_0 \end{pmatrix}, \quad \begin{pmatrix} 0 & a \\ aa_0 & 0 \end{pmatrix}, \text{ or } \begin{pmatrix} (1+xr^{-1})a & xaa_0r^{-1} \\ xar^{-1} & (1+xr^{-1})aa_0 \end{pmatrix},$$

with $a \in \mathcal{O}^*, a_0 \in \{\pm 1, \pm i, \pm j, \pm k\}$ and $x \in \{-i, k, \frac{\pm 1 - i \pm j + k}{2}\}$.

Using that $\mathcal{O}^{\oplus 2}m_L = \mathcal{O}^{\oplus 2}m_Lh$ for $h \in \Gamma_2$ if and only if there is an element $n_L \in \mathrm{GL}_2(\mathcal{O})$ such that $n_Lm_L = m_Lh$, i.e., $m_L^{-1}n_Lm_L = h$ we see that actually $m_L = m = \begin{pmatrix} 1 & -1 \\ 0 & r \end{pmatrix}$. With the same argument, we see that $\Gamma_4 = \mathrm{Aut}(\hat{L}) = \left(\begin{array}{c|c} m_L^{-1} & \\ \hline & m_L^{-1} \end{array}\right) \mathrm{GL}_4(\mathcal{O}) \left(\begin{array}{c|c} m_L & \\ \hline & m_L \end{array}\right) \cap G$. Thus, $\left(\begin{array}{c|c} A & \\ \hline & B \end{array}\right), \left(\begin{array}{c|c} & A \\ \hline B & \end{array}\right) \in \Gamma_4$ for any $A, B \in \Gamma_2$. Therefore, we have $|\Gamma_4| \geq 2 \cdot 1920^2$.

To show that actually $|\Gamma_4| = 2 \cdot 1920^2$, using SageMath together with the following reasoning, we found that there are no other elements in Γ_4 besides the mentioned ones.

Let $h \in \Gamma_4 = \left(\begin{array}{c|c} m_L^{-1} & \\ \hline & m_L^{-1} \end{array}\right) \mathrm{GL}_4(\mathcal{O}) \left(\begin{array}{c|c} m_L & \\ \hline & m_L \end{array}\right) \cap G$. Note that the norm of an arbitrary element in $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}$ is an element of $\mathbb{Z}_{\geq 0}$, since $N\left(a + bi + cj + d\frac{1+i+j+k}{2}\right), a, b, c, d \in \mathbb{Z}$ equals

$$\left(a + \frac{d}{2}\right)^2 + \left(b + \frac{d}{2}\right)^2 + \left(c + \frac{d}{2}\right)^2 + \left(\frac{d}{2}\right)^2 = a^2 + ad + b^2 + bd + c^2 + cd + d^2 \in \mathbb{Z}.$$

Thus, we see that for any matrix in $\left(\begin{array}{c|c} m_L^{-1} & \\ \hline & m_L^{-1} \end{array}\right) \mathrm{GL}_4(\mathcal{O}) \left(\begin{array}{c|c} m_L & \\ \hline & m_L \end{array}\right)$, all the norms of the entries are in $\frac{1}{2}\mathbb{Z}_{\geq 0}$.

If we write $h = (h_{I,J})_{1 \leq I,J \leq 4}$, where we now assume $N(h_{I,J}) \in \frac{1}{2}\mathbb{Z}_{\geq 0}$, the condition $h \in G$ is

- $\sum_{J=1}^4 N(h_{I,J}) = 1$ for all $I \in \{1, 2, 3, 4\}$,
- $\sum_{K=1}^4 h_{I,K}\bar{h}_{J,K} = 0$ for all $I, J \in \{1, 2, 3, 4\}, I \neq J$.

The first condition leads to finding 10000 16-tuples of possible norms $(N(h_{I,J}))_{1 \leq I,J \leq 4}$, or 5200 after we exclude the already considered cases corresponding to the previously known $2 \cdot 1920^2$ matrices and the cases when $(N(h_{I,J}))_{1 \leq I,J \leq 4}$ has a zero row or zero column using that h needs to have full rank. Note that in each row of such h there are at most two non-zero elements. The second condition defining a matrix in G combined with that remark, gives us that in sums

$$\sum_{K=1}^{4} h_{I,K}\bar{h}_{J,K} \text{ for any } I, J \in \{1, 2, 3, 4\}, I \neq J,$$

at most two summands are non-zero. Therefore for each I, J as before, one of the following possibilities holds:

- $\sum_{K=1}^4 N(h_{I,K})N(h_{J,K}) = 0$,
- $\sum_{K=1}^3 N(h_{I,K})N(h_{J,K}) = N(h_{I,4})N(h_{J,4})$,
- $\sum_{K=1}^2 N(h_{I,K})N(h_{J,K}) = \sum_{K=3}^4 N(h_{I,K})N(h_{J,K})$, or
- $N(h_{I,1})N(h_{J,1}) = \sum_{K=2}^4 N(h_{I,K})N(h_{J,K})$.

These conditions leave us with 120 possible 16-tuples $(N(h_{I,J}))_{1 \leq I,J \leq 4}$. If we write $h = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$, we have

$$\left(\begin{array}{c|c} m_L & \\ \hline & m_L \end{array}\right) \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \left(\begin{array}{c|c} m_L^{-1} & \\ \hline & m_L^{-1} \end{array}\right) = \left(\begin{array}{c|c} m_L A m_L^{-1} & m_L B m_L^{-1} \\ \hline m_L C m_L^{-1} & m_L D m_L^{-1} \end{array}\right).$$

Therefore, if one of A, B, C or D is a matrix with precisely one element of norm 1 and three zeroes, or one element of norm 1/2 and three zeroes or two elements of norm 1/2 and two zeroes, the condition $m_L A m_L^{-1}, m_L B m_L^{-1}, m_L C m_L^{-1}, m_L D m_L^{-1} \in \mathrm{Mat}_2(\mathcal{O})$ will not be satisfied since at least one element of h will be of norm $1/2$ or $1/4$, so not in $\mathcal{O}$.

To conclude,

$$\Gamma_4 = \left(\begin{array}{c|c} m_L^{-1} & \\ \hline & m_L^{-1} \end{array}\right) \mathrm{GL}_4(\mathcal{O}) \left(\begin{array}{c|c} m_L & \\ \hline & m_L \end{array}\right) \cap G = \left\{ \left(\begin{array}{c|c} A & \\ \hline & B \end{array}\right) : A, B \in \Gamma_2 \right\} \cup \left\{ \left(\begin{array}{c|c} & A \\ \hline B & \end{array}\right) : A, B \in \Gamma_2 \right\},$$

so $|\Gamma_4| = 2 \cdot 1920^2$. We obtained the following result.

Theorem 3.5. *The supersingular locus $\mathcal{S}_4 = \mathcal{S}_4 \otimes \overline{\mathbb{F}}_2$ is irreducible in the moduli space of the principally polarized abelian varieties $\mathcal{A}_4 = \mathcal{A}_4 \otimes \overline{\mathbb{F}}_2$.*

3.3 Other irreducibility questions over $\overline{\mathbb{F}}_2$

Using the well-known relation between the values of the Riemann zeta function at odd negative integers and the Bernoulli numbers

$$B_{2n} = -n\zeta(1-2n), \quad n \in \mathbb{Z}_{>0},$$

for $g \in \mathbb{Z}_{>0}$ even and $p \in \mathbb{Z}_{>0}$ a prime number, the mass formula occurring in Theorem 3.4 can be rewritten as

$$\mathrm{Mass}(\mathcal{L}_g(1,p)) = \frac{(-1)^{g(g+3)/2}}{2g!} \left(\prod_{i=1}^{g} B_{2i} \right) \prod_{i=1}^{g/2} (p^{4i-2} - 1).$$

For a first few even dimensions $g > 4$, we get

$$\mathrm{Mass}(\mathcal{L}_6(1,2)) = \frac{1}{2^{10} \cdot 3^4 \cdot 5^2 \cdot 11}, \quad \mathrm{Mass}(\mathcal{L}_8(1,2)) = \frac{1 \cdot 31 \cdot 691}{2^{15} \cdot 3^5 \cdot 5^3 \cdot 7 \cdot 13}$$

$$\mathrm{Mass}(\mathcal{L}_{10}(1,2)) = \frac{1 \cdot 31 \cdot 43 \cdot 127 \cdot 691 \cdot 3617 \cdot 43867}{2^{18} \cdot 3^8 \cdot 5^5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 19}, \ldots$$

Therefore, we can conclude that $\mathcal{S}_8$ and $\mathcal{S}_{10}$ are not irreducible, but we cannot say much about the number of their irreducible components. It can happen that $\mathcal{S}_6$ is irreducible. However, intuitively, we believe that is not the case. Namely, similarly as we used an $\mathcal{O}$-lattice L in $B^{\oplus 2}$ to construct an $\mathcal{O}$-lattice $\hat{L}$ in $B^{\oplus 4}$, we could try to construct an $\mathcal{O}$-lattice $\bar{L}$ in $B^{\oplus 6}$. By the same idea we used to find the elements of Γ_4 in Section 3.2, we expect that the automorphism group of $\bar{L}$ has at least $1920^3 \simeq 7 \cdot 10^9$ elements, which is bigger that the number $2^{10} \cdot 3^4 \cdot 5^2 \cdot 11 \simeq 2 \cdot 10^7$ that occurs in the formula for $\mathrm{Mass}(\mathcal{L}_6(1,2))$.

We should also remark that we are not able to reproduce the same approach for computing the (size of the) automorphism groups for even $g > 4$ we used for $\mathcal{S}_4$ since the computations are becoming more demanding when increasing the dimension.

For $p = 2$ and g odd, we can also discuss the irreducibility of S_g in A_g. Here, we explore [17], Remark 2, and use it to present that $\mathcal{S}_3$ is irreducible, while $\mathcal{S}_5$ is not. As in Example 3.1, take $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ ramified only at $p = 2$, and $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}$.

Using that the norm map $N : \mathcal{O} \to \mathbb{Z}$ maps the invertible elements in $\mathcal{O}$ to a $\{-1, 1\} \subseteq \mathbb{Z}$, a direct check of all possibilities gives us the first auxiliary fact $|\mathcal{O}^*| = 24$. The lattice $L = \mathcal{O}^g$ is in $\mathcal{L}_g(2,1)$, and hence, it contributes in the formula for computing $H_g = H_g(2,1)$.

By looking at the formulas for G-masses in [17], Proposition 9, for G the group of similitudes, by definition we have

$$M_G(M_g(\mathcal{O})) = \sum_{k=1}^{H_g} \frac{1}{[\Lambda_k^* \cap G : 1]}, \tag{8}$$

with Λ_k some representatives of G-ideals of Λ, while using [16], page 235, we have

$$M_G(M_g(\mathcal{O})) = \prod_{k=1}^{g} (2^k + (-1)^k) \frac{|B_{2k}|}{4k}. \tag{9}$$

Since $M_g(\mathcal{O}) \in \mathcal{L}_g(2,1)$, we can take $\Lambda_1 = M_g(\mathcal{O})$. Furthermore, we can conclude

$$|GL_g(\mathcal{O}) \cap G| = |\mathcal{O}^*|^g \cdot g!$$

by discussing the possibilities for a matrix to be in $GL_g(\mathcal{O}) \cap G$ and using that the norms of elements in $\mathcal{O}$ lie in $\mathbb{Z}_{\geq 0}$. Namely, if $a_1, \dots, a_g$ are the entries of the first row of $m \in GL_g(\mathcal{O}) \cap G$, from $m \in G$ we see that $N(a_1) + \dots + N(a_g) = n(m)$, and $n(m) = 1$ from $m \in GL_g(\mathcal{O})$. Therefore, one a_i has to be in $\mathcal{O}^*$ and others must be zeroes. There are $g|\mathcal{O}^*|$ ways to choose such a g-tuple of a_is. Continue this with the second row and use that the element in ith row has to be zero, giving us $(g-1)|\mathcal{O}^*|$ ways, and so on. Hence, we computed

$$[M_g(\mathcal{O})^* \cap G : 1] = |GL_g(\mathcal{O}) \cap G| = |\mathcal{O}^*|^g \cdot g! = 24^g g!. \tag{10}$$

Collecting (8), (9) and (10), we get that for $g \in \mathbb{Z}_{>0}$ odd

$$H_g = 1 \iff \frac{1}{24^g \cdot g!} = \prod_{k=1}^{g} (2^k + (-1)^k) \frac{|B_{2k}|}{4k}.$$

For example, since

$$\frac{1}{24^3 \cdot 3!} = 1 \cdot \frac{1}{6 \cdot 4} \cdot 5 \cdot \frac{1}{30 \cdot 8} \cdot 7 \cdot \frac{1}{42 \cdot 12},$$

we get that $\mathcal{S}_3$ is irreducible, while since

$$\frac{1}{24^5 \cdot 5!} \neq 1 \cdot \frac{1}{6 \cdot 4} \cdot 5 \cdot \frac{1}{30 \cdot 8} \cdot 7 \cdot \frac{1}{42 \cdot 12} \cdot 17 \cdot \frac{1}{30 \cdot 16} \cdot 31 \cdot \frac{5}{66 \cdot 22},$$

we can see that $\mathcal{S}_5$ is not irreducible.

Lastly, using that

$$B_{2k} \sim 4\sqrt{\pi k}\,(k/\pi e)^{2k} \tag{11}$$

we can verify a well-known result that for large g, the locus $\mathcal{S}_g$ will not be irreducible in $\mathcal{A}_g$. Namely, using the asymptotic (11), by the mass formulas described in this section, we see that there is some $g_0 \in \mathbb{Z}_{>0}$ such that $H_g(1,2) > 1$, for $g > g_0$ even, as well as $H_g(2,1) > 1$ for $g > g_0$ odd.

4 The supersingular locus in $\mathcal{M}_4$

In this section, we will discuss some properties of the moduli space of curves of genus four in characteristic two $\mathcal{M}_4 = \mathcal{M}_4 \otimes \overline{\mathbb{F}}_2$. First, we recall some notions and facts from the general algebro-geometric theory, and present the classification of all curves of genus four over an algebraically closed field. Then, we discuss the results of paper [49], where Xarles determined all the non-isomorphic representatives for genus 4 curves over $\mathbb{F}_2$. We use these results to get some intuition on the geometry of the supersingular locus in $\mathcal{M}_4$. Our focus will be on non-hyperelliptic curves and we will describe them mainly via the Ekedahl-Oort type, with emphasis on the types closely related with the supersingular locus in $\mathcal{M}_4$.

4.1 Classification of curves of genus four

Let C be a curve of genus g an algebraically closed field $k = \bar{k}$. Before we classify the curves of genus four over an algebraically closed field, let us recall some algebro-geometric notions.

Recall that an invertible sheaf $\mathcal{L}$ on C is *very ample* if it is isomorphic to $\mathcal{O}_C(1)$ for some immersion of C in a projective space. In other words, $\mathcal{L}$ is very ample if it defines an embedding of C in $\mathbb{P}^n$ for some n. We say that a divisor D on C is very ample if $\mathcal{O}_C(D)$ is.

A *complete linear system* $|D|$ is the set of all effective divisors $E = \sum_{i=1}^{N} n_i P_i \geq 0$ that are linearly equivalent to the divisor D on C. We call $|K_C|$ the *canonical linear system.* Note that there is a one-to-one correspondence

$$|D| \to (H^0(C, \mathcal{O}_C(D)) - \{0\})/k^*, \quad D + \operatorname{div} f \mapsto [f],$$

which is often useful for defining a morphism from a curve to a projective space, noting that $\mathbb{P}^n \cong (H^0(C, \mathcal{O}_C(D)) - \{0\})/k^*$ with $n = \dim H^0(C, \mathcal{O}_C(D)) - 1$. In particular, if D is a very ample divisor on C, the corresponding immersion is given on the set of points by

$$C \to \mathbb{P}^n, \quad P \mapsto [f_0(P), f_1(P), \dots, f_n(P)],$$

for $\{f_0, f_1, \dots, f_n\}$ a basis of $\dim H^0(C, \mathcal{O}_C(D))$; see [15], Section II.7. The degree of $f(C)$ can then be defined as the degree of D.

A *linear system* $\mathcal{D}$ is a linear subspace of some complete linear system $|D|$, and we say that the degree of the linear system $\mathcal{D}$ is the degree of any divisor in it. If $\mathcal{D}$ is a linear system of dimension r and degree d, we say that it is a $\mathfrak{g}^r_d$. Note that a $\mathfrak{g}^r_d$ on C defines a morphism $C \to \mathbb{P}^r$ so that the degree of image of C is d. For example, $|K_C|$ is a $\mathfrak{g}^{g-1}_{2g-2}$, and it holds that a curve C is hyperelliptic if it has a $\mathfrak{g}^1_2$.

An important fact, [15], Proposition IV.3.1, is that a divisor D is very ample if and only if

$$\dim |D - P - Q| = \dim |D| - 2,$$

for any two points $P, Q \in C$. Using this criterion, in [15], Proposition IV.5.2, it follows for a curve C of genus $g \geq 2$ that the canonical linear system $|K_C|$ is very ample if and only if C is not hyperelliptic.

Therefore, if C is a non-hyperelliptic curve of genus $g \geq 3$, we have the embedding $C \to \mathbb{P}^{g-1}$ determined by $|K_C|$ called the **canonical embedding**. The image of C in $\mathbb{P}^{g-1}$ is a curve of degree $2g - 2$, which we call the *canonical model of* C. Moreover, this embedding is determined up to a projective automorphism, or in other words, two curves C_1 and C_2 with canonical models

C_1' and C_2' are isomorphic, if there is a $\mathrm{PGL}_g(\bar{k})$-transformation that induces an isomorphism $C_1' \cong C_2'$.

Recall further that a projective variety $X \subseteq \mathbb{P}^n$ is a **complete intersection** if its defining ideal is generated by exactly $n - \dim X$ polynomials. [15], Exercise II.8.4, gives that if a curve $C \subseteq \mathbb{P}^n$ is a complete intersection $\cap_{i=1}^{n-1} H_i$ of hypersurfaces $H_i = Z(F_i)$ for some homogeneous polynomials F_i of $\deg F_i = d_i$, then it holds that

$$\mathcal{O}_C(K_C) \sim \mathcal{O}_C\left(\sum_{i=1}^{N-1} d_i - n - 1\right). \tag{12}$$

Theorem 4.1 ([15], Example IV.5.2.2)**.** *Let C be a genus 4 curve over an algebraically closed field k. Then C is either a hyperelliptic curve, or it is a complete intersection of a unique irreducible quadratic surface and an irreducible cubic surface.*

Proof. Let firstly C be a complete intersection of an irreducible quadratic surface and an irreducible cubic surface. Then $\mathcal{O}_C(K_C) \sim \mathcal{O}_C(1)$ by 12, and the degree of C is $3 \cdot 2 = 6$ by intersection theory. Therefore, C is a canonical model of a curve of genus 4.

