Radboud Universiteit

Master thesis

Space filling curves in their Jacobian

Autor
Thijs Limbeek

Supervisors
Prof. Dr. Ben Moonen
Dr. Arne Smeets

November 24, 2020

Preface

We want to study curves that are space filling in their Jacobian. If X/k is a curve with a rational point P, then the Jacobian J is the unique abelian variety such that for every field extension $k \subset K$, we have $J(K) = \mathrm{Pic}^0(X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(K))$. Moreover if the genus of X is bigger than 0, then we have a closed embedding of X in the Jacobian J, which is given on points by $Q \mapsto [\mathcal{O}_X(Q-P)]$. For an elliptic curve E, this closed embedding is an isomorphism. This is not really a surprise since we already know that we have an isomorphism of groups $E(k) \to \mathrm{Pic}^0(E)$ by the map $P \mapsto [\mathcal{O}_X(P-O)]$. Let X be a curve of genus $g \geq 2$ over a finite field k with a k-rational point. Then X is called space filling in its Jacobian J or simply space filling if $|X(k)| = |J(k)|$. Since we have a closed embedding of the curve in its Jacobian, we see that $|X(k)| \leq |J(k)|$. We will also look at the almost space filling curves in their Jacobian. A curve X is called almost space filling in its Jacobian or simply almost space filling if $|J(k)| = |X(k)| + 1$.

We want to know under which conditions the curve is (almost) space filling. If the genus of the curve X is g, then its Jacobian is an abelian variety of dimension g. Our intuition says that it is not very likely that a curve is space filling or almost space filling, because in general a higher dimensional space has a lot more rational points, than a lower dimensional space. But we have to show that this is also really the case. Note that the number of k-rational points of J is equal to the class number of X. By giving lower bounds on the class number, we can reduce the problem, when curves are (almost) space filling to the case of low genus. To give these lower bounds, we will study the zeta function of curve. These zeta function give us a relation between the number of effective divisors and the class number. By giving a lower bound in terms of the rational points of X, we can show that X can be only (almost) space filling in specific cases.

We know have reduced that a curve can only be space filling by low genus. Our goal is to find all these (almost) space filling curves. Here comes the use in of computer algebra. We will see that every (almost) space filling curves has genus 2 or 3. The method to find all (almost) space filling curves, is to enumerate over all curves of genus 2 and 3 and check if they are space filling. We therefore need to give a description of all curves of genus 2 and 3. In general, it is not possible to give a description of all curves of a given genus g. However in the case of genus 2 and 3, we can give an easy description of all curves.

We want to make an algorithms that gives us all the (almost) space filling curves up to isomorphism. Since all (almost) space filling curves are defined over $\mathbb{F}_2$ and $\mathbb{F}_3$, there aren't that many curves that of genus 2 or 3. So we can find every (almost) space filling curve by checking for every curve if it is (almost) space filling or not. Then the last step is to find all (almost) space filling curves up to isomorphism. We therefore check for all space filling curves, when they are isomorphic to each other.

Contents

1 Jacobian Varieties **4**
- 1.1 Picard scheme . . . 4
- 1.2 Embedding Curve in its Jacobian . . . 6
- 1.3 Albenese embedding . . . 6

2 The zeta function of a curve over a finite field **9**
- 2.1 The zeta function of a curve . . . 9
- 2.2 The relation between the class number and the number of effective divisors . 12
- 2.3 A brief introduction to l-adic cohomology . . . 17
- 2.4 The zeta function and Frobenius . . . 20

3 Space filling curves in their Jacobian **24**
- 3.1 Space filling curves . . . 24
- 3.2 Almost space filling curves . . . 29

4 Computations on space filling curves **32**
- 4.1 Description of curves . . . 32
- 4.2 Algorithm for space filling curves . . . 38
  - 4.2.1 Check step . . . 38
  - 4.2.2 Result step . . . 39
- 4.3 The enumeration step . . . 39
- 4.4 Results . . . 41

A Implementations in magma **42**
- A.1 L-Polynomial function . . . 42
- A.2 Check step and Result step . . . 43
- A.3 Enumeration Step . . . 44
  - A.3.1 Hyperelliptic curves . . . 44
  - A.3.2 Non-Hyperelliptic curve . . . 45

Notation and Conventions

Notation 0.0.1. Let X be a scheme over S and let T be scheme. Then $X(T)$ denotes the set of T-rational points of X and we will write X_T for $X \times_S T$. If X is k-scheme. Then $X(k)$ is the set of k-rational points.

Convention 0.0.2. A variety over a field k is a separated k-scheme, which is of finite type over k and is geometrically integral.

Convention 0.0.3. A curve over a field k is a variety of dimension 1. We will moreover assume that every curve is smooth and projective.

Chapter 1

Jacobian Varieties

In this chapter, we will introduce the Jacobian of a curve X and show that the Jacobian is an abelian variety. Later we will show that we have an embedding of a curve in his Jacobian if the curve has a rational point. In the last section, we show that every map from a curve to an abelian variety factors through this embedding. The proofs and the details can be read in Chapter 6 and 14 of [EGM12].

1.1 Picard scheme

In this section, we define the Jacobian in terms of the Picard scheme and show that it is an abelian variety. We will first define some Picard functors and give a relation between them.

Definition 1.1.1. Let S be a Noetherian scheme and let $X \in \mathrm{Sch}/S$. Then the contravariant functor $P_X : (\mathrm{Sch}/S)^0 \to \mathrm{Ab}$ with $\mathrm{Pic}_X(T) = \mathrm{Pic}(X_T)$ is the absolute Picard functor.

The problem with this functor is that it is almost never representable. Therefore we define the relative Picard functor.

Definition 1.1.2. Let $\mathrm{Pic}_{X/S} : (\mathrm{Sch}/S)^0 \to \mathrm{Ab}$ be the fppf sheaf associated to the presheaf P_X. We call this functor the relative Picard functor.

The following functor, we are going to define is an alternative Picard functor. The benefit of this Picard functor is that it is easy to compute. Later we will see that the alternative Picard functor is the same as the relative Picard functor under certain conditions.

Definition 1.1.3. Let

$$P_{X/S} : (Sch/S)^0 \to Ab$$

be the contravariant functor with

$$P_{X/S}(T) = \mathrm{Pic}(X_T)/p^*\mathrm{Pic}(T),$$

where $p : X_T \to T$ is the second projection map.

The following theorem of from [Kle05], gives us a relation between these Picard functors.

Theorem 1.1.4. *Let S be the scheme $\mathrm{Spec}(k)$ and let $f : X \to S$ be the structure morphism. Suppose that X/k is separated and that $(f_T)_*\mathcal{O}_{X_T} = \mathcal{O}_T$ for any S-scheme T. Then there is a natural injection from $P_{X/S} \to \mathrm{Pic}_{X/S}$ and if f has a section, then this injection is an isomorphism and moreover $\mathrm{Pic}_{X/S}$ is a sheaf in the Zariski topology.*

If X is a complete k-variety with a k-rational point, then X satisfies the conditions in the theorem above. So if $S = \mathrm{Spec}(k)$ we have $\mathrm{Pic}_{X/S} \cong P_{X/S}$.

The following theorem we get from [Mur64] that uses a theorem of [Oor62] to reduce to the case that X is reduced. In this theorem we see under which conditions the relative Picard functor is representable.

Theorem 1.1.5. *Suppose that $S = \mathrm{Spec}(k)$ is the spectrum of a field k and that f is proper, then the relative Picard functor $\mathrm{Pic}_{X/S}$ is representable by a scheme that is separated and locally of finite type over k. We denote this scheme by $\mathrm{Pic}_{X/k}$.*

By the theorem we see in particular that the relative Picard functor is representable for every proper k-variety X by the group scheme $\mathrm{Pic}_{X/k}$.

In the next proposition, we will see some important properties of $\mathrm{Pic}_{X/k}$. For the proof, we refer to 6.6 of [EGM12].

Proposition 1.1.6. *Suppose X is a proper variety over a field k. Then*

(i) The tangent space of $\mathrm{Pic}_{X/k}$ at the identity element is isomorphic to $H^1(X, \mathcal{O}_X)$

(ii) The scheme $\mathrm{Pic}^0_{X/k}$ is smooth over k if and only if $\dim(\mathrm{Pic}^0_{X/k}) = \dim(H^1(X, \mathcal{O}_X)$. If $\mathrm{Char}(k) = 0$, then this is always the case.

(iii) If X/k is smooth over k, then the components of $\mathrm{Pic}_{X/k}$ are complete.

Definition 1.1.7. Let X be a curve. We define the Jacobian Variety or the Jacobian of X to be the scheme $\mathrm{Pic}^0_{X/k}$. We will denote the Jacobian by J.

We have the following general proposition about group schemes; see [EGM12] proposition 3.17 for the proof.

Proposition 1.1.8. *Let G be a group scheme, that is locally finite over a field k and let G^0 be the identity compound of G. Then*

1. *The following is equivalent*
   - *(i) The group scheme G is smooth over k*
   - *(ii) The group scheme G^0 is smooth over k*
2. *Every connected component of G is of finite type over K and is irreducible.*

Although we call $\mathrm{Pic}^0_{X/k}$ a Jacobian variety, we haven't showed that $\mathrm{Pic}^0_{X/k}$ is a variety yet. By the proposition above, we have that $\mathrm{Pic}^0_{X/k}$ is a variety if it is reduced. In general, the scheme $\mathrm{Pic}^0_{X/k}$ is in general not reduced in characteristic p. However if X is curve, then the $\mathrm{Pic}^0_{X/k}$ is reduced. By [EGM12] 6.8, we see that if X is curve, then $\mathrm{Pic}_{X/k}$ is smooth over k. Hence $\mathrm{Pic}^0_{X/k}$ is smooth by the proposition above. In particular $\mathrm{Pic}^0_{X/k}$ is reduced.

Since X is smooth over k, we see by proposition 1.1.6 that $\mathrm{Pic}^0_{X/k}$ is complete and hence defines an abelian variety.

Suppose that X is a curve of genus g. Then we see from the proposition 1.1.6, that J has dimension g. The following theorem summarises our results.

Theorem 1.1.9. *Let X be a curve. Then the Jacobian J of X is an abelian variety of dimension g.*

1.2 Embedding Curve in its Jacobian

In this section, we will see that every curve X can be embedded in its Jacobian.

First we show that the Jacobian can be described as the kernel of a degree map on the Picard scheme $\mathrm{Pic}_{X/k}$. Let us now define this degree map.

Let $\mathcal{L}$ be a line bundle on X_T. By [Har77], Theorem III.9.9, we have that the Euler-Poincaré characteristic $\chi(\mathcal{L}_t)$ is locally constant and by Riemann-Roch, we have $\deg(\mathcal{L}_t) = \chi(\mathcal{L}_t) + g - 1$. This shows that the function $d_{\mathcal{L}} : |T| \to \mathbb{Z}$ is given by $t \mapsto \deg(\mathcal{L}_t)$, is locally constant. Note that the function $d_{\mathcal{L}}$ can be seen as a T-valued of the constant group scheme $\mathbb{Z}$. Since $d_{\mathcal{L}} + d_{\mathcal{M}} = d_{\mathcal{L}\otimes\mathcal{M}}$, we have that the map $\mathcal{L} \mapsto d_{\mathcal{L}}$ is a homomorphism of presheaves $d : P_X \to \mathbb{Z}$. Let $\deg : \mathrm{Pic}_{X/k} \to \mathbb{Z}$ be the associated homomorphism on group schemes.

Suppose that X has a k-rational point, then each T-rational point of $\mathrm{Pic}_{X/k}$ is defined by a line bundle $\mathcal{L}$ and we have $\deg(\mathcal{L}) = d_{\mathcal{L}}$.

For every $n \in \mathbb{Z}$, We define the scheme

$$\mathrm{Jac}^n(X) = \deg^{-1}(n).$$

We have that $\mathrm{Jac}^n(X)$ is non-empty, since it has $\overline{k}$-rational points.

In the next proposition, we see that the Jacobian of a curve is equal to the kernel of the degree map.

Proposition 1.2.1. *Let X be a curve, then $\mathrm{Jac}^0(X) = J$.*

We want to prove that every curve X of genus $g \geq 1$ with a rational point can be embedded in his Jacobian. The following theorem of [EGM12] gives us that every curve X of genus $g \geq 1$ can be embedded in $\mathrm{Jac}^1(X)$.

Theorem 1.2.2. *Let X be a curve of genus $g \geq 1$ over a field k. Let $j : X \to \mathrm{Jac}^1(X)$ be the morphism, that to every T-rational point P associates the class of the line bundle $\mathcal{O}_{X_T}(P)$. Then j is a closed immersion.*

Suppose that P is k-rational point of X. Then the morphism $t_P : \mathrm{Jac}^1(X) \to J$ given on points by $[\mathcal{L}] \mapsto [\mathcal{L}(-P)]$ is an isomorphism. If we combine this with the Theorem above, we see that the curve X can be embedded in his Jacobian.

Corollary 1.2.3. Let X be a curve of genus $g \geq 1$ over a field k and suppose that P is a k-rational point. Then the morphism $\varphi_P : X \to J$, that is given on points by $Q \mapsto [\mathcal{O}_X(Q - P)]$ is a closed immersion.

1.3 Albenese embedding

In the previous section, we have seen that the morphism $\varphi_P : X \to J$ is a closed embedding. In this section, our goal is to see that every morphism to an abelian variety factors through this embedding. But first we will see that the n-th symmetric power is a smooth k-variety.

Let X/k be a curve of genus g. Let X^n be the n-fold product $X \times_k \cdots \times_k X$. Then we have an action of the symmetric group $\mathcal{S}_n$ on X^n via permutation of the coordinates. Let

$$X^{(n)} := X^n/\mathcal{S}_n$$

be the quotient of X^n under this action.

Lemma 1.3.1. *Let X/k be a curve of genus g. Then $X^{(n)}$ is a smooth k-variety.*

The variety $X^{(n)}$ is called the n-th symmetric power. Before we can show the end result, we want to show that g-th symmetric power is birational equivalent to $\mathrm{Jac}^g(X)$. We therefore need an alternative description of the n-th symmetric powers. The n-th symmetric power, we can also be described in terms of Cartier divisors. We will therefore first define relative effective Cartier divisors.

Definition 1.3.2. Let Y be a scheme over S. An effective Cartier divisor on Y is a closed subscheme D such that it's ideal sheaf $\mathcal{I}_D$ is a invertible $\mathcal{O}_Y$-module.
An effective Cartier divisor D is called a relative effective Cartier divisor if D is flat over S.

For every relative effective Cartier divisor D, we have the exact sequence

$$0 \longrightarrow \mathcal{I}_D \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_D \longrightarrow 0. \tag{1.1}$$

Let X be a curve. Then we define $\mathcal{O}_X(D)$ to be the invertible sheaf $\mathcal{I}_D^{-1}$, the inverse of the ideal sheaf of D. Tensoring the exact sequence 1.1 with $\mathcal{O}_X(D)$ gives us a morphism $\mathcal{O}_X \to \mathcal{O}_X(D)$. Let s_D be the corresponding section to this morphism. Then for every relative effective Cartier divisor D, we have an associated pair $(\mathcal{O}_X(D), s_D)$.

Let $(\mathcal{L}, s)$ be a pair, where $\mathcal{L}$ is an invertible sheaf and s is a global section of $\mathcal{L}$, such that

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{L} \longrightarrow \mathcal{L}/s\mathcal{O}_X \longrightarrow 0$$

is exact and $\mathcal{L}/s\mathcal{O}_X$ is flat over T. Let $(\mathcal{L}, s)$ and $(\mathcal{L}', s')$ be two such pairs, then these pairs are isomorphic if there exists an isomorphism $h : \mathcal{L} \to \mathcal{L}'$ with $h(s) = s'$. In the next proposition, we see that there exists a 1-1 correspondence between the isomorphism classes of these pairs and the relative effective Cartier divisors.

Proposition 1.3.3. *Let X/T be a curve. There exists an 1-1 correspondence between every relative effective Cartier divisors and the pair of isomorphism classes $(\mathcal{L}, s)$, where $\mathcal{L}$ is an invertible sheaf and s is a global section of $\mathcal{L}$, such that*

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{L} \longrightarrow \mathcal{L}/s\mathcal{O}_X \longrightarrow 0$$

is exact and $\mathcal{L}/s\mathcal{O}_X$ is flat over T. This correspondence is given by the map

$$D \mapsto [(\mathcal{O}_X(D), s_D)].$$

Remark 1.3.4. Let D and D' be two relative effective Cartier divisors that corresponds to the pair $(\mathcal{O}_X(D), s)$ respectively $(\mathcal{O}_X(D'), s')$, then $D + D'$ is a relative effective Cartier divisor and corresponds to $[(\mathcal{O}_X(D) \otimes \mathcal{O}_X(D'), s \otimes s')]$.

