Algebraic Geometry Codes

Applications of Algebraic Curves in Coding Theory

Martin Sig Nørbjerg

P6 Project, Group 5.239a, Mathematics

Dept. of Mathematical Sciences
Skjernvej 4A
DK-9220 Aalborg Ø
http://math.aau.dk

Title
Algebraic Geometry Codes

Theme
Algebraic Geometry Codes

Project Period
Spring Semester 2022

Project Group
Group 5.239a

Participants
Martin Sig Nørbjerg

Supervisor
Matteo Bonini

Page Numbers
39

Date of Completion
June 15, 2023

Abstract

In this bachelors project we study the theory of algebraic geometry codes, these are linear error correcting codes constructed using the theory of algebraic geometry and in particular the theory of algebraic curves. Using the Reimann Roch Theorem we show that there exists good lower bounds on the parameters of these codes. Finally, we discuss the asymptotic properties of these codes and in particular how one can construct algebraic geometry codes which execed the asymptotic Giblert-Varshamov bound.

Preface

This is a Bachelor project written at the Department of Mathematical Sciences at Aalborg University. As such, it is expected that the reader has taken courses in abstract algebra and linear algebra. It is also expected that the reader is acquainted with the basics of topology. However, no prior knowledge in algebraic geometry or error correcting codes is required.

The work on the project took place from the 1. of February to the 25. of May 2023.

Sources are stated at the start of each chapter / section, using the Harvard method, that is: Last name of the author(s) [year of publication].

Definitions, propositions, theorems, lemmas, corollaries, and remarks are numbered according to each chapter and consecutively. Equations are numbered separately and likewise with figures and tables. The conclusions of proofs and examples are marked with ■ and □ respectively.

A table of notation and shorthands is given after the list of contents. Please note that some symbols may be used differently in different chapters.

Finally, I wish to thank and acknowledge my supervisor Matteo Bonini for his guidance and for being indulgent enough, to answer questions with no imitate application to the project.

Aalborg University, June 15, 2023

Martin Sig Nørbjerg
mnarbj20@student.aau.dk

Contents

Notation and Shorthands

Abstract Algebra

$\mathbb{F}_q$	The finite field with q elements.
$R[X_1, X_2, \ldots, X_n]$	The multivariate polynomial ring over R.
$X^{(k)}$	The mononomial $\prod_{i=1}^{n} X_i^{k_i}$.
R^*	The set of units in R.
$\langle S \rangle$	The ideal generated by the elements in the set S.
$\mathbb{K}/\mathbb{F}$	A field extension, meaning $\mathbb{F}$ is a subfield of the field $\mathbb{K}$.
$\overline{\mathbb{F}}$	An algebraic closure of the field $\mathbb{F}$.
$Rad(I)$	The radical of the ideal I.
$\mathrm{Ev}_{\mathcal{P}}$	The evaluation map.

Algebraic Geometry

$\Bbbk$	An arbitrary algebraically closed field.
$\mathbb{A}^n, \mathbb{P}^n$	The n-dimensional affine and projective space.
$V(S), V_{\mathbb{P}}(S)$	The affine and projective zero sets a set of polynomials S.
$I(X), I_{\mathbb{P}}(X)$	The affine and projective vanishing ideals a set of points X
$\mathcal{T}_Z$	The Zariski topology.
F^*, F_*	The homogenisation and dehomogenisation of the polynomial F.
$\mathcal{X}$	An affine or projective variety.
$\Bbbk[\mathcal{X}], \Bbbk(\mathcal{X})$	The coordinate ring and function field of the affine variety $\mathcal{X}$.
$\Bbbk_{\mathbb{P}}[\mathcal{X}], \Bbbk_{\mathbb{P}}(\mathcal{X}), \Bbbk[\mathcal{X}]$	The homogeneous coordinate ring and homogeneous function field and function field
$\Bbbk(\mathcal{X})$	The function field over $\mathcal{X}$.
$\mathcal{O}_P(\mathcal{X}), \mathfrak{m}_P$	The local ring of $\mathcal{X}$ at P, and it's maximal ideal.
v_P	The discrete valuation on $\mathcal{O}_P(\mathcal{X})$.
$I(P, \mathcal{X}, \mathcal{Y})$	The intersection multiplicity of $\mathcal{X}$ and $\mathcal{Y}$ at the point p.
$Div(\mathcal{X})$	The set of divisors on $\mathcal{X}$.
$\mathrm{supp}(D)$	The support of a divisor D.
(f)	The principal divisor of $f \in \Bbbk[\mathcal{X}]$.
$L(D), \ell(D)$	A special vector space of divisors and it's dimension.

Coding theory

$\mathcal{C}$	A linear code.
G	A generator matrix.
H	A parity check matrix.
d	The Hamming metric.
wt	The Hamming weight.
$\overline{B_r}(x)$	The hamming ball of radius r with center in x.
H_q	The q-ary entropy function.
$\mathcal{C}^\perp$	The dual code of $\mathcal{C}$.
δ	The relative distance.
R	The relative distance.

Algebraic Geometry Codes

$\mathcal{C}_{D,G}$	A Goppa Code.
ψ	The extended Frobenius map
$N_q(\mathcal{X})$	The number of $\mathbb{F}_q$-rational points on $\mathcal{X}$
$N_q^*(g)$	The maximum number of rational points on a curve of genus g

Introduction

We start by introducing the concept of a linear error correcting code in Chapter 1. Our disposition of linear error correcting codes includes a section on bounds on the parameters of an error correcting code. In this section we prove the Singleton bound (Corollary 1.18) and show that Reed-Solomon codes are MDS codes (Example 1.21). Afterwards we prove the Gilbert bound (Corollary 1.24) and the asymptotic Gilbert-Varshamov bound (Theorem 1.29).

Chapter 2 is on the theory of algebraic geometry, which is the study of the geometry of the zero sets of polynomials. The chapter is divided into three sections:

1. The first section is devoted to algebraic preliminaries, most notably the definition of different kinds of multivariate polynomials, algebraically closed fields (Definition 2.1) and results on Noetherian rings, including Hilbert's Basis Theorem 2.20.

2. In the second section the basics of algebraic geometry is introduced, however our disposition on the topic is quite limited. We introduce affine and projective varieties (Definitions 2.41 and 2.48 respectively) and various algebraic objects associated with these varieties.

3. The third and final section is devoted to the study of algebraic curves, especially the theory of algebraic plane curves. Our focus will be on the study of divisors and the Reimann-Roch Theorem 2.91 which we state without proof.

In Chapter 3 we introduce Goppa codes, which is a special type of error correcting curve, constructed on an absolutely irreducible regular projective algebraic curve over $\mathbb{F}_q$. The parameters of these codes are investigated using the theory of divisors on algebraic curves. We show that Reed-Solomon codes are a subfamily of Goppa codes (Example 3.4). Finally, we discuss the Tsfasman-Vlădut-Zink bound (Equation 3.2), which shows the existence of sequences of Goppa codes which exceed the Gilbert-Varshamov bound.

1 Error Correcting Codes

This chapter is based on Huffman and Pless (2003)[Chapter 1 and 3] as well as Tsfasman et al. (2007)[Chapter 1]. We will be considering subspaces of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$.

Definition 1.1. A k-dimensional linear subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ is called a $[n,k]_q$ *code*, the elements of $\mathcal{C}$ are called *codewords*. The natural numbers n and k are called the *length* and *dimension* of $\mathcal{C}$ respectively and field $\mathbb{F}_q$ the *alphabet* of $\mathcal{C}$.

What we shall refer to as a $[n,k]_q$ code is normally refereed to as a *linear code*, as such we will use the terminology interchangeably. Moving on we define a metric on $\mathbb{F}_q^n$, named after Richard Hamming, one of the founders of coding theory.

Definition 1.2. The *Hamming metric* $\mathrm{d} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$ is defined as

$$\mathrm{d}(x,y) := |\{i \in \{1,2,\ldots,n\} | x_i \neq y_i\}|.$$

Further more let $x \in \mathbb{F}_q^n$, then the *weight* of x is defined as $\mathrm{wt}(x) := \mathrm{d}(x,0)$.

Remark 1.3. Clearly $\mathrm{d}(x,y) = \mathrm{wt}(x-y)$ for all $x, y \in \mathbb{F}_q^n$.

It is no accident that we refereed to d as a metric, we will prove this in the following proposition.

Proposition 1.4. $(\mathbb{F}_q^n, \mathrm{d})$ *is a metric space, that is*

(i) $\mathrm{d}(x,y) \geq 0$ *and* $\mathrm{d}(x,y) = 0$ *if and only if* $x = y$.

(ii) d *is symmetric, meaning* $\mathrm{d}(x,y) = \mathrm{d}(y,x)$.

(iii) d *complies with the triangle inequality, meaning* $\mathrm{d}(x,z) \leq \mathrm{d}(x,y) + \mathrm{d}(y,z)$.

for all $x, y, z \in \mathbb{F}_q^n$

Proof. Assertion (i) is trivial, and (ii) follows as $\neq$ is a symmetric binary operation. Finally, (iii) holds since:

$$\mathrm{d}(x,y) \leq |\{i \in \{1,2,\ldots,n\} | x_i \neq z_i\}| + |\{i \in \{1,2,\ldots,n\} | y_i \neq z_i\}| = \mathrm{d}(x,z) + \mathrm{d}(z,y)$$

where the inequality follows since $x_i \neq y_i$ implies that either $x_i \neq z_i$ or $y_i \neq z_i$. ∎

Definition 1.5. Let $\mathcal{C}$ be a $[n,k]_q$ code, then $d = \min\{\mathrm{d}(c,c') \mid c,c' \in \mathcal{C}, c \neq c'\}$ is called the *minimum distance* of $\mathcal{C}$, and we say that $\mathcal{C}$ is a $[n,k,d]_q$ code.