Conversely, let C be a canonical model of a non-hyperelliptic curve of genus 4 in $\mathbb{P}^3$. Since $\varphi : C \to \mathbb{P}^3$ is an immersion, there is the fundamental exact sequence of $\mathcal{O}_{\mathbb{P}^3}$-modules

$$0 \to \mathcal{I} \to \mathcal{O}_{\mathbb{P}^3} \to \varphi_* \mathcal{O}_C \to 0,$$

with $\mathcal{I}$ the ideal sheaf of C; recall that $\mathcal{I}$ is the sheaf of functions that are "zero on C". If we tensor the previous sequence with the invertible sheaf $\mathcal{O}_C(2)$ and take a look at the long exact sequence in cohomology, we get

$$\begin{aligned} 0 \to H^0(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)) \to H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(2)) \to H^0(C, \mathcal{O}_C(2)) \to \\ \to H^1(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)) \to 0 = H^1(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(2)) \to \dots \end{aligned}$$

Using $H^i(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(2)) \neq 0$ only for $i \in \{0, 3\}$, see [15], Theorem 5.1 for this standard result, and $H^i(C, \mathcal{O}_C(2)) = 0$ for $i > 1$ since C is of dimension 1, we get $H^1(C, \mathcal{O}_C(2)) \cong H^2(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2))$ and $H^2(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)) \cong H^3(\mathbb{P}^3, \mathcal{O}_C(2))$. In particular, that gives us

$$\dim H^0(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)) + \dim H^0(C, \mathcal{O}_C(2)) = \dim H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(2)) + \dim H^1(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)). \tag{13}$$

It is well-known that $\dim H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(2)) = 10$. Using $\mathcal{O}_C(K_C) \cong \mathcal{O}_C(1)$ so $\mathcal{O}_C(2K_C) \cong \mathcal{O}_C(2)$ and the Riemann-Roch theorem, we obtain

$$\dim H^0(C, \mathcal{O}_C(2)) = \dim H^0(C, \mathcal{O}_C(2K_C)) - \dim H^0(C, \mathcal{O}_C(-K_C)) = 2 \deg K_C + 1 - 4 = 9.$$

Hence, (13) gives us

$$\dim H^0(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)) \geq 1,$$

meaning that there is at least one non-zero quadratic form F vanishing on C. In other words, C is contained in a quadratic surface $Q_2 = Z(F)$ in $\mathbb{P}^3$. Since C is irreducible, if Q_2 is not irreducible, then C would be contained in a plane in $\mathbb{P}^3$. However, since $C \to \mathbb{P}^3$ is an embedding, that cannot be the case, so Q_2 is irreducible. Additionally, if it is contained in any other quadratic surface Q', then $C = Q_2 \cap Q'$ will be of degree 4. Since $\deg C = 6$, we find that the quadric Q_2, such that $C \subseteq Q_2$, is unique.

A similar discussion as above gives

$$\dim H^0(\mathbb{P}^3, \mathcal{I} \otimes \mathcal{O}_{\mathbb{P}^3}(2)) \geq 5.$$

We want to show that there is a cubic form defining an irreducible cubic surface that contains C. C is not contained in a plane as discussed above, and if it is contained in a quadratic surface Q', then $Q' = Q_2$. Therefore, the only possibilities are that the cubic form vanishing on C is the product of $F, Q_2 = Z(F)$ and a linear factor. The dimension of the space of linear factors is 4, namely $\langle T, X, Y, Z\rangle_k$ as $C \subseteq \mathbb{P}^3$, so we can find an irreducible cubic form G vanishing on C, i.e., $Q_3 = Z(G)$ so that $C \subseteq Q_3$. Since both Q_2 and Q_3 are irreducible and of different degrees, we have that $Q_2 \cap Q_3$ is a complete intersection containing C. Both $Q_2 \cap Q_3$ and C have degree 6, so $C = Q_2 \cap Q_3$. □

By the previous theorem, a non-hyperelliptic curve C of genus four is contained in a unique irreducible quadric. Being irreducible means that such quadric is either of rank 3 or of rank 4, i.e., it is a *quadric cone* (*singular* quadric) isomorphic over an algebraically closed field k to $Q_{sq} : TZ + X^2 = 0$, or it is a *non-singular* quadric over k isomorphic to $Q_{nsq} : TZ + XY = 0$.

In any case, C is **trigonal**, that is, there is a morphism $C \to \mathbb{P}^1$ of degree 3, or in other words, C has a $\mathfrak{g}^1_3$. On a non-singular quadric, there are two families of lines, the ones with $aT = bX, bZ = aY$ and with $aT = bY, bZ = aX$. If C lies on a non-singular quadric, then these two families define two $\mathfrak{g}^1_3$s. Otherwise, if C lies on a quadric cone, there is a unique $\mathfrak{g}^1_3$ on it.

4.2 Genus four curves over $\mathbb{F}_2$

In his paper [49], Xarles determined all curves of genus 4 over $\mathbb{F}_2$. By that we mean that he gave an algorithm how to compute a representative for each isomorphism class of these curves. The Magma code based on the results of that paper and the collected data can be found on `https://github.com/XavierXarles/CensusforGenus4curvesoverF2`. Besides equations for all such representatives, for each curve from the list, the number of its points over $\mathbb{F}_{2^i}, i \in \{1, 2, 3, 4\}$ is included.

As we saw above, the curves of genus four are either hyperelliptic or trigonal. Hyperelliptic curves of genus 4 over $\mathbb{F}_2$ have a model

$$y^2 + q(x)y = p(x),$$

for some polynomials $p(x), q(x) \in \mathbb{F}_2[x]$ whose degrees satisfy $9 \leq \max\{2\deg q(x), \deg p(x)\} \leq 10$. The trigonal curves of genus 4 are the ones whose canonical model in $\mathbb{P}^3$ is an intersection of a quadratic (of rank ≥ 3) and a cubic surface. Over $\mathbb{F}_2$ and after a suitable choice of coordinates, by [49], Lemma 9, the quadratic surfaces are one of the following

$$Q_{nssq} : TZ + XY = 0, \quad Q_{nsnsq} : TZ + X^2 + XY + Y^2 = 0, \quad \text{or} \quad Q_{sq} : TZ + X^2 = 0.$$

We say that Q_{nssq} is the non-singular split quadric, Q_{nsnsq} is the non-singular non-split quadric and Q_{sq} is the quadric cone.

In determining representatives for all non-isomorphic curves of genus 4 over $\mathbb{F}_2$, Xarles separately considered the hyperelliptic and non-hyperelliptic ones. For the first kind, it was determined when two such curves are isomorphic. Using that, certain normal forms of hyperelliptic curves over $\mathbb{F}_2$ were found. We use the same ideas as Xarles in Section 5, where we determine the (representatives of the isomorphism classes of the) hyperelliptic curves of genus 5 over $\mathbb{F}_2$.

The non-hyperelliptic isomorphism classes of curves were determined using that the embedding of non-hyperelliptic curves in $\mathbb{P}^3$ is canonical, so the isomorphisms of curves are induced by the projective automorphisms.

Using the data and the Weil's conjecture for curves C over $\mathbb{F}_2$

$$Z(C/\mathbb{F}_2, t) = \exp\left(\sum_{s=1}^{\infty} \frac{\#C(\mathbb{F}_{2^s})t^s}{s}\right) = \frac{L(C/\mathbb{F}_2, t)}{(1-t)(1-2t)},$$

we computed the coefficient with $t^i, i \in \{1,2,3,4\}$ in the L-polynomial of each curve of genus 4 over $\mathbb{F}_2$. Using the symmetry of Newton polygons, that was enough to deduce which of these curves are supersingular. In particular, there are 20 supersingular curves of genus 4 over $\mathbb{F}_2$, out of which 12 are hyperelliptic and 8 are trigonal (i.e., non-hyperelliptic). Furthermore, using that any automorphism of the trigonal ones is induced by a projective automorphism, we computed their automorphism groups over $\mathbb{F}_2$.

We present the obtained non-hyperelliptic supersingular curves together with their automorphism groups over $\mathbb{F}_2$ in Table 1. Note that all the automorphism groups presented there are of order 2.

C	Quadric q_2 and cubic q_3 that define C, $C = Z(q_2, q_3)$	Generator σ of $\mathrm{Aut}_{\mathbb{F}_2}(C) = \langle\sigma\rangle$
A_1	$TZ + XY$ $T^2X + TX^2 + X^2Y + XYZ + Y^3 + Y^2Z + Z^3$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ X+Z & T+Y & Z & Y \end{pmatrix}$
A_2	$TZ + XY$ $T^2X+TX^2+TXY+TY^2+X^3+X^2Z+XY^2+XZ^2+Y^2Z+YZ^2$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ T & T+X & T+Y & T+X+Y+Z \end{pmatrix}$
A_3	$TZ + XY$ $T^2X + TX^2 + TXY + TY^2 + XYZ + XZ^2 + Y^3 + Y^2Z + YZ^2$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ X+Z & T+Y & Z & Y \end{pmatrix}$
A_4	$TZ + XY$ $T^2X + TX^2 + TY^2 + X^2Z + Y^2Z + YZ^2$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ Z & Y & X & T \end{pmatrix}$
B_1	$TZ + X^2 + XY + Y^2$ $T^2X + TXY + TY^2 + X^3 + XY^2 + Y^2Z + Z^3$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ T+X+Z & X & Y+Z & Z \end{pmatrix}$
B_2	$TZ + X^2 + XY + Y^2$ $T^2X + TY^2 + X^2Z + XZ^2 + Y^2Z$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ Z & X & X+Y & T \end{pmatrix}$
B_3	$TZ + X^2 + XY + Y^2$ $T^2X + TX^2 + X^3 + X^2Y + XYZ + Y^2Z + YZ^2$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ T+X+Z & X & Y+Z & Z \end{pmatrix}$
B_4	$TZ + X^2 + XY + Y^2$ $T^2X + TXY + X^3 + X^2Y + X^2Z + XZ^2 + Y^3 + Y^2Z$	$\sigma : \begin{pmatrix} T & X & Y & Z \\ T+X+Z & T+Y & T+Z & T+X+Y+Z \end{pmatrix}$

Table 1: Non-hyperelliptic supersingular curves of genus 4 over $\mathbb{F}_2$

4.2.1 Computations based on the data

Let A_1, A_2, A_3 and A_4 be the supersingular curves of genus 4 defined over $\mathbb{F}_2$ as in Table 1, and for $i \in \{1,2,3,4\}$ let us denote with $Q(A_i)$ the quotient of a curve A_i by $\mathrm{Aut}_{\mathbb{F}_2}(A_i)$.

Proposition 4.2. *Let $A_i, i \in \{1,2,3,4\}$ be genus 4 curves over $\mathbb{F}_2$ as above. Then all the quotient curves $Q(A_i)$, are hyperelliptic supersingular curves of genus 2. Moreover, we have the following isomorphism*

$$Q(A_1) \cong Q(A_4) \cong \{y^2 + y = x^5 + x^3\}, \quad Q(A_2) \cong Q(A_3) \cong \{y^2 + y = x^5 + x\}.$$

Proof. Let us firstly consider curve A_1 which is defined as

$$A_1: \quad TZ + XY = 0, \quad T^2X + TX^2 + X^2Y + XYZ + Y^3 + Y^2Z + Z^3 = 0.$$

The computations for A_3 and A_4 are completely analogous to this one. Note that $P = (1:1:0:0)$ is the point fixed by $\mathrm{Aut}_{\mathbb{F}_2}(A_1) = \langle \sigma_1^A \rangle$ do the change of coodinates $T \mapsto T = T_{new}, X \mapsto X + T = X_{new}, Y \mapsto Y = Y_{new}, Z \mapsto Z = Z_{new}$, so that new coordinates of P are $(1:0:0:0)$. Projection from that point leads to replacing T with $XY/(Z+Y)$ in new coordinates and inserting it in the defining cubic equation in new coordinates. We therefore obtained a model

$$A_1: Y^5 + X^3YZ + Y^4Z + X^2YZ^2 + XY^2Z^2 + Y^3Z^2 + XYZ^3 + Z^5 = 0,$$

which is a quintic in $\mathbb{P}^2$ with exactly two nodes $(0:1:1), (1:0:0)$. After another change of coordinates $X \mapsto X = X_{new}, Y \mapsto Y + Z = Y_{new}, Z \mapsto Z = Z_{new}$ we obtain

$$A_1: Y^5 + X^3YZ + X^3Z^2 + X^2YZ^2 + XY^2Z^2 + Y^3Z^2 + X^2Z^3 + XYZ^3 + Y^2Z^3 = 0$$

and we see that in these coordinates, σ_1^A acts as $X \mapsto X + Y, Y \mapsto Y, Z \mapsto Z$. Take therefore $w = X/Y, z = Z/Y$ and see that $w(w+1), z(z+1)$ are the elements fixed by $\mathrm{Aut}_{\mathbb{F}_2}(A_1)$, which leads us to the first equation of the quotient curve $(w+1)z^2 + w^3z + 1 = 0$, i.e.,

$$z^2 + \frac{w^3}{w+1}z + \frac{1}{w+1} = 0.$$

After the substitution $y = \frac{w+1}{w^3}z, x = 1/w$ we find that $y^2 + y = x^6 + x^5$, which is finally, after $y \mapsto y + x^3$, isomorphic to $y^2 + y = x^5 + x^3$.

In case of A_2, the idea is the same, with a difference that instead of changing the coordinates and projecting from $(1:0:0:0)$, we project from $(0:0:0:1)$ right away (that is now fixed by $\mathrm{Aut}_{\mathbb{F}_2}(A_2) = \langle \sigma_2^A \rangle$). In other words, let us subsitute $Z = XY/T$ into the cubic. Take then $x = X/T, y = Y/T$, to get the affine equation

$$(y^2 + y + 1)x^3 + (y^3 + 1)x^2 + (y^3 + y^2 + y + 1)x + y^2 = 0$$

and see that $\sigma_2^A : x \mapsto x+1, y \mapsto y+1$. Hence, taking $w = x(x+1), z = y(y+1)$ gives as an equation of the quotient similarly as in the first part. Using the same argument as above, we can find that $Q(A_2)$ is isomorphic to $y^2 + y = x^5 + x^3$.

There are several ways to see that the $Q(A_i)$'s are supersingular of genus 2. For example, from van der Geer and van der Vlugt's construction we mentioned in Section 2.3.1, we can immediately see that they are supersingular hyperelliptic of genus 2, and moreover, that they belong to GV_2. Alternatively, using that A_i's have 2-rank 0 since they are supersingular, we can conclude that the $Q(A_i)$'s have 2-rank 0 and therefore, using that the $Q(A_i)$s are (hyperelliptic) of genus 2 it follows that they are supersingular. □

Proposition 4.3. *For $i \in \{1,2,3,4\}$, let B_i be the supersingular curves of genus 4 defined over $\mathbb{F}_2$ as in Table 1, $Q(B_i)$ the quotient of the curve B_i by $\mathrm{Aut}_{\mathbb{F}_2}(B_i)$. Then all the quotient curves $Q(B_i)$ are hyperelliptic supersingular curves of genus 2. Moreover, we have the isomorphism*

$$Q(B_1) \cong Q(B_4) \cong \{y^2 + y = x^5\}, \quad Q(B_2) \cong Q(B_3) \cong \{y^2 + y = x^5 + x^3 + x\}.$$

Proof. Consider the curve B_3; the cases of B_1 and B_2 are completely analogous. Note that the point $P = (1:0:0:0)$ is fixed by $\mathrm{Aut}_{\mathbb{F}_2}(B_3) = \langle \sigma_3^B \rangle$. As in the proof of the previous theorem, we project the points on the curve from P, i.e., we take $T = (X^2 + XY + Y^2)/Z$ from the defining quadric to get the model of B_3 in $\mathbb{P}^2$ which is the quintic with two nodes $(\zeta_2 : 1 : 0), (\zeta_2 + 1 : 1 : 0)$, where $\zeta_2 \in \overline{\mathbb{F}}_2$, is such that $\zeta_2^2 + \zeta_2 + 1 = 0$:

$$B_3 : X^5 + X^3Y^2 + XY^4 + X^4Z + X^3YZ + X^2Y^2Z + X^3Z^2 + X^2YZ^2 + XYZ^3 + Y^2Z^3 + YZ^4 = 0.$$

Consider the affine equation of this model by taking $x = X/Z, y = Y/Z$ and see that $\sigma_3^B : x \mapsto x, y \mapsto y + 1$. Hence $u = x, v = y(y+1)$ are the elements fixed by $\mathrm{Aut}_{\mathbb{F}_2}(B_3)$, and the quotient equals $v^2u + (u^3 + u^2 + u + 1)v = u^5 + u^4 + u^3$, i.e., to

$$v^2 + \frac{(u+1)^3}{u} v = u^4 + u^3 + u^2.$$

If we take $y = \frac{u}{(u+1)^3} v$ and firstly $t = u + 1$, and then $x = 1/t$, we get $y^2 + y = x^6 + x^5 + x^4 + x^2 + x + 1$. Lastly, the substitution $x \mapsto x + 1$ and then $y \mapsto y + x^3 + x$ gives us the isomorphism between $Q(B_3)$ and $y^2 + y = x^5 + x^3 + x$.

To find $Q(B_4)$, consider $T \mapsto T = T_{new}, X \mapsto X + T = X_{new}, Y \mapsto Y = Y_{new}, Z \mapsto Z + T = Z_{new}$ so that $P = (1:0:0:0)$ is the fixed point under $\mathrm{Aut}_{\mathbb{F}_2}(B_4) = \langle \sigma_4^B \rangle$ and project the curve from P as before. Another change of coordinates $X \mapsto X + Y = X_{new}, Y \mapsto Y = Y_{new}, Z \mapsto Z + Y = Z_{new}$ leads to the equation of B_4

$$B_4 = X^5 + X^3Y^2 + XY^4 + X^4Z + X^3YZ + X^2Y^2Z + X^3Z^2 + X^2YZ^2 + XYZ^3 + Y^2Z^3 + XZ^4 + YZ^4$$

for which $\sigma_4^B : X \mapsto X, Y \mapsto Y + Z, Z \mapsto Z$. Take $x = X/Z, y = Y/Z$ and note that $x, y(y+1)$ are fixed by $\mathrm{Aut}_{\mathbb{F}_2}(B_4)$, so the same steps as before lead us to the isomorphism between $Q(B_4)$ and $y^2 + y = x^5$.