The degree of a relative effective Cartier divisor D is the degree of $\mathcal{O}_D$ as $\mathcal{O}_T$-module.

Remark 1.3.5. If D is relative effective Cartier divisor of degree n over X_T and we have a morphism $h : T' \to T$, then the pullback h^*D is a relative effective Cartier divisor of degree n over $X_{T'}$.

By this remark we obtain a contravariant functor

$$\mathrm{CaDiv}_n^{\mathrm{eff}} : \mathrm{Sch}/k \to \mathrm{Sets},$$

where $\mathrm{CaDiv}_n^{\mathrm{eff}}(T)$ are the relative effective Cartier divisors $D \subset X_T$ of degree n over T.

For every $P \in X(T)$, we have an corresponding section $s : T \to X_T$, whose image is an relative effective Cartier divisor of degree 1 over T. This Cartier divisor will also be denoted by P. So let $P_1, \ldots, P_n \in X(T)$, then we have a relative effective Cartier divisor $P_1 + \cdots + P_n$. This gives a morphism of functors $X^n \to \mathrm{CaDiv}_n^{\mathrm{eff}}$. This morphism is $\mathcal{S}_n$-invariant and hence we obtain a morphism $h : X^{(n)} \to \mathrm{CaDiv}_n^{\mathrm{eff}}$.

Proposition 1.3.6. *The morphism $h : X^{(n)} \to \mathrm{CaDiv}_n^{\mathrm{eff}}$ from above is an isomorphism.*

In the previous section we have seen a morphism $j : X \to \mathrm{Jac}^1(X)$ and if $P_1, \ldots, P_n \in X(T)$ for a k-scheme T, then $j(P_1) + \cdots + j(P_n)$ is a T-valued point of $\mathrm{Jac}^n(X)$.

For Cartier divisors, the morphism $j^{(n)}$ sends a relative effective Cartier divisor D to the class of the invertible sheaf $\mathcal{O}_X(D)$. If we describe relative Cartier divisors by the isomorphism class of the pair $(\mathcal{L}, s)$, then the morphism is simply the forgetful map $[(\mathcal{L}, s)] \mapsto [\mathcal{L}]$. One can see that the k-valued points of the fibre of $j^{(n)}$ is the projective space $\mathbb{P}(H^0(X, \mathcal{L}))$.

Theorem 1.3.7 (Abel's theorem)**.** *Let X be a curve and suppose that $\mathcal{L}$ is a line bundle on X of degree n. Then the scheme-theoretic fibre of the morphism $j^{(n)} : X^{(n)} \to \mathrm{Jac}^n(X)$ over the point $[\mathcal{L}]$ is equal to $\mathbb{P}(H^0(X, \mathcal{L}))$, which is the complete linear system of a effective divisor D with $\mathcal{O}_X(D) \cong \mathcal{L}$.*

The Jacobi's Inversion theorem is now a corollary of Abel's theorem. The idea of the proof is that we can assume that k is algebraically closed. Then we see by Riemann-Roch, that for every isomorphism class $[\mathcal{L}]$ of invertible sheaves of degree g, there exists an effective divisor D of degree g with $[\mathcal{L}] = [\mathcal{O}_X(D)]$ and hence $j^{(g)}$ is surjective. To prove that $j^{(n)}$ is a birational morphism, it is enough to prove that there exists an effective divisor D of degree g such that $h^1(D) = 1$. This can be proved by induction by n for $1 \leq n \leq g$ and using Riemann-Roch.

Corollary 1.3.8 (Jacobi's Inversion Theorem)**.** Let X be a curve of genus g, then the morphism $j^{(g)} : X^{(g)} \to \mathrm{Jac}^g(X)$ is a birational equivalence.

Now we can show that for every morphism from a curve X to an abelian variety factors through the embedding φ_P of the previous section if X has a rational point P.

Proposition 1.3.9. *Let X/k be a curve and let $P \in X(k)$ be a k-rational point. Let $\varphi_P : X \to J$ be the morphism that is given on points by $Q \mapsto [\mathcal{O}_X(Q - P)]$. Suppose that A is an abelian variety. Then every morphism of $\beta : X \to A$ factors uniquely through φ_P.*

For the detailed proof, we refer to [EGM12] proposition 14.36. We will show, how we can use the Jacobian Inversion Theorem. The idea of the proof is to construct a morphism $\psi : J \to X$ and then show that $\beta = \psi \circ \varphi_P$.

We can assume that $\beta(P) = 0$ after a translation. The morphism $\beta : X \to A$ induced an morphism $\beta^{(g)} : X^{(g)} \to A$ and the Jacobian inversion theorem gives us a rational map $\mathrm{Jac}^g(X) \to X^{(g)}$. By these two maps we obtain a rational map $\mathrm{Jac}^g(X) \to A$, which can be extended to a morphism $b : \mathrm{Jac}^g(X) \to A$. Note we have a morphism $t_{gP} : J \to \mathrm{Jac}^g(X)$, that is given by $[\mathcal{L}] \mapsto [\mathcal{L} \otimes \mathcal{O}_X(gP)]$. Hence we found a morphism $\psi : J \to X$, one now have to check that we have indeed $\beta = \psi \circ \varphi_P$.

Chapter 2

The zeta function of a curve over a finite field

In this chapter, we will look at the zeta function of curves over finite fields. The goal of this chapter is to prove some relations between the class number of the curve and the number of effective divisors. Our exposition is based on [LM90]. In the last two sections, we will give a short introduction to the l-adic cohomology and we will see that the zeta function can also be defined in terms of eigenvalues of Frobenius.

2.1 The zeta function of a curve

In this section we will define two zeta functions of a curve and state a theorem by Weil. We first discuss some notions, which we need in this section.

During our discussion the field k will be a perfect field. In most of the section it is even a finite field. However we start with an arbitrary perfect field. Let $G_k = \mathrm{Gal}(\overline{k}|k)$ be the absolute Galois group.

Let X be a curve over k and recall that, by our convention 0.0.3, X is smooth and projective. By [GW10], proposition 5.4, the G_k-orbits of $X(\overline{k})$ are in bijection with the closed points of X. Define the degree of a closed point P to be the number of elements in the corresponding G_k-orbits and denote it by $\deg(P)$. Another way to calculate the degree of a closed point is by the degree of the residue field $\kappa(P)$ over k; so $\deg(P) = [\kappa(P) : k]$.

Definition 2.1.1. A divisor D is a formal sum

$$D := \sum_P n_P P$$

where the sum ranges over the closed points of X, with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P. We define the degree of a divisor D by

$$\deg(D) = \sum_P n_P \cdot \deg(P).$$

A divisor is said to be *effective* if $n_P \geq 0$ for all closed points P. We denote the set of all effective divisors by $\mathrm{Div}^{\mathrm{eff}}(X)$ and denote the set of all effective divisors of degree n by $\mathrm{Div}_n^{\mathrm{eff}}(X)$.

Let q be a prime power. We specialise to the case that $k = \mathbb{F}_q$. Let $X/\mathbb{F}_q$ be a curve.

Note that for a curve over a finite field, there are only finitely many closed points of degree $\leq n$. Therefore there are only finitely may effective divisors of degree n. We define the norm of a divisor $D \in \mathrm{Div}^{\mathrm{eff}}(X)$ by $N(D) = q^{\deg(D)}$. In particular, if P is closed point, then the norm is defined by $N(P) = N(1 \cdot P) = q^{\deg(P)}$.

Definition 2.1.2. Let $X/\mathbb{F}_q$ be a curve. The (lowercase) zeta function of the curve X is defined by

$$\zeta_X(s) = \sum_{D \in \mathrm{Div}^{\mathrm{eff}}(X)} \frac{1}{N(D)^s} = \sum_{n=0}^{\infty} \frac{D_n}{q^{ns}} \in \mathbb{C}[[s]], \tag{2.1}$$

where $D_n = \#\mathrm{Div}_n^{\mathrm{eff}}(X)$

In the following lemma, it is easy to see the analogy with the Riemann zeta function. We will see later that we can write the zeta function in an explicit form.

Lemma 2.1.3. *The zeta function can also be written as*

$$\zeta_X(s) = \prod_P \frac{1}{1 - N(P)^{-s}} = \prod_{d \geq 0} \Big(\frac{1}{1 - q^{-ds}}\Big)^{a_d} \tag{2.2}$$

where P ranges over all closed points of X and where a_d is the number of closed points of degree d.

Proof. If $D = \sum n_P P$ is an effective divisor, then

$$N(D)^{-s} = \prod_P N(P)^{-s \cdot n_P}.$$

Summing this over all effective divisors give the same as the product

$$\prod_P \sum_{n=0}^{\infty} \frac{1}{N(P)^{-ns}},$$

which by the geometrical series equals

$$\prod_P \frac{1}{1 - N(P)^{-s}}.$$

The last expression in 2.2 is just a rewriting of second expression in 2.2. □

We can now define the second zeta function.

Definition 2.1.4. Let $X/\mathbb{F}_q$ be a curve. The (uppercase) zeta function of the curve X is defined by

$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} |X(\mathbb{F}_{q^n})|\right) \in \mathbb{Q}[[T]].$$

We have the following relation between the two zeta function: $\zeta_X(s) = Z_X(q^{-s})$; see Propostion 2.7 of [Mus]. If we substitute T for q^{-s} , then using the last expression in 2.1 we find

$$Z_X(T) = \sum_{n=0}^{\infty} D_n T^n.$$

We define a further function defined by the relation:

$$L(T) = Z_X(T) \cdot (1 - T) \cdot (1 - qT). \tag{2.3}$$

The following theorem gives an important result by André Weil. The results first appeared in 1948 [Wei48]. The third property is also called the Riemann hypothesis, because for every root α of Z_X we have $|\alpha| = q^{-1/2}$. This means that every root of ζ_X has norm $1/2$. This is analogue to the situation of the Riemann hypothesis of the Riemann zeta function, where all the non-trivial roots are complex numbers with real part $1/2$.

Theorem 2.1.5. *Let $X/\mathbb{F}_q$ be curve and define $L(T)$ as in 2.3.*

(i) The function $L(T)$ is a polynomial in $\mathbb{Z}[T]$ with $L(0) = 1$ and $L(1) = h = |J(\mathbb{F}_q)|$, where J is the Jacobian of X.

(ii) We have

$$L(1/(qT)) = q^{-g}T^{-2g}L(T)$$

(This is called the functional equation).

(iii) If in the ring $\mathbb{C}[T]$ we factor $L(T)$ as

$$L(T) = \prod_{i=1}^{2g}(1 - \alpha_i T),$$

then the inverse roots α_i satisfies $|\alpha_i| = \sqrt{q}$ for $1 \leq i \leq 2g$.

From these results it follows that if α is an inverse root, then $\overline{\alpha} = q/\alpha$ is an inverse root too. The inverse roots α, that are not real, come in pairs $(\alpha, \overline{\alpha})$. The only exceptions are the real inverse roots, but in the next proposition we will see that they are of even multiplicity.

Proposition 2.1.6. *The real roots of the polynomial L all have even multiplicity.*

Proof. Suppose that some real root of the polynomial $L(T)$ is of odd multiplicity. We know that the only possible real inverse roots are $\pm\sqrt{q}$ by part (iii) of Theorem 2.1.5. Since $L(T) \in \mathbb{Z}[T]$ (part (i) of Theorem 2.1.5), we know that the multiplicity of both the roots are the same. So we have that $(1 - \sqrt{q}T)$ and $(1 + \sqrt{q}T)$ are both a factor of $L(T)$ of odd multiplicity. All the other factors of $L(T)$ come in pairs. So we can write

$$L(T) = (1 - \sqrt{q}T)(1 + \sqrt{q}T) \prod_{i=1}^{g-1}(1 - \alpha_T)(1 - \overline{\alpha_i}T).$$

Note that the product $(1 - \alpha)(1 - \overline{\alpha})$ for an inverse root α is a positive real number. If we fill in $T = 1$, we have

$$L(1) = h = (1 - q) \prod_{i=1}^{g-1}(1 - \alpha_i)(1 - \overline{\alpha}_i) < 0,$$

but this is in contradiction with part (i) of Theorem 2.1.5. □

As a result of the proposition we can write

$$L(T) = \prod_{i=1}^{g}(1 - \alpha_i T)(1 - \overline{\alpha_i} T),$$

and we see that the coefficient of T^{2g} is equal to q^{2g}. The polynomial $L(T)$ is also called the L-polynomial.

2.2 The relation between the class number and the number of effective divisors

In this section we prove some relation between the class numbers and the number of effective divisors. In this section X is a curve and we take as extra assumption that X has a $\mathbb{F}_q$-rational point. Recall from chapter 1, that $\mathrm{Jac}^n(X)(\mathbb{F}_q)$ is the set of isomorphism classes of invertible sheaves on X of degree n. We denote the isomorphism class of an invertible sheaf $\mathcal{L}$ of degree n by $[\mathcal{L}] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)$. Let $H^0(X, \mathcal{L})$ be the vector space of global sections, let $h^0(X, \mathcal{L})$ be the dimension of $H^0(X, \mathcal{L})$ over $\mathbb{F}_q$ and denote the sheaf of differentials forms on X by ω_X.

We start with a few remarks.

Remark 2.2.1.

1. For every effective divisor D, we have an invertible sheaf $\mathcal{O}_X(D)$ and if the degree of D is n, then $[\mathcal{O}_X(D)] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)$. So we have a map from $\mathrm{Div}_n^{\mathrm{eff}}(X)$ to $\mathrm{Jac}^n(X)(\mathbb{F}_q)$.
2. Suppose that D, E are two effective divisors, then the two divisors have the same image in the map above if and only if there exists a $f \in H^0(X, \mathcal{O}_X(D))$, such that $E = \mathrm{div}(f) + D$. Hence, the inverse image of a class $[\mathcal{L}] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)$ is in bijection with the projective space $\mathbb{P}(H^0(X, \mathcal{L}))$.
3. For every $\mathbb{F}_q$-rational point P, we have a corresponding effective divisor of degree 1, also denoted by P. We have a one-to-one correspondence between $J(\mathbb{F}_q)$ and $\mathrm{Jac}^n(X)(\mathbb{F}_q)$ by the map defined by $[\mathcal{L}] \mapsto [\mathcal{L} \otimes \mathcal{O}_X(nP)]$. So in particular $|J(\mathbb{F}_q)| = |\mathrm{Jac}^n(X)(\mathbb{F}_q)|$.
4. Note that there are no effective divisors of negative degree. So $D_n = 0$ for $n < 0$.

We will use the Riemann-Roch theorem for curves in the next lemma. Since there are a few different versions, we recall the version which we will use. The version we use, is a combination with Serre duality. Recall from Serre duality that for a line bundle $\mathcal{L}$, the spaces $H^1(X, \mathcal{L})$, $H^0(X, \omega_X \otimes \mathcal{L}^{-1})$ are dual to each other.

Theorem 2.2.2 (Riemann-Roch for curves)**.** *Let X be a curve and let $\mathcal{L}$ be a line bundle on X of degree n. Then*

$$h^0(X, \mathcal{L}) - h^0(X, \omega_X \otimes \mathcal{L}^{-1}) = n - 1 - g$$

Now we can start with the following lemma. Recall that $D_n = |\mathrm{Div}_n^{\mathrm{eff}}(X)|$.

Lemma 2.2.3. *For $n \geq 0$, we have*

$$D_n = q^{n+1-g} D_{2g-2-n} + h\frac{q^{n+1-g} - 1}{q - 1}, \tag{2.4}$$

where $h = |J(\mathbb{F}_q)|$ the number of $\mathbb{F}_q$-rational points of the Jacobian.