Remark 1.6. As $\mathcal{C}$ is a linear subspace we have $d = \min\{\mathrm{wt}(c) | c \in \mathcal{C} \setminus \{0\}\}$, since $c_1 - c_2 \in \mathcal{C}\setminus\{0\}$, for all $c_1, c_2 \in \mathcal{C}$ such that $c_1 \neq c_2$, and $\mathrm{d}(c_1,c_2) = \mathrm{wt}(c_1 - c_2)$. For this reason the minimum distance of $\mathcal{C}$ is also refereed to as the *minimum weight* of $\mathcal{C}$.

The minimum distance has a massive impact on the error correcting properties of a code, as we will see in Section 1.1.

Example 1.7. Fix $n \in \mathbb{N}$. We will be considering the perhaps simplest, yet useful, code called the *repetition code* of length n, taking $x \in \mathbb{F}_q$ to $(x,x,\ldots,x) \in \mathbb{F}_q^n$. Since $\mathcal{C} = \mathrm{span}_{\mathbb{F}_q}\{(1,1,\ldots,1)\}$ and hence $\mathrm{d}(c,c') = n$ for all $c,c' \in \mathcal{C}$. We see that the repetition code of length n is a $[n,1,n]_q$ code. □

Not all linear codes $\mathcal{C}$ are this simple. However as $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$, there exists a $\mathbb{F}_q$-basis of $\mathcal{C}$, such that every $c \in \mathcal{C}$ can be written as a $\mathbb{F}_q$-linear combination of the basis vectors, this idea forms the foundation of the following definition.

Definition 1.8. Let $\mathcal{C}$ be a $[n,k]_q$ code, and suppose $g_1, g_2, \ldots, g_k \in \mathbb{F}_q^n$ forms a $\mathbb{F}_q$-basis of $\mathcal{C}$, then

$$G = \begin{bmatrix} g_1 & g_2 & \cdots & g_k \end{bmatrix}^T \in \mathbb{F}_q^{n\times k}$$

is called a *generator matrix* for $\mathcal{C}$.

Often one uses a generator matrix G as a mean of specifying a code. Below we introduce another way of specifying a code, namely as the null space of a matrix.

Definition 1.9. Suppose $\mathcal{C}$ is a $[n,k]_q$ code. Then a matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ such that

$$\mathcal{C} = \{x \in \mathbb{F}_q^n \mid Hx = 0\}$$

is called a *parity check matrix* of $\mathcal{C}$.

A parity check matrix H gives us a way to check if a vector $x \in \mathbb{F}_q^n$ belongs to the code $\mathcal{C}$. More concretely $x \in \mathcal{C}$ if and only if $Hx = 0$.

Lemma 1.10. *Let H be a parity check matrix of a $[n,k]_q$ code, then* $\mathrm{rank}(H) = n - k$.

Proof. Follows as $\mathrm{rank}(H) = n - \dim(\mathrm{null}(H)) = n - \dim(\mathcal{C}) = n - k$. ■

Since every $[n,k]_q$ code is a linear subspace of $\mathbb{F}_q^n$, it makes sense to consider code given as the orthogonal complement of $\mathcal{C}$, which we shall now define, in more detail:

Definition 1.11. Let $\mathcal{C}$ be a $[n,k]_q$ code, then we define the *dual code* of $\mathcal{C}$ as:

$$\mathcal{C}^\perp := \left\{x \in \mathbb{F}_q^n \middle| \langle x,c\rangle = 0 \text{ for all } c \in \mathcal{C}\right\}$$

where $\langle\cdot,\cdot\rangle$ denotes the usual canonical inner product on $\mathbb{F}_q^n$.

Dual codes have some nice properties, which allows us to use them to study their non-dual counterparts and vice versa. Some of these properties will be shown in the following lemma, the proof of which is based on the proofs of Lemma 1.8 and Corollary 1.9 in Giulietti (2003).

Lemma 1.12. *Suppose $\mathcal{C}$ is a $[n,k]_q$ code, with generator matrix G and parity check matrix H then:*

(i) *G is a parity check matrix of $\mathcal{C}^\perp$*

(ii) $\dim(\mathcal{C}^\perp) = n - k$.

(iii) *H is a generator matrix of $\mathcal{C}^\perp$.*

(iv) $\mathcal{C} = (\mathcal{C}^\perp)^\perp$.

Proof. Let $g_1, g_2 \ldots, g_k$ be the rows of G, and let $x \in \mathbb{F}_q^n$ then

$$Gx = (\langle x, g_1\rangle, \langle x, g_2\rangle, \ldots, \langle x, g_k\rangle) = 0 \iff x \perp g_i$$

for all $i \in \{1, 2, \ldots, k\}$. This implies Assertion (i) as $g_1, g_2, \ldots, g_k$ forms a $\mathbb{F}_q$-basis of $\mathcal{C}$. Assertion (ii) follows from (i) as $\mathcal{C}^\perp$ is the null space G and $\operatorname{rank}(G) = k$, since the rows of G are $\mathbb{F}_q$-linearly independent, so $\dim(\operatorname{null}(G)) = n - k$. Continuing with (iii): Since H is a parity check matrix of the $[n,k]_q$ code $\mathcal{C}$, we have that $\operatorname{rank}(H) = n - k$, confer Lemma 1.10. This implies that the $n - k$ rows of H are $\mathbb{F}_q$-linearly independent. Thus they form a $\mathbb{F}_q$-basis of some $(n-k)$-dimensional linear subspace $V \subseteq \mathbb{F}_q^n$, which is orthogonal to $\mathcal{C}$ as $Hc = 0$ for all $c \in \mathcal{C}$. Now since V and $\mathcal{C}^\perp$ are both orthogonal to $\mathcal{C}$ both with dimension $n - k$, confer Assertion (ii), it follows that $V = \mathcal{C}^\perp$. Finally, $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$, as $c \in \mathcal{C}$ implies $c \perp c'$ for all $c' \in \mathcal{C}^\perp$ combining this with $\dim(\mathcal{C}) = \dim(\left(\mathcal{C}^\perp\right)^\perp)$ gives (iv). ∎

Remark 1.13. Given a $[n,k]_q$ code $\mathcal{C}$, we can find a parity check matrix of $\mathcal{C}$ by taking a generator matrix of $\mathcal{C}^\perp$. Hence one can always find a parity check matrix of $\mathcal{C}$.

1.1 Transmission and Nearest Neighbour Decoding

We will now explain how one can use a $[n,k,d]_q$ code $\mathcal{C}$ when transmitting data through a noisy channel. There are many different assumptions one can impose on the distribution of this noise, we will however not consider this in this project.
Given some $x \in \mathbb{F}_q^k$, which we shall refer to as the *message*, we *encode* said message by computing the corresponding codeword $c := x^T G$, please note the linear transformation $T : \mathbb{F}_q^k \to \mathcal{C}$, defined as $x \mapsto x^T G$, is injective since the rows of G forms a $\mathbb{F}_q$-basis of $\mathcal{C}$. Since $c \in \mathbb{F}_q^n$, with $n \geq k$, more data has to be transmitted. However we have added redundant information, which will hopefully help correct any errors induced by the noise in the channel.

Since the codeword $c \in \mathcal{C}$ is subjected to random noise, during transmission, we receive some $y \in \mathbb{F}_q^n$, which is not necessarily equal to c. Now the main question is: How does one get back the original c or at least a good estimate of c say $\hat{c}$? Multiple of such estimates exists, and the best choice depends highly on the distribution of the random noise. However, we will only consider the perhaps most intuitive, named *nearest neighbour decoding*, where we chose the estimate:

$$\hat{c}_{\mathrm{d}} = \operatorname*{arg\,min}_{c \in \mathcal{C}} \mathrm{d}(c, y).$$

Please note that this estimate might not be unique. Finally, we can obtain an estimate $\hat{x}$ of x, by *decoding* $\hat{c}$. The decoding of $\hat{c}$ is often highly dependent on the specific code, and we will not discuss it in this general setting.

Continuing our disposition on nearest neighbor decoding, we prove the following theorem:

Theorem 1.14. *Let $\mathcal{C}$ be a $[n,k,d]_q$ code, $r = \lfloor \frac{d-1}{2} \rfloor$, and $c, c' \in \mathcal{C}$ such that $c \neq c'$ then*

$$\overline{B_r}(c) \cap \overline{B_r}(c') = \emptyset$$

where $\overline{B_r}(x) = \left\{ y \in \mathbb{F}_q^n \middle| d(x,y) \leq r \right\}$.

Proof. Assume for the sake of contradiction that $\overline{B_r}(c) \cap \overline{B_r}(c') \neq \emptyset$, then pick $x \in \overline{B_r}(c) \cap \overline{B_r}(c')$. Now since d complies with the triangle inequality confer Proposition 1.4(iii), we have:

$$\mathrm{d}(c,c') \leq \mathrm{d}(c,x) + \mathrm{d}(x,c') \leq 2r$$

but $2r = 2\lfloor \frac{d-1}{2} \rfloor \leq d-1$, which contradicts the assumption that d is the minimum distance of $\mathcal{C}$. ■

Remark 1.15. A natural implication of Theorem 1.14 is that if a maximum of $r = \lfloor \frac{d-1}{2} \rfloor$ entries in c are corrupted during transmission, and we receive $y \in \mathbb{F}_q^k$ then $\mathrm{d}(y,c) \leq r$. Therefore, $\hat{c}_{\mathrm{d}} = c$ since $\overline{B_r}(c) \cap \overline{B_r}(c') = \emptyset$ for all $c' \in \mathcal{C} \setminus \{c\}$. From this it follows that a $[n,k,d]_q$ code $\mathcal{C}$ can correct $\lfloor \frac{d-1}{2} \rfloor$ errors. However we can detect $d-1$ errors, since the received vector, will not be a codeword in this case.

The contents of Remark 1.15 indicate that when we are interested in finding a $[n,k]_q$ code $\mathcal{C}$, with the best error correcting capabilities then we need to find one with a high minimum distance. However, upper bounds on the minimum distance d given n and k do exist, a one of which will be presented in the following section.