We can prove that the $Q(B_i)$'s are supersingular hyperelliptic curves of genus 2 using the same argument as for the $Q(A_i)$'s. Alternatively, we compute that the L-polynomials L_1 of $Q(B_1)$ and $Q(B_4)$ and L_2 of $Q(B_2)$ and $Q(B_3)$ are $L_1 = 4t^4 + 1$ and $L_2 = 4t^4 + 2t^2 + 1$. Hence, all the Newton polygons of these curves are in fact the straight line from $(0,0)$ to $(4,2)$ with slope $1/2$. □

If we denote with $S = \{(T:X:Y:Z) \in \mathbb{P}^3 : TZ = XY\}$ the non-singular quadric in $\mathbb{P}^3$, using the isomorphism $\mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{\simeq} S$ obtained via the Segre embedding

$$\mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{\simeq} \mathbb{P}^3, ((a_1 : a_2), (b_1 : b_2)) \to (a_1b_1 : a_1b_2 : a_2b_2 : a_2b_2),$$

we may recognize the affine plane $\mathbb{A}^2$ as a subset of S, being the set $\{(1 : a : b : ab) \in S : a, b \in \overline{\mathbb{F}}_2\}$. This gives us an affine equation of any non-hyperelliptic curve lying on a non-singular quadric

$$C : f(x,y) = \sum_{i,j=0}^{3} a_{i,j} x^i y^j = 0.$$

In [45], Section 2, a basis of regular differentials $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ for C is given as

$$\omega_1 = \frac{1}{\partial f/\partial y} \mathrm{d}x, \quad \omega_2 = \frac{x}{\partial f/\partial y} \mathrm{d}x, \quad \omega_3 = \frac{y}{\partial f/\partial y} \mathrm{d}x \text{ and } \omega_4 = \frac{xy}{\partial f/\partial y} \mathrm{d}x,$$

and its Hasse-Witt matrix is computed

$$HW(C) = \begin{pmatrix} a_{11} & a_{31} & a_{13} & a_{33} \\ a_{01} & a_{21} & a_{03} & a_{23} \\ a_{10} & a_{30} & a_{12} & a_{32} \\ a_{00} & a_{20} & a_{02} & a_{22} \end{pmatrix}.$$

Using this description, we compute the Ekedahl-Oort type of the curves from Table 1.

Proposition 4.4. *All curves from Table 1 have Ekedahl-Oort type $\mu = [4]$.*

Proof. We will show this for A_1 and B_1, while the argument for the other curves is similar.

For A_1, we can instantly apply the previously given description to get its affine equation

$$A_1 : x^3y^3 + x^2y^2 + xy^3 + x^2y + y^3 + x^2 + x = 0.$$

In the case of B_1, we firstly need to change the coordinates over $\overline{\mathbb{F}}_2$ (here it is enough over $\mathbb{F}_4$), $X \mapsto X_1, Y \mapsto Y_1$ with $X = (\zeta_2 + 1)X_1 + \zeta_2 Y_1, Y = X_1 + Y_1$, and then to consider the affine part $T \neq 0$, $x = X_1/T, y = Y_1/T$ and $Z/T = xy$ to get

$$B_2 : x^3y^3 + x^3y + xy^3 + \zeta_2 x^3 + x^2y + xy^2 + (\zeta_2 + 1)y^3 + \zeta_2 x^2 + xy + (\zeta_2 + 1)y^2 + (\zeta_2 + 1)x + \zeta_2 y = 0.$$

Therefore, we compute their Hasse-Witt matrices

$$HW(A_1) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad HW(B_1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \zeta_2 & 1 & \zeta_2 + 1 & 0 \\ \zeta_2 + 1 & \zeta_2 & 1 & 0 \\ 0 & \zeta_2 & \zeta_2 + 1 & 0 \end{pmatrix},$$

that are both of rank 3. Therefore, the a-numbers of A_1 and B_1 are $4 - 3 = 1$ so $\mu_2 = 0$ in their Ekedahl-Oort type. Finally, as they are supersingular, they are in the 2-rank zero locus, so $\mu_1 = 4 - 0 = 4$ in both cases. □

4.3 Supersingular curves of genus four over $\overline{\mathbb{F}}_2$ lying on a quadric cone

Using [42], Proposition 3.1 and Theorem 3.1 combined with [51], Theorem 2.1 we get that all genus 4 curves C over $\overline{\mathbb{F}}_2$ satisfy $a(C) \in \{0, 1, 2\}$. Moreover, $1 \leq$ 2-rank$(C) + a(C) \leq 4$, leads to the conclusion that for curves in the 2-rank zero locus, so in particular for the supersingular ones, it holds that

$$a(C) \in \{1, 2\}.$$

When C is a hyperelliptic curve of genus 4 in characteristic two with 2-rank$(C) = 0$, by [40], Lemma 5.4, it satisfies $a(C) = 2$.

Here, we focus on the locus D of non-hyperelliptic curves of genus 4 over $\overline{\mathbb{F}}_2$ that lie on a quadric cone. We will briefly show that such curves with 2-rank zero have a-number two. Using that, we discuss the existence of supersingular curves in D. The motivation to do that originates from the computations regarding Xarles's data, which gave us that there is no supersingular non-hyperelliptic curve of genus 4 over $\mathbb{F}_2$ that lies an a quadric cone.

The Cartier operator $\mathcal{C}$ on the space of regular differentials on a curve C of genus 4 over $k = \overline{\mathbb{F}}_2$ by definition is

$$\mathcal{C}((f_0^2 + f_1^2 x)\mathrm{d}x) = f_1 \mathrm{d}x,$$

for a separating variable x of $\kappa(C)$, $f_0, f_1 \in \kappa(C)$, and $\omega = (f_0^2 + f_1^2 x)\mathrm{d}x \in H^0(C, \Omega_C^1)$. It is not hard to check that $\mathcal{C}$ satisfies the following properties for $\omega, \omega_1, \omega_2 \in H^0(C, \Omega_C^1), f \in \kappa(C)$:

- $\mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2)$,
- $\mathcal{C}(f^2\omega) = f\mathcal{C}(\omega)$,
- $\mathcal{C}(\mathrm{d}f) = 0$,
- $\mathcal{C}\left(\frac{\mathrm{d}f}{f}\right) = \frac{\mathrm{d}f}{f}$.

Recall that, for a given basis $\{\omega_1, \dots, \omega_4\}$ of $H^0(C, \Omega_C^1)$ and $\omega = \sum_{i=1}^4 h_{i,j}\omega_i$ with $h_{i,j} \in k$, the Hasse-Witt matrix of C is $HW(C) = (h_{i,j}^2)_{1 \le i,j \le g}$. Note that, by definition, the rank of $HW(C)$ equals the rank of the Cartier operator $\mathcal{C}$. Also, recall that in (4) we saw that the Verschiebung operator V on $H_{dR}^1(C)$ is defined as $V(f, \omega) = (0, \mathcal{C}(\omega))$.

Using the notion of the Cartier operator, we give alternative definitions of 2-rank and a-number of a curve C. Namely, we have 2-rank$(C) = f$ where

$$f = \mathrm{rk}(\mathcal{C}^g) = \dim(\mathrm{Im}(\mathcal{C}^g)),$$

and the a-number of C is given as

$$a(C) = \dim(\ker(\mathcal{C})) = g - \mathrm{rk}(\mathcal{C}).$$

Let C be a smooth projective curve of genus g over $\overline{\mathbb{F}}_2$ and $\kappa(C)$ its function field. We say that a divisor class θ is a **theta characteristic** if 2θ is the canonical divisor K_C. The main reference for this is [45], where all the following properties of theta characteristics are discussed. For a separating variable $x \in \kappa(C) - \kappa(C)^2$, the non-zero differential $\mathrm{d}x$ is of the form $2D_0$, for a divisor D_0. Furthermore, the class of D_0 is a theta characteristic, called the *canonical theta characteristic* and denoted by θ_0; the definition does not depend on the choice of x. Note that any other theta characteristic is of form $\theta_0 + D_2$, where D_2 is a 2-torsion element of $\mathrm{Pic}(C)$.

Stöhr and Voloch in [45], Proposition 3.1. concluded that, in our setting, the space of regular exact differentials is in $\frac{1}{2}$-linear bijection with $H^0(C, \mathcal{O}(D_0))$. Using that a differential in characteristic $p = 2$ is exact if and only if it is contained in $\ker(\mathcal{C})$, it holds that

$$a(C) = g - \mathrm{rk}(\mathcal{C}) = \dim H^0(C, \mathcal{O}(\theta_0)).$$

In case of a supersingular curve C of genus 4 over $\overline{\mathbb{F}}_2$ that lies on a quadric cone, we get that there is exactly one theta characteristic, namely, the canonical one θ_0, as the 2-rank of C is zero. Furthermore, for example $\mathfrak{g}_3^1$ on C is a theta characteristic with $\dim H^0(C, \mathcal{O}(\mathfrak{g}_3^1)) = 2$; see for example [26], Remark 29.9. Therefore

$$a(C) = 2. \tag{14}$$

In order to investigate the locus of non-hyperelliptic supersingular curves C of genus 4 over $\overline{\mathbb{F}}_2$ lying on a quadric cone, it is thus enough to restrict ourselves to the case $a(C) = 2$. In other words, we should investigate only the curves C with Ekedahl-Oort type $[4,1], [4,2]$ and $[4,3]$.

4.3.1 Curves with Ekedahl-Oort type $[4,3]$

Given a Young diagram μ corresponding to the final type v, denote with Z_μ both the set of geometric points in $\mathcal{A}_g$ with Ekedahl-Oort type μ, and its pull-back via the Torelli morphism, i.e., the locus of curves of genus g with Ekedahl-Oort type μ. Since we work here only with curves, there should be no confusion.

In Lemma 2.2, we saw that for a given Ekedahl-Oort type μ and the corresponding final type v, if it holds that $v(\lfloor \frac{g+1}{2} \rfloor) = 0$, then Z_μ is contained in the supersingular locus in $\mathcal{A}_g$. For $g = 4$, the Ekedahl-Oort loci Z_μ that are contained in the supersingular locus are the ones with $v(2) = 0$, corresponding to the μ such that $[4,3] \leq \mu$, i.e.,

$$\mu \in \{[4,3],[4,3,1],[4,3,2],[4,3,2,1]\}.$$

By the previous discussion on a-numbers of curves of genus 4 over $\overline{\mathbb{F}}_2$ lying on a quadric cone, we immediately get that $Z_{[4,3,1]}, Z_{[4,3,2]}$ and $Z_{[4,3,2,1]}$ have empty intersection with the locus of curves lying on a quadric cone. Moreover, we show in Theorem 4.5 that there is no non-hyperelliptic curve of genus 4 over $\overline{\mathbb{F}}_2$ lying on a quadric cone with Ekedahl-Oort type $\mu = [4,3]$.

Let C be an arbitrary non-hyperelliptic curve of genus 4 over $\overline{\mathbb{F}}_2$ lying on a quadric cone. After a possible change of coordinates, we may choose that the cone is given by

$$Q = \{(T : X : Y : Z) \in \mathbb{P}^3 : TZ = X^2\}.$$

Consider further the embedding

$$\mathbb{A}^2 \to Q, (a,b) \mapsto (1 : a : b : a^2),$$

which enable us to consider an affine equation

$$C : f(x,y) = \sum_{i+2j\leq 6} a_{i,j} x^i y^j.$$

A basis for $H^0(C, \Omega^1_C)$ is given in [45], Section 2 by

$$\omega_1 = \frac{1}{\partial f/\partial y}\mathrm{d}x, \quad \omega_2 = \frac{x}{\partial f/\partial y}\mathrm{d}x, \quad \omega_3 = \frac{y}{\partial f/\partial y}\mathrm{d}x \text{ and } \omega_4 = \frac{x^2}{\partial f/\partial y}\mathrm{d}x. \tag{15}$$

Using [45], Theorem 1.1 for the formula

$$\mathcal{C}\left(\frac{h}{\partial f/\partial y}\mathrm{d}x\right) = \left(\frac{\partial^2}{\partial x \partial y} fh\right)^{1/2} \frac{\mathrm{d}x}{\partial f/\partial y},$$

the Hasse-Witt matrix of C, $HW(C)$ is computed. Namely, we have

$$HW(C) = \begin{pmatrix} a_{11} & a_{31} & 0 & 0 \\ a_{01} & a_{21} & a_{03} & a_{41} \\ a_{10} & a_{30} & a_{12} & a_{50} \\ 0 & a_{11} & 0 & a_{31} \end{pmatrix}. \tag{16}$$

Theorem 4.5. *Let D be the locus in $\mathcal{M}_4 = \mathcal{M}_4 \otimes \overline{\mathbb{F}}_2$ consisting of non-hyperelliptic curves that lie on a quadric cone. Then, the set of geometric points of $D \cap Z_{[4,3]}$ is empty.*

Proof. Let C be a curve corresponding to a point of $D \cap Z_{[4,3]}$. Possessing Ekedahl-Oort type $\mu = [4,3]$ is equivalent to having final type v, with

$$v(1) = 0, \quad v(2) = 0, \quad v(3) = 1, \quad v(4) = 2.$$

$\mathcal{C}(H^0(C,\Omega_C^1))$ is thus of dimension two, i.e., rank$HW(C) = 2$, and $\mathcal{C}^2(H^0(C,\Omega_C^1)) = 0$. We discuss the possible forms of the Hasse-Witt matrix of C.

Case $a_{11} \neq 0$. Without loss of generality, we may suppose that $a_{11} = 1$. Using that $\mathcal{C}^2(\omega_1) = 0$, we firstly conclude that $a_{31} \neq 0$, and then, using that $\mathrm{rk}(HW(C)) = 2$, we get $a_{03} = a_{12} = 0$ and $a_{41} = a_{31}(a_{21} + a_{31}a_{01}), a_{50} = a_{31}(a_{30} + a_{31}a_{10})$. From

$$\mathcal{C}^2(\omega_1) = (1 + \sqrt[4]{a_{31}}\sqrt{a_{01}})\omega_1 + (\sqrt{a_{31}} + \sqrt[4]{a_{31}}\sqrt{a_{21}})\omega_2 + \sqrt[4]{a_{31}}\sqrt{a_{41}}\omega_4 = 0,$$

it follows that $a_{41} = 0$ and $a_{21} = \sqrt{a_{31}}$. However, that leads to

$$\mathcal{C}^2(\omega_4) = \sqrt{a_{01}}\omega_1 + \sqrt[4]{a_{31}^3}\omega_4 = 0,$$

and therefore to $a_{31} = 0$, which is a contradiction with our first conclusion.

Case $a_{11} = 0$. From $\mathcal{C}^2(\omega_4) = \sqrt[4]{a_{31}^3}\omega_4 = 0$, we immediately get $a_{31} = 0$. If $a_{21} \neq 0$, without loss of generality, we may assume $a_{21} = 1$, and get

$$\mathcal{C}^2(\omega_2) = \mathcal{C}(\omega_2) + \sqrt[4]{a_{03}}\mathcal{C}(\omega_3) = 0$$

which is a non-trivial $\overline{\mathbb{F}}_2$-linear relation between the second and the third row of $HW(C)$. This is not possible since $\mathrm{rk}(HW(C)) = 2$, and hence $a_{21} = 0$. The restriction on the rank of the Hasse-Witt matrix gives us that

$$\mathcal{C}^2(\omega_2) = \sqrt[4]{a_{03}}\mathcal{C}(\omega_3) = 0$$

implies that $a_{03} = 0$. Similarly

$$\mathcal{C}^2(\omega_3) = \sqrt[4]{a_{30}}\mathcal{C}(\omega_2) + \sqrt[4]{a_{12}}\mathcal{C}(\omega_3)$$

implies that $a_{30} = a_{12} = 0$. We ended up with a Hasse-Witt matrix of the form

$$HW(C) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a_{01} & 0 & 0 & a_{41} \\ a_{10} & 0 & 0 & a_{50} \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \mathrm{rk}(HW(C)) = 2.$$

The condition $\mathrm{rk}(HW(C)) = 2$ gives us that C is non-singular at all affine points with $T = 1$. However, if we observe the equation in $\mathbb{P}^3$

$$C : \begin{cases} TZ + X^2 = 0 \\ a_{00}T^3 + a_{01}T^2Y + a_{10}T^2X + a_{41}YZ^2 + a_{50}XZ^2 = 0 \end{cases}$$

and take a look at the point $P = (0:0:1:0)$, we may see that P is a singular point of C.

Therefore, we obtained that there are no non-hyperelliptic curves of genus 4 over $\overline{\mathbb{F}}_2$ with Ekedahl-Oort type $[4,3]$ that lie on a quadric cone. □

4.3.2 Curves with Ekedahl-Oort type $[4,1]$ or $[4,2]$

By the previous theorem, we in particular get that there is no non-hyperelliptic supersingular curve C of genus 4 over $\overline{\mathbb{F}}_2$ that lies on a quadric cone and has Ekedahl-Oort type $[4,3]$. As we mentioned above, the relevant Young diagrams for curves C on a quadric cone that have 2-rank zero and a-number two, in particular supersingular, are also $[4,1]$ and $[4,2]$. The computations similar to the ones above, that we collect in the following example, give us that we cannot a priori discard such possibilities. Furthermore, we will see what the possible equations are for a curve with 2-rank zero (and thus a-number two) lying on a quadric cone.

Example 4.6. *For C a non-hyperelliptic curve of genus 4 over $\mathbb{F}_2$ that lies on a quadric cone with Ekedahl-Oort type either $[4,2]$ or $[4,1]$, its final type satisfies*

$$v(1) = 0, \quad v(2) = 1 \quad \textit{and} \quad v(4) = 2.$$

Similarly as above, we discuss the possible Hasse-Witt matrices for C.

Let us firstly show that $a_{11} = 0$. Suppose to the contrary that $a_{11} = 1$. We immediately get $a_{31} \neq 0$ since otherwise $\mathcal{C}^n(\omega_1) = \omega_1 \neq 0$ for any $n \in \mathbb{Z}_{>0}$, and then the rank discussion gives $a_{03} = a_{12} = 0$ as well as $a_{41} = a_{31}(a_{21} + a_{31}a_{01}), a_{50} = a_{31}(a_{30} + a_{31}a_{10})$. Since $\dim_{\overline{\mathbb{F}}_2}(\mathcal{C}^2(H^0(C, \Omega^1_C))) = 1$, we get that $\mathcal{C}^2(\omega_1)$ and $\mathcal{C}^2(\omega_4)$ cannot be two linearly independent vectors. $\mathcal{C}^2(\omega_1) = 0$, implies as before that $a_{41} = 0$ and $a_{01} = \frac{1}{\sqrt{a_{31}}}, a_{21} = \sqrt{a_{31}}$. However, $\mathcal{C}^3(\omega_4) = 0$ then gives a contradiction with $a_{31} \neq 0$. Similarly, we obtain $\mathcal{C}^2(\omega_4) \neq 0$ by considering $\mathcal{C}^3(\omega_1) = 0$. The last possibility is

$$\mathcal{C}^2(\omega_1) \neq 0, \quad \mathcal{C}^2(\omega_4) \neq 0, \quad \mathcal{C}^2(\omega_1) = \lambda \mathcal{C}^2(\omega_4)$$

for some $\lambda \in \overline{\mathbb{F}}_2^*$. Comparing the coefficients with ω_1, ω_2 and ω_4, we get $a_{21} = \sqrt{a_{31}}, a_{01} \neq 0$, $\lambda = \frac{1}{a_{01}} + \sqrt{a_{31}}$. We compute

$$\begin{aligned}\mathcal{C}^3(\omega_1) &= \mathcal{C}((1 + \sqrt[4]{a_{31}}\sqrt{a_{01}})\omega_1 + \sqrt[4]{a_{31}}\sqrt{a_{41}}\omega_4) \\ &= \sqrt{1 + \sqrt[4]{a_{31}}\sqrt{a_{01}}}(\omega_1 + \sqrt{a_{31}}\omega_2) + \sqrt[8]{a_{31}}\sqrt[4]{a_{41}}(\omega_2 + \sqrt{a_{31}}\omega_4).\end{aligned}$$

Since $\mathcal{C}^3(\omega_1) = 0$, we get $a_{01} = \frac{1}{\sqrt{a_{31}}}$, and thus $\lambda = 0$. This is a contradiction with the choice of λ.