Proof. As we seen in the first part of Remark 2.2.1, there is a map $\mathrm{Div}_n^{\mathrm{eff}}(X) \to \mathrm{Jac}^n(X)(\mathbb{F}_q)$ for every $n \geq 0$ and the inverse image of a class $\mathcal{L}$ is the projective space $\mathbb{P}(H^0(X, \mathcal{L}))$. So we have that the number of effective divisors of degree n is

$$D_n = \sum_{[\mathcal{L}] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)} \frac{q^{h^0(X,\mathcal{L})} - 1}{q-1}.$$

The theorem of Riemann-Roch gives us

$$h^0(X, \mathcal{L}) = n + 1 - g + h^0(X, \omega \otimes \mathcal{L}^{-1}),$$

thus for any n

$$(q-1)D_n = \sum_{[\mathcal{L}] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)} q^{n+1-g+h^0(X,\omega\otimes\mathcal{L}^{-1})} - 1$$

By the second part of the Remark 2.2.1, we have$|\mathrm{Jac}^n(X)(\mathbb{F}_q)| = |J(\mathbb{F}_q)| = h$. So we can write

$$(q-1)D_n = h(q^{n+1-q} - 1) + q^{n+1-q} \sum_{[\mathcal{L}] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)} q^{h^0(\omega\otimes\mathcal{L}^{-1})} - 1.$$

The map $[\mathcal{L}] \mapsto [\omega_X \otimes \mathcal{L}^{-1}]$ gives a bijection $\mathrm{Jac}^n(X)(\mathbb{F}_q) \xrightarrow{\sim} \mathrm{Jac}^{2g-2-n}(X)(\mathbb{F}_q)$ So

$$(q-1)D_{2g-2-n} = \sum_{[\mathcal{L}] \in \mathrm{Jac}^n(X)(\mathbb{F}_q)} q^{h^0(X,\omega\otimes\mathcal{L}^{-1})} - 1,$$

which gives us the desired statement about D_n. □

In particular for $n \geq 2g-1$, we have $D_{2g-2-n} = 0$, so

$$D_n = h\frac{q^{n+1-g} - 1}{q-1}. \tag{2.5}$$

In the following lemma we will see a relation of the number of divisors with the L-polynomial of X.

Lemma 2.2.4. *Let $X/\mathbb{F}_q$ be a curve with genus $g \geq 2$. Let $L(T)$ be the L-polynomial of X. Then we have*

$$\sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} = \frac{L(T)}{(1-T)(1-qT)} + h\frac{T^{g-1}}{q-1}\Big(\frac{1}{1-T} - \frac{1}{1-qT}\Big).$$

Proof. We have seen in the first section of this chapter that we can write the zeta function in different ways. We can write $Z_X(T) = \frac{L(T)}{(1-T)(1-qT)}$ and $Z_X(T) = \sum_n D_n T^n$. So it is enough to show that

$$\sum_{n=0}^{\infty} D_n T^n = \sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} - h\frac{T^{g-1}}{q-1}\Big(\frac{1}{1-T} - \frac{1}{1-qT}\Big).$$

By the equations 2.4 and 2.5 we see that

$$\begin{aligned}\sum_{n=0}^{\infty} D_n T^n &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=g-1}^{2g-2} D_n T^n + \sum_{n=2g-1}^{\infty} D_n T_n \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=g-1}^{2g-2} \Big(q^{n+1-g} D_{2g-2-n} + h\frac{q^{n+1-g}-1}{q-1}\Big) T^n + \sum_{n=0}^{\infty} h\frac{q^{n+1-g}-1}{q-1} T^n \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=g-1}^{2g-2} q^{n+1-g} D_{2g-2-n} T^n + h\sum_{n=g-1}^{\infty} \frac{q^{n+1-g}-1}{q-1} T^n.\end{aligned}$$

For the second sum of the last expression, we will substitute $2g-2-n$ for n and for the third sum, we will substitute $n+g-1$ for n.

$$\begin{aligned}\sum_{n=0}^{\infty} D_n T^n &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} + h\sum_{n=0}^{\infty} \frac{q^n-1}{q-1} T^{n+g+1} \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{q-1-n} D_n T^{2g-2-n} + h\frac{T^{g-1}}{q-1}\sum_{n=0}^{\infty} (q^n-1) T^n \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{q-1-n} D_n T^{2g-2-n} + h\frac{T^{g-1}}{q-1}\left(\frac{1}{1-qT} - \frac{1}{1-T}\right).\end{aligned}$$

Note that the last step follows by the geometrical series. □

Theorem 2.2.5. *Let X be a curve over $\mathbb{F}_q$ with genus $g \geq 2$. Let D_n be the number of effective divisors of degree n and let $(\alpha_i, \overline{\alpha_i})$ be the pairs of inverse roots of the zeta function $Z_X(T)$. Then*

$$\sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n = h\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2}. \tag{2.6}$$

Proof. We introduce the following auxiliary function

$$F(T) = \frac{L(T)}{1-qT} + h\frac{T^{g-1}}{q-1}.$$

By Lemma 2.2.4, we have

$$\sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} = \frac{F(T)}{1-T} - h\frac{T^{g-1}}{(q-1)(1-qT)} \tag{2.7}$$

We claim that

$$\sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n = -F'(1) + h\frac{1}{(q-1)^2} \tag{2.8}$$

By definition of the derivative, we can write

$$F'(1) = \lim_{T\to 1} \frac{F(T)-F(1)}{T-1} = \lim_{T\to 1} \frac{F(T)}{T-1},$$

because $F(1) = \frac{L(1)}{1-q} + \frac{h}{q-1} = 0$. By equation 2.7 we find that

$$-F'(1) = \lim_{T\to 1} \Big(\sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} + h \frac{T^{g-1}}{(q-1)(1-qT)} \Big)$$

and this gives 2.8, which proves the claim.

We can also compute the derivative of F by the product rule and we see that

$$F'(T) = \frac{L'(T)}{(1-qT)} + q\frac{L(T)}{(1-qT)^2} + h(g-1)\frac{T^{g-2}}{q-1},$$

and hence

$$F'(1) = \frac{L'(1)}{(1-T)} + q\frac{L(1)}{(1-q)^2} + h(g-1)\frac{1}{q-1}.$$

In order to calculate $F'(1)$, we have to determine $L'(1)$. We can write $L(T)$ as

$$L(T) = \sum_{i=1}^{g} (1-\alpha_i T)(1-\overline{\alpha_i} T).$$

We have

$$\frac{L'(T)}{L(T)} = -\sum_{i=1}^{g} \frac{\alpha_i}{1-\alpha_i T} + \frac{\overline{\alpha_i}}{1-\overline{\alpha_i} T} = -\sum_{i=1}^{g} \frac{\alpha_i + \overline{\alpha_i} - 2qT}{(1-\alpha_i T)(1-\overline{\alpha_i} T)},$$

which for $T = 1$ gives

$$\frac{L'(1)}{L(1)} = \sum_{i=1}^{g} \frac{2q - (\alpha_i + \overline{\alpha_i})}{|1-\alpha_i|^2}.$$

We observe that $L(1) = h$ and

$$(1-\alpha_i)(1-\overline{\alpha_i}) + q - 1 = 2q - (\alpha_i + \overline{\alpha_i}).$$

So we obtain

$$\frac{L'(1)}{h} = \sum_{i=1}^{g} \frac{(1-\alpha_i)(1-\overline{\alpha_i}) + q - 1}{|1-\alpha_i|^2} = g + \sum_{i=1}^{g} \frac{q-1}{|1-\alpha_i|^2}.$$

Now we can calculate the value of $F'(T)$ at $T = 1$,

$$\begin{aligned} F'(1) &= \frac{gh}{1-q} - h\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2} + q\frac{h}{(1-q)^2} + h(g-1)\frac{1}{q-1} \\ &= q\frac{h}{(1-q)^2} - \frac{h}{q-1} - h\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2} \\ &= \frac{h}{(1-q)^2} - h\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2}. \end{aligned}$$

We combine this with equation 2.8 and we obtain the desired result. □

By the theorem, we see that we have a relation between class number h and the number of effective divisors of degree $< g$. In the next proposition we will see a upper bound for

$$\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2.}$$

Proposition 2.2.6. *Let $X/\mathbb{F}_q$ be a curve with genus g and let $(\alpha_i, \overline{\alpha_i})$ be the pairs of inverse roots of the zeta function $Z_X(T)$. Then*

$$\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2} \leq \frac{1}{q-1}\big((g+1)(q+1) - |X(\mathbb{F}_q)|\big). \tag{2.9}$$

Proof. Since $|\alpha_i| = \sqrt{q}$, we observe the following

$$|1-\alpha_i^2|^2 \geq (q-1)^2,$$

we can this rewrite as

$$|(1-\alpha_i)(1+\alpha_i)|^2 \geq (q-1)^2,$$

hence

$$|1-\alpha_i|^2 \geq \frac{(q-1)^2}{|1+\alpha_i|^2}.$$

We now obtain the upper bound

$$\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2} \leq \frac{1}{(q-1)^2} \sum_{i=1}^{n} |1+\alpha_i|^2.$$

By rewriting this upper bound, we see that

$$\begin{aligned}\sum_{i=1}^{g} \frac{1}{|1-\alpha_i|^2} &\leq \frac{1}{(q-1)^2} \sum_{i=1}^{g} (1+q+\alpha_i+\overline{\alpha_i}) \\ &= \frac{1}{(q-1)^2}\big(g(q+1) + \sum_{i=1}^{g}(\alpha_i+\overline{\alpha_i})\big).\end{aligned}$$

To prove the equation 2.9, it is enough to show that

$$|X(\mathbb{F}_q)| = 1 + q - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i}).$$

By equation 2.3, we see that

$$\log \frac{L(T)}{(1-qT)(1-T)} = \sum_{n=0}^{\infty} \frac{T^n}{n} |X(\mathbb{F}_q)|.$$

If we write out the left hand side, we obtain

$$\begin{aligned}\log\frac{L(T)}{(1-qT)(1-T)} &= \log(L(T)) - \log(1-T) - \log(1-qT)\\ &= \sum_{i=1}^{2g}\log(1-\alpha_i T) - \log(1-T) - \log(1-qT)\\ &= -\sum_{i=1}^{2g}\sum_{n=1}^{\infty}\frac{\alpha_i^n T^n}{n} + \sum_{m=1}^{\infty}\frac{T^m}{m} + \sum_{k=0}^{\infty}\frac{q^k T^k}{k}\\ &= \sum_{n=1}^{\infty}\big(q^n + 1 - \sum_{i=1}^{2g}\alpha_i^n\big)\frac{T^n}{n}.\end{aligned}$$

So we see that

$$|X(\mathbb{F}_q)| = q + 1 - \sum_{n=1}^{g}\alpha_i + \overline{\alpha_i}.$$

□

2.3 A brief introduction to l-adic cohomology

In this section we give a short introduction to l-adic cohomology. In order to show that the zeta function can be written in terms of eigenvalues of Frobenius, we need theorems like the Lefschetz fixed point theorem. But to state such theorem, we need some knowledge about l-adic cohomology. We will not use Zariski sheaves, but étale sheaves. For more information about the étale topology see [Mil13]. We look at special étale sheaves, which are defined on a curve X over k. Let $\overline{X} = X \otimes \overline{k}$, then this gives a curve over $\overline{k}$.

Let us give some examples of étale sheaves:

Example 2.3.1. 1. $\mathbb{G}_m$: For every scheme U which is étale over X, we have $\mathbb{G}_m = \Gamma(U, \mathcal{O}_U^\times)$. This is the étale sheaf associated to $\mathcal{O}_X^\times$ and it is called the multiplicative group.

2. μ_n: For every scheme U which is étale over X, $\mu_n(U)$ is the group of nth roots of unity in $\Gamma(U, \mathcal{O}_U)$. If X is defined over an algebraically closed field k and the characteristic of k does not divide n, then the sheaf μ_n is isomorphic to the constant sheaf $\mathbb{Z}/n\mathbb{Z}$.

These two examples give rise to an exact sequence of étale sheaves. Note that this sequence is not exact in the Zariski topology. The exact sequence is known as the Kummer exact sequence

Proposition 2.3.2. *Let X be a curve over k and suppose that n does not divide the characteristic of k. Then the the sequence of étale sheaves of abelian groups*

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{x\mapsto x^n} \mathbb{G}_m \longrightarrow 0$$

is exact.

One goal of this section is to compute the cohomology of the sheaf μ_n for a curve over an algebraically closed field. In order to compute this, we use the following theorem.

Theorem 2.3.3. *Let $\overline{X}$ be a curve over an algebraically closed field $\overline{k}$. Then,*

$$H^r(\overline{X}_{\text{et}}, \mathbb{G}_m) = \begin{cases} \Gamma(\overline{X}, \mathcal{O}_{\overline{X}}^{\times}) & r = 0 \\ \text{Pic}(\overline{X}) & r = 1 \\ 0 & r > 1 \end{cases}$$

Note that the map $x \mapsto x^n$ on $H^0(\overline{X}, \mathbb{G}_m) = \overline{k}^{\times}$ is surjective. So if we take the exact sequence in cohomology in degree 0 associated to the Kummer exact sequence, we see that

$$0 \longrightarrow H^0(\overline{X}, \mu_n) \longrightarrow H^0(\overline{X}, \mathbb{G}_m) \xrightarrow{x \mapsto x^n} H^0(\overline{X}, \mathbb{G}_m) \longrightarrow 0.$$

If we combine this with the long exact sequence associated to the Kummer exact sequence, we obtain an exact sequence

$$0 \longrightarrow H^1(\overline{X}, \mu_n) \longrightarrow \text{Pic}(\overline{X}) \xrightarrow{n} \text{Pic}(\overline{X}) \longrightarrow H^2(\overline{X}, \mu_n) \longrightarrow 0.$$

In order to compute the cohomology with values in μ_n, we need to know the kernel and the cokernel of the multiplication by n map on $\text{Pic}(\overline{X})$. Recall from section 1.2 that we have a degree map $\deg : \text{Pic}(\overline{X}) \to \mathbb{Z}$ and this give rise to an exact sequence

$$0 \longrightarrow \text{Pic}^0(\overline{X}) \longrightarrow \text{Pic}(\overline{X}) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0 \ .$$

Note that for a $\mathcal{L} \in \text{Pic}(\overline{X})$, that

$$\deg\big(n(\mathcal{L})\big) = n \cdot \deg(\mathcal{L}).$$

So we have that the kernel of the multiplication by n map on $\text{Pic}(\overline{X})$ is the same as the kernel of the multiplication by n map on the Jacobian $J(\overline{X}) = \text{Pic}^0(\overline{X})$. By Proposition 5.9 and Corollary 5.11 of [EGM12], we have that the map $n : J \to J$ is surjective on $\overline{k}$-valued points and we see that the kernel of $n : J(\overline{k}) \to J(\overline{k})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$. Since the map $n : J(\overline{k}) \to J(\overline{k})$ is surjective, we have that the map $n : \text{Jac}^m(\overline{X})(\overline{k}) \to \text{Jac}^{mn}(\overline{X})(\overline{k})$, where $\text{Jac}^m(\overline{X})(\overline{k})$ is the set of isomorphism classes of line bundles on $\overline{X}$ of degree m, is a bijection if $m \neq 0$. So we see that the cokernel of the map $n : \text{Pic}(\overline{X}) \to \text{Pic}(\overline{X})$ is $\mathbb{Z}/n\mathbb{Z}$. Now we obtain the following theorem.

Theorem 2.3.4. *Let $\overline{X}$ be a curve over an algebraically closed field k and suppose that n is prime to the characteristic of k. Then,*

$$H^r(\overline{X}, \mu_n) = \begin{cases} \mu_n(k) & r = 0 \\ (\mathbb{Z}/n\mathbb{Z})^{2g} & r = 1 \\ \mathbb{Z}/n\mathbb{Z} & r = 2 \\ 0 & r > 2 \end{cases}.$$

Definition 2.3.5. Let X be a curve over k and suppose that l is a prime that is not equal to the characteristic of k. Then we define

$$H^r(X, \mathbb{Z}_l) = \varprojlim_n H^r(X, \mathbb{Z}/l^n\mathbb{Z}),$$

where the homomorphisms for $m \geq n$

$$f_{mn} : H^r(X, \mathbb{Z}/l^m\mathbb{Z}) \to H^r(X, \mathbb{Z}/l^n\mathbb{Z})$$

are induced by the quotient maps

$$\mathbb{Z}/l^m\mathbb{Z} \to \mathbb{Z}/l^n\mathbb{Z}.$$

Furthermore we define

$$H^r(X, \mathbb{Q}_l) = H^r(X, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

If $\overline{k}$ is algebraically closed, then $\mu_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}$. So by Theorem 2.3.4, we obtain the following result.