1.2 Bounds on the Parameters of Linear Codes

In this section we will introduce a few select bounds for the parameters of codes, namely the Singleton, Gilbert and asymptotic Gilbert-Varshamov bound. We will start by stating and proving the following lemma, its proof will be based upon the ideas presented in the proof of Theorem 2 found in Shum and Zhang (2016).

Proposition 1.16. *Let $\mathcal{C}$ be a $[n,k,d]_q$ code, with parity check matrix H then any $d-1$ columns of H are $\mathbb{F}_q$-linearly independent.*

Proof. Let $h_1, h_2, \ldots, h_n$ be the columns of H, assume for the sake of contradiction that there exists distinct indices $i_1, i_2, \ldots, i_{d-1}$ such that $h_{i_1}, h_{i_2}, \ldots, h_{i_{d-1}}$ are $\mathbb{F}_q$-linearly dependent. We will now construct a $c \in \mathcal{C} \setminus \{0\}$ with $\mathrm{wt}(c) \leq d-1$. We start by setting $c_k = 0$ for all $k \notin \{i_1, i_2 \ldots, i_{d-1}\}$. Now as $h_{i_1}, h_{i_2}, \ldots, h_{i_{d-1}}$ are $\mathbb{F}_q$-linearly dependent, there exists $c_{i_1}, c_{i_2}, \ldots, c_{i_{d-1}} \in \mathbb{F}_q$, not all 0, such that

$$\sum_{j=1}^{n} c_j h_j = \sum_{j=1}^{d-1} c_{i_j} h_{i_j} = 0 \implies c \in \mathcal{C}.$$

Which is a contradiction since $\mathrm{wt}(c) \leq d-1$. ■

Remark 1.17. Another perhaps more natural connection between the minimum distance of a $[n,k]_q$ code $\mathcal{C}$ and one of its parity check matrices H, is that the minimum distance of $\mathcal{C}$ corresponds to the minimum number of linearly dependent columns of H. This can be seen easily as the minimum distance of $\mathcal{C}$ corresponds to the minimum weight of $\mathcal{C}$.

Using Proposition 1.16 we can now state and prove our first upper bound on the parameters of a $[n, k, d]_q$ code.

Corollary 1.18 (Singleton Bound)**.** *Let $\mathcal{C}$ be a $[n, k, d]_q$ code then $d - 1 \leq n - k$.*

Proof. Let H be a parity check matrix of $\mathcal{C}$, then $d-1 \leq \operatorname{rank}(H)$ as any collection of $d-1$ columns of H are $\mathbb{F}_q$-linearly independent, confer Proposition 1.16. The rest follows from Lemma 1.10 as $\operatorname{rank}(H) = n - k$. ■

Remark 1.19. Rearranging the Singleton bound to obtain $d + k \leq n + 1$ the trade-off between minimum distance and dimension of a code, becomes even more self-evident, as such we can either wish to find a code with a high minimum distance d or a high dimension k, relative to the length of the code, but not both!

Definition 1.20. If a $[n, k, d]_q$ code $\mathcal{C}$ meets the singleton bound, that is $d - 1 = n - k$, it is called a *maximum distance seperable (MDS)* code.

We have actually already seen a MDS code in Example 1.7. We will now introduce a more interesting example of a MDS code, based on elements of Tsfasman et al. (2007)[Subsection 1.2.1] as well as Giulietti (2003)[Chapter 2].

Example 1.21. [Reed-Solomon Codes] Let q be a prime power, and fix $n, k \in \mathbb{N}$ such that $1 \leq k \leq n \leq q$. Since $n \leq q$ we can chose $P_1, P_2, \ldots, P_n \in \mathbb{F}_q$ all distinct and define the set $\mathcal{P} := \{P_1, P_2, \ldots, P_n\}$. Finally, we define the vector space

$$L_k := \{F \in \mathbb{F}_q[X] \mid \deg(F) \leq k - 1\}.$$

Please note that $0 \in L_k$, as we use the convention that $\deg(0) = 0$, confer remark 2.14. Then the evaluation map:

$$\mathrm{Ev}_{\mathcal{P}} \colon L_k \to \mathbb{F}_q^n, \quad F \mapsto (F(P_1), F(P_2), \ldots, F(P_n))$$

is injective, since $\mathrm{Ev}_{\mathcal{P}}$ is a linear map and $F \in \mathbb{F}_q[X] \backslash \{0\}$ can have at most $\deg(F)$ roots, so $\mathrm{Ev}_{\mathcal{P}}(F) = 0$ if and only if $F \equiv 0$. The linear code $\mathcal{C} := \mathrm{Ev}_{\mathcal{P}}(L_k)$, is called the Reed-Solomon code of degree k, we will show that $\mathcal{C}$ is a $[n, k, n - k + 1]_q$ code. Since $1, X, \ldots, X^{k-1}$ form a basis of L_k, we see that $\mathcal{C}$ has dimension k, and that

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ P_1 & P_2 & \cdots & P_n \\ \vdots & \vdots & \ddots & \vdots \\ P_1^{k-1} & P_2^{k-1} & \cdots & P_n^{k-1} \end{bmatrix}$$

is a generator matrix for $\mathcal{C}$.
Let $F \in L_k$ and $c := (F(P_1), F(P_2), \ldots, F(P_n))$ then F vanishes at $n - \mathrm{wt}(c)$ of the points, therefore we have $n - \mathrm{wt}(c) \leq \deg(F) \leq k - 1$. In the special case $\mathrm{wt}(c) = d$ and d is the minimum distance of $\mathcal{C}$, we see that $n - d \leq k - 1$ from rearranging this inequality we obtain $n - k \leq d - 1$. Combining this with the Singleton bound (Corollary 1.18) we obtain $n - k = d - 1$, and thus $\mathcal{C}$ is a MDS code, with minimum distance $n - k + 1$. □

Later on we will show that Reed-Solomon codes are a special case of what will be our main object of study, namely algebraic geometry codes.

1.2.1 The Assymptotic Gilbert-Varshamov Bound

The following subsection is based on Huffman and Pless (2003)[Section 2.1, 2.8 and 2.10] and Giulietti (2003)[Chapter 5]. We will start by proving a few technical results before moving onto to the Gilbert bound. Following this we introduce some new notation before reaching the main result of this subsection, namely the asymptotic Gilbert-Varshamov bound.

Lemma 1.22. *Let $x \in \mathbb{F}_q^n$, then $\left|\overline{B_r}(x)\right| = V_q(n,r)$ where $V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$.*

Proof. Let $S_i(x) = \left\{x' \in \mathbb{F}_q^n \middle| \mathrm{d}(x,x') = i\right\}$ for $i = 0, 1, \ldots, r$. Then $S_0(x), S_1(x), \ldots, S_r(x)$ are all finite and pairwise disjoint and $\overline{B_r}(x) = \bigcup_{i=0}^{r} S_i(x)$. Combining these facts we see that:

$$\left|\overline{B_r}(x)\right| = \sum_{i=0}^{r} \left|S_i(x)\right|. \tag{1.1}$$

Additionally we have that $|S_i(x)| = \binom{n}{i}(q-1)^i$, since $x' \in S_i$ differ from x in exactly i out of n entries. The result follows immediately by combining this with Equation (1.1). ■

Moving forward we follow the convention of Huffman and Pless (2003) and let $B_q(n,d)$ be the maximum number of codewords in a linear code of length n and minimum distance at least d.

Theorem 1.23. *If $\mathcal{C}$ is linear code over $\mathbb{F}_q$ of length n, with minimum distance d and $B_q(n,d)$ codewords then:*

$$\mathbb{F}_q^n = \bigcup_{c \in \mathcal{C}} \overline{B_{d-1}}(c)$$

The proof of is due to Lahtonen (2023).

Proof. If there exists an $x \in \mathbb{F}_q^n \notin \bigcup_{c\in\mathcal{C}} \overline{B_{d-1}}(c)$. Then $\mathcal{C}' := \mathcal{C} + \mathrm{span}\{x\}$ is another linear code, such that $|\mathcal{C}'| > |\mathcal{C}|$. We will show that $\mathcal{C}'$ has minimum distance d which in turn contradicts that $\mathcal{C}$ had $B_q(n,d)$ codewords.
Assume for the sake of contradiction, that $\mathcal{C}'$ has minimum distance less than d, then there exists a $c' \in \mathcal{C}'$ such that $\mathrm{wt}(c') \leq d-1$. Since $c' \in \mathcal{C}'$ we may write $c' = c + ax$ for some $c \in \mathcal{C}$ and $a \in \mathbb{F}_q$. Furthermore, we have that $a \neq 0$, as $\mathrm{wt}(c') \leq d-1$ implies that $c' \notin \mathcal{C}$. In addition, we have that $\mathrm{wt}(by) = \mathrm{wt}(y)$ for all $b \in \mathbb{F}_q$ and $y \in \mathbb{F}_q^n$, since $\mathbb{F}_q$ is a domain. Combining the earlier observations we get that:

$$d - 1 \geq \mathrm{wt}(c') = \mathrm{wt}(-a^{-1}c') = \mathrm{wt}(-a^{-1}c - x) = \mathrm{d}(-a^{-1}c, x).$$

However this is a contradiction since this means that $x \in \overline{B_{d-1}}(-a^{-1}c)$ after all. ■

We are now able to state and prove the Gilbert bound which we will use to prove the asymptotic Gilbert-Varshamov bound.