Therefore, $a_{11} = 0$ and then also $a_{31} = 0$. We compute

$$\mathcal{C}^2(\omega_2) = \sqrt[4]{a_{21}}\mathcal{C}(\omega_2) + \sqrt[4]{a_{03}}\mathcal{C}(\omega_3), \quad \mathcal{C}^2(\omega_3) = \sqrt[4]{a_{30}}\mathcal{C}(\omega_2) + \sqrt[4]{a_{12}}\mathcal{C}(\omega_3),$$

and using $v(4) = 2, v(2) = 1$ discuss three potential cases:

$$\mathcal{C}^2(\omega_2) = 0, \quad \mathcal{C}^2(\omega_3) = 0, \quad \textit{or} \;\; \mathcal{C}^2(\omega_2) = \lambda \mathcal{C}^2(\omega_3), \lambda \in \overline{\mathbb{F}}_2^*.$$

$\mathcal{C}^2(\omega_2) = 0$ leads to $a_{21} = a_{03} = 0$ and then $\mathcal{C}^3(\omega_3) = 0$ to $a_{12} = 0$. In that case, we get the Hasse-Witt matrix

$$HW(C) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a_{01} & 0 & 0 & a_{41} \\ a_{10} & a_{30} & 0 & a_{50} \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and

$$C: \begin{cases} TZ + X^2 = 0 \\ a_{00}T^3 + a_{01}T^2Y + a_{10}T^2X + a_{41}YZ^2 + a_{50}XZ^2 + bX^3 + (b + a_{30})TXZ = 0 \end{cases},$$

so we can see that $P = (0:0:1:0)$ is a singular point of C, and thus such C does not give a class in $\mathcal{M}_4$.

Another possibility is $\mathcal{C}^2(\omega_3) = 0$, which leads to

$$HW(C) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a_{01} & 0 & a_{03} & a_{41} \\ a_{10} & 0 & 0 & a_{50} \\ 0 & 0 & 0 & 0 \end{pmatrix}, a_{03} \neq 0. \tag{17}$$

The final possibility is $\mathcal{C}^2(\omega_2) \neq 0, \mathcal{C}^2(\omega_3) \neq 0$ and there is $\lambda \in \overline{\mathbb{F}}_2^*$ such that $\mathcal{C}^2(\omega_2) = \lambda \mathcal{C}^2(\omega_3)$, i.e.,

$$\sqrt[4]{a_{21}} = \lambda \sqrt[4]{a_{30}}, \sqrt[4]{a_{03}} = \lambda \sqrt[4]{a_{12}}.$$

$a_{03} = 0$ implies that C is singular at $P = (0:0:1:0)$, so let suppose $a_{03} = 1$. Computing $\mathcal{C}^3(\omega_2) = 0, \mathcal{C}^3(\omega_3) = 0$, we get $a_{30} = a_{12}^3, a_{21} = a_{12}^2$ and $a_{12}^3 + 1 = 0$. Writing $a_{12} = b, b \in \overline{\mathbb{F}}_2^*$ we get

$$HW(C) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a_{01} & b^2 & 1 & a_{41} \\ a_{10} & b^3 & b & a_{50} \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{18}$$

Both (17) *and* (18) *are valid possibilities, and we can exclude only some partial cases from them using the conditions coming from the facts that* $\mathrm{rk}(HW(C)) = 2$ *and that C is non-singular.*

Remembering the embedding $\mathbb{A}^2 \to Q = \{TZ = X^2\}$, we can rephrase the conclusions obtained in Example 4.6. Namely, we concluded above that genus four curves over $\overline{\mathbb{F}}_2$ with 2-rank zero and a-number two lying on a quadric cone have an equation of the form

$$\begin{cases} TZ + X^2 = 0 \\ Y^3 + m_0XY^2 + m_1T^2Y + m_2T^2X + m_3YZ^2 + m_4XZ^2 + m_5T^3 + \\ \quad + m_6X^2Y + (m_6 + m_0^2)TYZ + m_7X^3 + (m_7 + m_0^3)TXZ = 0 \end{cases} \tag{19}$$

with $m_i \in \overline{\mathbb{F}}_2$ so that $\begin{pmatrix} m_1 & m_0^2 & 1 & m_3 \\ m_2 & m_0^3 & m_0 & m_4 \end{pmatrix}$ is a matrix of rank 2.

Even though there is no non-hyperelliptic supersingular curve of genus 4 over $\mathbb{F}_2$ lying on a quadric cone as we saw in Table 1, using the previous description, we found that over $\mathbb{F}_4$ such a curve exists. Therefore, the supersingular locus has a nonempty intersection with the locus of non-hyperelliptic curves of genus 4 over $\overline{\mathbb{F}}_2$ that lie on a quadric cone.

Example 4.7. *Consider C the non-hyperelliptic genus 4 curve over $\mathbb{F}_4$ that lies on a singlar quadric, given by the equation*

$$C : \begin{cases} TZ + X^2 = 0 \\ Y^3 + \zeta_2T^2X + \zeta_2XZ^2 + T^3 = 0 \end{cases},$$

with ζ_2 a root of $x^2 + x + 1 = 0$ in $\overline{\mathbb{F}}_2$. We claim that C is a supersingular curve.

Let us briefly check that C is non-singular. In the affine part $T \neq 0$, if we denote $x = X/T$, $y = Y/T, z = x^2$ we get

$$C|_{T\neq 0} : f(x,y) = y^3 + \zeta_2 x + \zeta_2 x^5 + 1 = 0,$$

and hence

$$\frac{\mathrm{d}f}{\mathrm{d}x}(x,y) = \zeta_2(x+1)^4 = 0, \quad \frac{\mathrm{d}f}{\mathrm{d}y}(x,y) = y^2 = 0$$

have a common solution $(x,y) = (1,0)$ *that is not a point on* C*. Using*

$$T = 0 \implies X = 0, Y = 0,$$

we find that the remaining point that needs to be checked is $(0:0:0:1)$*, where we may look at the affine part* $Z \neq 0$ *and similarly see that it will be non-singular.*

With the help of SageMath*, we computed*

$$\#C(\mathbb{F}_4) = 13, \quad \#C(\mathbb{F}_{4^2}) = 49, \quad \#C(\mathbb{F}_{4^3}) = 193, \quad \#C(\mathbb{F}_{4^4}) = 769.$$

Weil's conjecture for curves gives us

$$Z(C/\mathbb{F}_4, t) = \exp\left(\sum_{s=1}^{\infty} \frac{\#C(\mathbb{F}_{4^s})t^s}{s}\right) = \frac{L(C/\mathbb{F}_4,t)}{(1-t)(1-4t)},$$

so we can compute the coefficients in $L(C/\mathbb{F}_4,t)$ *with* $1, t, t^2, t^3$ *and* t^4 *and use the symmetry of the Newton polygons to see that the Newton polygon of* C *is the supersingular one.*

Note that C from Example 4.7 is in fact of form (19). Namely, choose in (19) m_i's as follows:

$$m_2 = m_4 = \zeta_2, \; m_5 = 1 \text{ and } m_0 = m_1 = m_3 = m_6 = m_7 = 0.$$

If we would like to decide whether the curve C has the Ekedahl-Oort type $[4,1]$ or $[4,2]$, we will need to have the basis for the whole $H^1_{dR}(C)$ and not only for the space of differentials $H^0(C, \Omega^1_C) \subseteq H^1_{dR}(C)$ that we have from (15). Then, we could try to understand how the Verschiebung operator acts on subspaces of $H^1_{dR}(C)$ in order to compute what is $v(3)$, the final type evaluated at 3.

4.4 Cyclic covers of $\mathbb{P}^1$ of genus four, 2-rank zero and a-number two

Let $k = \overline{\mathbb{F}}_p$, for a prime number $p \in \mathbb{Z}_{>0}$ (we are still primarily interested in $p = 2$), and let $m \in \mathbb{Z}_{\geq 2}$ be such that $p \nmid m$. Further, let $a = (a_1, \dots, a_N) \in (\mathbb{Z}_{>0})$ be an N-tuple with $\gcd(a_i, m) = 1$, $i \in \{1, \dots, N\}$ for $N \geq 3$ such that

$$\sum_{i=1}^{N} a_i \equiv 0 \mod m.$$

For $c_1 = 0$ and $c_i \in k^*, i \in \{1, \dots, N\}$, consider a curve

$$C : y^m = f_a(x) = \prod_{i=1}^{N-1} (x - c_i)^{a_i}, \tag{20}$$

whose genus, computed using the Riemann-Hurwitz formula equals

$$g(C) = 1 + \frac{(N-2)m - N}{2}.$$

We say that C in (20) is the *cyclic cover of the projective line*, inspired by the fact that $\mathbb{Z}/m\mathbb{Z}$ acts on C via $(x,y) \mapsto (x, \zeta y)$ for ζ a primitive m-th root of unity.

If we denote by $\langle z\rangle$ the fractional part of any $z \in \mathbb{R}$, i.e., $\langle z\rangle = z - \lfloor z\rfloor$, and for $n, i \in \mathbb{Z}_{>0}$, $b(i,n) = \lfloor (na_i)/m\rfloor$, for example [31], Lemma 2.7 gives us that the space of regular differentials $H^0(C, \Omega^1_C)$ is generated by

$$\omega_{n,l} = y^{-n}x^l \prod_{i=1}^{N-1}(x-c_i)^{b(i,n)}, \quad 1 \le n \le m, 0 \le l \le -2 + \sum_{i=1}^{N} \langle na_i/m\rangle .$$

Moreover, if we write $s_a = \prod_{i=1}^{N-1}(x-c_i)^{b(i,n)}$ for an N-tuple a as above, and define

$$f_{n,l} = y^n x^{-l-1} \prod_{i=1}^{N-1}(x-c_i)^{-b(i,n)},$$

and write $h_a(x) \in k[x]$ for the polynomial satisfying

$$\frac{nxs_a(x)f'(x) + ((l+1)s_a(x) + xs'_a(x))f_a(x)}{s_a^2(x)} = h_a(x)\prod_{i=1}^{N-1}(x-c_i)^{a_i - b(i,n)-1},$$

for $n, l \in \mathbb{Z}_{>0}$, Zhou in [51], Section 4 computed a basis for $H^1_{dR}(C)$, where C is as in (20).

Theorem 4.8 ([51], Theorem 4.2). *Let C be a (non-singular projective) curve over k given by affine equation (20), and let $\pi : C \to \mathbb{P}^1$ be the m-covering. For the open affine cover $\{U_1, U_2\}$ of C with $U_1 = \pi^{-1}(\mathbb{P}^1 - \{0\}), U_2 = \pi^{-1}(\mathbb{P}^1 - \{\infty\})$, a basis of $H^1_{dR}(C)$, for $1 \le n \le m-1$, $0 \le l \le -2 + \sum_{i=1}^{N} \langle na_i/m\rangle$, consists of the following elements*

$$\alpha_{n,l} = \left[(0, \omega_{n,l}, \omega_{n,l})\right],$$

$$\beta_{n,l} = \left[(f_{n,l}, \frac{\psi_{n,l}(x)t(x)}{x^{l+2}y^{m-n}}\mathrm{d}x, \frac{\phi_{n,l}(x)t(x)}{x^{l+2}y^{m-n}}\mathrm{d}x)\right],$$

where $t(x) = \prod_{i=1}^{N-1}(x-c_i)^{a_i-b(i,n)-1}$ and $\psi_{n,l}(x), \phi_{n,l}(x) \in k[x]$ are such that $\psi_{n,l}(x) + \phi_{n,l}(x) = h_a(x)$ and $\psi_{n,l}(x)$ is the sum of all monomials in $h_a(x)$ of degree less than or equal to $l+1$.

Furthermore, in $H^1_{dR}(C)$ we have

$$\langle \alpha_{i_1,j_1}, \beta_{i_2,j_2}\rangle \neq 0 \Longleftrightarrow (i_1, j_1) = (i_2, j_2).$$

Using the genus formula for the curves described above, i.e., for the *cyclic covers of the projective line*, we can get some genus 4 curves over $\overline{\mathbb{F}}_2$ for choices

$$(m, N) \in \{(3,6), (5,4), (9,3)\}.$$

There is precisely one curve coming from the choice $m = 9$ and $N = 3$, namely the curve

$$y^9 = x(x+1),$$

for which it is known that it is supersingular. Alternatively, one can compute its Newton polygon using the counts over the finite extensions of $\mathbb{F}_2$.

Using Theorem 4.8 with $m = 5, N = 4$, Zhou in [51], Corollary 4.6, obtained that any curve

$$y^5 = x(x+1)(x+\xi),$$

over $\overline{\mathbb{F}}_2$, for $\xi \in \overline{\mathbb{F}}_2 - \{0,1\}$ arbitrary, has Ekedahl-Oort type $[4,2]$. Therefore, the locus $Z_{[4,2]}$ in $\mathcal{M}_4$ is at least 1-dimensional. It should be mentioned that such a result is in fact obtained over any $\overline{\mathbb{F}}_p$ with $p \equiv \pm 2 \mod 5$. For odd p with $p \equiv \pm 2 \mod 5$, by considering the curves of the form

$$y^5 = x(x-\zeta)(x+\zeta),$$

with $\zeta \in \overline{\mathbb{F}}_p$, in [51], Theorem 4.7, Zhou concluded that the locus $Z_{[4,3]}$ is non-empty in $\mathcal{M}_4 \otimes \overline{\mathbb{F}}_p$.

We discuss the remaining case $m = 3$ and $N = 6$ below, and obtain that the locus of curves in $\mathcal{M}_4$ with 2-rank zero and a-number two is at least 2-dimensional.

Theorem 4.9. *Let u, v, w be three mutually distinct elements of $k - \{0,1\}$ which satisfy the condition $u + v + w + uv + uw + vw = 0$. Then the equation*

$$y^3 = x(x-1)(x-u)(x-v)(x-w)$$

defines a curve C of genus $g(C) = 4$ with 2-rank$(C) = 0$ and $a(C) = 2$.

Proof. For u, v, w and the equation of C as in the statement of the theorem, in terms of notions introduced in (20) we have $a = (a_i)_{1 \le i \le 6}$ with $a_i = 1$ and

$$f_a = x^5 + (1+u+v+w)x^4 + (u+v+w+uvw)x^2 + uvwx.$$

Therefore, Theorem 4.8 gives us the basis of $H^0(C, \Omega^1_C)$ consisting of the following elements:

$$\alpha_{1,0} = \frac{1}{y}\mathrm{d}x = \left[0, \frac{1}{y}\mathrm{d}x, \frac{1}{y}\mathrm{d}x\right], \quad \alpha_{2,0} = \frac{1}{y^2}\mathrm{d}x, \quad \alpha_{2,1} = \frac{x}{y^2}\mathrm{d}x, \quad \alpha_{2,2} = \frac{x^2}{y^2}\mathrm{d}x,$$

If $Y_8 = H^1_{dR}(C)$, we know that $Y_4 = V(Y_8) = H^0(C, \Omega^1_C)$. Recall that V on $H^0(C, \omega^1_C) \subseteq H^1_{dR}(C)$ coincides with $\mathcal{C}$, so we compute

$$V(a_{2,0}) = \mathcal{C}(\frac{1}{y^2}\mathrm{d}x) = \frac{1}{y}\mathcal{C}(\mathrm{d}x) = 0, \quad V(\alpha_{2,1}) = \frac{1}{y}\mathcal{C}(x\mathrm{d}x) = \frac{1}{y}\mathrm{d}x = \alpha_{1,0}, \quad V(\alpha_{2,2}) = 0,$$

and

$$V(\alpha_{1,0}) = \mathcal{C}(\frac{y^3}{y^4}\mathrm{d}x) = \frac{1}{y^2}\mathcal{C}(f\mathrm{d}x) = \frac{\sqrt{uvw} + x^2}{y^2}\mathrm{d}x = \sqrt{uvw} \cdot \alpha_{2,0} + \alpha_{2,2}.$$

Hence, we get $v(4) = 2, v(2) = 1$ and similarly $v(1) = 0$, so in the Ekedahl-Oort type μ of C we have $\mu_1 = 4, \mu_2 \in \{1,2\}$ and $\mu_3 = 0$. In particular, we get 2-rank$(C) = 0$ and $a(C) = 2$. □

For precise computing the Ekedahl-Oort type of the curve occurring in Theorem 4.9, we will also need to consider the basis elements $\beta_{n,l} \in H^1_{dR}(C)$. However, will not do that here, and we refer to [51], Corollary 4.6 for a similar problem.

5 Computing curves of genus $g = 5$ defined over $\mathbb{F}_2$

A standard result is that the smooth curves of genus 5 are either hyperelliptic, trigonal, or complete intersections of three quadric hypersurfaces in $\mathbb{P}^4$. Therefore, to understand the moduli space $\mathcal{M}_5$ of smooth curves of genus 5, we should understand the subvarieties parametrizing these three kinds of smooth curves. Denote with $\mathcal{H}_5$ the subvariety of $\mathcal{M}_5$ parameterizing hyperelliptic curves of genus 5, with $\mathcal{T}_5$ the subvariety parameterizing trigonal curves of genus 5, and lastly, let $\mathcal{U}_5$ be the subvariety parameterizing curves whose canonical model in $\mathbb{P}^4$ is a complete intersection of three quadric hypersurfaces.