Proposition 2.3.6. *Let $\overline{X}$ be a curve over an algebraically closed field $\overline{k}$ and let J be the Jacobian of X, then*

$$H^0(\overline{X}, \mathbb{Q}_l) = \mathbb{Q}_l$$
$$H^1(\overline{X}, \mathbb{Q}_l) = \mathrm{Hom}\big(\mathbb{Q}_l/\mathbb{Z}_l, J(\overline{k})\big) \otimes \mathbb{Q}_l$$
$$H^2(\overline{X}, \mathbb{Q}_l) = \varprojlim \mathrm{Pic}(\overline{X})/l^n\mathrm{Pic}(\overline{X}) \otimes \mathbb{Q}_l \cong \mathbb{Q}_l.$$

Proof. The first and last statement are clear. So we prove the second statement. We have seen before that

$$H^1(\overline{X}, \mathbb{Z}/l^n\mathbb{Z}) = \mathrm{Hom}\big(\mathbb{Z}/l^n\mathbb{Z}, J(\overline{k})\big).$$

Note that the map

$$\mathrm{Hom}\big(\mathbb{Z}/l^{n+1}\mathbb{Z}, J(\overline{k})\big) \to \mathrm{Hom}\big(\mathbb{Z}/l^n\mathbb{Z}, J(\overline{k})\big),$$

is induced by the map $\mathbb{Z}/l^n\mathbb{Z} \to \mathbb{Z}/l^{n+1}\mathbb{Z}$, which is multiplication by l. So we see that the inverse system comes from the direct system $(\mathbb{Z}/l^n\mathbb{Z})_n$ and we have the property that

$$\varprojlim_n \mathrm{Hom}(X_i, Y) = \mathrm{Hom}(\varinjlim X_i, Y)$$

for a direct system $(X_i)_i$. So we see that

$$H^1(\overline{X}, \mathbb{Z}_l) = \varprojlim \mathrm{Hom}\big(\mathbb{Z}/l^n\mathbb{Z}, J(\overline{k})\big) = \mathrm{Hom}\big(\varinjlim \mathbb{Z}/l^n\mathbb{Z}, J(\overline{k})\big).$$

By proposition 1 of [Ser73], we have that

$$\varinjlim_n \mathbb{Z}/l^n\mathbb{Z} \cong \varinjlim_n \mathbb{Z}_l/l^n\mathbb{Z}_l.$$

Note that $\mathbb{Q}_l = \mathbb{Z}_l[1/l]$ and hence we have an isomorphism $\mathbb{Q}_l/\mathbb{Z}_l \cong \varinjlim_n \mathbb{Z}_l/l^n\mathbb{Z}_l$. So we get

$$H^1(\overline{X}, \mathbb{Q}_l) = \mathrm{Hom}\big(\mathbb{Q}_l/\mathbb{Z}_l, J(\overline{k})\big).$$

□

2.4 The zeta function and Frobenius

In this section we will see a description of the zeta function in terms of eigenvalues of Frobenius. We will first state an important theorem, which is called the Lefschetz Fixed-Point Formula. Then we will define the Frobenius map on a variety and give some properties. After that we will explain how the zeta function is related to the Frobenius map. We refer to [Mil13] for the details and proofs in this section.

In the previous section, we have seen a brief introduction to the l-adic cohomology and we will apply this cohomology in this section. Let X/k be a curve and let $\overline{k}$ be an algebraic closure of k. Then $\overline{X} = X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ is a curve over $\overline{k}$. Later in the discussion we will assume that k is a finite field. We begin with a definition.

Definition 2.4.1. Let Y be a surface over k and let Z_1, Z_2 be two different prime divisors. Suppose that $P \in Z_1 \cap Z_2$, then we can describe Z_1 and Z_2 locally around P as the zero scheme of polynomials f_1 and f_2. We define the intersection multiplicity of Z_1 and Z_2 at P by

$$(Z_1 \cdot Z_2)_P = \dim_k\big(\mathcal{O}_{Y,P}/(f_1, f_2)\big).$$

Additionally we define the intersection number of Z_1 and Z_2 by

$$(Z_1 \cdot Z_2) = \sum_{P \in Z_1 \cap Z_2} (Z_1 \cdot Z_2)_P.$$

Suppose $\varphi : \overline{X} \to \overline{X}$ is a non-constant morphism, then φ induces a morphism $\varphi^* : H^r(\overline{X}, \mathbb{Q}_l) \to H^r(\overline{X}, \mathbb{Q}_l)$. As we have seen in the previous section, the spaces $H^r(\overline{X}, \mathbb{Q}_l)$ are finite-dimension $\mathbb{Q}_l$-vector spaces. So we can take their traces $\mathrm{Tr}\big(\varphi^* | H^r(\overline{X}, \mathbb{Q}_l)\big)$. By the following theorem, we see that the traces compute the fixed points of φ.

Theorem 2.4.2 (Lefschetz Fixed-Point Formula)**.** *Let $\overline{X}$ be a curve over an algebraically closed field and let $\varphi : \overline{X} \to \overline{X}$ be a non-constant morphism. Then*

$$(\Gamma_\varphi \cdot \Delta) = \sum_r (-1)^r \mathrm{Tr}\big(\varphi^*, H^r(\overline{X}, \mathbb{Q}_l)\big),$$

where Γ_φ is the graph of φ and Δ is the diagonal of $\overline{X} \times \overline{X}$.

The number $(\Gamma_\varphi \cdot \Delta)$ is the number of fixed points of φ counted with multiplicities. The following lemma shows that the multiplicity of the fixed point of a morphism φ is in most cases 1.

Lemma 2.4.3. *Let $\overline{X}\,/\,\overline{k}$ be a curve and let $\varphi : \overline{X} \to \overline{X}$ be a morphism. Suppose that P is a fixed point. Then $(\Gamma_\varphi \cdot \Delta)_P = 1$ if $(d\varphi)_P : T_{\overline{X},P} \to T_{\overline{X},P}$ is not the identity, where $T_{\overline{X},P}$ is the tangent space of $\overline{X}$ at P.*

The Frobenius map

Let Y be a variety over $\mathbb{F}_q$ and let $\mathbb{F}$ be an algebraic closure of a finite field $\mathbb{F}_q$. We want to define the Frobenius map for a variety $\overline{Y}$ over $\mathbb{F}$, where $\overline{Y} = Y \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})$. We will first define the Frobenius map for an affine variety.

Definition 2.4.4. Let A be an affine $\mathbb{F}_q$-algebra and let $\overline{A} = A \otimes_{\mathbb{F}_q} \mathbb{F}$. Then the map $f : A \to A$, where $a \mapsto a^q$, is a homomorphism of $\mathbb{F}_q$-algebras. We call the corresponding map $F_A : \mathrm{Spec}(A) \to \mathrm{Spec}(A)$ the Frobenius endorphism. By base change we obtain the map $F : \mathrm{Spec}(\overline{A}) \to \mathrm{Spec}(\overline{A})$ and we call this the Frobenius map.

Now we define the Frobenius endomorphism for a general variety over $\mathbb{F}_q$.

Definition 2.4.5. Let Y be a variety over $\mathbb{F}_q$ and let $\overline{Y} = Y \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})$. Then the Frobenius endomorphism $F_Y : Y \to Y$ is the unique morphism, such that for every affine open $U = \mathrm{Spec}(A) \subset Y$, we have that $F_U = F_Y|_U : U \to U$ is the Frobenius endomorphism. By base change we obtain a map $F : \overline{Y} \to \overline{Y}$ and we call it the Frobenius map.

We have the following properties, which are easy to check:

1. the Frobenius map $F : \mathbb{A}^n \to \mathbb{A}^n$ is defined by $(t_1, t_2, \ldots, t_n) \mapsto (t_1^q, t_2^q, \ldots, t_n^q)$.
2. the Frobenius map $F : \mathbb{P}^n \to \mathbb{P}^n$ is defined by $(t_0 : t_1 : \cdots : t_n) \mapsto (t_0^q : t_1^q : \cdots : t_n^q)$.
3. for every morphism $\varphi : Y_1 \to Y_2$ of varieties over $\mathbb{F}_q$, the following diagram

$$\begin{array}{ccc} \overline{Y_1} & \xrightarrow{\varphi} & \overline{Y_2} \\ \downarrow F & & \downarrow F \\ \overline{Y_1} & \xrightarrow{\varphi} & \overline{Y_2} \end{array}$$

commutes, where $\overline{Y_i} = Y_i \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})$.

When we combine these statements, we see that the Frobenius map on every subvariety of $\mathbb{A}^n$ is defined by $(t_1, \ldots, t_n) \mapsto (t_1^q, \ldots, t_n^q)$ and the Frobenius map on every subvariety of $\mathbb{P}^n$ is defined by $(t_0 : \cdots : t_n) \mapsto (t_0^q : \cdots : t_n^q)$.

In the next lemma we see that the Frobenius map is of finite degree.

Lemma 2.4.6. *Let $\overline{Y}$ be a variety over $\mathbb{F}$. The Frobenius map $F : \overline{Y} \to \overline{Y}$ is a finite morphism of degree $q^{\dim(\overline{Y})}$.*

We now want to connect the Frobenius with the first part of this section and we will show in the next lemma, that all fixed points, have multiplicity 1.

Lemma 2.4.7. *Let $X/\mathbb{F}_q$ be a curve and let $\overline{X}$ be the corresponding curve over $\mathbb{F}$. Then the fixed points of the Frobenius map $F : \overline{X} \to \overline{X}$ are the $\mathbb{F}_q$-rational points $X(\mathbb{F}_q)$. Each fixed point occurs with multiplicity* 1.

Proof. Suppose that $P \in X(\mathbb{F})$ is a fixed point of F . Then $P \circ F = P$, where $F : \mathrm{Spec}(\mathbb{F}) \to \mathrm{Spec}(\mathbb{F})$ is the Frobenius map.

Note that a $\mathbb{F}$-rational point $P : \mathrm{Spec}(\mathbb{F}) \to X$ is given by a homomorphism $\varphi_P : \kappa(P) \to \mathbb{F}$, where $\kappa(P)$ is the residue field of P and the $\mathbb{F}$-rational point $P \circ F : \mathrm{Spec}(\mathbb{F}) \to X$ is given by $\varphi_P^q : \kappa(P) \to \mathbb{F}$, where $\varphi_P^q(x) = \varphi_P(x)^q$. We have that $\varphi_P^q(x) = \varphi_P(x)^q = \varphi_P(x)$ if and only if $x \in \mathbb{F}_q$. So $\kappa(P) \cong \mathbb{F}_q$ and hence a fixed point of $F : \overline{X} \to \overline{X}$ is equivalent to a $\mathbb{F}_q$-rational point.

We claim that $(dF)_P = 0$ for fixed point P and then by Lemma 2.4.3, it shows that every fixed point occurs with multiplicity 1.

We can compute the tangent map at P as follows, we have $T_{\overline{X},P} = (\mathfrak{m}_P/\mathfrak{m}_P^2)^\vee$, where $\mathfrak{m}_P$ is the maximal ideal of $\mathcal{O}_{X,P}$ and the map $(dF)_P : T_{\overline{X},P} \to T_{\overline{X},P}$ is defined by $(dF)_P(t) = t \circ F$. The map $t \circ F = 0$, since $t \circ F(x) = t(x^q) = qx^{q-1}t(x) = 0$ for all $x \in \mathfrak{m}_P/\mathfrak{m}_P^2$. Hence $(dF)_P = 0$.

□

Relation of the Frobenius map with the Zeta function

In the following proposition, we will see that we can describe the number of $\mathbb{F}_{q^m}$-rational points $|X(\mathbb{F}_{q^m})|$ in terms of the trace of Frobenius.

Proposition 2.4.8. *Let $X/\mathbb{F}_q$ be a curve and let $\overline{X} = X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})$. Then for any $m \geq 1$*

$$|X(\mathbb{F}_{q^m})| = \sum_{r=0}^{2} (-1)^r \mathrm{Tr}\big(F^m | H^r(\overline{X}, \mathbb{Q}_l)\big).$$

Proof. This application of the previous lemma with the Lefschetz Fixed-Point Formula. Note that the F^m is the Frobenius map of the curve $X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F}_{q^m})$ and then by lemma 2.4.7 we have that $(\Gamma_{F^m} \cdot \Delta) = X(\mathbb{F}_{q^m})$. If we combine this with Theorem 2.4.2 we obtain the assertain. □

Before we connect this all to the Zeta function Z_X, we need one more elementary lemma about vector spaces.

Lemma 2.4.9. *Let $\varphi : V \to V$ be an endomorphism of a vector space over a field k and let $P_\varphi(T) = \det(1 - \varphi T | V)$ be the characteristic polynomial of φ. If we write $P_\varphi(T) = \prod_i (1 - c_i T)$ then*

$$\log \frac{1}{P_\varphi(T)} = \sum_{i=1}^{\infty} \mathrm{Tr}(\varphi^m | V) \frac{T^m}{m}$$

Proof. We may assume after possibly extending k that there exists a basis of V such that the matrix of φ is upper triangular and has the c_i's on the diagonal. Now it is clear that the matrix of φ^m is also upper triangular and has the c_i^m's on the diagonal. We see that

$$\log\Big(\frac{1}{1 - c_i T}\Big) = -\log(1 - c_i T) = -\sum_{i=1}^{m} c_i^m \frac{T^m}{m}.$$

If we now sum on both sides by i, we get the result that we wanted. □

Theorem 2.4.10. *Let $X/\mathbb{F}_q$ be a curve and let $\overline{X} = X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})$. We have*

$$Z_X(T) = \frac{P_1(T)}{P_0(T) P_2(T)},$$

where $P_r(T) = \det\big(1 - FT | H^r(\overline{X}, \mathbb{Q}_l)\big)$.

Proof. We have

$$\begin{aligned} Z_X(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} |X(\mathbb{F}_{q^n})|\right) \\ &= \exp\left(\sum_{n=1}^{\infty} \Big(\sum_{r=0}^{2} (-1)^r \mathrm{Tr}\big(F^n | H^r(\overline{X}, \mathbb{Q}_l)\big)\Big) \frac{T^n}{n}\right) \qquad (2.4.8) \\ &= \prod_{r=0}^{2} \left(\exp\Big(\sum_{n=1}^{\infty} \mathrm{Tr}\big(F^n | H^r(\overline{X}, \mathbb{Q}_l)\big) \frac{T^n}{n}\Big)\right)^{(-1)^r} \qquad \text{(Moving inner sum outside)} \\ &= \prod_{r=0}^{2} P_r(T)^{(-1)^{r+1}} \qquad (2.4.9) \end{aligned}$$

□

Remark 2.4.11. By Remark 24.2(f) of [Mil13], we have that F^* acts as the identity on $H^0(\overline{X}, \mathbb{Q}_l)$ and on $H^2(\overline{X}, \mathbb{Q}_l)$ as the multiplication by the degree of F, which by lemma 2.4.6 is multiplication by q. So we have that

$$Z_X(T) = \frac{P_1(T)}{(1-T)(1-qT)}$$

and so we have that $L(T) = P_1(T)$. We can now describe the inverse roots of $L(T)$ as eigenvalues of Frobenius on $H^1(\overline{X}, \mathbb{Q}_l)$.

This gives us the following corollary, which is called the Lefschetz trace formula.

Corollary 2.4.12 (Lefschetz trace formula)**.** Let $X/\mathbb{F}_q$ be curve of genus g and let α_i be the eigenvalues of Frobenius on $H^1(\overline{X}, \mathbb{Q}_l)$. Then

$$|X(\mathbb{F}_{q^m})| = 1 + q^m - \sum_{i=1}^{2g} \alpha_i^m.$$

Proof. If we combine Proposition 2.4.8 with the remark above, we see that

$$|X(\mathbb{F}_{q^m})| = 1 + q^m - \mathrm{Tr}\big(F^m | H^1(\overline{X}, \mathbb{Q}_l)\big).$$

Then by Lemma 2.4.9 and the remark above, we have

$$|X(\mathbb{F}_{q^m})| = 1 + q^m - \sum_{i=1}^{2g} \alpha_i^m.$$

□

Chapter 3

Space filling curves in their Jacobian

In this chapter we look at space filling curves. In the first part of this chapter, we will define space filling curves and we will see that curves are in most cases not space filling. In the second part of this chapter we will do the same, but then with almost space filling curves. Our exposition is based on [Sti17].