Corollary 1.24 (Gilbert bound)**.** *Suppose $V_q(n,r)$ is defined as in Lemma 1.22 then:*

$$B_q(n,d) \geq \frac{q^n}{V_q(n,d-1)}$$

Proof. Let $\mathcal{C}$ be a linear code of length n, with minimum distance d and $B_q(n,d)$ codewords, then $\mathbb{F}_q^n = \bigcup_{c\in\mathcal{C}} \overline{B_{d-1}}(c)$ by Theorem 1.23, combining this with Lemma 1.22, we get:

$$q^n = \left|\mathbb{F}_q^n\right| \leq \sum_{c\in\mathcal{C}} \left|\overline{B_{d-1}}(c)\right| = B_q(n,d)V_q(n,d-1). \qquad \blacksquare$$

Continuing we define the following function which will be used in the asymptotic Gilbert-Varshamov bound.

Definition 1.25. Let $q \in \mathbb{N}$ such that $q \geq 2$, then the function $H_q : [0,(q-1)/q] \to \mathbb{R}$ defined as $H_q(0) = 0$ and $H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$ otherwise is called the *q-ary entropy function.*

We will now state Lemma 2.10.3, from Huffman and Pless (2003), but we will omit its computation heavy proof.

Lemma 1.26. *Let $\delta \in [0,(q-1)/q]$ where $q \in \mathbb{N}$ such that $q \geq 2$, then:*

$$\lim_{n\to\infty} \frac{1}{n}\log_q(V_q(n,\lfloor \delta n \rfloor)) = H_q(\delta).$$

Moving on we introduce two invariants which can be used to gauge the quality of a code.

Definition 1.27. Let $\mathcal{C}$ be a $[n,k,d]_q$ code, then the invariants $R := k/n$ and $\delta := d/n$ is called the *transmission rate* and *relative distance* of $\mathcal{C}$ respectively.

Following the definition a natural question arise, namely why would one consider the invariants R and δ instead of using n,k and d directly, when gauging the quality of a $[n,k,d]_q$ code? To answer this consider the repetition code of length n, as seen in Example 1.7, when n increases then so will the minimum distance d as $d = n$, however δ will stay constant. In addition to this we are still only able to encode a single symbol hence we are sacrificing transmission rate. Hence, R and δ better reflect the properties of a code, especially for large n.

Remark 1.28. Let $\mathcal{C}$ be a $[n,k,d]_q$ code with transmission rate R and relative minimum distance δ, then $d + k \leq n + 1$ by Remark 1.19, dividing by n we get that

$$\delta + R \leq 1 + \frac{1}{n}.$$

Thus a long code, with good parameters have $\delta + R$ close to 1.

Remember that $B_q(n,d)$ is the maximum number of codewords of a linear code $\mathcal{C}$, with length n and minimum distance at least d. Since $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$, we have that $\dim(\mathcal{C}) = \log_q(B_q(n,d))$. Thus, it makes sense to define what we shall refer to as the *maximal rate*:

$$R^*(n,d) = \frac{\log_q(B_q(n,d))}{n}.$$

We will now investigate the behavior of $R^*(n,d)$ as $n \to \infty$, for this we define, the function $\alpha_q^{lin} : [0,1] \to [0,1]$ as a function of a relative distance δ, specifically $\delta \mapsto \limsup_{n\to\infty} R^*(n, \delta n)$. Finally, we can state and prove the asymptotic Gilbert-Varshamov[1] bound.

Theorem 1.29 (Asymptotic Gilbert-Varshamov bound)**.** *Let $0 \leq \delta \leq (q-1)/q$, then:*

$$\alpha_q^{lin}(\delta) \geq 1 - H_q(\delta).$$

Proof. First note that $B_q(n, \delta n) = B_q(n, \lceil \delta n \rceil)$. Since $B_q(n,d)$ is the maximum number of codewords of a code of length n with minimum distance at least d and the minimum distance of a linear code is always a natural number. Thus, we have

$$\begin{aligned}\alpha_q^{lin}(\delta) = \limsup_{n\to\infty} \frac{\log_q(B_q(n, \lceil \delta n \rceil))}{n} &\geq \limsup_{n\to\infty} \frac{\log_q\left(\dfrac{q^n}{V_q(n, \lceil \delta n \rceil - 1)}\right)}{n} \\ &\geq \limsup_{n\to\infty} 1 - \frac{\log_q(V_q(n, \lfloor \delta n \rfloor)}{n}\end{aligned}$$

where the first inequality follows from the Gilbert bound (Corollary 1.24) and the last inequality follows since $\lceil \delta n \rceil - 1 \leq \lfloor \delta n \rfloor$ implies $\frac{q^n}{V_q(n, \lceil \delta n \rceil - 1)} \geq \frac{q^n}{V_q(n, \lfloor \delta n \rfloor)}$. The rest follows by applying Lemma 1.26, as

$$\lim_{n\to\infty} \frac{\log_q(V_q(n, \lfloor \delta n \rfloor)}{n} = H_q(\delta) \implies \limsup_{n\to\infty} \frac{\log_q(V_q(n, \lfloor \delta n \rfloor)}{n} = H_q(\delta). \qquad \blacksquare$$

[1]The Varshamov bound is another bound for the parameters of linear codes, which can be used to prove the theorem as well.

2 Algebraic Geometry

In this chapter we will first present some algebraic preliminaries, afterwards we move on and study the very basics of algebraic geometry, before we finish up by introducing the theory of algebraic curves.

Algebraic geometry is the geometry of zero sets of multivariate polynomials. Although algebraic geometry is a large subject, our disposition on the subject will be quite limited, since we are primarily interested in algebraic curves, as they form the foundation of algebraic geometry codes.

2.1 Algebraic Preleminaries

Unless otherwise specified the definitions and results in this section will be based on those found in Lang (2002)[Section 5.2]. Later when we will introduce the theory of algebraic geometry, we will be considering polynomials over a field, since we are interested in the geometry of the zero sets of these polynomials, it would be nice to know that our non-constant polynomials has at least one root.

Definition 2.1. Let $\mathbb{F}$ be a field, if there for all $F \in \mathbb{F}[X] \backslash \mathbb{F}^*$, exists an $\alpha \in \mathbb{F}$ such that $F(\alpha) = 0$. Then $\mathbb{F}$ is said to be *algebraically closed*.

Remark 2.2. We often denote an arbitrary closed field with the letter $\Bbbk$.

Example 2.3. The complex numbers $\mathbb{C}$ is perhaps the most well known algebraically closed field. □

Later when we try to apply algebraic geometry to error correcting codes we will be working with finite fields. These fields are however not algebraically closed, as we will show in the following proposition.

Proposition 2.4. *Let $\mathbb{F}_q$ be a finite field, then $\mathbb{F}_q$ is not algebraically closed.*

Proof. We will enumerate the distinct elements of $\mathbb{F}_q$ as $a_0, \ldots, a_{q-1}$, since $\mathbb{F}_q$ is finite. Consider the polynomial $F = 1 + \prod_{k=0}^{q-1}(a_k - X) \in \mathbb{F}_q[X] \backslash \mathbb{F}_q^*$. If $\alpha \in \mathbb{F}_q$ then

$$F(\alpha) = 1 + \prod_{k=0}^{q-1}(a_k - \alpha) = 1,$$

since $\alpha = a_k$ for some $k \in \{0, 1, \ldots, q-1\}$. Hence, F has no roots in $\mathbb{F}_q$. Hence $\mathbb{F}_q$ is in fact not algebraically closed. ■

Definition 2.5. Let $\mathbb{K}$ be a field, if $\mathbb{F} \subseteq \mathbb{K}$ is a subfield, we say that $\mathbb{K}$ is a *field extension* of $\mathbb{F}$, which we denote $\mathbb{K}/\mathbb{F}$. The field extension $\mathbb{K}/\mathbb{F}$ is called an *algebraic closure* of $\mathbb{F}$, if $\mathbb{K}$ is algebraically closed.

Remark 2.6. Our definition of algebraic closures, is less strict than the standard definition where an algebraic closure is required to be the smallest algebraically closed field extension. In this stricter setting the algebraic extension is unique, however our definition is sufficient for the scope of this project.

Remark 2.7. It can be shown that if $\mathbb{F}$ is an arbitrary field, then there exists an algebraic closure of $\mathbb{F}$, see for instance Weintraub (2020)[Section 5.3].

Instead of proving the result stated in Remark 2.7, we will restrict ourselves and only show the case where $\mathbb{F}$ is a finite field, with a prime number of elements.

The proof will be based on the ideas found in Weintraub (2020)[Proof of Theorem 2.2.6] and Lauritzen (2003)[Remark 4.6.8].

Theorem 2.8. *Let p be prime, then $\overline{\mathbb{F}}_p := \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is an algebraic closure of $\mathbb{F}_p$.*

Proof. Let $F \in \overline{\mathbb{F}}_p[X]$ then there exists $n \in \mathbb{N}$ such that $F \in \mathbb{F}_{p^n}[X]$. We can without loss of generality assume F to be irreducible, otherwise write F as a product of irreducible polynomials and continue the proof by replacing F with one of its irreducible factors. Then $F := \mathbb{F}_p[X]/\langle F \rangle$ is a finite field with $p^{\deg(F)}$ elements. This in turn imply that $F \cong \mathbb{F}_{p^{\deg(F)}}$, since finite fields with the same number of elements are isomorphic. Furthermore we have $[X] \in F$ and $F([X]) = 0 \in F$, this combined with the fact that F is isomorphic to a subfield of $\overline{\mathbb{F}}_p$ implies that F must have a root in $\overline{\mathbb{F}}_p$. ■

2.1.1 Multivariate Polynomials

Moving on we define multivariate polynomials over an arbitrary ring R. A multivariate polynomial, with n variables, can be thought of as a polynomial with coefficients which are themselves multivariate polynomials, with $n-1$ variables. The following definitions are based on those found in Fulton (2008)[Section 1.1] and Lang (2002)[Section 2.3].

Definition 2.9. Let R be a ring, then we define the ring of *multivariate polynomials* with $n \geq 1$ variables $X_1, X_2, \ldots, X_n$ over R inductively as

$$R[X_1, X_2, \ldots, X_n] := R[X_1, X_2 \ldots, X_{n-1}][X_n]$$

with $R[X_1]$ defined the usual way.