Let us write $\mathrm{Hyp}_g(\mathbb{F}_2)$ for the set on non-isomorphic (over $\mathbb{F}_2$) hyperelliptic curves of genus g over $\mathbb{F}_2$, $\mathrm{Tri}_g(\mathbb{F}_2)$ for the set on non-isomorphic (over $\mathbb{F}_2$) trigonal curves of genus g over $\mathbb{F}_2$, and $\mathrm{ComInt}_g(\mathbb{F}_2)$ for the set of non-isomorphic (over $\mathbb{F}_2$) curves of genus g over $\mathbb{F}_2$ that are complete intersections of three quadric hypersurfaces in $\mathbb{P}^4$ in their canonical models. The aim of this section is to find algorithms for computing all $\mathbb{F}_2$-isomorphism classes of smooth curves of genus 5 defined over $\mathbb{F}_2$, and to extract a piece of information on the supersingular locus in $\mathcal{M}_5$, by finding the supersingular curves over $\mathbb{F}_2$ among all of them. We do that separately for $\mathrm{Hyp}(\mathbb{F}_2)$, $\mathrm{Tri}(\mathbb{F}_2)$ and $\mathrm{ComInt}(\mathbb{F}_2)$. Furthermore, we are interested in automorphism groups over $\mathbb{F}_2$ for curves in the previous three sets. With them, we can get the insight into the moduli count, i.e., in computing the numbers $|\mathcal{H}_5(\mathbb{F}_2)|, |\mathcal{T}_5(\mathbb{F}_2)|$ and $|\mathcal{U}_5(\mathbb{F}_2)|$.

We collect the obtained results on `https://github.com/DusanDragutinovic/MT_Curves`, and mention some parts of the implementations in the appendix too.

Note that a non-hyperelliptic curve C of genus $g \geq 2$ in its canonical model in $\mathbb{P}^4$ has degree 8. For the presentation of the following examples, we also consult [12].

Example 5.1. *Any curve C of genus 5 and degree 8 in $\mathbb{P}^4$ lies on three quadric surfaces.*

The idea for showing this is similar to the one when we saw that a non-hyperelliptic genus 4 curve lies on a quadric and a cubic, at the beginning of Section 4. Namely, consider the fundamental exact sequence of $\mathcal{O}_{\mathbb{P}^4}$-modules, tensor it by $\mathcal{O}_{\mathbb{P}^4}(2)$, and take the long exact sequence in cohomology to get

$$0 \to H^0(\mathbb{P}^4, \mathcal{I}_C \otimes \mathcal{O}_C(2)) \to H^0(\mathbb{P}^4, \mathcal{O}_{\mathbb{P}^4}) \to H^0(\mathbb{P}^4, \mathcal{O}_C) \to \dots$$

Using $\deg(\mathcal{O}_C(K_C) \otimes \mathcal{O}_C(-2)) < 0$ *so* $\dim H^0(C, \mathcal{O}_C(K_C) \otimes \mathcal{O}_C(-2)) = 0$*, and the Riemann-Roch theorem for*

$$\dim H^0(C, \mathcal{O}_C) - \dim H^0(C, \mathcal{O}_C(K_C) \otimes \mathcal{O}_C(-2)) = 12,$$

we get $\dim H^0(C, \mathcal{O}_C) = 12$*. Hence,* $H^0(\mathbb{P}^4, \mathcal{I}_C \otimes \mathcal{O}_C(2)) \geq 3$*, so C lies on three quadric hypersurfaces.*

Recall that a curve C is trigonal by definition if it has a $\mathfrak{g}^1_3$, i.e., if there is a map $C \to \mathbb{P}^1$ of degree 3. In [15], Example IV.5.5.3, using that a non-hyperelliptic curve C of genus 5 is trigonal if and only if it has a trisecant, it is shown that a non-singular complete intersection of three quadric hypersurfaces in $\mathbb{P}^4$ is not a trigonal curve. A consequence of the famous Noether-Enriques theorem is the converse to that. Namely, if a non-hyperelliptic curve C of genus 5 is not trigonal, then it is a complete intersection of quadric hypersurfaces in $\mathbb{P}^4$. We collect these in the following theorem.

Theorem 5.2. *Let C be a non-hyperelliptic curve of genus 5. Then it is either a trigonal curve or its canonical model is a complete intersection of three quadric hypersurfaces in $\mathbb{P}^4$.*

Lastly, we give a useful (for our purposes) description of the trigonal curves of genus 5. Before that, we mention the well-known formula for computing the genus of a plane curve which possibly has some *ordinary* singularities. We say that a singularity is of **delta invariant** 1 if it is either a node (an ordinary double point), where a curve is locally of the form $xy = 0$, or an ordinary cusp, so that the curve is locally $y^2 = x^3$. For a curve C, whose singularities are all of delta invariant 1, we compute its genus as

$$g(C) = \frac{(d-1)(d-2)}{2} - \#\text{singularities}.$$

Example 5.3. *A curve C of genus 5 is trigonal if and only if it can be represented as a plane quintic with precisely one singularity of delta invariant 1.*

We offer a sketch of this result. Let D be an effective $\mathfrak{g}_3^1$. Since $\deg(K_C - D) = 5$ and $\dim H^0(C, \mathcal{O}_C(D)) = 2$, the Riemann-Roch theorem gives us $\dim H^0(C, \mathcal{O}_C(K_C - D)) = 3$. Therefore, $K_C - D$ is a $\mathfrak{g}_5^2$, so defines a morphism

$$|K_C - D| : C \to \mathbb{P}^2$$

of degree 5. By the genus formula for plane curves, we conclude that the image of C has exactly one singularity and that it is of delta invariant 1. Conversely, for a curve $f : C \to \mathbb{P}^2$, we may take the divisor E to be such that $\mathcal{O}_C(E) \cong f^*\mathcal{O}_{\mathbb{P}^1}(1)$, when a similar discussion gives that $K_C - E$ is a $\mathfrak{g}_3^1$.

5.1 Hyperelliptic curves

It is known that any hyperelliptic curve of genus g over $\mathbb{F}_2$ can be represented in a standard (affine) equation

$$y^2 + q(x)y = p(x), \quad \text{for } p(x), q(x) \in \mathbb{F}_2[x] \text{ with } 2g+1 \le \max\{2\deg(q(x)), \deg(p(x))\} \le 2g+2. \tag{21}$$

As we mentioned in Section 4, Xarles in [49] gave the approach to compute all (smooth) curves of genus 4 over $\mathbb{F}_2$ up to isomorphism. The given algorithm for determining the hyperelliptic curves over $\mathbb{F}_2$ can be generalized to higher genera, and here, we will use it to obtain the set $\mathrm{Hyp}_5(\mathbb{F}_2)$. Some of the claims made in [49] we can use directly, while for the other, we will mention the analogs in the genus 5 case.

Let $\mathbb{F}_2[x]_n = \{h(x) \in \mathbb{F}_2[x] : \deg(h(x)) \le n\}$ for $n \in \mathbb{Z}_{\ge 0}$, and for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_2)$ and $q(x) \in \mathbb{F}_2[x]_n$, define an action of $\mathrm{PGL}_2(\mathbb{F}_2)$ into $\mathbb{F}_2[x]_n$ by

$$\psi_n(A)(q(x)) = (cx+d)^n q\left(\frac{ax+b}{cx+d}\right);$$

we will also use the notation $A.q(x)$ for this. Further, denote the quotient set of $\mathbb{F}_2[x]_n$ under this action by $\overline{\mathbb{F}_2[x]_n} = \mathbb{F}_2[x]_n/\mathrm{PGL}_2(\mathbb{F}_2)$.

Let H_1 and H_2 be two hyperelliptic curves over $\mathbb{F}_2$ given by equations $H_1 : y^2 + q_1(x)y = p_1(x)$ and $H_2 : y^2 + q_2(x)y = p_2(x)$, where it holds that $2g+1 \le \max\{2\deg(q_i(x)), \deg(p_i(x))\} \le 2g$ with $q_i(x)$ monic, for $i \in \{1, 2\}$. Using that any isomorphism of such H_1 and H_2 has to be of the form

$$(x, y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{r(x)+y}{(cx+d)^{g+1}}\right)$$

for some $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_2)$ and $r(x) \in \mathbb{F}_2[x]_{g+1}$, Xarles showed the following lemma.

Lemma 5.4 ([49], Lemma 1)**.** *Let H_1 and H_2 be as above. Then there exists $A \in \mathrm{PGL}_2(\mathbb{F}_2)$ such that $q_2(x) = \psi_{g+1}(A)(q_1(x))$.*

Using the lemma, we can see that when determining all hyperelliptic curves of genus 5 over $\mathbb{F}_2$, $C : y^2 + q(x)y = p(x)$, it is enough to consider only elements of $\overline{\mathbb{F}_2[x]_6}$ for the representatives of $q(x)$.

For any $q(x) \in \overline{\mathbb{F}_2[x]_{g+1}}$, let $\mathrm{Stab}(q(x))$ be the stabilizer of $q(x)$ under the $\mathrm{PGL}_2(\mathbb{F}_2)$-action. We cite two results from [49].

Lemma 5.5 ([49], Lemma 4)**.** *Let H_1 and H_2 be two hyperelliptic curves of genus g over $\mathbb{F}_2$ given by standard equations (21): $y^2 + q(x) = p_i(x)$, $i \in \{1, 2\}$. If H_1 and H_2 are isomorphic over $\mathbb{F}_2$, then there are $A \in Stab(q(x))$ and $r(x) \in \mathbb{F}_2[x], \deg(r(x)) \le g + 1$ such that*

$$p_2(x) = \psi_{2g+1}(p_1(x) + r(x)^2 + q(x)r(x)).$$

Lemma 5.6 ([49], Lemma 5)**.** *Let $g \in \mathbb{Z}_{\ge 1}$. Given nonzero $q(x) \in \mathbb{F}_2[x]$ with $q(x) \le g + 1$ and $p(x) \in \mathbb{F}_2[x]$ with $2g + 1 \le \max\{2\deg(q(x)), \deg(p(x))\} \le 2g + 2$, the equation $y^2 + q(x)y = p(x)$ defines a hyperelliptic curve of genus g if and only if*

$$\gcd(q(x), p'(x)^2 + q'(x)^2 p(x)) = 1,$$

and either $\deg(q(x)) = g + 1$ or $a_{2g+1}^2 \ne a_{2g+2} b_g^2$, where $p(x) = \sum_{i=0}^{2g+2} a_i x^i$ and $q(x) = \sum_{i=0}^{g+1} b_i x^i$.

The previous three lemmas offer us a possibility to completely determine the set $\mathrm{Hyp}_5(\mathbb{F}_2)$. The initial idea is to check for pair of $p(x), q(x) \in \mathbb{F}_2[x]$ with

$$11 \le \max\{2\deg(q(x)), \deg(p(x))\} \le 12$$

whether $y^2 + q(x)y = p(x)$ defines a hyperelliptic curve of genus 5 over $\mathbb{F}_2$. Lemma 5.4 reduces that job, by considering some smaller set of possible $q(x)$'s, namely, only the set of representatives for $\mathbb{F}_2[x]_6$ for the $\mathrm{PGL}_2(\mathbb{F}_2)$-action, called $Q_5(\mathbb{F}_2)$. In other words, $Q_5(\mathbb{F}_2)$ is the set of representatives of elements in $\overline{\mathbb{F}_2[x]_6}$. Then, using Lemma 5.5, for fixed $q(x) \in Q_5(\mathbb{F}_2)$, we can reduce the list of possible polynomials $p(x)$, and finally, Lemma 5.6 helps us to decide whether such pairs $(q(x), p(x))$ define hyperelliptic curves of genus 5. Therefore, it is only left to determine $Q_5(\mathbb{F}_2)$. We do that below using the same ideas as in [49], Lemma 2.

Lemma 5.7. *For $q(x) \in \mathbb{F}_2[x]_6$, let $D_{q(x)} = \mathcal{Z}'(q(x)) + (6 - \deg(q(x))) \cdot \infty$ be the zero divisor of $q(x)$ in $\mathbb{P}^1$, where $\mathcal{Z}'(q(x)) = \{P \in \overline{\mathbb{F}}_2 : q(P) = 0\}$. Then the action of $\mathrm{PGL}_2(\mathbb{F}_2)$ on $\mathbb{F}_2[x]_6$ naturally translates to the (standard) action of $\mathrm{PGL}_2(\mathbb{F}_2)$ on $\mathrm{Div}_6(\mathbb{F}_2)$, and these actions are compatible, i.e., $D_{A.q(x)} = A.D_{q(x)}$.*

Proof. For an arbitrary polynomial $q(x) = e_6 x^6 + e_5 x^5 + \ldots + e_1 x + e_0 \in \mathbb{F}_2[x]_6$ and a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_2)$ we compute

$$q_{new}(x) = A.q(x) = e_6(ax+b)^6 + e_5(ax+b)^5(cx+d) + \ldots + e_1(ax+b)(cx+d)^5 + e_0(cx+d)^6.$$

For $P = d/c, c \ne 0$, we see that $P \in \mathcal{Z}'(A.q(x))$ if and only if $\deg(q(x)) < 6$, and moreover, its multiplicity as a zero of $A.q(x)$ is precisely $6 - \deg(g(x))$; this means that the multiplicity of $P = d/c$ in $D_{A.q(x)}$ is the same as the multiplicity of ∞ in $D_{q(x)}$. Using A^{-1} and changing the roles of $q(x)$ and $q_{new}(x)$ we can similarly get the conclusion on the degree of $q_{new}(x)$ when inspecting $P = \infty$. For other $P \in \overline{\mathbb{F}}_2$, we see $P \in \mathcal{Z}'(q(x))$ if and only if $\frac{aP+b}{cP+d} \in \mathcal{Z}'(q(x))$ and the corresponding multiplicities match. From these explicit relations, we see that the asserted claim holds. □

The previous lemma implies that determining $\overline{\mathbb{F}_2[x]_6}$ (and hence $Q_5(\mathbb{F}_2)$) is the same as determining $\mathrm{Div}_6(\mathbb{F}_2)/\mathrm{PGL}_2(\mathbb{F}_2)$. Note further that if P is a K-point, for $K/\mathbb{F}_2$ some finite extension, and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_2)$, then $A.P = \frac{aP+b}{cP+d}$ is again a K-point (∞ is a $\mathbb{F}_2$-point).

Theorem 5.8. *The set $Q_5(\mathbb{F}_2)$ consists of the following elements $q(x) \in \mathbb{F}_2[x]$:*

$\deg(q(x)) \leq 2$*:* $\quad 1, x, x^2, x(x+1), x^2+x+1$

$\deg(q(x)) = 3$*:* $\quad x^3, x^2(x+1), (x^2+x+1)x, x^3+x+1$

$\deg(q(x)) = 4$*:* $\quad x^2(x+1)^2, (x^2+x+1)^2, (x^2+x+1)x^2, (x^2+x+1)x(x+1), (x^3+x+1)x, (x^3+x^2+1)x, x^4+x+1, x^4+x^3+1$

$\deg(q(x)) = 5$*:* $\quad (x^2+x+1)^2x, (x^3+x+1)(x^2+x+1), (x^3+x+1)x(x+1), (x^4+x+1)x, (x^4+x^3+x^2+x+1)x, x^5+x^2+1, x^5+x^3+1, x^5+x^3+x^2+x+1$

$\deg(q(x)) = 6$*:* $\quad (x^2+x+1)^3, (x^3+x+1)^2, (x^3+x+1)(x^3+x^2+1), (x^4+x+1)(x^2+x+1), x^6+x+1, x^6+x^3+1.$

Proof. For $q(x) \in \mathbb{F}_2[x]_6$, let $D_{q(x)}$ be as in Lemma 5.7. As we mentioned above, in order to find $Q_5(\mathbb{F}_2)$, we will firstly determine $\mathrm{Div}_6(\mathbb{F}_2)/\mathrm{PGL}_2(\mathbb{F}_2)$. We use the well-known fact that given any three $\mathbb{F}_2$-points p_∞, p_0, p_1 there is a (unique) projective automorphism $A \in \mathrm{PGL}_2(\mathbb{F}_2)$ that sends $p_\infty \mapsto \infty, p_0 \mapsto 0, p_1 \mapsto 1$.

Firstly, any $D_{q(x)}$ that consists only of $\mathbb{F}_2$-point, in $\mathrm{Div}_6(\mathbb{F}_2)/\mathrm{PGL}_2(\mathbb{F}_2)$ is equal to the unique one $n_\infty \cdot \infty + n_0 \cdot 0 + n_1 \cdot 1$ with $n_1 \leq n_0 \leq n_\infty$. Since $\deg(D_{q(x)}) = 6$, we get that all the possible triples (n_∞, n_0, n_1) are

$$\{(6,0,0), (5,1,0), (4,2,0), (4,1,1), (3,3,0), (3,2,1), (2,2,2)\}.$$

Using the correspondence from Lemma 5.7, this gives us the subset of polynomials $q(x)$ in $Q_5(\mathbb{F}_2)$,

$$\{1, x, x^2, x(x+1), x^3, x^2(x+1), x^2(x+1)^2\}.$$

If $D_{q(x)}$ contains only one point of degree 2 and no other points of degree ≥ 2 in its support, similarly as above, we get that $D_{q(x)}$ is equal to one of

$$3\zeta_2,\ 2\zeta_2 + 2\infty,\ 2\zeta_2 + \infty + 0,\ \zeta_2 + 4\infty,\ \zeta_2 + 3\infty + 0,\ \zeta_2 + 2\infty + 2\cdot 0,\ \zeta_2 + 2\infty + 0 + 1.$$

This induces the set of polynomials in $Q_5(\mathbb{F}_2)$ (we use ζ_n as notation for any primitive $\zeta_n \in \overline{\mathbb{F}}_2$ of degree n over $\mathbb{F}_2$):

$$\{(x^2+x+1)^3, (x^2+x+1)^2, (x^2+x+1)^2x, x^2+x+1, (x^2+x+1)x, (x^2+x+1)x^2, (x^2+x+1)x(x+1)\},$$

If $D_{q(x)}$ contains a point of degree 3, then the possibilites are the following

$$D_{q(x)} \in \{2\zeta_3, \zeta_3 + \zeta_3', \zeta_3 + \zeta_2 + \infty, \zeta_3 + 3\infty, \zeta_3 + 2\infty + 0, \zeta_3 + \infty + 0 + 1\},$$

where ζ_3, ζ_3' are of degree 3. Since $x \mapsto x+1$, which is induced by action of $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, translates $q_1(x) = x^3+x+1$ to $q_2(x) = x^3+x^2+1$, we have that $D_{q_1(x)}$ and $D_{q_2(x)}$ are the same in $\mathrm{Div}_6(\mathbb{F}_2)/\mathrm{PGL}_2(\mathbb{F}_2)$, and that $D_{(q_1(x))^2}, D_{(q_1(x))(x^2+x+1)}, D_{(q_1(x))x(x+1)}$ are the same as $D_{(q_2(x))^2}$, $D_{(q_2(x))(x^2+x+1)}, D_{(q_2(x))x(x+1)}$. Therefore, this case gives us the new list of possible polynomials

$q(x)$: $\{(x^3+x+1)^2, (x^3+x+1)(x^3+x^2+1), (x^3+x+1)(x^2+x+1), x^3+x+1, (x^3+x+1)x, (x^3+x^2+1)x, (x^3+x+1)x(x+1)\}$.