Let $X/\mathbb{F}_q$ be a curve of genus $g \geq 2$ and suppose that X has a $\mathbb{F}_q$-rational point. Let $(\alpha_i)_i$ be the eigenvalues of Frobenius on $H^1(\overline{X}, \mathbb{Q}_l)$ with $\alpha_{i+g} = q/\alpha_i$.

3.1 Space filling curves

In this section we will show that a curve can be space filling only if it has genus 2 and if it is defined over $\mathbb{F}_2$. By the Albanese embedding $X \to J$ (see Proposition 1.3.9), we have

$$N := |X(\mathbb{F}_q)| \leq |J(\mathbb{F}_q)| = h.$$

Definition 3.1.1. Let $X/\mathbb{F}_q$ be a curve of genus $g \geq 2$ with a $\mathbb{F}_q$-rational point and let J be its Jacobian. Then a curve is called space filling in its Jacobian or simply space filling if $|X(\mathbb{F}_q)| = |J(\mathbb{F}_q)|$.

The first question one can ask is how likely it is that a curve is space filling. For every curve of genus g, we know that the Jacobian of the curve is g dimensional. Intuitively we would expect that a higher dimensional variety has more rational points than lower dimensional variety. So we can say that in most situations it is unlikely that a curve is space filling. We will now show that there are only space filling curves in specific conditions.

Recall from chapter 2, that D_n is the number of effective divisors of degree n on X. If we combine the equations 2.6 and 2.9, we see that

$$h \geq \frac{(q-1)^2}{(g+1)(q+1)-N}\left(\sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n\right). \tag{3.1}$$

Observe that $D_0 = 1$ and $D_n \geq N$ for $n \geq 1$. By this observation, we obtain the following lower bound for h:

$$h \geq (q-1)^2 \frac{1 + q^{g-1} + N\left(g - 2 + \frac{q^{g-1}-1}{q-1}\right)}{(g+1)(q+1)-N}. \tag{3.2}$$

We want to know when a curve is space filling. Write B for the right hand side of 3.2. We will rewrite the inequality $B > N$ and look for which g and q this inequality holds. Of course if $B > N$, then we know that the curve is not space filling. Let $n = N/(q-1)$, then $B > N$ is equivalent to

$$1 + q^{g-1} + n\big((g-2)(q-1) + q^{g-1} - 1\big) > n\Big((g+1)\frac{q+1}{q-1} - n\Big), \tag{3.3}$$

which can be rewritten as

$$n^2 + n\left(q^{g-1} + (g-2)(q-1) - 1 - (g+1)\cdot\frac{q+1}{q-1}\right) + 1 + q^{g-1} > 0.$$

Let a be the linear term of n in the above equation. We can rewrite a as follows

$$\begin{aligned} a &= q^{g-1} + (g-2)\big(q - 1 - \frac{q+1}{q-1}\big) - 1 - 3\frac{q+1}{q-1} \\ &= q^{g-1} + q(g-2)\big(1 - \frac{2}{q-1}\big) - 4 - \frac{6}{q-1} \end{aligned}$$

So we see that $B > N$ is equivalent to

$$n^2 + n\left(q^{g-1} + q(g-2)\big(1 - \frac{2}{q-1}\big) - 4 - \frac{6}{q-1}\right) + 1 + q^{g-1} > 0 \tag{3.4}$$

The linear coefficient of 3.4 is monotone increasing as function in g and q for all $g \geq 3$ and $q \geq 3$. If $g = q = 3$, then the linear coefficient is 2. Hence we see that inequality of 3.4 always holds for $q \geq 3$ and $g \geq 3$. So a curve $X/\mathbb{F}_q$ can be space filling only if $g = 2$ or $q = 2$.

The case of genus 2

A curve of genus 2 is general not space filling. We will show that such a curve can be space filling only if $q = 2$.

For $g = 2$, the inequality 3.4 can be written as follows

$$n^2 + n(q - 4 - \frac{6}{q-1}) + 1 + q > 0. \tag{3.5}$$

The left hand side of 3.5 is equal to

$$(n-2)^2 + n\frac{(q-1)(q-4) - 6}{q-1} + q - 3 = (n-2)^2 + n\frac{(q+2)(q-3)}{q-1} + q - 3.$$

Therefore the inequality 3.5 is equivalent to

$$(n-2)^2 + n\frac{(q+2)(q-3)}{q-1} + q - 3 > 0.$$

We see that this inequality holds for $n \geq 0$ and $q \geq 4$ and for $q = 3$ if $n \neq 2$. So if $h = N$ then we have $q = 2$ or we have $q = 3$ with $n = 2$ and hence $N = 4$. We will show that the latter is not possible.

The L-polynomial can be written in terms of the elementary symmetric polynomials. In the next lemma, we obtain the following relation of the elementary symmetric polynomials of the α_i. We denote $\sigma_k(\alpha)$ to be the k-th elementary symmetric polynomial of the α_i.

Lemma 3.1.2. *Let $X/\mathbb{F}_q$ be a curve of genus g. Then*

$$\sigma_{2g-k}(\alpha) = q^{g-k}\sigma_k(\alpha)$$

Proof. We observe that $\prod_i \alpha_i = q^g$ and

$$\sigma_{2g-r}(\alpha) = \sum_{i_1<\cdots<i_{2g-r}} \alpha_{i_1}\cdots\alpha_{i_{2g-r}} = \sum_{i_1<\cdots<i_r} \prod_{k\notin\{i_1,\ldots,i_r\}} \alpha_k.$$

Then we can write

$$\begin{aligned}\sigma_{2g-r}(\alpha) &= \sum_{i_1<\cdots<i_k} q^g/(\alpha_{i_1}\cdots\alpha_{i_r}) \\ &= q^{g-r}\sum_{i_1<\cdots<i_r} (q/\alpha_{i_1})\cdots(q/\alpha_{i_r}) \\ &= q^{g-r}\sum_{i_1<\cdots<i_r} \alpha_{i_1}\cdots\alpha_{i_r} = q^{g-r}\sigma_r(\alpha).\end{aligned}$$

□

We can now write the L-polynomial of X for $g = 2$ as

$$L(T) = 1 - \sigma_1(\alpha)T + \sigma_2(\alpha)T^2 - q\sigma_1(\alpha)T^3 + q^2T^4.$$

Let $S_m = \sum_i \alpha_i^m$, then the Lefschetz trace formula gives us

$$S_m = 1 + q^m - |X(\mathbb{F}_{q^m})|.$$

Note that $\sigma_1(\alpha) = S_1$ and $2\sigma_2(\alpha) = S_1^2 - S_2$. Recall from Theorem 2.1.5, that $L(1) = h$ and therefore we have

$$\begin{aligned}h = L(1) &= 1 + q^2 - (1+q)(1+q-N) + \frac{1}{2}\Big((1+q-N)^2 - (1+q^2) + |X(\mathbb{F}_{q^2})|\Big) \\ &= 1 - 2q + (1+q)N + \frac{1}{2}\Big(2q - 2(1+q)N + N^2 + |X(\mathbb{F}_{q^2})|\Big) \\ &= -q + \frac{1}{2}\big(N^2 + |X(\mathbb{F}_{q^2})|\big).\end{aligned}$$

Note that $|X(\mathbb{F}_{q^2})| \geq N$ and if $h = N$, we obtain by the computation above that

$$2q = N^2 + |X(\mathbb{F}_{q^2})| - 2N \geq N^2 - N.$$

But this is impossible for $N = 4$ and $q = 3$.

The conclusion of this discussion is that a curve of genus 2 can be space filling only if $q = 2$.

The case $q = 2$ and large genus

For $q = 2$, the inequality 3.4 can be written as

$$n^2 + n(2^{g-1} - 2g - 6) + 1 + 2^{g-1} > 0.$$

This inequality holds for $n \geq 0$ and $g \geq 5$ and for $g = 4$ if $n \neq 3$. Hence if $h = N$, then $g = 2$ or $g = 3$, or we have $g = 4$ and $N = n = 3$. We will show that the latter is not possible. If $g = 4$ and $N = 3$, then 3.2 is an equality. Note that we obtained 3.2 by combining 3.1 and the assumption that $D_n \geq N$ for $n \geq 1$. In particular, we find that equality 3.2 can hold only if $D_2 = N$. But this is impossible, since we can make a sharper bound

$$D_2 \geq \frac{N(N+1)}{2} > N.$$

This bound is given by the following fact. Suppose that $P_1, \cdots, P_N$ are rational points, then $P_i + P_j$ is a degree 2 divisor on X. The number of such divisors is the number of pairs (i, j) with $1 \leq i < j \leq N$. One can easily see that the number of these pairs is equal to $\frac{N(N+1)}{2}$.

The conclusion of this discussion is that a curve can be space filling only if the genus is 2 or 3.

The case of genus 3 and $q = 2$

To simplify notation, we will abbreviate $N_m := |X(\mathbb{F}_{q^m})|$. We continue to write N for $N_1 = |X(\mathbb{F}_q)|$.

As in the case of genus 2, the L-polynomial can be written in terms of the elementary symmetric polynomials $\sigma_i(\alpha)$. The relation, given by lemma 3.1.2, gives us a formula for the class number h of X.

$$h = L(1) = 9 - 5\sigma_1(\alpha) + 3\sigma_2(\alpha) - \sigma_3(\alpha). \tag{3.6}$$

In the next lemma we will see that we can write the elementary symmetric polynomials in terms of the number of $\mathbb{F}_{q^m}$-rational points of X.

Lemma 3.1.3. *Let $(\alpha_i)_i$ be the eigenvalues of Frobenius on $H(\overline{X}, \mathbb{Q}_l)$. Then*

$$\begin{aligned}
\sigma_1(\alpha) &= S_1 = 1 + q - N, \\
\sigma_2(\alpha) &= q - (1+q)N + (N^2 + N_2)/2, \\
\sigma_3(\alpha) &= \frac{1}{3}\left(1 + q^3 - N_3 + (1 - q - N)\Big(-1 + q - q^2 - (1+q)N + \frac{N^2 + 3N_2}{2}\Big)\right).
\end{aligned}$$

Proof. The first equality follows from the Lefschetz trace formula. Observe that $\sigma_2(\alpha) = (S_1^2 - S_2)/2$ and if we combine this with the Lefschetz trace formula, we see that

$$\begin{aligned}
\sigma_2(\alpha) &= \frac{1}{2}\big((1 - q - N)^2 - 1 - q^2 + N_2\big) \\
&= \frac{1}{2}\big(2q - 2(1+q)N + N^2 + N_2 \\
&= q - (1+q)N + (N^2 + N_2)/2.
\end{aligned}$$

For the last statement, we have the following relation

$$\begin{aligned}
6\sigma_3(\alpha) &= \sum_i \alpha_i \sum_{j\neq i} \alpha_j \sum_{i\neq k\neq j} \alpha_k \\
&= S_1^3 - \sum_i \alpha_i^2 \sum_k \alpha_k - \sum_i \alpha_i^2 \sum_{j\neq i} \alpha_j - \sum_i \alpha_i \sum_{j\neq i} \alpha_j^2 \\
&= S_1^3 - S_2S_1 - (S_2S_1 - S_3) - (S_2S_1 - S_3) = 2S_3 + S_1(S_1^2 - 3S_2) \\
&= 2\left(1 + q^3 - N_3 + (1 - q - N)\Big(-1 + q - q^2 - (1+q)N + \frac{N^2 + 3N_2}{2}\Big)\right),
\end{aligned}$$

and this proves the statement. □

As a result of the lemma and 3.6, the class number can be written as

$$h = -2 + \frac{N_3}{3} + \frac{N_2 N}{2} + \frac{N^3}{6}. \tag{3.7}$$

The next remark and lemma will give us another description of the $\mathbb{F}_{q^m}$-rational points. This will lead to a new formula for the class number.

Remark 3.1.4.
1. If x is a closed point of X, then the residue field $\kappa(x) = \mathcal{O}_{X,x}/m_x$ is a finite field extension of the field $\mathbb{F}_q$ with $\deg(x) = [\kappa(x) : \mathbb{F}_q]$.
2. If P is a $\mathbb{F}_{q^m}$-rational point of X with image $x \in X$. Then P corresponds to a $\mathbb{F}_q$-homomorphism $\kappa(x) \to \mathbb{F}_{q^m}$, where $\kappa(x)$ is the residue field of x.

Lemma 3.1.5. *Let X be a curve and let $X_m(x)$ be the number of $\mathbb{F}_q$-homomorphisms $\kappa(x) \to \mathbb{F}_{q^m}$. Then*

$$X_m(x) = \begin{cases} \deg(x) & \text{if } \deg(x) | m \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By the previous remark, we see that $\kappa(x) \cong \mathbb{F}_{q^{\deg(x)}}$ We know from field theory that there exists a field homomorphism from $\mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ if and only if n divide m. So if the degree of x does not divide m, then $X_m(x) = 0$.

If $\deg(x)$ divides m, then this gives an embedding of $\mathbb{F}_{q^{\deg(x)}}$ in $\mathbb{F}_{q^m}$. Note that the number of embeddings is equal to the number of automorphism of $\mathbb{F}_{q^{\deg(x)}}$ and there are $\deg(x)$ automorphisms of $\mathbb{F}_{q^{\deg(x)}}$. □

Now we can write $N_2 = 2n_2 + N$ and $N_3 = 3n_3 + N$, where $n_i = |\{x \in X; \deg(x) = i\}|$, so the formula for the class number becomes

$$h = n_3 + Nn_2 + \frac{1}{6}N(N-2)(N+5).$$

If $N \geq 3$, then $(N-2)(N+5) > 6$ and therefore $h > N$. It is easy to check that the triples (N, n_2, n_3) for which $h = N$ are $(1,1,1)$, $(1,2,0)$, $(1,0,2)$, $(2,0,2)$ and $(2,1,0)$

The L-polynomial can be determined for each triple. We have written a programme in magma, that computes the real roots of each corresponding L-polynomial. See the appendix $A.1$ for more details about the magma programme. By the programme, all the corresponding L-polynomials have two real roots and their real roots are not of absolute value $\frac{1}{\sqrt{2}}$.

The conclusion of this discussion is that a curve can be space filling only if $q = 2$ and $g = 2$.

3.2 Almost space filling curves

In this section we will show that a curve can be almost space filling only if it has a small genus and if it can be defined over $\mathbb{F}_q$ for a small q. We will do the same approach as in section 3.1. We first define almost space filling curves.

Definition 3.2.1. Let $X/\mathbb{F}_q$ be a curve of genus $g \geq 2$ with a $\mathbb{F}_q$-rational point and let J be its Jacobian. Then a curve is called almost space filling in its Jacobian or simply almost space filling if $|J(\mathbb{F}_q)| = |X(\mathbb{F}_q)| + 1$.

We have seen that a curve is space filling only if it is defined over $\mathbb{F}_2$ and if it has genus 2. We could wonder when a curve is almost space filling. We will see in this section, that there are more cases, where a curve can be almost space filling then where it can be space filling. But by the same argument as we have made for space filling curves, we could say that in general it is still unlikely that a curve is almost space filling.

To prove that in most cases a curve is not almost space filling, we will do a similar approach to space filling curves. As in section 3.1, we will look at when $B > N + 1$ (where we recall that B is defined to be the right hand side of equation 3.2), and we see that $B > N + 1$ is equivalent to

$$1 + q^{g-1} + n\big((g-2)(q-1) + q^{g-1} - 1\big) > n\Big((g+1)\frac{q+1}{q-1} - n\Big) - \frac{n}{q-1} + \frac{(g+1)(q+1)}{(q-1)^2},$$

Since 3.3 and 3.4 are equivalent, we see that the equation above is equivalent to

$$n^2 + n\left(q^{g-1} + q(g-2)\big(1 - \frac{2}{q-1}\big) - 4 - \frac{6}{q-1}\right) + 1 + q^{g-1} > \frac{g+1}{q-1} + \frac{2(g+1)}{(q-1)^2} - \frac{n}{q-1}.$$

This gives that $B > N + 1$ is equivalent to

$$n^2 + n\left(q^{g-1} + q(g-2)\big(1 - \frac{2}{q-1}\big) - 4 - \frac{5}{q-1}\right) + 1 + q^{g-1} - \frac{g+1}{q-1} - \frac{2(g+1)}{(q-1)^2} > 0 \quad (3.8)$$

We see that the linear term and the constant term are monotone increasing functions for all $q \geq 3$ and $g \geq 3$. For $g = q = 3$, both the linear term and the constant term are positive. Therefore a curve can be almost space filling only if $q = 2$ or $g = 2$.