Remark 2.10. When $n = 1, 2$ or 3 we usually write $R[X]$, $R[X, Y]$ or $R[X, Y, Z]$ respectively instead of $R[X_1, X_2, \ldots, X_n]$.

A polynomial $f \in R[X_1, X_2, \ldots, X_n]$, can be thought of as a function, similarly to univariate polynomials over R. Next we introduce some special types of multivariate polynomials, with the end goal of being able to define the degree of an arbitrary multivariate polynomial.

Definition 2.11. Let R be a ring and $k \in \mathbb{N}^n$, then a polynomial of the form $X^{(k)} := \prod_{i=1}^{n} X_i^{k_i} \in R[X_1, X_2, \ldots, X_n]$ is called a *monomial*, the *degree* of the monomial $X^{(k)}$ is defined as $\deg\left(X^{(k)}\right) := \sum_{i=1}^{n} k_i$.

Next we consider polynomials given as linear combinations of monomials of the same degree.

Definition 2.12. Let $d, m \in \mathbb{N}$, and $X^{(k_1)}, X^{(k_2)}, \ldots, X^{(k_m)} \in R[X_1, X_2, \ldots, X_n]$ be monomials of degree d. Furthermore if $a_1, a_2, \ldots, a_m \in R \setminus \{0\}$, then the polynomial $H := \sum_{i=1}^{k} a_i X^{(k_i)}$ is called a *homogeneous* polynomial or a *form* and we define the *degree* of H as $\deg(H) := d$.

Finally, we are able to define the degree of an arbitrary non-zero multivariate polynomial.

Definition 2.13. Let $F \in R[X_1, X_2, \ldots, X_n] \setminus \{0\}$ then there exists some $d \in \mathbb{N}$ and homogeneous polynomials $H_0, H_1, \ldots, H_d \in R[X_1, X_2, \ldots, X_n]$, such that with $\deg(H_i) = i$ and $F = \sum_{i=1}^{d} H_i$. Then we define the *degree* of F to be $\deg(F) = d$.

The existence of a $d \in \mathbb{N}$, as described in Definition 2.13, is guaranteed since every polynomial consist of a finite number of terms.

Remark 2.14. We will use the convention that the polynomial $0 \in R[X_1, X_2, \ldots, X_n]$ has degree 0.

It is worth noting that if F is a monomial or a homogeneous polynomial, the degree defined in Definition 2.13 agrees with the definitions of degree found in Definition 2.11 or 2.12 respectively. Finally, a univariate polynomial $F \in R[X]$ the degree defined in definition 2.13 also corresponds to the standard definition for the degree of F, since X^k where $k \in \mathbb{N}$ are the only monomials found in $R[X]$.

Consider the polynomial $F = \sum_{k \in \mathbb{N}^n} a_{(k)} X^{(k)} \in R[X_1, X_2, \ldots, X_n]$ where $a_{(k)} = 0$ for all but a finite number of k's. Then the *partial derivative of F with respect to X_j* denoted F_{X_j} is defined as:

$$F_{X_j} := \sum_{k \in \mathbb{N}^n} k_j a_{(k)} X^{(k - e_j)}$$

where $X^{(k-e_j)}$ is interpreted as 0 if $k_j - e_j < 0$.

Example 2.15. The calculations with partial derivatives depends strongly on the characteristic of R. For instance let R be a ring of non-zero characteristic p and $m \in \mathbb{N}$. Consider the homogeneous polynomial $F = X^m + Y^m + Z^m \in R[X, Y, Z]$, then $\deg(F) = m$ and the partial derivatives of F are $F_X = mX^{m-1}$, $F_Y = mY^{m-1}$ and $F_Z = mZ^{m-1}$. However, if m and p are not coprime, then $F_X = F_Y = F_Z = 0$. □

Below we note two important results on polynomial rings, which will come in handy later. The first result will be stated without proof, to avoid introducing otherwise unnecessary concepts, however its proof can be found in Lang (2002)[Section 2.2].

Theorem 2.16. *Let R be a UFD, then $R[X]$ is also a UFD.*

The theorem above have a very natural extension to multivariate polynomial rings.

Corollary 2.17. *If R is a UFD, then $R[X_1, X_2, \ldots, X_n]$ is also a UFD.*

Proof. Follows directly by induction, since $R[X_1, X_2, \ldots, X_{k-1}]$ being a UFD means $R[X_1, X_2, \ldots, X_n]$ is a UFD, by Theorem 2.16. ■

2.1.2 Noetherian Rings and Hilbert Basis Theorem

In this subsection we will show that if $\mathbb{F}$ is a field, then all ideals of $\mathbb{F}[X_1, X_2, \ldots, X_n]$ are finitely generated. This fact will become particularly useful in Subsection 2.2.1 and 2.2.4. The contents will be based on those presented in Fulton (2008)[Section 1.4].

Definition 2.18. A ring R is called *Noetherian* if all ideals of R are finitely generated.

Noetherian rings have many nice properties, some of these will be presented and proved in the following results. We start by showing the following fundamental property:

Proposition 2.19. *Let R be a Noetherian ring, and $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, then the chain has a maximal member, meaning there exists an $n \in \mathbb{N}$ such that $I_n = I_k$ for all $k \geq n$.*

Proof. Since R is Noetherian, the ideal $I = \bigcup_{j=1}^{\infty} I_j$, is finitely generated. Suppose $x_1, x_2, \ldots, x_m \in I$ generates I. Then for each $i \in \{1, 2, \ldots, m\}$ there exists an $n_i \in \mathbb{N}$ such that $x_i \in I_k$ whenever $k \geq n_i$. Setting $n = \max\{n_1, n_2, \ldots, n_m\}$ concludes the proof. ■

We now state and prove the main result of this section.

Theorem 2.20 (Hilbert Basis Theorem)**.** *Let R be a Noetherian ring, then $R[X_1, X_2, \ldots, X_n]$ is also a Noetherian ring.*

Proof. The theorem will follow by induction if we can show that if R is a Noetherian ring then $R[X]$ is Noetherian. As such let I be an ideal in $R[X]$, and J be the ideal which consist of the leading coefficients of all polynomial in I. However, as J is an ideal in R a finite set of polynomials $\mathcal{F} = \{F_1, F_2, \ldots, F_k\} \subseteq I$ exists, such that the leading coefficients of the polynomials in $\mathcal{F}$ generate J. Furthermore, let $M := \max\{\deg(F_1), \deg(F_2), \ldots, \deg(F_r)\}$ and J_m be the ideal consisting of all leading coefficients of polynomials with degree less than or equal to m for $m \leq M$. By a similar argument there exists a finite set of polynomials $\mathcal{F}_m = \{F_{m,1}, F_{m,2}, \ldots, F_{m,r_m}\}$ whose leading coefficients generate J_m.

Let I' be the ideal generated by the elements in the finite set $\mathcal{F} \cup (\bigcup_{m=1}^{M} \mathcal{F}_m)$. We will show that $I' = I$, and hence that I is finitely generated. Assume for the sake of contradiction that $I' \subset I$ then pick $G \in I \setminus I'$ of the lowest degree possible. Then either $\deg(G) > M$ or $\deg(G) \leq M$:

(i) If $\deg(G) > M$, then there exists polynomials $H_1, H_2, \ldots, H_r$ such that $\sum_{i=1}^{r} H_i F_i$ and G have the same leading term, since $F_1, F_2, \ldots, F_r$ generated I. Now define $G' := G - \sum_{i=1}^{r} H_i F_i$ then $\deg(G') < \deg(G)$ and the hence we have $G' \in I'$, which in turn imply that $G \in I'$, since I' is an ideal.

(ii) Else if $\deg(G) = m \leq M$, then we can apply a similar argument this time by setting $G' := G - \sum_{i=1}^{r_m} H_i F_{m,i}$.

This proves the theorem as I' was finitely generated by a subset of I and we have showed that I' is not smaller than I. ■

The following corollary is rather trivial, since every field is a principal ideal domain. However, it is a fact, that we will use frequently in Section 2.2.

Corollary 2.21. *Let $\mathbb{F}$ be a field, then $\mathbb{F}[X_1, X_2, \ldots, X_n]$ is a Noetherian ring.*

The following proposition and its proof are derived from Fulton (2008)[Problem 1.22]

Proposition 2.22. *Let R be a Noetherian ring, and $I \subseteq R$ be an ideal, then R/I is also a Noetherian ring.*

Proof. Suppose $J' \subseteq R/I$ is an ideal, consider the natural ring homomorphism π defined as $R \ni x \mapsto [x] \in R/I$, then $J := \pi^{-1}(J')$ is an ideal in R. This can be seen by letting $x, y \in J$, then $[x], [y] \in J'$ and thus $[x+y] \in J'$ and hence $x + y \in \pi^{-1}([x+y]) \subseteq J$, which implies that J is closed under addition. To see that J is closed under multiplication: Let $c \in R$ and $x \in J$, then $cx \in \pi^{-1}([c][x])$ and $[c][x] \in J'$. Suppose that $x_1, x_2, \ldots, x_n \in J$ generates J and let $[y] \in J'$, and $z \in \pi^{-1}([y])$, then there exists $a_1, a_2, \ldots, a_n \in R$ such that

$$z = \sum_{i=1}^{n} a_i x_i$$

This implies that $[y] = \pi(z) = \pi(\sum_{i=1}^{n} a_i x_i) = \sum_{i=1}^{n} [a_i][x_i]$ where the last equality follows from the fact that π is a ring homomorphism. However, as $[y]$ was chosen arbitrarily, this shows that R/I is a Noetherian ring. ■

2.2 Algebraic Geometry

In this section we are going to fix an algebraically closed field $\Bbbk$ and a positive natural number n. Most of the definitions and results will be stated either in the n-dimensional affine or projective spaces, we start by considering the affine case, as it is the simplest to understand.