In the case when $D_{q(x)}$ contains a point of degree 4, it should be either $\zeta_4+\zeta_2, \zeta_4+2\infty$ or $\zeta_4+\infty+0$. There are three irreducible polynomials over $\mathbb{F}_2$ of degree 4, so out of all possible combinations, discussing the $\mathrm{PGL}_2(\mathbb{F}_2)$ action on $\mathbb{F}_2[x]_6$ as above, we extract the following list of representatives for $q(x)$:

$$\{(x^4+x+1)(x^2+x+1), x^4+x+1, x^4+x^3+1, (x^4+x+1)x, (x^4+x^3+x^2+x+1)x\}.$$

When $D_{q(x)}$ contains a point of degree 5, there is only one possibility for the form of $D_{q(x)}$, namely $D_{q(x)}=\zeta_5+\infty$. Among six irreducible polynomials of degree 5, we found that for example, the following three are the representatives of $q(x)$ for the considered action:

$$\{x^5+x+1, x^5+x^3+1, x^5+x^3+x^2+x+1\}.$$

Lastly, among nine irreducible polynomials of degree 6, we found two x^6+x+1, x^6+x^3+1, so that acting via $\mathrm{PGL}_2(\mathbb{F}_2)$ on them we can get all the others. This corresponds to a unique choice for the form of divisor $D_{q(x)}$ that contains a point of degree 6, $D_{q(x)}=(\zeta_6)$. □

The previously described reasoning leads to an algorithm for computing the set $\mathrm{Hyp}_5(\mathbb{F}_2)$, that is practically the same to the one for computing $\mathrm{Hyp}_4(\mathbb{F}_2)$ from [49].

- From the previous theorem, we get **list_of_qs**, the list of all possible representatives for a polynomial $q(x)$.

- For each $q(x)$ in **list_of_qs** compute the stabilizer $\mathrm{Stab}(q(x)) \subseteq \mathrm{PGL}_2(\mathbb{F}_2)$ of $q(x)$ under the action defined by $\psi_6(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(q(x)) = (cx+d)^6 q(\frac{ax+b}{cx+d})$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{F}_2)$.

- For fixed $q(x)$ in **list_of_qs**, check if $p(x)\in\mathbb{F}_2[x]$, $11 \leq \max\{2\deg(q(x)), \deg(p(x))\} \leq 12$ is such that $C: y^2+q(x)y=p(x)$ is a (nonsingular) curve; collect all such $p(x)$'s in the list **q_list_of_ps** of potential $p(x)$'s for $q(x)$. The smoothness condition can be checked using Lemma 5, [49], saying that C is a (nonsingular) curve of genus 5 if and only if $\gcd(q(x), p'(x)^2+q'(x)^2p(x))=1$ and either $\deg(q(x))=6$ or $a_{11}^2 \neq a_{12}b_5^2$, where $p(x)=\sum_{i=0}^{12} a_i x^i$ and $q(x)=\sum_{i=0}^{6} b_i x^i$.

- Fix $q(x)$ in **list_of_qs** and consider **q_list_of_ps**, its associated list of potential $p(x)$'s. For curves $C_1: y^2+q(x)y=p_1(x)$ and $C_2: y^2+q(x)y=p_2(x)$, we write $p_1(x)\sim p_2(x)$ if they are isomorphic over $\mathbb{F}_2$. Refine **q_list_of_ps** by taking only the representatives $p(x)$ for this relation $\sim$. With the same argument as in Lemma 4, [49], we find that the relation $\sim$ is defined as: $p_1(x)\sim p_2(x)$ if and only if $(cx+d)^{12}p_2(\frac{ax+b}{cx+d}) = p_1(x)+r(x)^2+r(x)q(x)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in Stab(q(x))$ and some $r(x)\in\mathbb{F}_2[x]$ of degree $\deg(q(x)) \leq 6$.

In such a manner, using the mathematical software SageMath, we computed the list of all non-isomorphic hyperelliptic curves of genus 5 defined over $\mathbb{F}_2$. We found that there are in total 1070 such curves, i.e. $|\mathrm{Hyp}_5(\mathbb{F}_2)| = 1070$, and we confirmed that $|\mathcal{H}_5(\mathbb{F}_2)| = 512 = 2^{2\cdot5-1}$. For them, we computed the number of points over finite fields $\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}, \mathbb{F}_{2^4}$ and $\mathbb{F}_{2^5}$, and then we found their Newton polygons. In particular, all the Newton polygons but one occurs for elements of this class of genus 5 (nonsingular) curves over $\mathbb{F}_2$. In the following table, for each eligible non-supersingular Newton polygon, we present the standard affine equation and the index in our list of the first hyperelliptic curve for which such a polygon occurs.

Slopes of Newton polygon	Index	The affine equation of the curve
$[0,0,0,0,0,1,1,1,1,1]$	387	$y^2+(x^3+x+1)(x+1)xy+x^{12}+x=0$
$\left[0,0,0,0,\frac{1}{2},\frac{1}{2},1,1,1,1\right]$	208	$y^2+(x^2+x+1)(x+1)xy+x^{12}+x^{11}+x=0$
$\left[0,0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1,1\right]$	170	$y^2+(x^2+x+1)xy+x^{12}+x^{11}+x=0$
$\left[0,0,\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3},1,1\right]$	64	$y^2+(x+1)xy+x^{12}+x^{11}+x=0$
$\left[0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1\right]$	104	$y^2+(x+1)x^2y+x^{12}+x^{11}+x=0$
$\left[0,\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4},1\right]$	none	N/A
$\left[0,\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2},\frac{2}{3},\frac{2}{3},\frac{2}{3},1\right]$	33	$y^2+xy+x^{12}+x^{11}+x^9+x^5+x^4+x^3+x^2+x=0$
$\left[0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1\right]$	32	$y^2+xy+x^{12}+x^{11}+x=0$
$\left[\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5}\right]$	436	$y^2+(x^3+x^2+1)(x^3+x+1)y+x^{12}+x^{11}+x^{10}+x^7+x^6+x^3+x=0$
$\left[\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{2},\frac{1}{2},\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4}\right]$	437	$y^2+(x^3+x^2+1)(x^3+x+1)y+x^{11}+x^9+x^7+x^6+x=0$
$\left[\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{2}{3},\frac{2}{3},\frac{2}{3}\right]$	1	$y^2+y+x^{12}+x^{11}+x^{10}+x^7+x^6+x^3+x=0$
$\left[\frac{2}{5},\frac{2}{5},\frac{2}{5},\frac{2}{5},\frac{2}{5},\frac{3}{5},\frac{3}{5},\frac{3}{5},\frac{3}{5},\frac{3}{5}\right]$	7	$y^2+y+x^{12}+x^{11}+x^6+x^5+x^4+1=0$

Table 2: Some hyperelliptic curves of genus 5 over $\mathbb{F}_2$ and their Newton polygons

In the following table, we collected all the supersingular hyperelliptic curves of genus 5 defined over $\mathbb{F}_2$.

Slopes of Newton polygon	Index	The affine equation of the curve
$\left[\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right]$	0	$y^2+y+x^{12}+x^{11}=0$
	5	$y^2+y+x^{11}+x^{10}+x^9+x^4+x^3+x+1=0$
	9	$y^2+y+x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^2+x=0$
	11	$y^2+y+x^{12}+x^{11}+x^{10}+x^5+x^2=0$
	15	$y^2+y+x^{11}+x^{10}+x^6+x^5+x^3+x^2+x=0$
	20	$y^2+y+x^{12}+x^{11}+x^{10}+x^9+x^8+x^3+x=0$
	25	$y^2+y+x^{12}+x^{11}+x^{10}+x^5+x^2+x+1=0$
	31	$y^2+y+x^{11}+x^8+x^2+1=0$
	879	$y^2+(x^6+x+1)y+x^{11}+x^{10}+x^9+x^4+x^3+x+1=0$
	887	$y^2+(x^6+x+1)y+x^{12}+x^5+x^2+x=0$
	898	$y^2+(x^6+x+1)y+x^{11}+x^{10}+x^6+x^5+x^3+x^2+x=0$
	926	$y^2+(x^6+x+1)y+x^{12}+x^{11}+x^6+x^3+x^2+x+1=0$
	981	$y^2+(x^6+x+1)y+x^6+x^2=0$
	996	$y^2+(x^6+x+1)y+x^{12}+x^6+x^3+1=0$
	1000	$y^2+(x^6+x^3+1)y+x^{12}+x^{10}+x^7+x^3+1=0$
	1022	$y^2+(x^6+x^3+1)y+x^{12}+x^{11}+x^9+x^8+x^7+x^5+x^3+x^2+x=0$
	1032	$y^2+(x^6+x^3+1)y+x^{11}+x^9+x^6+x^4+x^3+x^2+x+1=0$
	1036	$y^2+(x^6+x^3+1)y+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1=0$
	1039	$y^2+(x^6+x^3+1)y+x^{10}+x^9+x^8+x^6+x^5+x=0$
	1041	$y^2+(x^6+x^3+1)y+x^{12}+x^{11}+x^10+x^5+x^2=0$
	1042	$y^2+(x^6+x^3+1)y+x^{12}+x^{10}+x^8=0$
	1058	$y^2+(x^6+x^3+1)y+x^{10}+x^8+x^7+x^6+x^5+x^4+x+1=0$

Table 3: All supersingular hyperelliptic curves of genus 5 over $\mathbb{F}_2$ (22 in total)

5.2 Trigonal curves

Recall that a singularity of a projective plane curve has delta invariant 1 if and only if it is an ordinary node or an ordinary cusp. We also saw that a curve C has a $\mathfrak{g}^1_3$ if and only if it can be represented as a plane quintic with exactly one singularity of delta invariant 1.

Any isomorphism of projective plane curves C_1, C_2 extends to an automorphism of $\mathbb{P}^2$. Therefore, in order to determine the list of all trigonal curves of genus 5 defined over $\mathbb{F}_2$, it is sufficient only to find $\mathrm{PGL}_3(\mathbb{F}_2)$-representatives among all the quintic homogeneous polynomials in X, Y, Z that define projective plane curves with delta invariant 1.

For computing all trigonal curves of genus $g = 5$ over $\mathbb{F}_2$, we have used the following idea.

- Make the list of all the monomials in X, Y, Z of degree 5 and fix the order of these, e.g. the lexicographic order $X^5 > X^4Y > X^4Z > X^3Y^2 > X^3YZ > X^3Z^2 > X^2Y^3 > X^2Y^2Z > X^2YZ^2 > X^2Z^3 > XY^4 > XY^3Z > XY^2Z^2 > XYZ^3 > XZ^4 > Y^5 > Y^4Z > Y^3Z^2 > Y^2Z^3 > YZ^4 > Z^5$. Since the previous list consists of 21 monomials, we can represent all homogeneous polynomials of degree 5 using coordinates of $\mathbb{P}^{20}(\mathbb{F}_2)$. Call the list of coordinates **quintics**. (*For example we have* $X^5 + YZ^4 \longleftrightarrow (1:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:1:0)$ *under the mentioned correspondence.*)

- From the starting list **quintics** obtain the new list **quintics_repr** consisting only of representatives under the action of $\mathrm{PGL}_3(\mathbb{F}_2)$ on X, Y, Z.

- Deduce whether a plane quintic corresponding to an element of **quintics_repr** has exactly one singularity of order 2 to reduce the previous list, and get list **good_quintics**.

- For all quintics with exactly one singularity P of order 2, represented by elements of **good_quintics**, find a $\mathrm{PGL}_3(\mathbb{F}_2)$-isomorphic quintic with a singularity at $(0:0:1)$, such that its tangent space at $(0:0:1)$ is either xy or $x^2 + xy + y^2$ (nodal case), or y^2 (potentially cuspidal case). The resulting list is **good_quintics_001**.

- For all potentially cuspidal quintics, decide whether there is a $\mathrm{PGL}_3(\mathbb{F}_2)$-isomorphic quintic with lowest terms $y^2 + x^3$, since only they are the cuspidal with delta invariant 1. Collect all such quintics, as well as the nodal quintics from **good_quintics_001** into the resulting list **trigonal_curves**.

We found 2854 trigonal curves in total that are not isomorphic (via $\mathrm{PGL}_3(\mathbb{F}_2)$-transformation), i.e. $|\mathrm{Tri}_5(\mathbb{F}_2)| = 2854$, and we computed their automorphism groups over $\mathbb{F}_2$. In particular, we have obtained that $|\mathcal{T}_5(\mathbb{F}_2)|$, the number of (non-isomorphic) smooth trigonal curves of genus 5 defined over the finite field with two elements weighted by the size of their automorphism group, precisely equals

$$|\mathcal{T}_5(\mathbb{F}_2)| = 2817 = 2^{11} + 2^{10} - 2^8 + 1.$$

This matches Wennink's results from [48], where he, using a partial sieve method for plane curves, computed these weighted numbers $|\mathcal{T}_5(\mathbb{F}_q)|$ for any finite field with q elements $\mathbb{F}_q$, namely $|\mathcal{T}_5(\mathbb{F}_q)| = q^{11} + q^{10} - q^8 + 1$.

Moreover, we computed the number of points of these curves over finite fields $\mathbb{F}_{2^i}$ for $i \in \{1, 2, 3, 4, 5\}$. Using that, we found that all the eligible Newton polygons occur for these curves, and that there are exactly 4 supersingular trigonal curves of genus 5 over $\mathbb{F}_2$ and all of them have trivial automorphism groups.

In the following table, for each eligible Newton polygon N one trigonal curve having N as its Newton polygon is presented, and its index in our list is mentioned.

Slopes of Newton polygon	Index	The affine equation of the curve
$[0,0,0,0,0,1,1,1,1,1]$	0	$x^4y + x^3y^2 + y^5 + x^4 + x^3y + x^2y^2 + x^3 + y^2 = 0$
$[0,0,0,0,\frac{1}{2},\frac{1}{2},1,1,1,1]$	4	$x^4y + x^3y^2 + xy^4 + y^5 + x^4 + x^3y + x^2y^2 + x^3 + xy = 0$
$[0,0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1,1]$	2	$x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + x^4 + x^3y + x^2y^2 + xy^3 + x^3 + y^2 = 0$
$[0,0,\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3},1,1]$	9	$x^5 + x^4y + x^3y^2 + y^5 + x^4 + x^3 + y^2 = 0$
$[0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1]$	3	$x^4y + xy^4 + x^4 + x^3y + x^2y^2 + xy^3 + y^4 + x^2y + xy^2 + xy = 0$
$[0,\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4},1]$	66	$x^5 + x^3y^2 + x^2y^3 + xy^4 + y^5 + x^4 + xy^3 + x^3 + y^2 = 0$
$[0,\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2},\frac{2}{3},\frac{2}{3},\frac{2}{3},1]$	136	$x^5 + x^4y + y^5 + x^4 + x^3y + y^4 + x^3 + xy^2 + y^3 + xy = 0$
$[0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1]$	46	$x^5 + xy^4 + y^4 + x^2y + xy^2 + y^3 + x^2 + xy + y^2 = 0$
$[\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{1}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5},\frac{4}{5}]$	32	$x^5 + x^2y^2 + xy^3 + y^4 + x^2y + xy = 0$
$[\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{2},\frac{1}{2},\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4}]$	419	$x^5 + x^3y^2 + x^2y^3 + xy^4 + y^5 + x^3y + x^2y^2 + xy^3 + x^2y + xy^2 + xy = 0$
$[\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{2}{3},\frac{2}{3},\frac{2}{3}]$	455	$x^5 + x^4y + x^3y^2 + x^2y^3 + x^4 + x^3y + y^4 + x^2y + xy^2 + xy = 0$
$[\frac{2}{5},\frac{2}{5},\frac{2}{5},\frac{2}{5},\frac{2}{5},\frac{3}{5},\frac{3}{5},\frac{3}{5},\frac{3}{5},\frac{3}{5}]$	711	$x^3y^2 + xy^4 + y^5 + x^4 + x^3y + x^2y^2 + xy^3 + x^3 + xy = 0$

Table 4: Some trigonal curves of genus 5 over $\mathbb{F}_2$ and their Newton polygons

In the following table, we collected all the supersingular trigonal curves of genus 5 defined over $\mathbb{F}_2$.

Slopes of Newton polygon	Index	The affine equation of the curve
$[\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}]$	259	$x^3y^2 + x^2y^3 + xy^4 + x^4 + x^2y^2 + xy^3 + xy^2 + y^3 + xy = 0$
	2050	$x^5 + x^4y + y^5 + x^3y + xy^3 + y^4 + xy^2 + xy = 0$
	2212	$x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5 + xy^3 + y^4 + x^2y + xy^2 + x^2 + xy + y^2 = 0$
	2803	$x^2y^3 + xy^4 + y^5 + x^4 + x^3y + xy^3 + y^4 + x^3 + x^2y + y^3 + xy = 0$

Table 5: All supersingular trigonal curves of genus 5 over $\mathbb{F}_2$ (4 in total)

5.3 Complete intersections of three quadric hypersurfaces

The remaining curves of genus 5 over $\mathbb{F}_2$ are the ones whose canonical embedding in $\mathbb{P}^4$ is a complete intersection of three quadric hypersurfaces. In other words, these curves C are of the form $C = S_P \cap S_Q \cap S_R$ with $S_P = Z(q_P), S_Q = Z(q_Q), S_R = Z(q_R)$, where q_P, q_Q and q_R are some (irreducible) homogeneous polynomials of degree 2 in X, Y, Z, T, U. We denote the set of all the non-isomorphic representatives of these curves by $\mathrm{ComInt}_5(\mathbb{F}_2)$, and such non-isomorphic classes of curves, weighted by the size of their automorphism groups, represent the points of $\mathcal{U}_5(\mathbb{F}_2)$. The idea behind computing all such curves C in $\mathrm{ComInt}_5(\mathbb{F}_2)$ is therefore to consider all possible triples (q_P, q_Q, q_R) of quadratic homogeneous polynomials and to check whether they satisfy certain conditions. Namely, to decide whether such a triple (q_P, q_Q, q_R) defines C as above, in practice, we should check whether the ideal $I = \langle q_P, q_Q, q_R \rangle$ is a radical ideal generated by exactly three elements of I, and whether C is smooth. Recall the fact we mentioned in Section 4.1, that the curves with canonical embedding into $\mathbb{P}^4$ are isomorphic if and only if their canonical models in $\mathbb{P}^4$ are isomorphic via some projective automorphism $M \in \mathrm{PGL}_5(\mathbb{F}_2)$.

The algorithm of determining the set $\mathrm{ComInt}_5(\mathbb{F}_2)$ consists of three parts we describe below: first do the Part I, then Part II and finally Part III.