The case of genus 2

In contrast to the case of space filling curves, we will see that a curve can be also almost space filling if $q = 3$. For $g = 2$, we can write the inequality 3.8 as

$$n^2 + n\Big(q - 4 - \frac{5}{q-1}\Big) + 1 + q - \frac{3}{q-1} - \frac{6}{(q-1)^2} > 0. \quad (3.9)$$

The linear term and the constant term are both monotone increasing functions for $q \geq 2$. That gives that the left hand side is a increasing function for $q \geq 2$ and $n \geq 0$. Note that the inequality 3.9 for $q = 4$ holds for all $n \geq 0$. So we see that the inequality holds for all $q \geq 4$ and $n \geq 0$.

The conclusion of this discussion is that a curve with genus 2 can be almost space filling only if $q = 2$ or $q = 3$.

The case of q=2

In contrast to the case of space filling curves, we see that a curve is possibly almost space filling if the genus is 3. If $q = 2$, we can write the inequality 3.8 as

$$n^2 + n(2^{g-1} - 2g - 5) + 1 + 2^{g-1} - 3(g + 1) > 0. \tag{3.10}$$

The constant and linear term are monotone increasing for $g \geq 3$. For $g \geq 6$, the constant and linear coefficient are both positive. So the inequality holds for $g \geq 6$ and $n \geq 0$.

If $g = 5$, then the equality holds for $n \geq 1$. So if a curve of genus 5 is almost space filling, we have that $n = N = 0$, but that is in contradiction with the assumption that every almost space filling curve has a $\mathbb{F}_2$-rational point.

In the case that the genus is 4, we first show that X has one or two $\mathbb{F}_2$-rational points. To show this, we will look at the equation 3.1 for $g = 4$, $q = 2$ and $h = N + 1$. We can write this equation as

$$-N^2 + 14N + 15 \geq \sum_{n=0}^{2} D_n + \sum_{n=0}^{3} 2^{3-n} D_n. \tag{3.11}$$

Note that $D_0 = 1$, $D_1 = N$, $D_2 \geq \frac{N(N+1)}{2}$ and $D_3 > \frac{N(N+1)}{2}$. If we combine these estimations with 3.11, we see that

$$-N^2 + 14N + 15 > 9 + 7N + 2N^2.$$

This is equivalent to

$$-3N^2 + 7N + 6 > 0 \tag{3.12}$$

This shows that the equation only holds for $N = 1$ or $N = 2$. We can actually say that there are no almost space filling curves of genus 4.

Now we want to show that there are no almost space filling curves of genus 4. Note that by lemma 3.1.2, the class number can be written as

$$h = L(1) = 17 - 9\sigma_1(\alpha) + 5\sigma_2(\alpha) - 3\sigma_3(\alpha) + \sigma_4(\alpha)$$

We have seen in the case of space filling curves of genus 3, that we can write the symmetric polynomials $\sigma_i(\alpha)$ for $i \leq 3$ in terms of $\mathbb{F}_{q^m}$-rational points of X and Now we show that $\sigma_4(\alpha)$ can be written in terms of $S_i := 1 + q^i - N_i$ and hence in terms of the $\mathbb{F}_{2^i}$-rational points of X.

Lemma 3.2.2. *Let $(\alpha_i)_i$ be the eigenvalues of Frobenius on $H(\overline{X}, \mathbb{Q}_l)$. Then*

$$\sigma_4 = \frac{1}{24}(S_1^4 + 8S_3S_1 + 3S_2^2 - 6S_2S_1^2 - 6S_4).$$

Proof. We can write the elementary symmetric polynomial as

$$24\sigma_4(\alpha) = \sum_i \alpha_i \sum_{j \neq i} \alpha_j \sum_{i \neq k \neq j} \alpha_k \sum_{l \notin \{i,j,k\}} \alpha_l$$

Observe that

$$\sum_i \beta_i \sum_{j \neq i} \alpha_j = \sum_i \alpha_i \sum_{i \neq j} \beta_j.$$

So if $\beta_i = \alpha_i^2$, then we can say that

$$\sum_i \alpha_i \sum_{j \neq i} \alpha_j^2 = \sum_i \alpha_i^2 \sum_{j \neq i} \alpha_j.$$

So we have

$$\begin{aligned} 24\sigma_4(\alpha) &= S_1^4 - \Big(\sum_i \alpha_i^2 \sum_k \alpha_k \sum_l \alpha_l + 2 \sum_i \alpha_i^2 \sum_{j \neq i} \alpha_j \sum_l \alpha_l + 3 \sum_i \alpha_i^2 \sum_{i \neq j} \alpha_j \sum_{i \neq k \neq j} \alpha_k \Big) \\ &= S_1^4 - \Big(S_2 S_1^2 + 2(S_2 S_1^2 - S_3 S_1) + 3(S_2 S_1^2 - S_3 S_1 - S_3 S_1 + S_4 - S_2^2 + S_4 \Big) \\ &= S_1^4 + 8 S_3 S_1 + 3 S_2^2 - 6 S_2 S_1^2 - 6 S_4. \end{aligned}$$

□

This result gives us now the formula for the class number h, which is

$$h := \frac{N^4}{24} + \frac{N^2 N_2}{4} - N^2 + \frac{N N_3}{3} + \frac{N_2^2}{8} - N_2 + \frac{N_4}{4}.$$

We only have to look at, when $N = 1$ and $N = 2$. Like we did for the case of genus 3 for space filling curves, we can write $N_2 = 2n_2 + N$, $N_3 = 3n_3 + N$ and we have by lemma 3.1.5, that $N_4 = 4n_4 + 2n_2 + N$, where $n_i = |\{x \in X; \deg(x) = i\}|$. If $N = 2$, then we see that

$$h = \frac{n_2^2 + 3n_2}{2} + 2n_3 + n_4 - 1.$$

We want to know for which n_2, n_3 and n_4, we have that $h = N + 1 = 3$. The triples $(1, 1, 0)$, $(1, 0, 2)$, $(0, 2, 0)$, $(0, 1, 2)$ and $(0, 0, 4)$ are the triples (n_2, n_3, n_4) such that $h = N + 1 = 3$. We can determine for each triple the L-polynomial. Like in the case of genus 3 for space filling curve, we have written a programme in magma, that computes the real roots of each corresponding L-polynomial. We see that every corresponding L-polynomial has real roots and they are not of absolute value $\frac{1}{\sqrt{2}}$. See the appendix A.1 for more details about the magma programme. If $N = 1$, then the formula for the class number becomes

$$h := \frac{n_2^2 - n_2}{2} + n_3 + n_4 - 1.$$

For each triple (n_2, n_3, n_4), where $h = N + 1 = 2$, we have that $n_2, n_3, n_4 \leq 3$. So we look at all triples (n_2, n_3, n_4) with $n_2, n_3, n_4 \leq 3$ and if $h = 2$, then we look at the real roots of the corresponding L-polynomial. We see that all triples (n_2, n_3, n_4) such that $h = 2$ have real roots and they are not of absolute value $\frac{1}{\sqrt{2}}$. So there are no space filling curves of genus 4. See the appendix A.1 for more information about the computations in magma.

The conclusion of this discussion is that a curve over $\mathbb{F}_2$ can be almost space filling only if the genus is 2 or 3.

Chapter 4

Computations on space filling curves

In the last chapter we have seen that a curve can be (almost) space filling only if it has small genus and if it is defined over $\mathbb{F}_q$ for small q. We want to know if (almost) space filling curves also really exist. To show this, we will use computer programmes in magma. In this chapter we will first give a general description of all curves that are possibly (almost) space filling. In the next section we will look at the algorithms that we have used for the computations of the (almost) space filling curves and give some explanations about the algorithm. In the last section we give a list of all (almost) space filling curves up to isomorphism. The implementations of the algorithms in magma can be read in the Appendix.

4.1 Description of curves

In this section we will give a description of the curves that are possibly (almost) space filling. In general it is hard to give a description of all the curves of a given genus g. But we have seen in chapter 3 that curves can be (almost) space filling only if they have genus ≤ 3 and if they are defined over $\mathbb{F}_2$ or $\mathbb{F}_3$. We will consider two type of curves: hyperelliptic curves and non-hyperelliptic curves. The hyperelliptic curves can be described by a simple equation. Since the genus is ≤ 3, we can also describe the non-hyperelliptic curves in an easy way. First we will look at hyperelliptic curves.

Hyperelliptic curves

We will show that every hyperelliptic curve can be described by a simple equation. We will furthermore show when two such equations define isomorphic curves. We refer to section 7.4 [Liu02] for more details and proofs about hyperelliptic curves.

Definition 4.1.1. A curve X/k of genus $g \geq 2$ is called hyperelliptic if there exists finite morphism $\varphi : X \to \mathbb{P}^1_k$ of degree 2.

Let $\varphi : X \to \mathbb{P}^1_k$ be a finite morphism of degree 2. Then φ is separable. Otherwise we have that φ is purely inseparable and then by proposition 7.4.21 of [Liu02], we have that the genus of X is 0, which is in contradiction with the genus of X is greater than 1.

Let X/k be a hyperelliptic curve of genus g. We have a separable morphism $\varphi : X \to Y = \mathbb{P}^1$ of degree 2. Before we state the following proposition, we will first introduce some notation. We can write Y as $U \cup V$, where $U = \mathrm{Spec}(k[t])$ and $V = \mathrm{Spec}(k[s])$ with $s = 1/t$ on the intersection of $U \cap V$. Let $U' = \varphi^{-1}(U)$ and $V' = \varphi^{-1}(V)$.

Proposition 4.1.2. *Let X/k be a hyperelliptic curve with genus g. Then $k(X)$ is isomorphic to the fraction field of*

$$k(t)[y]/(y^2 + h(t)y - f(t)),$$

where $f(t), h(t) \in k[t]$ and

$$2g + 1 \leq \max\big(2 \cdot \deg(h(t)), \deg(f(t))\big) \leq 2g + 2.$$

In the next remark we will first give some facts, that we need for the proof of the proposition.

Remark 4.1.3.

1. Let $\varphi : X \to Y$ be the separable morphism from above. Then the sequence
$$0 \longrightarrow \varphi^*\Omega^1_{Y/k} \longrightarrow \Omega^1_{X/k} \longrightarrow \Omega^1_{X/Y} \longrightarrow 0$$
is exact.
2. The dimension of $H^0(X, \Omega^1_{X/Y})$ is $2g + 2$, where g is the genus of the curve X.
3. Let X be a curve and let $\kappa(x)$ be the residue field of x. If $\mathcal{L}$ is a coherent sheaf, with
$$\dim_{\kappa(x)} \mathcal{L}_x \otimes_{\mathcal{O}_{X,x}} \kappa(x) = n$$
for all $x \in X$, then $\mathcal{L}$ is locally free of rank n.

Proof. We will first prove the case, where the characteristic of k is 2. The morphism $\varphi : X \to Y$ gives us the following exact sequence

$$0 \longrightarrow \mathcal{O}_Y \longrightarrow \varphi_*\mathcal{O}_X \longrightarrow \mathcal{L} \longrightarrow 0 \tag{4.1}$$

for a coherent sheaf $\mathcal{L}$. By [Liu02], corollary 3.4.10, φ is a flat morphism. So $\varphi_*\mathcal{O}_X$ is locally free of rank 2. Let $\kappa(y)$ be the residue field for a point $y \in Y$. Note that the morphism $\kappa(y) \to \varphi_*\mathcal{O}_X \otimes_{\mathcal{O}_Y} \kappa(y)$ is injective for every $y \in Y$. Hence for every $y \in Y$ we obtain the exact sequence

$$0 \longrightarrow \kappa(y) \longrightarrow \varphi_*\mathcal{O}_X \otimes_{\mathcal{O}_Y} \kappa(y) \longrightarrow \mathcal{L} \otimes_{\mathcal{O}_Y} \kappa(y) \longrightarrow 0\ .$$

We see by remark 4.1.3, that $\mathcal{L}$ is locally free of rank 1. Since we have that $\mathcal{O}_Y(U)$ is a principal ideal domain, we get that $\mathcal{L}|_U$ is free of rank 1. That means that the sequence 4.1 is split exact over U. So we can write

$$\mathcal{O}_X(U') = \mathcal{O}_Y(U) \oplus \mathcal{O}_Y(U)y,$$

for a $y \in \mathcal{O}_X(U')$. The same is true for V, so we have

$$\mathcal{O}_X(V') = \mathcal{O}_Y(V) \oplus \mathcal{O}_Y(V)z$$

for a $z \in \mathcal{O}_X(V')$.

Consequently, we have two bases $\{1, y\}$ and $\{1, z\}$ of $\mathcal{O}_X(U' \cap V')$ over $\mathcal{O}_X(U \cap V)$. We have $\mathcal{O}_Y^*(U \cap V) = k^* t^{\mathbb{Z}}$, and after a possible multiplication of z by an element of k^*, we can write

$$y = R(t) + H(s) + t^r z,$$

with $R(t) \in k[t]$ and $H(s) \in k[s]$. If $r < 1$, then $y - R(t)$ glues to a global section and so $y - R(t) \in H^0(X, \mathcal{O}_X) = k$. Hence $r \geq 1$. We can write $y - R(t) = t^r(s^r H(s) + z)$. It is easy to see that we can modify y and z in such a way that $y = t^r z$. This gives us the following two equations

$$y^2 + h(t)y = f(t), \quad f(t), h(t) \in k[t]. \tag{4.2}$$

and

$$z^2 + (h(t)/t^r)z = f(t)/t^{2r}. \tag{4.3}$$

Note that z is integral over $k[s]$. So we see that $\deg(h(t)) \leq r$ and $\deg(f(t)) \leq 2r$.

We want to know the number r. To compute this, we compute the space $H^0(X, \Omega^1_{X/Y})$. We have

$$\Omega^1_{U'/U} = \mathcal{O}_X(U')dy/(h(t)dy) \cong k[t, y]/(h(t), y^2 - f(t)),$$

and

$$\Omega^1_{V/V'} = \mathcal{O}_X(V')dz/(s^r h(1/s)dz) \cong k[s, z]/(s^r h(1/s), z^2 - f(1/s)s^{2r}).$$

The support of $\Omega^1_{X/Y}$ consists of the ramification points. Almost all ramification points are in the support of $\Omega^1_{U'/U}$. Only the points on the fibre of the point $(1 : 0)$ are not in the support of $\Omega^1_{U'/U}$. So we have

$$H^0(X, \Omega^1_{X/Y}) = k[t, y]/(h(t)) \oplus k[s, z]_{\mathfrak{m}}/(s^r(h(1/s)),$$

where $\mathfrak{m} = sk[y, s]$ and see that $h^0(X, \Omega^1(X/Y)) = 2 \cdot \deg(h(t)) + 2(r - \deg(h(t)) = 2r$. Hence $r = q + 1$. If $\deg(h(t)) < g + 1$, then the degree of $f(t)$ is $2g + 1$ or $2g + 2$, otherwise the point above $(1 : 0)$ in X is singular.

Suppose now that $\mathrm{Char}(k) \neq 2$. Although the construction before the computations of $H^0(X, \Omega^1_{X/Y})$ works also for this case, we can do it better. If we modify y and z, we can assume that $h(t) = 0$, because 2 is invertible. Since X is smooth, we can also assume that $f(t)$ is separable. So we have $y^2 = f(t)$ and $z^2 = f(t)/t^{2r}$. Now we compute r in the same way as the case of characteristic 2. We see that

$$\Omega^1_{U'/U} = \mathcal{O}_X(U')dy/(2ydy) \cong k[t, y]/(y^2 - f(t), y) = k[t]/(f(t))$$

and also $\Omega_{V'/V} = k[s]/(s^{2r} f(1/s))$. So we have that

$$H^0(X, \Omega^1_{X/Y}) = k[t]/(f(t) \oplus k[s]_{\mathfrak{m}}/(s^{2r} f(1/s)).$$

Since $f(t)$ and $s^{2r} f(1/s)$ are both separable, we have that $\deg(f(t))$ is $2r$ or $2r - 1$. We see that if $\deg(f(t)) = 2r$, then $s^{2r} f(1/s) \neq 0$ and hence the second term is of dimension 0. So we have $r = q + 1$. If $\deg(f(t)) = 2r - 1$, then the second term is of dimension 1. So we get that $\deg(f(t)) = 2g + 1$ or $2g + 2$. $\square$

Remark 4.1.4. Let X and Y be two hyperelliptic curves. Note that if $k(X)$ and $k(Y)$ are isomorphic, then X and Y are birationally equivalent and since X and Y are projective and smooth, we have that X and Y are isomorphic.