Definition 2.23. The n-dimensional *affine space* over $\Bbbk$ is defined as

$$\mathbb{A}^n(\Bbbk) := \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \Bbbk\}$$

If $\Bbbk$ is understood from the context we omit it, and simply write $\mathbb{A}^n$.

Suppose $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ and $F \in \Bbbk[X_1, X_2, \ldots, X_n]$, then P is called a *point* and we may write $F(P)$ instead of $F(a_1, a_2, \ldots, a_n)$.

Definition 2.24. Let $S \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$, then we define the *zero set* of S as

$$V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}.$$

Furthermore the zero set $V(S)$ is called an *affine algebraic set* in $\mathbb{A}^n$.

Remark 2.25. It is easy to see that if $S \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ and $T \subseteq S$, then $V(S) \subseteq V(T)$, since $P \in V(S)$ implies $F(P) = 0$ for all $F \in S$ and in particular for all $F \in T$.

When $S := \{F_1, F_2, \ldots, F_m\} \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$, we may write $V(S)$ as $V(F_1, F_2, \ldots, F_m)$. If $F \in \Bbbk[X_1, X_2, \ldots, X_n]$ we call $V(F)$ a *hypersurface*. Next we will show that every affine algebraic set, is the zero set of some ideal in $\Bbbk[X_1, X_2, \ldots, X_n]$.

Lemma 2.26. *Let $S \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$, then $V(S) = V(\langle S \rangle)$.*

Proof. Since $S \subseteq \langle S \rangle$, it follows from remark 2.25 that $V(\langle S \rangle) \subseteq V(S)$. Now suppose $P \in V(S)$, then $F(P) = 0$ for all $F \in S$, now let $G \in \langle S \rangle$, then G can be written as

$$G = \sum_{i=1}^{m} H_i F_i$$

for some $m \in \mathbb{N}$ and $H_i \in \Bbbk[X_1, X_2, \ldots, X_n], F_i \in S$ for $i = 1, 2, \ldots, m$. Evaluating G at the P gives:

$$G(P) = \sum_{i=1}^{m} H_i(P) F_i(P) = 0$$

since $F_i(P) = 0$ for all $i = 1, 2, \ldots, m$, and hence $V(S) \subseteq V(\langle S \rangle)$. ■

An interesting consequence of Lemma 2.26 and Corollary 2.21, is that every affine algebraic subset $V(S)$ is the intersection of finitely many hypersurfaces, this can be seen as follows: From Lemma 2.26 we have that $V(S) = V(\langle S \rangle)$. The ideal $\langle S \rangle$ is finitely generated since $\Bbbk[X_1, X_2, \ldots, X_n]$ is Noetherian, by Corollary 2.21, hence there exists some $k \in \mathbb{N}$ and $F_1, F_2, \ldots, F_k \in \Bbbk[X_1, X_2, \ldots, X_n]$ such that:

$$V(S) = V(\langle F_1, F_2, \ldots, F_k \rangle) = \bigcap_{i=1}^{k} V(F_i).$$

We will now define a topology on $\mathbb{A}^n$, where the affine algebraic sets form the closed sets.

Definition 2.27. The topology $\mathcal{T}_Z = \{V(S)^c \mid S \subseteq \Bbbk[X_1, X_2, \ldots, X_n]\}$ is called the *Zariski topology* on $\mathbb{A}^n$.

We will now prove that the Zariski topology is indeed actually a topology on $\mathbb{A}^n$. We do however first require the following proposition.

Proposition 2.28. *Let $S, T \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ and $\{S_i\}_{i \in \mathcal{I}}$ be a family of subsets of $\Bbbk[X_1, X_2, \ldots, X_n]$ then:*

(i) *$\mathbb{A}^n$ and $\emptyset$ are both algebraic sets.*

(ii) *$V(S) \cup V(T) = V(S \cdot T)$ where $S \cdot T = \{FG \mid F \in S, G \in T\}$.*

(iii) *$\bigcap_{i \in \mathcal{I}} V(S_i) = V\left(\cup_{i \in \mathcal{I}} S_i\right)$ is an algebraic subset*

Proof. We will prove each claim individually.

(i) We have $\mathbb{A}^n = V(\emptyset)$ and $\emptyset = V(\Bbbk^*)$.

(ii) Suppose $P \in V(S) \cup V(T)$, then $F(P) \cdot G(P) = 0$ for all $F \in S$ and $G \in T$. Thus $V(S) \cup V(T) \subseteq V(S \cdot T)$.

On the other hand if $P \in V(S \cdot T)$, then $F(P) \cdot G(P) = 0$ for all $F \in S$ and $G \in T$, assuming $P \notin V(S)$, then there exists $F \in S$ such that $F(P) \neq 0$ however this implies that $G(P) = 0$ for all $G \in T$, since $\Bbbk$ is a domain, and it therefore follows $V(S \cdot T) \subseteq V(S) \cup V(T)$.

(iii) Follows from Definition 2.24. ■

Corollary 2.29. *$(\mathbb{A}^n, \mathcal{T}_Z)$ is a topological space.*

Proof. Let $U, U' \in \mathcal{T}_Z$, then there exists $S, T \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ such that $U = \mathbb{A}^n \backslash V(S)$ and $U' = \mathbb{A}^n \backslash V(T)$, thus it follows that

$$U \cap U' = \mathbb{A}^n \backslash (V(S) \cup V(T)) = \mathbb{A}^n \backslash V(S \cdot T) = V(S \cdot T)^c \in \mathcal{T}_Z$$

confer Assertion (ii) of Proposition 2.28. Let $\{U_i\}_{i \in \mathcal{I}}$ be an indexed family of open sets, then there exists an indexed family $\{S_i\}_{i \in \mathcal{I}}$ of subsets of $\Bbbk[X_1, X_2, \ldots, X_n]$, such that $U_i = \mathbb{A}^n \backslash V(S_i)$ for all $i \in \mathcal{I}$. It therefore follows that

$$\bigcup_{i \in \mathcal{I}} U_i = \bigcup_{i \in \mathcal{I}} \mathbb{A}^n \backslash V(S_i) = \mathbb{A}^n \backslash \bigcap_{i \in \mathcal{I}} V(S_i) = \mathbb{A}^n \backslash V\left(\bigcup_{i \in \mathcal{I}} S_i \right) \in \mathcal{T}_Z$$

which follows from De Morgan Law for set differences and Assertion (iii) of Proposition 2.28. Finally since $\emptyset$ and $\mathbb{A}^n$ are both algebraic, by Assertion (i) of Proposition 2.28, we have $\emptyset^c = \mathbb{A}^n \in \mathcal{T}_Z$ as well as $(\mathbb{A}^n)^c = \emptyset \in \mathcal{T}_Z$. ■

Example 2.30. From the fundamental theorem of algebra we know that a univariate polynomial $F \in \Bbbk[X]^*$ has exactly $\deg(F)$ roots. Hence the algebraic and hence closed subsets of $\mathbb{A}^1$ consists of the finite subsets as well as $\mathbb{A}^1$ itself. □

2.2.1 Vanishing Ideals and Hilberts Nullstellensatz

So far we have only considered how subsets of $\Bbbk[X_1, X_2, \ldots, X_n]$ define subsets of $\mathbb{A}^n$, a natural next step is to introduce a way in which subsets of $\mathbb{A}^n$, defines ideals in $\Bbbk[X_1, X_2, \ldots, X_n]$.

Definition 2.31. Let $V \subseteq \mathbb{A}^n$, be an algebraic set, then the *vanishing ideal* of V is defined as

$$I(V) := \{F \in \Bbbk[X_1, X_2, \ldots, X_n] \mid F(P) = 0 \text{ for all } P \in V\}$$

This is clearly an ideal of $\Bbbk[X_1, X_2, \ldots, X_n]$ as $F, G \in I(V)$ implies that $(F + G)(P) = F(P) + G(P) = 0$ and $(FG)(P) = F(P)G(P) = 0$ for all $P \in V$. If $V = \{P_1, P_2, \ldots, P_n\}$ then we may write $I(P_1, P_2, \ldots, P_n)$ instead of $I(V)$.

Example 2.32. Let $P := (0, 0, \ldots, 0) \in \mathbb{A}^n$, then the vanishing ideal $I(P)$ consist of the set of polynomials with no constant terms. Additionally $I(\mathbb{A}^n) = \{0\}$ since every polynomial consist of a finite number of terms and every algebraically closed field is infinite. □

Before we prove the main result of this section, we need to introduce a special type of ideal.

Definition 2.33. Let R be a commutative ring and I be an ideal in R, then the *radical* of I is defined as:

$$\mathrm{Rad}(I) := \{x \in R \mid \text{there exists } n \in \mathbb{N} \text{ such that } x^n \in I\}$$

During the proof of the main theorem, the following proposition will be used. We will omit the proof of this result, instead we refer to the proof found in Fulton (2008)[Section 1.7 and 1.10].

Proposition 2.34 (Weak Nullstellensatz)**.** *Let $I \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ be a proper ideal then $V(I) \neq \emptyset$.*

The proposition above is interesting in itself, since it means that every proper ideal I of $\Bbbk[X_1, X_2, \ldots, X_n]$, there exists at least one point $P \in \mathbb{A}^n$ such that $F(P) = 0$ for all $F \in I$.

Theorem 2.35 (Hilbert Nullstellensatz)**.** *Let $I \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ be an ideal, then $I(V(I)) = \mathrm{Rad}(I)$.*

Before we prove the theorem, we will dissect the statement of the theorem. Recall that I is finitely generated, by Corollary 2.21. Assume $G_1, G_2, \ldots, G_m \in \Bbbk[X_1, X_2, \ldots, X_n]$ generates I. Then if $F \in \Bbbk[X_1, X_2, \ldots, X_n]$ vanishes whenever $G_1, G_2, \ldots, G_m$ vanish, then there exists a $k \in \mathbb{N}$ such that $F^k \in I$ and hence $F^k = \sum_{i=1}^m H_i G_i$ for some $H_1, H_2, \ldots, H_m \in \Bbbk[X_1, X_2, \ldots, X_n]$.