Take any $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$, and a triple (q_1, q_2, q_3) of quadratic polynomials that represents curve C. We would firstly like to find a set of triples of quadratic polynomials such that for any such C, we can represent it with an element of that set, and that such a set is minimal in some sense. Precisely, we describe below how to find a set **triples_repr** of triples (q_P, q_Q, q_R) of quadratic polynomials such that *for any triple* (q_1, q_2, q_3) *that represents* $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$, *there is an element* $(q_P, q_Q, q_R) \in$ **triples_repr** *and an automorphism* $A \in \mathrm{PGL}_5(\mathbb{F}_2)$, *so that* $A : q_1 \mapsto q_P, q_2 \mapsto q_Q, q_3 \mapsto q_Q$. Moreover, we want that for any two triples (q_P, q_Q, q_R) and (q_S, q_T, q_U) in **triples_repr** there is no $A \in \mathrm{PGL}_5(\mathbb{F}_2)$ so that $A : q_P \mapsto q_S, q_Q \mapsto q_T, q_R \mapsto q_U$.

Hence, we can find some normal form of these triples, where for the first coordinate q_P we can choose only the representatives for the action of $\mathrm{PGL}_5(\mathbb{F}_2)$. Then, for fixed q_P, for the potential second coordinate we can only choose the representatives for the action of $\mathrm{Aut}(Z(q_P))$ and similarly for the third one. We describe the algorithm for determining **triples_repr** and mention some partial results.

Part I

- Make a list of all the monomials in X, Y, Z, T, U of degree 2, and put them in lexicographic order:

$$X^2 > XY > XZ > XT > XU > Y^2 > YZ > YT > YU > Z^2 > ZT > ZU > T^2 > TU > U^2.$$

  Represent homogeneous polynomials of degree 2 in X, Y, Z, T, U using the mentioned ordered monomials by elements of $\mathbb{P}^{14}(\mathbb{F}_2)$. Using all elements of $\mathrm{PGL}_5(\mathbb{F}_2)$, find the representatives for the first quadratic polynomial for $\mathrm{PGL}_5(\mathbb{F}_2)$-action on X, Y, Z, T, U. *After the filtering with* 9999360 *elements of* $\mathrm{PGL}_5(\mathbb{F}_2)$, *we ended up with a list of seven possible representatives* $P_1, \dots, P_7$, *corresponding to the list of seven possible quadratic polynomials* $q_{P_1}, \dots, q_{P_7}$. *Two of them, namely* P_2 *and* P_5, *represent the quadratic polynomials that are not irreducible, and* P_7 *always defines a singular curve, so the final list of potential first coordinates is* $[P_1, P_3, P_4, P_6]$:

$$\textbf{list\_of\_Ps} = [(1,0,1,1,0,0,1,0,0,0,1,0,0,1,0),(0,0,0,1,0,1,1,0,0,1,1,0,0,0,0),$$
$$(0,0,1,0,0,1,1,0,0,0,0,0,0,0,0),(0,1,0,0,0,1,0,1,0,1,1,0,0,0,0)]$$

- For each element P in **list_of_Ps** and the corresponding homogeneous polynomial q_P compute $\mathrm{Stab}(P) \coloneqq \mathrm{Stab}(q_P) = \mathrm{Aut}_{\mathbb{F}_2}(Z(q_P))$, that is the stabilizer of q_P under $\mathrm{PGL}_5(\mathbb{F}_2)$-action on X, Y, Z, T, U. *Since we can now assume that the first coordinate of the triple* (q_P, q_Q, q_R) *corresponds to one of only five elements of* **list_of_Ps**, *we can also put some restrictions on the second quadratic polynomials of the desired triples.* For fixed P in **list_of_Ps** compute the list **P_list_of_Qs** of the representatives for the second quadratic polynomial for the action of $\mathrm{Stab}(P)$ on X, Y, Z, T, U.

- For fixed P in **list_of_Ps** and fixed Q in P's list **P_list_of_Qs**, find the subgroup of $\mathrm{Stab}(P)$ that fixes Q, i.e., compute $G_{PQ} = \mathrm{Stab}(P) \cap \mathrm{Stab}(Q)$. Find the representatives for R, i.e., for the third coordinate q_R in triple (q_P, q_Q, q_R) when q_P, q_Q are fixed, with respect to the G_{PQ}-action. Check the desired conditions for the third quadratic polynomial of a triple, represented by $R \in \mathbb{P}^{14}(\mathbb{F}_2)$. If the conditions are satisfied put the triple (P, Q, R) in the list **triples_repr**.

The list **triples_repr** contains 22228 triples, out of which 13798 have q_{P_1} as its first coordinate, 4636 have q_{P_3} as the first coordinate, 3750 have q_{P_4} as the first coordinate, and the remaining 44 have q_{P_6} as the first coordinate.

Since a curve $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$ is defined as a zero set of the ideal generated by one of the triples we mentioned, in particular, we see the set of three quadratic polynomials determines a curve and not their order. Therefore, the second step is as follows.

Part II

- Compute the orbits of q_{P_4}, q_{P_6} and q_{P_3} under the action of $\mathrm{PGL}_5(\mathbb{F}_2)$.
- Look at the sublist L_4 of **triples_repr** of triples whose first coordinate is q_{P_4}. If the second or the third coordinate of an element from that sublist is q_{P_3}- conjugate, then only by changing the order of coordinates, and after some projective transformation, we get that such a triple is already in the sublist of **triples_repr** of triples whose first coordinate is q_{P_3}. Hence, we can remove all such triples from L_4 and still have all the representatives for curves $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$.
- Similarly, remove from the sublist L_6 of triples in **triples_repr** whose first coordinate is q_{P_6} all the triples whose second or third coordinate is either q_{P_3}- or q_{P_4}- conjugate. And finally, remove from the sublist L_1 of triples in **triples_repr** whose first coordinate is q_{P_1} all the triples whose second or third coordinate is q_{P_3}- or q_{P_4}- or q_{P_6}- conjugate.
- To further compress the data, in all the sublists of triples starting with $q_{P_1}, q_{P_3}, q_{P_4}$ and q_{P_6}, consider all the ideals defined by such triples. Remove the triples that define duplicates of ideals.

After the first three steps of this idea, we ended up with 9489 triples of quadratic polynomials defining curves $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$, and after the additional fourth step, we ended up with 7118 such triples.

Lastly, out of the previously obtained shortened list of triples which represent all the curves in $\mathrm{ComInt}_5(\mathbb{F}_2)$, we need to extract only the triples that define non-isomorphic curves. We do that using the following idea which will be explained and confirmed in Theorem 5.9.

Part III

- We separate the cases when all three quadratic polynomials of a triple are in the same orbit (*Case 1*) and the cases when there is precisely one quadratic polynomial (call it *special*) in some orbit while the other two are not in that orbit (*Case 2*).
  - In Case 2, we divide them into distinct lists using some order - firstly the ones when the special quadratic polynomial can be chosen to be in the orbit of q_{P_3}, then when there are no special quadratic polynomials in the orbit of q_{P_3} and the special polynomial can be in orbit of q_{P_4}. Call these lists **list_3**, **list_4**. Similarly, the list **list_6** consists of

triples that are not in the previous lists and the special quadratic polynomial can be chosen to be in the orbit of q_{P_6}, and **list_1** when the special one is in the orbit of q_{P_1} and not in the orbits of q_{P_4}, q_{P_3} and q_{P_6}. We call the number $i \in \{1,3,4,6\}$ chosen by this criterion *specially chosen i*.

- In case when a triple consists of polynomials that are all in the same orbit $\mathrm{Orbit}(q_{P_i})$, we make three copies of that list, and use some $\mathrm{PGL}_5(\mathbb{F}_2)$-transformation that maps the first coordinate to q_{P_i} to transform all the elements from the first list, then doing the same for the second list using a $\mathrm{PGL}_5(\mathbb{F}_2)$-transformation that maps the second coordinate to q_{P_i}, and analogously for the third list. Call these **three_in_P_i_list_j** for $i \in \{1,3,4,6\}$ and $j \in \{1,2,3\}$.
- For (f_1, f_2, f_3) in **list_i** and without loss of generality $f_1 \in \mathrm{Orbit}(\mathrm{q_{P_i}})$, find a $\mathrm{PGL}_5(\mathbb{F}_2)$ transformation sending f_1 to q_{P_i} and map all f_1, f_2, f_3 using that map to get the new image of the triple (defining the isomorphic curve).
- Reduce each list **list_i** so that no two of its elements give the same ideal. Similarly with **three_in_P_i_list_j**. *After this step, we ended up with* 6305 *triples.*
- For any $P_i, i \in \{1,3,4,6\}$ collect all **three_in_P_i_list_1** and all **list_i** into a list **all**.
- For any triple in **all**, firstly remove it from that list and append to **final_list**, do all possible $\mathbb{F}_2$-basis transformations and check whether they are in (*cases 1*) or (*cases 2*). For any of these triples obtained using the base change:
  - If it is in Case 1, find specially chosen i, find a $\mathrm{PGL}_5(\mathbb{F}_2)$-transformation that maps the first coordinate to q_{P_i} and map the triple by that transformation to get (g_1, g_2, g_3). Act by all transformations from $\mathrm{Stab}(P_i)$ on (g_1, g_2, g_3), and if some image is in **three_in_P_i_list_1**, remove it from that list, as well as the elements from the lists **three_in_P_i_list_2** and **three_in_P_i_list_3** that originated from the same triple. Similarly for the second and the third coordinate.
  - If it is in Case 2, find the specially chosen i, map the triple by some $\mathrm{PGL}_5(\mathbb{F}_2)$-transformation so that the special polynomial maps to q_{P_i}. Then using $\mathrm{Stab}(P_i)$ transformations remove all the triples from **list_i** that give the same ideal as that triple.

Theorem 5.9. *Algorithm for determining* $\mathrm{ComInt}_5(\mathbb{F}_2)$ *is correct.*

Proof. Recall that Part I gave us the set **triples_repr** of triples (q_P, q_Q, q_R) of quadratic polynomials such that for any triple (q_1, q_2, q_3) that represents $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$, there is an element $(q_P, q_Q, q_R) \in$ **triples_repr** and an automorphism $A \in \mathrm{PGL}_5(\mathbb{F}_2)$, so that $A : q_1 \mapsto q_P, q_2 \mapsto q_Q, q_3 \mapsto q_Q$. Therefore, for any curve $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$ there is at least one triple (q_P, q_Q, q_R) of quadratic polynomials in **triples_repr** such that C is isomorphic to a curve $Z(q_P, q_Q, q_R)$.

Part II only reduces the set **triples_repr**, and therefore exists only for quicker computations. To see that we have not lost any $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$ we note that the order of polynomials in the triple, or more generally the set of generators of the ideals are not important for giving the set $Z(q_P, q_Q, q_R)$ as long as they generate the same ideal.

In order to filter all triples in **triples_repr** so that we get the list only consisting of the triples that produce non-isomorphic curves, we use Part III. Using Part III is valid because of the following.

Let $I = \langle f_1, f_2, f_3 \rangle$ and $J = \langle g_1, g_2, g_3 \rangle$ be two ideals of $\mathbb{F}_2[X,Y,Z,T,U]$ with f_1, f_2, f_3, g_1, g_2 and g_3 quadratic polynomials that define isomorphic over $\mathbb{F}_2$ curves $C_I \in \mathrm{ComInt}_5(\mathbb{F}_2)$ and $C_J \in \mathrm{ComInt}_5(\mathbb{F}_2)$ respectively. $C_I \cong C_J$ implies that there are $A, B \in \mathrm{PGL}_5(\mathbb{F}_2)$ such that

$$A.I = \langle A.f_1, A.f_2, A.f_3 \rangle = \langle B.g_1, B.g_2, B.g_3 \rangle = B.J,$$

where the action of $\mathrm{PGL}_5(\mathbb{F}_2)$ on $\mathbb{F}_2[X,Y,Z,T,U]$ is defined as before, for $f = f(X,Y,Z,T,U)$ and $M \in \mathrm{PGL}_5(\mathbb{F}_2)$,

$$M.f = f\left(\left(M \cdot (X,Y,Z,T,U)^t\right)^t\right).$$

Acting by B^{-1} on both sides of $A.I = B.J$ we get that there is $C \in PGL_5(\mathbb{F}_2)$ such that $C.I = J$. Since $C.I = \langle C.f_1, C.f_2, C.f_3 \rangle = J$ we get that there is some $(\alpha_{i,j})_{1 \le i,j \le 3} \in \mathrm{PGL}_3(\mathbb{F}_2)$ such that

$$C.f_j = \sum_{i=1}^{3} \alpha_{i,j} g_i, \quad j = 1,2,3$$

so equivalently, there is $(\lambda_{i,j})_{1 \le i,j \le 3} \in \mathrm{PGL}_3(\mathbb{F}_2)$ such that

$$C.\left(\sum_{i=1}^{3} \lambda_{i,j} f_i\right) = g_j, \quad j = 1,2,3.$$

Denote $h_j = \sum_{i=1}^{3} \lambda_{i,j} f_i$ and note that we have that h_j and g_j are in the same $\mathrm{PGL}_5(\mathbb{F}_2)$-orbit for $j = 1,2,3$. If, without loss of generality, h_1 and g_1 are in the orbit of q_{P_4}, then, there are $D, E \in PGL_5(\mathbb{F}_2)$ such that $D.h_1 = q_{P_4} = E.g_1$. In particular, that leads to the equality

$$ECD^{-1}\langle D.h_1, D.h_2, D.h_3 \rangle = \langle E.g_1, E.g_2, E.g_3 \rangle,$$

where in addition $q_{P_4} = D.h_1 \mapsto E.g_1 = q_{P_4}$ gives us that $ECD^{-1} \in \mathrm{Stab}(P_4)$. □

We implemented in SageMath the algorithms for the first two parts of the algorithm for computing the representatives of all non-isomorphic curves of genus five over a field with two elements, and we already mentioned some of the obtained results. One can find these implementations as well as the obtained results on `https://github.com/DusanDragutinovic/MT_Curves`. For the third part, we have an implementation that can be found on the same link. However, by the time of submitting the thesis, we still do not have the complete results.

It should also be mentioned that a similar problem was discussed by Kudo and Harashita in [24]. There, they showed that any non-hyperelliptic and non-trigonal curve of genus five over a finite field can be represented as a normalization of a sextic in $\mathbb{P}^2$. For some of the possible cases, that they called *generic*, they gave an algorithm and an implementation in Magma for computing them.

Once we obtain the final results and thus get the set $\mathrm{ComInt}_5(\mathbb{F}_2)$, we can also try to compute the automorphism groups of curves $C \in \mathrm{ComInt}_5(\mathbb{F}_2)$. That could be used for computing $|\mathcal{U}_5(\mathbb{F}_2)|$. Perhaps some of the ideas from Part III of our algorithm for computing the complete intersections of three quadratic hypersurfaces in $\mathbb{P}^4$ over $\mathbb{F}_2$ can be used for that purpose, but currently, we do not have an algorithm for computing the mentioned automorphism groups.

References

[1] J. D. Achter and R. Pries. Monodromy of the p-rank strata of the moduli space of curves. *Int. Math. Res. Not. IMRN*, 15, 2008.

[2] T.E.V. Balaji. *An Introduction to Families, Deformations and Moduli.* Universitätsdrucke Göttingen, 2010.

[3] C. Chai and F. Oort. Moduli of abelian varieties and p-divisible groups. *Arithmetic geometry, Clay Mathematics Institute Summer School 2006, AMS Clay Math. Inst.*, 8:441–536, 2009.

[4] C. Chai and F. Oort. Monodromy and irreducibility of leaves. *Ann. of Math.*, 175:1359–1396, 2011.

[5] A. J. de Jong and F. Oort. Purity of the stratification by Newton polygons. *J. Amer. Math. Soc.*, 13, no. 1:209–241, 2000.

[6] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Publications Mathématiques de l'Institut des Hautes Scientifiques*, 36:75 – 109, 1969.

[7] D. Djounvouna. The construction of moduli spaces and geometric invariant theory. *ALGANT Masters Thesis*, 2017.

[8] T. Dupuy, K. Kedlaya, D. Roe, and C. Vincent. Isogeny Classes of Abelian Varieties over Finite Fields in the LMFDB, 2020. arXiv:2003.05380.

[9] A. Elkin and R. Pries. Ekedahl-Oort strata of hyperelliptic curves in characteristic 2. *Algebra Number Theory*, 7(3):507–532, 2013.

[10] C. Faber and G. van der Geer. Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.*, 573:117–137, 2004.

[11] J. Fogarty, D. Mumford, and F. Kirwan. *Geometric Invariant Theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge. Springer-Verlag Berlin Heidelberg, 1994.

[12] C. K. Fok. Example of genus 5 curves. 2015. `http://pi.math.cornell.edu/~ckfok/Examples\%20of\%20genus\%205\%20curves.pdf, (Accessed on 28.6.2021.)`.

[13] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition, 2017.

[14] S. Harashita. Ekedahl-Oort strata contained in the supersingular locus and Deligne-Lusztig varieties. *J. Algebraic Geom.*, 19:419–438, 2010.

[15] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, Berlin, New York, 1977.

[16] K. Hashimoto. On Brandt matrices associated with the positive definite quaternion hermitian forms. *I. J. Fac. Sci. Univ. Tokyo*, IA:227–245, 1980.

[17] K. Hashimoto and T. Ibukiyama. On the class numbers of positive definite binary quaternion hermitian forms. *I. J. Fac. Sci. Univ. Tokyo*, 27, 1980. Part II, *ibid.* 28, 1981. Part III, *ibid.* 30, 1983.

[18] T. Ibukiyama. On symplectic Euler factors of genus two. *J. Fac. Sci. Univ. Tokyo Sect.*, IA30:587–614, 1984.

[19] T. Ibukiyama, T. Katsura, and F. Oort. Supersingular curves of genus two and class numbers. *Compositio Mathematica*, Tome 57, no. 2:127 – 152, 1986.

[20] V. Karemaker, F. Yobuko, and C.-F. Yu. Mass formula and Oort's conjecture for supersingular abelian threefolds. *Advances in Mathematics*, 386, 2021.

[21] T. Katsura and F. Oort. Supersingular abelian varieties of dimension two or three and class numbers. *Adv. St. Pure Math*, 10:253–281, 1987.

[22] N. Katz. Slope filtration of f-crystals. In *Journées de Géométrie Algébrique de Rennes - (Juillet 1978) (I) : Groupe formels, représentations galoisiennes et cohomologie des variétés de caractéristique positive*, number 63 in Astérisque. Société mathématique de France, 1979.

[23] B. Köck and J. Tait. On the de-Rham cohomology of hyperelliptic curves. *Res. Number Theory*, 4, 2018.