Definition 4.1.5. We see by the previous proposition that $k(X)$ is the fraction field of $k[t,y]/(y^2+h(t)y-f(t))$ for $f(t),h(t)\in k[t]$ and where

$$2g+1\leq \max\big(\deg(f(t)),2\cdot\deg(h(t))\big)\leq 2g+2.$$

We call the equation $y^2+h(t)y=f(t)$ the hyperelliptic equation of X.

Remark 4.1.6. Let X be a hyperelliptic curve over a field k. Then smoothness can be checked on the hyperelliptic equation of X. Let $y^2+h(t)y=f(t)$ be a hyperelliptic equation of X. Let $h_1(s)=s^{g+1}h(1/s)$ and $f_1(s)=s^{2g+2}f(1/s)$.

If $\mathrm{Char}(k)\neq 2$, then X is smooth if $4f(t)+h(t)^2$ is a separable polynomial. If $\mathrm{Char}(k)=2$, then X is smooth if $h(t)$ and $h'(t)^2f(t)+f'(t)^2$ are coprime and $h_1'(0)^2f_1(0)+f_1'(0)^2\neq 0$ if $\deg(h)<g+1$.

We want know to show, when two hyperelliptic equations determine the same curve. First we will show that a separable map $\varphi:X\to\mathbb{P}^1_k$ of degree 2 is unique up to automorphism of $\mathbb{P}^1_k$.

Definition 4.1.7. Let X/k be a hyperelliptic curve. Then we have a separable morphism $\varphi:X\to\mathbb{P}^1_k$ of degree 2, which induces a Galois extension $k(X)|k(t)$. Now suppose that σ is the generator of $\mathrm{Gal}(k(X)|k(t))$. Then σ induces an automorphism of X of order 2, which we also denote by σ. We call this automorphism the hyperelliptic involution of X.

Proposition 4.1.8. *Suppose that X/k is a hyperelliptic curve with genus $g\geq 2$. Then the hyperelliptic involution of X is unique.*

Remark 4.1.9. The uniqueness of the hyperelliptic involution shows that $k(X)$ has a unique subfield of degree 2 that is isomorphic to $k(t)$. That means that a separable morphism $\varphi:X\to\mathbb{P}^1_k$ of degree 2 is unique up to automorphisms of X and $\mathbb{P}^1_k$.

Corollary 4.1.10. Let X/k be a hyperelliptic curve of genus $g\geq 2$. Let $\varphi:X\to\mathbb{P}^1_k$ be a separable morphism of degree 2. Suppose that σ is the hyperelliptic involution and τ is an automorphism. Then $\sigma\tau=\tau\sigma$ and τ induces an automorphism $\tilde{\tau}$ on $\mathbb{P}^1_k$. This gives the commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\tau} & X \\ \big\downarrow{\scriptstyle\varphi} & & \big\downarrow{\scriptstyle\varphi} \\ \mathbb{P}^1 & \xrightarrow{\tilde{\tau}} & \mathbb{P}^1 \end{array}.$$

Proof. Let $\tau'=\tau^{-1}\sigma\tau$. This is a hyperelliptic involution on X and by the previous proposition, we see that $\tau'=\sigma$ and hence $\sigma\tau=\tau\sigma$. The automorphisms τ, σ act on the field $k(X)$. Since τ and σ commute, we see that τ induces an automorphism on $k(X)^\sigma=k(t)$, which gives us an automorphism $\tilde{\tau}$ of $\mathbb{P}^1_k$ and we see that $\varphi\circ\tau=\tilde{\tau}\circ\varphi$. □

By this corollary, we see that every morphism $\varphi:X\to\mathbb{P}^1_k$ is unique up to automorphism of $\mathbb{P}^1_k$. In the next proposition, we will see that when two hyperelliptic curves are isomorphic.

Proposition 4.1.11. *Let X/k be a hyperelliptic curve of genus $g \geq 2$. Let $y^2 + h(t)y = f(t)$ be a hyperelliptic equation of X. Let $v^2 + q(u)v = p(u)$ be a equation with $q(u), p(u) \in k[u]$ and*

$$2g + 1 \leq \max(2 \cdot \deg(q), \deg(p)) \leq 2g + 2.$$

Then $v^2 + q(u)v = p(u)$ is a hyperelliptic equation of X if

$$u = \frac{at + b}{ct + d}, \quad v = \frac{r(t) + \alpha y}{(ct + d)^{g+1}}$$

such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k), \alpha \in k^*, r(t) \in k[t]$$

and $\deg(r(t)) \leq g + 1$.

For the proof, we refer to 7.4.33 of [Liu02]. We will only show how we can apply the theory about hyperelliptic involutation to this proposition. We will see if $v^2 + q(u)v = p(u)$ is a hyperelliptic equation of X, then we have that $k(u) \cong k(t)$ by remark 4.1.9. That means that $u = \frac{at+b}{ct+d}$. Then the only thing that is left to prove is that we can write $v = \frac{r(t)+\alpha y}{(ct+d)^{g+1}}$.

Non-hyperelliptic curves

We will show that non-hyperelliptic curves exists and that we can describe hyperelliptic curves of genus 3 in an easy way.

For every divisor D on X, we have a complete linear system $|D|$. If this linear system is base-point-free, then it gives a morphism from X to a projective space. We want to show that the divisor K gives a closed immersion into projective space if X is not hyperelliptic.

Definition 4.1.12. A divisor D is very ample if $\mathcal{O}_X(D)$ is very ample.

If a curve is defined over an algebraically closed field, then the following proposition gives us a criterion to check, when a complete linear system is base-point-free and when a divisor is very ample.

Proposition 4.1.13. *Let X be a curve over an algebraically closed field and let D be a divisor on X.*

1. *The complete linear system $|D|$ is base-point-free if and only if for all $P \in X$, we have*

$$h^0(X, \mathcal{O}_X(D)) - h^0(X, \mathcal{O}_X(D - P)) = 1$$

2. *The divisor D is very ample if and only if for all points $P, Q \in X$, we have*

$$h^0(X, \mathcal{O}_X(D)) - h^0(X, \mathcal{O}_X(D - P - Q) = 2.$$

For the proof see Prop IV.3.1 of [Har77]. We will now show that $|K|$ is base-point-free.

Proposition 4.1.14. *Let X/k be a curve with genus $g \geq 2$. Let K be the canonical divisor on X. The linear system $|K|$ is base-point-free.*

Proof. We may assume that k is algebraically closed by lemma 33.22.1 of [Sta20, Section 0B5W] and lemma II.7.8 of [Har77]. By the previous proposition, we see that $|K|$ is base-point-free if for all $P \in X$ we have

$$h^0(X, \mathcal{O}_X(K)) - h^0(X, \mathcal{O}_X(K - P)) = 1.$$

We know that $\mathcal{O}_X(P) = 1$ for all points P. So we see by Riemann-Roch that $h^0(X, \mathcal{O}_X(K - P)) = g - 1$ and this proves the proposition. □

By this proposition, we see that the canonical divisor gives us a morphism $\varphi : X \to \mathbb{P}^{g-1}$. In the following lemma, we will see that this morphism is even a closed embedding if X is non-hyperelliptic.

Proposition 4.1.15. *Let X be a curve with genus $g \geq 2$. Let K be the canonical divisor. Then the divisor K is very ample if and only if X is not hyperelliptic.*

Proof. We can check that φ is a closed embedding over an algebraic closure. We see then by proposition 4.1.13 that φ is a closed embedding if and only if

$$h^0(X, \mathcal{O}_X(K)) - h^0(X, \mathcal{O}_X(K - P - Q)) = 2$$

for all $P, Q \in X$. Riemann-Roch gives us

$$h^0(X, \mathcal{O}_X(K - P - Q)) = g - 3 + h^0(X, \mathcal{O}_X(P + Q))$$

for $P, Q \in X$. If φ is not a closed embedding, then there exists $P, Q \in X$ such that $h^0(X, \mathcal{O}_X(P + Q)) = 2$. We have found now a base-point-free linear system $|P + Q|$ of degree 2, this gives a degree 2 map to $\mathbb{P}^1$. So then X is hyperelliptic.

If $h^0(X, \mathcal{O}_X(P + Q)) = 1$ for all $P, Q \in X$, then we see that φ is a closed embedding and there does not exists a divisor D of degree 2 with $h^0(X, \mathcal{O}_X(D)) = 2$. By proposition 4.1.13 there is no base-point-free divisor D of degree 2. So there does not exist a degree 2 map to $\mathbb{P}^1$ and hence X is not hyperelliptic □

By this proposition we see that all curves of genus 2 are hyperelliptic. Let $\varphi : X \to \mathbb{P}^{g-1}$ be a morphism induced by the canonical divisor. If X is not hyperelliptic, then this morphism is called the canonical embedding. The canonical embedding is unique up to automorphisms of $\mathbb{P}^{g-1}$.

The canonical embedding gives us that every non-hyperelliptic curves with genus 3 are degree 4 curves in $\mathbb{P}^2$, because $\deg(K) = 4$.

Conversely, we claim that every plane curve X of degree 4 is canonically embedded.

For a plane curve, we have that

$$g = \frac{(d-1)(d-2)}{2},$$

where d is the degree of the plane curve. So we know that every plane curve X of degree 4 has genus 3. Let X be a plane curve of degree 4, then there exists a closed embedding $\varphi : X \to \mathbb{P}^2$. Suppose this map is induced by the divisor D. We have now that D is divisor of degree 4 and $h^0(X, \mathcal{O}_X(D)) = 4$. By Riemann-Roch we know that $h^0(X, \mathcal{O}_X(D))$ is 4 if and only if $D \cong K$. But that means that X is canonically embedded.

Since the canonical embedding is unique up to automorphism of $\mathbb{P}^2$, we have that two plane curves X, Y of degree 4 are isomorphic if there exists a projective transformation $A \in \mathrm{PGL}_3(k)$, such that $A(X) = Y$.

4.2 Algorithm for space filling curves

In this section we will give the algorithms, we will use to compute all the (almost) space filling curves.

We can divide the curves that are possibly (almost) space filling in the following three categories:

1. the hyperelliptic curves over $\mathbb{F}_2$,
2. the hyperelliptic curves over $\mathbb{F}_3$,
3. the non-hyperelliptic curves over $\mathbb{F}_2$ of genus 3,

The computations of the (almost) space filling curves consists of the same three steps. Although the algorithm of the first step will differ for the different categories.

The first step is called the enumeration step. In this step, we enumerate all the curves in the given category. For the hyperelliptic curves, the genus is part of the input. So we will only enumerate the hyperelliptic curves of the given genus.

The second step is called the check step. In this step, we check for all curves, that are enumerated, if they are (almost) space filling. We return all the curves that are (almost) space filling in a list.

The third step is called the result step. In this step, we return all the space filling curves up to isomorphism. So we choose one representative for every isomorphism class of curves.

4.2.1 Check step

For the check step, we are given a list, that consists of curves of a given category from above. We will return all the curves in the list that are (almost) space filling curves. In order to do this step, we have to compute two things: the number of rational points and the class number. All these curves can be embedded in projective space and so it is easy to check what the rational points are. The class number is computed by the L-polynomial. As we have seen in chapter 2, the class number of X is equal to $L(1)$. The L-polynomial can be written in terms of $X(\mathbb{F}_{q^n})$ for $n \leq g$ and this is easy to compute. In chapter 3, we have seen explicit examples for the computation of the L-polynomial in the case of genus 2 and 3.

The following algorithm gives the check step.

Algorithm 1: Check step

```
Input: Curves: a list that consists of curves; i ∈ {0, 1}.
Output: SpaceFillingCurves: a list that consists of all the curves in Curves, that are
  space filling if i = 0 and almost space filling if i = 1.
SpaceFillingCurves is an empty list;
for X in Curves do
    if the number of Rational Points of X is bigger then 1 then
        if the number of Rational Points of X + i = the class number of X then
            Add X to the list SpaceFillingCurves ;
return SpaceFillingCurves
```

This algorithm is actually very simple. It enumerates over all curves in Curves and checks if the curve is (almost) space filling or not by comparing the rational point of the

curve with the class number. If the curve is (almost) space filling, then the curve is added to the list SpaceFillingCurves. After we have checked all the curves, we see that the list SpaceFillingCurves consists of all curves that are (almost) space filling.

4.2.2 Result step

This algorithm works also in the more general setting, since magma can determine if two curves are isomorphic for most cases. However for the curves we are interested in, it is much more efficient then for a general curve.

Given a list of curves, we return all curves up to isomorphism. This means that we choose for every isomorphism class one representative.

We have the following algorithm.

Algorithm 2: Result Step

```
Input: Curves: a list that consists of curves.
Output: IsoCurves: a list that give all curves in Curves up to isomorphism.
IsoCurves is an empty list;
for X in Curves do
    ExistIso is false;
    for Y in IsoCurves do
        if The L-Polynomials of X and Y are the same then
            if X and Y are isomorphic then
                ExistIso := true ;
    if ExistIso is false then
        Add X to the list IsoCurves ;
return IsoCurves
```

By the algorithm we begin with an empty list IsoCurves. We want to know all curves up to isomorphism. We take some curve X in Curves and we want to know if X is isomorphic to a curve in IsoCurves. If this is the case, then we don't have to add it to the list IsoCurves, since we want all the curves up to isomorphism. If X is not isomorphic to any curve in IsoCurves, then we add X to the list IsoCurves.

Note that if we repeat this for all curves in Curves, then the list IsoCurves consists of all the curves in Curves up to isomorphism.

Before we check that a curve X in Curves is isomorphic to a Y in IsoCurves, we check if the L-Polynomials of X and Y are the same. If the L-Polynomials are not the same, then X and Y are automatically not isomorphic. If the L-Polynomials are the same, then X and Y are maybe not isomorphic. So we have to check if X and Y are isomorphic.

The reason, why we first check if the L-Polynomials are the same, is that the function in magma, that computes the L-Polynomial, is more efficient than the function, that computes if X and Y are isomorphic. This result in a shorter completion time. In the appendix A.2 one can read more about the implementations of this algorithm in magma.

4.3 The enumeration step

In this we will show the enumeration step for all the different categories. We will first start with the hyperelliptic curves over $\mathbb{F}_2$.

Hyperelliptic curves over $\mathbb{F}_2$

We have seen before that a hyperelliptic curve over $\mathbb{F}_2$ of genus g can be described by an equation

$$y^2 + h(x)y = f(x),$$

where

$$2g + 1 \leq \max\{2 \cdot \deg(h(x)), \deg(f(x))\} \leq 2g + 2.$$

We want to enumerate all hyperelliptic curves and these are by our convention 0.0.3 are all smooth. So we can assume that $h(x) \neq 0$ and $f(x) \neq 0$ by remark 4.1.6. For the enumeration of all the hyperelliptic curves we use the following algorithm.

Algorithm 3: Enumeration Step: Hyperelliptic curves over $\mathbb{F}_2$

Input: An integer g.
Output: HyperCurves: a list that consists of all smooth hyperelliptic curves over $\mathbb{F}_2$ of genus g.
HyperCurves is an empty list;
for *Polynomials* $f, h \in \mathbb{F}_2[x]$ *with* $0 \leq \deg(f) \leq 2g + 2$ *and* $0 \leq \deg(h) \leq g + 1$ **do**
    The curve H is defined by the equation $y^2 + h(x)y = f(x)$;
    if *The curve H is of genus g, smooth and hyperelliptic.* **then**
        Add H to the list HyperCurves;
return *HyperCurves*

This algorithm is pretty straightforward. We look at all curves that are defined by the equation $y^2 + h(t)y = f(t)$ with $0 \leq \deg(f), 2 \cdot \deg(h) \leq 2g + 2$ and look if they are smooth and hyperelliptic of genus g. If this is the case, we add the curve to the list HyperCurves. If we do this for all curves, the list HyperCurves consists of all hyperelliptic curves of genus g.

Hyperelliptic curves over $\mathbb{F}_3$

A hyperelliptic curve over $\mathbb{F}_3$ of genus g can be described by the equation $y^2 = f(t)$, where the degree of $f(t)$ is $2g + 1$ or $2g + 2$ as we have seen in the previous section. The algorithm will be similar to the Enumeration Step of the Hyperelliptic curves over $\mathbb{F}_2$.