Proof. We start by showing that $\mathrm{Rad}(I) \subseteq I(V(I))$. Suppose $P \in V(I)$, then if $F \in \mathrm{Rad}(I)$, then there exists $m \in \mathbb{N}$ such that $F^m \in I$, meaning $F^m(P) = 0$ which implies $F(P) = 0$, since $\Bbbk$ is a domain. Hence we have that $F \in I(V(I))$.

Next we show that $I(V(I)) \subseteq \mathrm{Rad}(I)$. Let $G_1, G_2, \ldots, G_m$ generate I, and $F \in I(V(I))$. Consider the ideal $J = \langle G_1, G_2, \ldots, G_m, X_{n+1}F - 1\rangle \subseteq \Bbbk[X_1, X_2, \ldots, X_{n+1}]$, then $V(J) = \emptyset$, since F vanishes whenever $G_1, G_2, \ldots, G_m$ vanish. Applying Proposition 2.34, we get that $J = \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ and hence $1 \in J$ therefore there exists $H_1, H_2, \ldots, H_{m+1} \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ such that

$$1 = \sum_{i=1}^{m} H_i(X_1, X_2, \ldots, X_{n+1})G_i + H_{m+1}(X_1, X_2, \ldots, X_{n+1})(X_{n+1}F - 1). \tag{2.1}$$

Let $Y = 1/X_{n+1}$ and $k \in \mathbb{N}$ such that $k \geq \max\{\deg(H_i) \mid i \in \{1, 2, \ldots, m+1\}\} + 1$. Then multiplying both sides of Equation (2.1) by Y^n we see that:

$$Y^k = \sum_{i=1}^{m} H_i'(X_1, X_2, \ldots, X_n, Y)G_i + H_{m+1}'(X_1, X_2, \ldots, X_n, Y)(F - Y) \tag{2.2}$$

where $H_1', H_2', \ldots, H_{m+1}' \in \Bbbk[X_1, X_2, \ldots, X_n, Y]$. The rest follows by substituting $Y = F$ in Equation (2.2). ∎

2.2.2 Projective Spaces

Next we will define protective spaces, we define these to introduce the notion of points at infinity. To illustrate why such a notion might be usefull consider the two curves, defined by the polynomial equations $XY - 1 = 0$ and $X = 0$ respectively. Then the two curves do not intersect, however they do approach each other asymptotically, it is in this setting that we would like to say that the two curves intersect at infinity.

Definition 2.36. The *n-dimensional projective space* over $\Bbbk$ written $\mathbb{P}^n$ is the set of equivalence classes on $\mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\}$, corresponding to the equivalence relation

$$(a_1, a_2, \ldots, a_{n+1}) \sim (b_1, b_2, \ldots, b_{n+1}) \iff \exists \lambda \in \Bbbk^* \text{ such that } b_i = \lambda a_i$$

for all $i = 1, 2, \ldots, n+1$. The elements in $\mathbb{P}^n$ are called *projective points* or simply *points*.

Most of the definitions and results which are stated and proved for affine spaces and their subsets have projective counterparts.

One can identify the elements in $\mathbb{P}^n$ with the lines in $\mathbb{A}^{n+1}$, as two points in $\mathbb{A}^{n+1} \setminus \{(0,0,\ldots,0)\}$ are equivalent if and only if they lie on the same line, though the origin. If $(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}$ is a representative of the equivalence class $P \in \mathbb{P}^n$ we call $x_1, x_2, \ldots, x_{n+1}$ *homogeneous coordinates* for P and we write $P = [x_1 : x_2 : \cdots : x_{n+1}]$.

We let $U = \{[x_1 : x_2 : \cdots : x_{n+1}] \in \mathbb{P}^n \mid x_{n+1} \neq 0\}$. The function $\varphi\colon \mathbb{A}^n \to U$, defined as $\varphi(x_1, x_2, \ldots, x_n) = [x_1 : x_2 : \cdots : x_n : 1]$, defines a bijection and thus there is a one to one correspondence between the elements in $\mathbb{A}^n$ and U. We define the *hyperplane at infinity*

$$H_\infty := \mathbb{P}^n \setminus U = \mathbb{P}^n \setminus \varphi(\mathbb{A}^n) = \{[x_1 : x_2 : \cdots : x_{n+1}] | x_{n+1} = 0\}.$$

The point $[x_1 : x_2 : \cdots : x_n] \in \mathbb{P}^{n-1}$ corresponds to the point $[x_1 : x_2 : \cdots : x_n : 0] \in \mathbb{P}^n$ which shows that $\mathbb{P}^{n-1}$ can be identified with H_∞. Hence $\mathbb{P}^n$ can be thought of as the union between a set corresponding to $\mathbb{A}^n$ and a set corresponding to $\mathbb{P}^{n-1}$.

Given a polynomial $F \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$, we need to be careful when defining if F has a root at a projecitve point $[x_1 : x_2 : \cdots : x_{n+1}] \in \mathbb{P}^n$, as it is not generally the case that $F(x_1, x_2, \ldots, x_{n+1}) = 0$ implies $F(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1}) = 0$ for all $\lambda \in \Bbbk^*$. Even though $(x_1, x_2, \ldots, x_{n+1}) \sim (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$ for all $\lambda \in \Bbbk^*$.

One situation where this is the case is when F is a homogeneous polynomial of degree d. Then we can write $F = \sum_{i=1}^k c_i G_i$, where $c_1, c_2, \ldots, c_k \in \Bbbk^*$ and $G_1, G_2, \ldots, G_k \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ are monomials of degree d. If we evaluate F at $(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1})$ we see that:

$$\begin{aligned} F(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1}) &= \sum_{i=1}^k c_i G_i(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1}) \\ &= \sum_{i=1}^k c_i \lambda^d G_i(x_1, x_2, \ldots, x_{n+1}) = \lambda^d \cdot F(x_1, x_2, \ldots, x_{n+1}) \end{aligned}$$

Now since $\Bbbk$ is a field, and hence a domain, we see that $F(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1}) = 0$ if and only if $F(x_1, x_2, \ldots, x_{n+1}) = 0$.

Definition 2.37. Let $F \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$. Then F has a *projective root* at $P = [x_1 : x_2 : \cdots : x_{n+1}] \in \mathbb{P}^n$ if $F(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1}) = 0$ for all $\lambda \in \Bbbk^*$. The *projective zero set* of a subset $S \subseteq \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ is defined as

$$V_{\mathbb{P}}(S) := \{P \in \mathbb{P}^n \mid F \text{ has a projective root at } P, \text{ for all } F \in S\}$$

A subset $V \subseteq \mathbb{P}^n$ is called *algebraic* if, there exists $S \subseteq \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ such that $V = V_{\mathbb{P}}(S)$

Remark 2.38. Like the algebraic subsets of $\mathbb{A}^n$, the algebraic subsets of $\mathbb{P}^n$ form the closed sets of an topology on $\mathbb{P}^n$, this topology is also refereed to as the *zariski topology* on $\mathbb{P}^n$. We will however not prove this, but the interested reader can have a look at Fulton (2008)[Section 6.1].

We likewise define the ideal of a set of projective points, analogously to the definition given for subsets of an affine space.

Definition 2.39. Let $V \subseteq \mathbb{P}^n$, then the *vanishing ideal* of V is defined as

$$I_{\mathbb{P}}(V) := \{F \in \Bbbk[X_1, X_2, \ldots, X_{n+1}] \mid F \text{ has a projective root at } P \text{ for all } P \in V\}$$

Finally we introduce a way to transform a polynomial $F \in \Bbbk[X_1, X_2, \ldots, X_n]$ to a homogeneous polynomial in $\Bbbk[X_1, X_2, \ldots, X_{n+1}]$, and by extension we show how affine algebraic sets correspond to projective ones and vice versa.

Definition 2.40. Let $F \in \Bbbk[X_1, X_2, \ldots, X_n]$ then the *homogenisation* of F denoted $F^* \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ is then defined as

$$F^* = X_{n+1}^{\deg(F)} F(X_1/X_{n+1}, X_2/X_{n+1}, \ldots, X_n/X_{n+1})$$

Furthermore for an ideal $I \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ we define it's *homogenisation* as $I^* := \{F^* \mid F \in I\}$.
On the contrary suppose $G \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$, then the *dehomogenisation* of G denoted $G_* \in \Bbbk[X_1, X_2, \ldots, X_n]$ is defined as:

$$G_*(X_1, X_2, \ldots, X_n) := G(X_1, X_2, \ldots, X_n, 1)$$

If $I \subseteq \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ is an ideal, we define it's *dehomogenisation* as $I_* := \{G_* | G \in I\}$.

If V is an affine algebraic set, we let $I := I(V)$ and we define the *projective closure* of V as $V^* = V_{\mathbb{P}}(I^*)$, conversely if V is a projective algebraic set, we let $I := I_{\mathbb{P}}(V)$ and define $V_* = V(I_*)$.

2.2.3 Affine and Projective Vararities

In this subsection we will define both affine and projective vararities, the contents will be based on Fulton (2008)[Chapter 2 and 4] as well as Pellikaan et al. (2018)[Subsection 11.1.1]. We will start in the affine case:

Definition 2.41. Let $V \subseteq \mathbb{A}^n$ be an algebraic set. Then V is called *reducible* if there exists proper algebraic subsets $V_1, V_2 \subset V$ such that $V = V_1 \cup V_2$. Otherwise, V is called an *irreducible*, an affine algebraic set which is irreducible is called an *affine variety*.

These varieties will be one of our main objects of study. We will usually follow the convention of Pellikaan et al. (2018) and use $\mathcal{X}$ to denote an affine variety.