[24] M. Kudo and S. Harashita. Parametrizing generic curves of genus five and its application to finding curves with many rational points. 2021. arXiv: 2102.07270.

[25] M. Kudo, S. Harashita, and H. Senda. The existence of supersingular curves of genus 4 in arbitrary characteristic. *Res. number theory*, 6(44), 2020.

[26] A. Landesman. Notes for Math 282: The geometry of algebraic curves, taught by Joseph Harris. *Harvard University*, 2015. `https://web.stanford.edu/~aaronlan/assets/math-282-harvard-algebraic-curves-notes.pdf`, `(Accessed on 28.6.2021.)`.

[27] K. Z. Li and F. Oort. *Moduli of Supersingular Abelian Varieties.* Springer-Verlag Berlin Heidelberg, 1998.

[28] W. Li, E. Mantovan, R. Pries, and Y. Tang. Newton polygons of cyclic covers of the projective line branched at three points. In *Research Directions in Number Theory*, pages 115–132, Cham, 2019. Springer International Publishing.

[29] J. S. Milne and W. C. Waterhouse. Abelian varieties over finite fields. *Proc. Sympos. pure math., Number Theory Institute (Stony Brook), AMS*, XX:53–64, 1969.

[30] J.S. Milne. *Abelian Varieties. In: Cornell G., Silverman J.H. (eds) Arithmetic Geometry.* Springer, New York, NY., 1986.

[31] B. Moonen. Special subvarieties arising from families of cyclic covers of the projective line. *Doc. Math.*, 15:793–819, 2010.

[32] B. Moonen and F. Oort. The Torelli locus and special subvarieties. *Handbook of moduli, Adv. Lect. Math*, II:549–594, 2013.

[33] D. Mumford. *Abelian Varieties.* Oxford University Press, 1970.

[34] P. Norman and F. Oort. Moduli of abelian varieties. *Ann. of Math.*, (2) 112, no. 3:413–439, 1980.

[35] F. Oort. Which abelian surfaces are products of elliptic curves? *Math. Ann.*, (214):35–47, 1975.

[36] F. Oort. Hyperelliptic supersingular curves. *Arithmetic algebraic geometry (Texel, 1989), Progr. Math., 89, Birkhäuser Boston, Boston, MA*, page 247–284, 1991.

[37] F. Oort. A stratification of a moduli space of polarized abelian varieties in positive characteristic. *Moduli of Curves and Abelian Varieties: The Dutch Intercity Seminar on Moduli, Vieweg+Teubner Verlag, Wiesbaden*, pages 47–64, 1999.

[38] F. Oort. Abelian varieties isogenous to a Jacobian; in problems from the Workshop on automorphisms of curves. *Rend. Sem. Mat. Univ. Padova*, 113:129–177, 2005.

[39] H. Popp. The singularities of the moduli schemes of curves. *Journal of number theory*, 1:90–107, 1969.

[40] R. Pries. The p-torsion of curves with large p-rank. *International Journal of Number Theory*, 05:1103–1116, 2009.

[41] R. Pries. Current results on Newton polygons of curves. *Open Problems in Arithmetic Algebraic Geometry, editor Oort, Advanced Lectures in Mathematics*, 46, chapter 6:179 – 208, 2019.

[42] R. Re. The rank of the Cartier operator and linear systems on curves. *Journal of Algebra*, 236:80 – 92, 2001.

[43] J. Scholten and H. J. Zhu. Hyperelliptic curves in characteristic 2. *International Mathematics Research Notices*, 2002:905–917, 2002.

[44] Joseph H Silverman. *The Arithmetic of Elliptic Curves.* Graduate texts in mathematics. Springer, Dordrecht, 2009.

[45] K.-O. Stöhr and J.F. Voloch. A formula for the Cartier operator on plane algebraic curves. *J. reine angew. Math.*, 377:49 – 64, 1987.

[46] G. van der Geer, B. Edixhoven, and B. Moonen. Abelian varieties. *(draft).* `https://www.math.ru.nl/~bmoonen/research.html#bookabvar`, (Accessed on 29.6.2021.).

[47] G. van der Geer and M. van der Vlugt. On the existence of supersingular curves of given genus. *J. Reine Angew. Math.*, 458:53 – 61, 1995.

[48] T. Wennink. Counting the number of trigonal curves of genus 5 over finite fields. *Geometriae Dedicata*, 208:31 – 48, 2020.

[49] X. Xarles. A census of all genus 4 curves over the field with 2 elements, 2020. arXiv:2007.07822.

[50] Z. Zhou. Ekedahl-Oort strata on the moduli space of curves of genus four. *Rocky Mountain J. Math.*, 2(50):747 – 761, 2018.

[51] Z. Zhou. The a-number and the Ekedahl-Oort types of Jacobians of curves. *Ph. D. Thesis at the University of Amsterdam*, 2019.

A Codes

Supporting code for Theorem 3.5

```
#Declaring the possible 16-tuples of norms
#Let Mat be the list of all possible matrices with entries 0, 1/2, 1

first_list = []
for M in Mat:
    if M[0, 0] + M[0, 1] + M[0, 2] + M[0, 3] == 1 and\
        M[1, 0] + M[1, 1] + M[1, 2] + M[1, 3] == 1 and\
            M[2, 0] + M[2, 1] + M[2, 2] + M[2, 3] == 1 and\
                M[3, 0] + M[3, 1] + M[3, 2] + M[3, 3] == 1:
        first_list.append(M)
newl = first_list.copy()
teml = []
for M in newl:
    if M[0, 0]==0 and M[0, 1] == 0 and M[1, 0]==0 and M[1, 1] == 0 and\
        M[2, 2]==0 and M[2, 3] == 0 and M[3, 2]==0 and M[3, 3] == 0:
        teml.append(M)
    if M[0, 2]==0 and M[0, 3] == 0 and M[1, 2]==0 and M[1, 3] == 0 and\
        M[2, 0]==0 and M[2, 1] == 0 and M[3, 0]==0 and M[3, 1] == 0:
        teml.append(M)
    if [M[0, 0], M[0, 1], M[0, 2], M[0, 3]] == [0, 0, 0, 0] or\
        [M[1, 0], M[1, 1], M[1, 2], M[1, 3]] == [0, 0, 0, 0] or\
            [M[2, 0], M[2, 1], M[2, 2], M[2, 3]] == [0, 0, 0, 0] or\
                [M[3, 0], M[3, 1], M[3, 2], M[3, 3]] == [0, 0, 0, 0]:
        teml.append(M)
    if [M[0, 0], M[1, 0], M[2, 0], M[3, 0]] == [0, 0, 0, 0] or\
        [M[0, 1], M[1, 1], M[2, 1], M[3, 1]] == [0, 0, 0, 0] or\
            [M[0, 2], M[1, 2], M[2, 2], M[3, 2]] == [0, 0, 0, 0] or\
                [M[0, 3], M[1, 3], M[2, 3], M[3, 3]] == [0, 0, 0, 0]:
        teml.append(M)
for M in teml:
    while M in newl:
        newl.remove(M)
final_list = []
for M in newl:
    if M[0,0]*M[1,0] + M[0,1]*M[1,1] + M[0,2]*M[1,2] + M[0,3]*M[1,3] == 0 or\
        M[0,0]*M[1,0] + M[0,1]*M[1,1] + M[0,2]*M[1,2] == M[0,3]*M[1,3] or\
            M[0,0]*M[1,0] + M[0,1]*M[1,1] == M[0,2]*M[1,2] + M[0,3]*M[1,3] or\
                M[0,0]*M[1,0] == M[0,1]*M[1,1] + M[0,2]*M[1,2] + M[0,3]*M[1,3]:
        if M[0,0]*M[2,0] + M[0,1]*M[2,1] + M[0,2]*M[2,2] + M[0,3]*M[2,3] == 0 or\
            M[0,0]*M[2,0] + M[0,1]*M[2,1] + M[0,2]*M[2,2] == M[0,3]*M[2,3] or\
                M[0,0]*M[2,0] + M[0,1]*M[2,1] == M[0,2]*M[2,2] + M[0,3]*M[2,3] or\
                    M[0,0]*M[2,0] == M[0,1]*M[2,1] + M[0,2]*M[2,2] + M[0,3]*M[2,3]:
            if M[0,0]*M[3,0] + M[0,1]*M[3,1] + M[0,2]*M[3,2] + M[0,3]*M[3,3] == 0 or\
                M[0,0]*M[3,0] + M[0,1]*M[3,1] + M[0,2]*M[3,2] == M[0,3]*M[3,3] or\
                    M[0,0]*M[3,0] + M[0,1]*M[3,1] == M[0,2]*M[3,2] + M[0,3]*M[3,3] or\
                        M[0,0]*M[3,0] == M[0,1]*M[3,1] + M[0,2]*M[3,2] + M[0,3]*M[3,3]:
                if M[1,0]*M[2,0] + M[1,1]*M[2,1] + M[1,2]*M[2,2] + M[1,3]*M[2,3] == 0 or\
                    M[1,0]*M[2,0] + M[1,1]*M[2,1] + M[1,2]*M[2,2] == M[1,3]*M[2,3] or\
                        M[1,0]*M[2,0] + M[1,1]*M[2,1] == M[1,2]*M[2,2] + M[1,3]*M[2,3] or\
                            M[1,0]*M[2,0] == M[1,1]*M[2,1] + M[1,2]*M[2,2] + M[1,3]*M[2,3]:
                    if M[1,0]*M[3,0] + M[1,1]*M[3,1] + M[1,2]*M[3,2] + M[1,3]*M[3,3] == 0 or\
                        M[1,0]*M[3,0] + M[1,1]*M[3,1] + M[1,2]*M[3,2] == M[1,3]*M[3,3] or\
                            M[1,0]*M[3,0] + M[1,1]*M[3,1] == M[1,2]*M[3,2] + M[1,3]*M[3,3] or\
                                M[1,0]*M[3,0] == M[1,1]*M[3,1] + M[1,2]*M[3,2] + M[1,3]*M[3,3]:
                        if M[2,0]*M[3,0] + M[2,1]*M[3,1] + M[2,2]*M[3,2] + M[2,3]*M[3,3] == 0 or\
                            M[2,0]*M[3,0] + M[2,1]*M[3,1] + M[2,2]*M[3,2] == M[2,3]*M[3,3] or\
                                M[2,0]*M[3,0] + M[2,1]*M[3,1] == M[2,2]*M[3,2] + M[2,3]*M[3,3] or\
                                    M[2,0]*M[3,0] == M[2,1]*M[3,1] + M[2,2]*M[3,2] + M[2,3]*M[3,3]:
                            final_list.append(M)
bad = [matrix([[0, 0], [0, 1]]), matrix([[0, 0], [1, 0]]), matrix([[0, 1], [0, 0]]),\
    matrix([[1, 0], [0, 0]]), matrix([[0, 0], [0, 1/2]]), matrix([[0, 0], [1/2, 0]]),\
        matrix([[0, 1/2], [0, 0]]), matrix([[1/2, 0], [0, 0]]), matrix([[0, 0], [1/2, 1/2]]),\
            matrix([[1/2, 1/2], [0, 0]]), matrix([[1/2, 0], [1/2, 0]]), matrix([[0, 1/2], [0, 1/2]]),\
                matrix([[0, 1/2], [1/2, 0]]), matrix([[1/2, 0], [0, 1/2]])]
while final_list!= [] and ind != 0:
    M = final_list[0]
    num1 = len(final_list)
    A = matrix([[M[0, 0], M[0, 1]], [M[1, 0], M[1, 1]]])
    B = matrix([[M[0, 2], M[0, 3]], [M[1, 2], M[1, 3]]])
    C = matrix([[M[2, 0], M[2, 1]], [M[3, 0], M[3, 1]]])
    D = matrix([[M[2, 2], M[2, 3]], [M[3, 2], M[3, 3]]])
    if A in bad or B in bad or C in bad or D in bad:
        while M in final_list:
            final_list.remove(M)
    num2 = len(final_list)
    ind = num1 - num2
print(len(final_list))
#result is 0
```

An example of a code for computing hyperelliptic curves

```
var('x, t')
#initializing the fixed polynomial q(x)
def q1(x):
    return x^3
rin.<X> = GF(2)[]
#initializing the set of invertible matrices
PGL = []
for a in GF(2):
    for b in GF(2):
        for c in GF(2):
            for d in GF(2):
                A = Matrix([[a,b],[c,d]])
                if A.det() != 0:
                    PGL.append(A)
#computing the stabilizer of q(x)
Gq1 = []
for A in PGL:
    f = (A[1, 0]*X + A[1, 1])^6*q1((A[0, 0]*X + A[0, 1])/(A[1, 0]*X + A[1, 1]))
    if f == q1(X):
        Gq1.append(A)
#initializing the set of polynomials p(x)
D12 = []
for a0 in range(0, 2):
    for a1 in range(0, 2):
        for a2 in range(0, 2):
            for a3 in range(0, 2):
                for a4 in range(0, 2):
                    for a5 in range(0, 2):
                        for a6 in range(0, 2):
                            for a7 in range(0, 2):
                                for a8 in range(0, 2):
                                    for a9 in range(0, 2):
                                        for a10 in range(0, 2):
                                            for a11 in range(0, 2):
                                                P = (a0, a1, a2, a3, a4, a5, a6, a7, a8, a9, a10, a11, 1)
                                                D12.append(P)
for a0 in range(0, 2):
    for a1 in range(0, 2):
        for a2 in range(0, 2):
            for a3 in range(0, 2):
                for a4 in range(0, 2):
                    for a5 in range(0, 2):
                        for a6 in range(0, 2):
                            for a7 in range(0, 2):
                                for a8 in range(0, 2):
                                    for a9 in range(0, 2):
                                        for a10 in range(0, 2):
                                            P = (a0, a1, a2, a3, a4, a5, a6, a7, a8, a9, a10, 1, 0)
                                            D12.append(P)
#initializing the set of polynomials r(x)
D6  = []
for a0 in range(0, 2):
    for a1 in range(0, 2):
        for a2 in range(0, 2):
            for a3 in range(0, 2):
                for a4 in range(0, 2):
                    for a5 in range(0, 2):
                        for a6 in range(0, 2):
                            P = (a0, a1, a2, a3, a4, a5, a6)
                            D6.append(P)
Qlist = []
q = q1(t) + 0*t
#finding all p(x) that satisfy the smoothness condition
for P in D12:
    def p1(t):
        return P[0] + P[1]*t + P[2]*t^2 + P[3]*t^3 + P[4]*t^4 + P[5]*t^5 + P[6]*t^6 +\
                      P[7]*t^7 + P[8]*t^8 + P[9]*t^9 + P[10]*t^10 + P[11]*t^11 + P[12]*t^12
    ri.<X> = GF(2)[]
    riq = ri(q1(X))
    p = (p1(t)).expand()
    rip = ri(p1(X))
    cond1 = gcd(riq, rip.derivative()^2 + riq.derivative()^2*rip) == 1
    cond2 = q.degree(t) == 6
    cond3 = (mod(p.coefficient(t^11), 2))^2 !=\
            (mod(p.coefficient(t^12), 2))*(mod(q.coefficient(t^5), 2))^2
    if cond1 and (cond2 or cond3):
        Qlist.append(P)
#reducing the list of potential p(x) by taking the representatives for the Gq1-action
q_list_of_ps = []
while Qlist != []:
    P = Qlist[0]
    Vqlist.append(P)
    temp = []
    temp.append(P)
    for R in D6:
        def f(t):
            return (P[0] + P[1]*t + P[2]*t^2 + P[3]*t^3 + P[4]*t^4 + P[5]*t^5 + P[6]*t^6 +\
                    P[7]*t^7 + P[8]*t^8 + P[9]*t^9 + P[10]*t^10 + P[11]*t^11 + P[12]*t^12) +\
                    q1(t)*(R[0] + R[1]*t + R[2]*t^2 + R[3]*t^3 + R[4]*t^4 + R[5]*t^5 + R[6]*t^6) +\
                    (R[0] + R[1]*t + R[2]*t^2 + R[3]*t^3 + R[4]*t^4 + R[5]*t^5 + R[6]*t^6)^2
        for A in Gq1:
            var('x')
            def ge(x):
                return (ZZ(A[1, 0])*x + ZZ(A[1, 1]))^12\
                        *f((ZZ(A[0, 0])*x + ZZ(A[0, 1]))/(ZZ(A[1, 0])*x + ZZ(A[1, 1])))
            ri.<X> = ZZ[]
            g = ri(ge(X))
            Q = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
            li = g.list()
            for i in range(0, len(li)):
                Q[i] = mod(li[i], 2)
            S = tuple(Q)
            temp.append(S)
    A = set(Qlist)
    B = set(temp)
    C = A - B
    Qlist = list(C)
HElist = []
q = q1(t) + 0*t
for P in q_list_of_ps:
    p = P[0] + P[1]*t + P[2]*t^2 + P[3]*t^3 + P[4]*t^4 + P[5]*t^5 + P[6]*t^6 +\
        P[7]*t^7 + P[8]*t^8 + P[9]*t^9 + P[10]*t^10 + P[11]*t^11 + P[12]*t^12
    HElist.append([q, p])
```

Finding trigonal curves from the list of a priori non-isomorphic quintics

```
#function that gives whether the quintic f has only one singularity that is either a cusp or a node
def only_one_node_or_cusp_check(f):
    ind = 0
    Polr.<x0,x1,x2> = PolynomialRing(GF(2), 3, order='lex')
    g = f(x0, x1, x2)
    gdx = g.derivative(x0)
    gdy = g.derivative(x1)
    gdz = g.derivative(x2)
    Id = Ideal(g, gdx, gdy, gdz)
    if Id.dimension()==1:
        F = GF(2).algebraic_closure()
        Pr3 = ProjectiveSpace(2)/F
        X = Pr3.subscheme(Id)
        rp = X.rational_points()
        if len(rp)==1:
            Polr.<x0,x1,x2> = PolynomialRing(F, 3, order='lex')
            g = f(x0, x1, x2)
            P = rp[0]
            if P[0]!=0:
                    h = g.reduce(Ideal(x0-1))
                    M = Ideal(x1 - P[1]/P[0], x2 - P[2]/P[0])
                    h1 = h.reduce(M^2)
                    h2 = h.reduce(M^3)
                    if (h1==0) and (h2!= 0):
                        return True
            elif P[1]!=0:
                    h = g.reduce(Ideal(x1-1))
                    M = Ideal(x0 - P[0]/P[1], x2 - P[2]/P[1])
                    h1 = h.reduce(M^2)
                    h2 = h.reduce(M^3)
                    if (h1==0) and (h2!= 0):
                        return True
            else:
                    h = g.reduce(Ideal(x2-1))
                    M = Ideal(x0 - P[0]/P[2], x1 - P[1]/P[2])
                    h1 = h.reduce(M^2)
                    h2 = h.reduce(M^3)
                    if (h1==0) and (h2!= 0):
                        return True
    return False
```