Algorithm 4: Enumeration Step: Hyperelliptic curves over $\mathbb{F}_3$

Input: An integer g.
Output: HyperCurves: a list that consists of all hyperelliptic curves over $\mathbb{F}_3$ of genus g.
HyperCurves is an empty list;
for *Polynomials* $f \in \mathbb{F}_3[t]$ *with* $2g + 1 \leq \deg(f) \leq 2g + 2$ **do**
    The curve H is defined by the equation $y^2 = f(t)$;
    if *The curve H is of genus g, smooth and hyperelliptic.* **then**
        Add H to the list HyperCurves;
return *HyperCurves*

In this algorithm we look at all hyperelliptic curves over $\mathbb{F}_3$ of genus 3. These can be described by the equation $y^2 = f(t)$, where $2g + 1 \leq \deg(f(t)) \leq 2g + 2$. If the curve is of genus g, smooth and hyperelliptic, then add the curve to the list HyperCurves. After we did this for all curves, we return the list HyperCurves. It's easy to see that this consists of all hyperelliptic curves of genus 3 over $\mathbb{F}_3$.

Non-hyperelliptic curves of genus 3 over $\mathbb{F}_2$

As we have seen in the previous section, we can describe the non-hyperelliptic genus 3 curves as plane curves of degree 4.

We look at all homogeneous polynomials of degree 4 with 3 variables and check if the curves defined by these polynomials are irreducible and smooth. If the curve is irreducible and smooth, we add them to the list curves. If we do this for all curves, we obtain a list of all non-hyperelliptic curves of genus 3 over $\mathbb{F}_2$.

Algorithm 5: Enumeration Step: Non-hyperelliptic curves over $\mathbb{F}_2$ of genus 3

Input: none.
Output: Curves: a list that consists of all smooth irreducible curves over $\mathbb{F}_2$ of genus 3.
Curves is an empty list;
for *all homogeneous polynomials* $f \in \mathbb{F}_2[x, y, z]$ *of degree* 4 **do**
  Let X be the curve that is defined by polynomial f;
  if *The curve* X *is a smooth and irreducible.* **then**
    Add X to the list Curves;
return *Curves*

4.4 Results

With the algorithms we have seen in the previous section, we can compute all the (almost) space filling curves. The following table gives all space filling curves up to isomorphism.

g	N=h	L(t)	equation
2	1	$1-2t+2t^2-4t^3-4t^4$	$y^2+y=x^5+x^3+1$
2	2	$1-t-2t^3+4t^4$	$y^2+(x^2+1)y=x^5+1$

The following table gives all almost space filling curves up to isomorphism. We see that there are 5 almost space filling curves of genus 2, where 3 are defined over $\mathbb{F}_2$ and 2 are defined over $\mathbb{F}_3$. Furthermore there are 6 almost space filling curves of genus 3, where 3 are hyperelliptic and 3 are not hyperelliptic.

g	q	N+1=h	L(t)	equation
2	2	2	$1-2t+3t^2-4t^3-4t^4$	$y^2+(x^2+x+1)y=x^5+x+1$
2	2	3	$1-t+t^2-2t^3+4t^4$	$y^2+(x^3+x+1)y=1$
2	2	4	$1-t^2+4t^4$	$y^2+(x^2+x)y=x^5+1$
2	3	3	$1-2t+t^2-6t^3+9t^4$	$y^2=x^6+x^4+x^3+x^2+2x+2$
2	3	4	$1-t-2t^2-3t^3+9t^4$	$y^2=x^5+x^3+x^2+2x$
3	2	2	$1-2t+2t^2-3t^3+4t^4-8t^5+8t^6$	$y^2+(x^3+x^2+1)y=x^7+x+1$
3	2	2	$1-t^2-2t^3-2t^4+8t^6$	$y^2+(x^3+x^2)y=x^7+x+1$
3	2	4	$1-2t+3t^2-6t^3+6t^4-8t^5+8t^6$	$y^2+(x^2+x+1)y=x^7+x+1$
3	2	2	$1-2t+2t^4-8t^5+8t^6$	$x_1^4+x_1x_2^3+x_2^4+x_1^2x_3^2+x_1x_3^3$
3	2	3	$1-t-t^2+2t^3-2t^4-4t^5+8t^6$	$x_1^4+x_1x_2^3+x_2^4+x_1x_2^2x_3+x_1^2x_3^2+x_1x_3^3$
3	2	2	$1-2t+3t^3-8t^5+8t^6$	$x_1^4+x_1x_2^3+x_4+x_1^2x_2x_3+x_1^2x_3^2+x_1x_2x_3^2+x_1x_3^3$

Appendix A

Implementations in magma

In this section, we will look at the implementations of the algorithms, that we have discussed in chapter 4, in magma. We also look at the computations of the L-polynomial for genus 3 and 4. See [Can+06] for more details about the magma functions.

A.1 L-Polynomial function

In chapter 3, we have seen that for space filling curves in the case of genus 3 and $q = 2$, that we can write the L-polynomial in terms of the elementary symmetric polynomials $\sigma_1(\alpha)$, $\sigma_2(\alpha)$ and $\sigma_3(\alpha)$ and we have seen in lemma 3.1.3 a formula for the these symmetric polynomials in terms of the number of rational points of $X(\mathbb{F}_{q^n})$. We have seen a formula for the class number h and there are five triples (N, n_2, n_3) such that $h = N$. In the following function in magma, given such a triple it computes the real roots of the corresponding L-polynomial and we see that all these polynomials have real roots but the L-polynomial have at least one real root that has not absolute value $\frac{1}{\sqrt{2}}$.

```
LPolynomialGenus3 := function(N,n2,n3)
P<t> := PolynomialRing(RealField(5));
N2 := 2*n2+N;
N3 := 3*n3+N;
sigma1 := 3-N;
sigma2 := 2-3*N+1/2*(N^2+N2);
sigma3 := 1/3*(9-N3+(3-N)*(-3-3*N+1/2*(N^2+3*N2)));
L := 1-sigma1*t+sigma2*t^2-sigma3*t^3+2*sigma2*t^4
     -4*sigma1*t^5+8*t^6;
return(Roots(L));
end function;
```

The real numbers have a precision 5 digits, this is enough to see that the roots are not of absolute value $\frac{1}{\sqrt{2}}$.

The function LPolynomialGenus4 is very similar to the function LPolynomialGenus3. The L-polynomial in the case of genus 4 and $q = 2$, we can write in terms of the elementary symmetric polynomials $\sigma_1(\alpha)$, $\sigma_2(\alpha)$, $\sigma_3(\alpha)$ and $\sigma_4(\alpha)$. Also $\sigma_4(\alpha)$ can be written in terms of the rational points $X(\mathbb{F}_{q^n})$. We compute for 5 triples $(n2, n3, n4)$ and $N = 2$, the L-polynomial and see that all these polynomials has real roots, but not of absolute value $\frac{1}{\sqrt{2}}$.

```
LPolynomialGenus4 := function(N,n2,n3,n4)
P<t> := PolynomialRing(RealField(5));
N2 := 2*n2+N;
N3 := 3*n3+N;
N4 := 4*n4+2*n2+N;
sigma1 := 3-N;
sigma2 := 2-3*N+1/2*(N^2+N2);
sigma3 := 1/3*(9-N3+(3-N)*(-3-3*N+(1/2)*(N^2+3*N2)));
sigma4 := N^4/24-N^3/2+N^2*N2/4+N^2-3*N*N2/2+N*N3/3+N2^2/8+N2-N3+N4/4;
L := 1-sigma1*t+sigma2*t^2-sigma3*t^3+sigma4*t^4-2*sigma3*t^5
     +4*sigma2*t^6-8*sigma1*t^7+16*t^8;
return(Roots(L));
end function;
```

Suppose now that $N = 1$. We have seen a formula for the class number in terms of n_2, n_3 and n_4 and we have $h = 2$ only if $n_i \leq 3$. The function CheckPolynomial computes the L-polynomial if $h = N + 1$ an if this polynomial has no real roots or the real roots are of absolute value $\sqrt(2)$, then it returns that it is possibly almost space filling. If this is not the case, then it returns that it is not almost space filling and we see after the computation that it returns not almost space filling.

```
CheckLPolynomial := function()
    for n2,n3,n4 in [0..3] do
        h := 1/2*(n2^2-n2)+n3+n4-1;
        if h eq 2 then
            Roots := LPolynomialGenus4(N,n2,n3,n4);
            if Abs(Roots[1][1]) eq (1/Sqrt(2))  then
                return("Possibly almost space filling");
            end if;
            if Roots eq [] then
                return("Possibly almost space filling");
            end if;
        end if;
    end for;
return("Not almost space filling");
end function;
```

A.2 Check step and Result step

We will show the implementations of the Check step and the Result step. First we show the implementations of the Check step.

```
CheckStep := function(Curves, i)
    SpaceFillingCurves := [];
    for X in Curves do
        if #RationalPoints(X) gt 0 then
            if #RationalPoints(X) + i eq Evaluate(LPolynomial(X),1) then
```

```
                Append(~SpaceFillingCurves,X);
            end if;
        end if;
    end for;
    return(SpaceFillingCurves);
end function;
```

We see that the code look like the algorithm we have seen in chapter 4. Most functions are self explanatory. For example the function RationalPoints(X) gives an indexed set of the rational points of a curve X and the function LPolynomial(X) gives the L-polynomial of a curve X. Other functions like the function Evaluate computes for given function f and a ring element a, it returns the value $f(a)$. The procedure Append gives for a given list it adds the element X.

```
ResultStep := function(Curves)
IsoCurves:=[];
for X in Curves do
    existIso :=  false;
    for Y in IsoCurves do
        if LPolynomial(X) eq LPolynomial(Y) then
            if #Isomorphisms(X,Y) gt 0 then
                existIso := true;
                break;
             end if;
        end if;
    end for;
    if existIso eq false then
        Append(~IsoCurves,X);
    end if;
end for;
return(IsoCurves);
end function;
```

To see if two curves are isomorphic, we will compute the number of Isomorphisms by the function Isomorphisms and if this is more than 0, then there exists an isomorphism. We can't use the function IsIsomorphic, because it gives an error for characteristic 2 for hyperelliptic curves.

A.3 Enumeration Step

A.3.1 Hyperelliptic curves

In the case of Hyperelliptic curves over $\mathbb{F}_2$, we have the following formula. IsHyperelliptic-CurveOfGenus is the function, that returns if a hyperelliptic curve is defined by $y^2 + h(t)y = f(t)$ is of genus g. Note that this function says that a curve is hyperelliptic if it is smooth and irreducible.

```
Hyper := function(g)
```

```
Curves := [];
for i in [1..2^(2*g+3)-1] do
    for j in [1..2^(g+2)-1] do
        f:= Polynomial(GF(2),Intseq(i,2));
        h:= Polynomial(GF(2),Intseq(j,2));
        if IsHyperellipticCurveOfGenus(g,[f,h]) then
            X:=HyperellipticCurve(f,h);
            Append(~Curves,X);
            end if;
        end if;
    end for;
end for;
return(Curves);
end function;
```

We want to enumerate over every hyperelliptic curve, we therefore use the function Intseq, this function gives for every positive integer a sequence over a base number b. So suppose that $n := a_0b^0 + \cdots + a_kb^k$. Then Intseq(n,b) returns the sequence $[a_0, \ldots, a_k]$. And the function Polynomial(GF(2), $[a_0, \ldots, a_k]$) gives the polynomial $a_0 + a_1t + \cdots + a_nt^n \in \mathbb{F}_2[t]$. So if we enumerate over all $i \in [1..2^{(2g+3)} - 1]$, we get exactly all the polynomials $f \in \mathbb{F}_2[t]$ with $0 \leq \deg(f) \leq 2g + 2$ and if we enumerate over all $j \in [1..2^{g+2} - 1]$, we get exactly all the polynomials $h \in \mathbb{F}_2[t]$ with $0 \leq \deg(h) \leq g + 1$. For hyperelliptic curves over $\mathbb{F}_3$, we have the following function.

```
Hyper3 := function(g)
Curves := [];
for i in [3^{2*g+1}..3^{2*g+3}-1] do
    f := Polynomial(GF(3),Intseq(i,3));
    if IsHyperellipticCurveOfGenus(g,[f,0]) then
        X := HyperellipticCurve(f,0);
        Append(~Curves,X);
    end if;
end for;
return(Curves);
end function;
```

For hyperelliptic curves of genus 3, we can do the same trick as for hyperelliptic curves of genus 2. We enumerate over all $i \in [3^{2g+1}..3^{2g+3} - 1]$, this gives us all polynomials $f \in \mathbb{F}_3[3]$ with $2g + 1 \leq \deg(f) \leq 2g + 2$.

A.3.2 Non-Hyperelliptic curve

Genus 3

The genus 3 curves can be computed by the following function

```
Curve3 := function()
    Curves:=[];
```

```
    Proj := ProjectiveSpace(GF(2),2);
    R := PolynomialRing(GF(2),3);
    Monomial := MonomialsOfDegree(R,4);
    for i in [1..2^15-1] do
        seq := Intseq(i,2);
        f := 0;
        for j in [1..#seq] do
            f +:= seq[j]*Monomial[j];
        end for;
        X := Curve(Proj,f);
        if IsNonSingular(X) and IsIrreducible(X) then
            Append(~Curves,X);
        end if;
    end for;
    return(Curves);
end function;
```

We consider that R is the polynomial ring over $\mathbb{F}_2$ in 3 variables. The function MonomialsOfDegree(R,4) gives all monomials of degree 4 of the polynomial ring R. There are 14 monomials of degree 4. Observe that the number of homogeneous polynomials of degree 4 is $2^{15}-1$, so we can make for every positive number smaller than 2^{15} an unique homogeneous polynomial of degree 4. We have a function Intseq, which makes from a integer a sequence, if h_j is the j-th monomial and we have an sequence $[a_0,\ldots,a_n]$ with $n \leq 14$, then we define f to be the homogeneous polynomial $a_0h_0 + \cdots + a_nh_n$. If we enumerate over all sequences $[a_0,\ldots,a_n]$ with $n \leq 14$, then we have enumerate all homogeneous polynomial of degree 4. We define then X as the curve in $\mathbb{P}^2$ and we want X to be smooth and irreducible. Note that the function IsNonSingular, which checks the smoothness if the curve is projective and that is the case for us.

Bibliography

[Can+06] John Cannon et al. "Handbook of MAGMA functions". In: *Edition* 2 (2006), p. 4350.

[EGM12] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. "Abelian varieties". In: *Book project, available on Ben Moonen's home page* (2012).

[GW10] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry I*. Advanced Lectures in Mathematics. Schemes with examples and exercises. Vieweg + Teubner, Wiesbaden, 2010, pp. viii+615. ISBN: 978-3-8348-0676-5. DOI: 10.1007/978-3-8348-9722-0.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[Kle05] Steven L Kleiman. "The picard scheme". In: *arXiv preprint math/0504020* (2005).

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford Graduate Texts in Mathematics. Translated from the French by Reinie Erné, Oxford Science Publications. Oxford University Press, Oxford, 2002, pp. xvi+576. ISBN: 0-19-850284-2.

[LM90] Gilles Lachaud and Mireille Martin-Deschamps. "Nombre de points des jacobiennes sur un corps fini". In: *Acta Arith* 56.4 (1990), pp. 329–340.

[Mil13] James S. Milne. *Lectures on Etale Cohomology (v2.21)*. Available at www.jmilne.org/math/. 2013.

[Mur64] Jaap P Murre. "On contravariant functors from the category of preschemes over a field into the category of abelian groups". In: *Publications Mathématiques de l'IHÉS* 23 (1964), pp. 5–43.

[Mus] Mircea Mustaţă. *Zeta Functions in Algebraic Geometry*. Lecture notes. URL: http://www-personal.umich.edu/~mmustata/zeta_book.pdf.

[Oor62] Frans Oort. "Sur le schéma de Picard". In: *Bulletin de la Société Mathématique de France* 90 (1962), pp. 1–14.

[Ser73] Jean-Pierre Serre. *A course in arithmetic*. Translated from the French, Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973, pp. viii+115.

[Sta20] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2020.

[Sti17] Jakob Stix. *Erratum: Springer LNM 2054 Rational Points and arithmetic of fundamental groups evidence for the section conjecture*. 2017.

[Wei48] André Weil. “Sur les courbes algébriques et les variétés qui s’en déduisent”. In: *Publ. Inst. Math. Univ. Strasbourg* 7 (1948), pp. 1–85.