Example 2.42. Consider the polynomial $F = X^2 - Y^2 \in \Bbbk[X, Y]$, then $V(F)$ is reducible. This can be seen as follows: The polynomial F can be factored as $(X + Y)(X - Y)$, and hence $V(F) = V(X + Y) \cup V(X - Y)$, so $V(F)$ is the union of two lines in $\mathbb{A}^2$. □

Below we prove a couple of useful results which well help us to determine whether an algebraic set is a variety.

Proposition 2.43. *The algebraic set $V \subseteq \mathbb{A}^n$ is an affine variety if and only if $I(V)$ is a prime ideal.*

Proof. Suppose $I(V)$ is not prime, and that $FG \in I(V)$, but $F, G \notin I(V)$, then $V = (V \cap V(F)) \cup (V \cap V(G))$, since $FG \in I(V)$ if and only if we for all $P \in V$ have either $F(P) = 0$ or $G(P) = 0$. However $V \cap V(F)$ and $V \cap V(G)$ are proper algebraic subsets of V, confer Proposition 2.28(iii), and thus V is reducible.

On the other hand suppose $V = V_1 \cup V_2$, where V_1, V_2 are algebraic and proper subsets of V, then $I(V) \subset I(V_i)$. Thus, there exists $F_1 \in I(V_1) \setminus I(V)$, and $F_2 \in I(V_2) \setminus I(V)$. However, we have $F_1 F_2 \in I(V)$ since $V = V_1 \cup V_2$ and hence either $F_1(P) = 0$ or $F_2(P)$ for all $P \in V$. ■

Recall that the polynomial F from Example 2.42, could be factorized into two unique factors, both with degree greater or equal to 1 meant that $V(F)$ was reducible. The corollary below, illustrates the opposite situation.

Corollary 2.44. *Let $F \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$, be an irreducible polynomial, then $V(F)$ is an affine variety.*

Proof. First we note that $\Bbbk$ is a field it is a PID and recall that every PID is a UFD. From this it follows that the ring $\Bbbk[X_1, X_2, \ldots, X_{n+1}]$ is a UFD, confer Corollary 2.17. This in turn imply that every irreducible element is a prime element, from this it follows that $\langle F \rangle$ is a prime ideal, and hence $V(F) = V(\langle F \rangle)$ is an affine variety, by Proposition 2.43. ■

Considering Example 2.42 and Corollary 2.44, it is natural to ask the following question: "Does $G \in \Bbbk[X_1, X_2, \ldots, X_n]$ being reducible imply that $V(G)$ is reducible." This is not the case consider for instance the polynomial $F = X^2 + Y^2 + 2XY$ which can be factorized as $(X + Y)^2$ so $V(F) = V(X + Y)$, but $X + Y$ is irreducible, so by Corollary 2.44, $V(F)$ is an affine variety.

Suppose we have a prime ideal $I \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$, consider the associated affine variety $\mathcal{X} := V(I)$. Let $F \in \Bbbk[X_1, X_2, \ldots, X_n]$ and $G \in I$, then $F(P) = F(P) + G(P)$ for all $P \in \mathcal{X}$. For this reason we consider the following ring, consisting of the left cosets $[F] = F + I$ for some $F \in \Bbbk[X_1, X_2, \ldots, X_n]$.

Definition 2.45. Let $I \subseteq \Bbbk[X_1, X_2, \ldots, X_n]$ be a prime ideal, consider the affine variety $\mathcal{X} := V(I)$ associated with I. Then the ring $\Bbbk[\mathcal{X}] := \Bbbk[X_1, X_2, \ldots, X_n]/I$ is called the *coordinate ring* of $\mathcal{X}$.

We will view the elements in $\Bbbk[\mathcal{X}]$ both as equivalence classes of polynomials, but also as functions on $\mathcal{X}$, as $[F] = [G]$ if and only if $F(P) = G(P)$ for all $P \in \mathcal{X}$. If F, G and H are polynomials, then their cosets modulo I, will be denoted as f, g and h respectively.

Consider the ideal I from Definition 2.45, since I is prime, it follows that $\Bbbk[\mathcal{X}]$ is an integral domain. This can be seen as follows given $f, g \in \Bbbk[\mathcal{X}]$, then $f \cdot g = [FG] + I = 0$ if and only if $FG \in I$, it now follows by the primality of I that either $F \in I$ or $G \in I$. Thus, we may form a quotient field of $\Bbbk[\mathcal{X}]$.

Definition 2.46. Let $\mathcal{X} \subseteq \mathbb{A}^n$ be an affine variety, then the quotient field of $\Bbbk[\mathcal{X}]$ denoted $\Bbbk(\mathcal{X})$, is called the *function field* of $\mathcal{X}$. We will refer to the elements of $\Bbbk(\mathcal{X})$ as *rational functions*. Let $\alpha \in \Bbbk(\mathcal{X})$ be a rational function, then α is said to be *defined* at $P \in \mathcal{X}$ if there exists $f, g \in \Bbbk[\mathcal{X}]$ such that $\alpha = f/g$ and $g(P) \neq 0$.

Example 2.47. Consider the irreducible polynomial $F = XY - Z^2 \in \Bbbk[X, Y, Z]$, then $\mathcal{X} := V(F)$ is an affine variety, by Corollary 2.44. Consider the point $P = (0, 1, 0) \in \mathcal{X}$, and the rational function $\alpha = X/Z$, then it would appear that α is not defined at P, however Z/Y is also a representative of α, since $XY = Z^2$ for all points in $\mathcal{X}$. So α is actually defined at P after all. □

As we mentioned in section 2.2.2 most of the definitions regarding affine spaces, have analogous projective counterparts, below we introduce more of these counterparts.

Definition 2.48. Let $V \subseteq \mathbb{P}^n$ be a projective algebraic set. Then V is called *reducible* if there exists proper projective algebraic subsets $V_1, V_2 \subset V$ such that $V = V_1 \cup V_2$. Otherwise, V is called *irreducible* or an *projective variety*.

Again we state an analogous result of Proposition 2.43 and Corollary 2.44, this time without proof.

Proposition 2.49. *The algebraic set $V \subseteq \mathbb{P}^n$ is a projective variety if and only if $I_{\mathbb{P}}(V)$ is a prime ideal.*

Corollary 2.50. *Let $F \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ be an irreducible homogeneous polynomial then $V_{\mathbb{P}}(f)$ is a projective variety.*

Let $\mathcal{X}$ be an affine variety, then the homogenization of $I(\mathcal{X})$ is a homogeneous prime ideal, which by Proposition 2.49 defines a projective variety $\mathcal{X}^*$. Similarly if $\mathcal{X}$ is a projective variety then the dehomogenization of $I(\mathcal{X})$ is a prime ideal, and hence by Proposition 2.43 the affine algebraic set X_* defines an affine variety.

Like in the affine case, we once again have that $I_{\mathbb{P}}(\mathcal{X})$ is a prime ideal if and only if $\mathcal{X}$ is a projective variety, as such we can make a definition analogously to Definition 2.45 and Definition 2.46.

Definition 2.51. Let $\mathcal{X}$ be a projective variety then he *homogenus cordinate ring* on $\mathcal{X}$ is defined as $\Bbbk_{\mathbb{P}}[\mathcal{X}] := \Bbbk[X_1, X_2, \ldots, X_{n+1}]/I_{\mathbb{P}}(\mathcal{X})$, an element $f \in \Bbbk_{\mathbb{P}}[\mathcal{X}]$ is called a *form of degree* $\deg(F)$ if F is a homogeneous polynomial. The *homogeneous function field* $\Bbbk_{\mathbb{P}}(\mathcal{X})$ is defined as the quotient field of $\Bbbk_{\mathbb{P}}[\mathcal{X}]$

Remark 2.52. In general elements in $\Bbbk_{\mathbb{P}}[\mathcal{X}]$ and $\Bbbk_{\mathbb{P}}(\mathcal{X})$, cannot be viewed as functions from $\mathcal{X}$, as a point $P \in \mathcal{X} \subseteq \mathbb{P}^n$ has multiple distinct homogeneous coordinates.

Recall from Section 2.2.2 that if $F = \sum_{i=1}^{k} c_i G_i \in \Bbbk[X_1, X_2, \ldots, X_{n+1}]$ is a homogeneous polynomial of degree d then $F(\lambda a_1, \lambda a_2, \ldots, \lambda a_{n+1}) = \lambda^d \cdot F(a_1, a_2, \ldots, a_{n+1})$. Hence:

$$\frac{F(\lambda a_1, \lambda a_2, \ldots, \lambda a_{n+1})}{G(\lambda a_1, \lambda a_2, \ldots, \lambda a_{n+1})} = \frac{F(a_1, a_2, \ldots, a_{n+1})}{G(a_1, a_2, \ldots, a_{n+1})}$$

when F and G are homogeneous polynomials of the same degree.

Definition 2.53. Let $\mathcal{X}$ be a projective variety the *function field* of $\mathcal{X}$ is defined as

$$\Bbbk(\mathcal{X}) := \{f/g \in \Bbbk_{\mathbb{P}}(\mathcal{X}) \mid f, g \in \Bbbk_{\mathbb{P}}[\mathcal{X}] \text{ are forms of the same degree}\}.$$

The elements in $\mathcal{X}$ are called *rational functions*, a rational function α is said to be *defined* at $P \in \mathcal{X}$ if there exists $f, g \in \Bbbk_{\mathbb{P}}[\mathcal{X}]$ such that $g(P) \neq 0$ and $\alpha = f/g$.

Remark 2.54. Let $\mathcal{X}$ be an affine variety, then $\Bbbk[\mathcal{X}]$ and $\Bbbk[\mathcal{X}^*]$ are isomorphic. Since the map $\Bbbk[\mathcal{X}] \ni f/g \mapsto x_{n+1}^m f^*/g^* \in \Bbbk[\mathcal{X}^*]$, where $m = \deg(g) - \deg(f)$, is an isomorphism. At first one might question why f^*/g^* is multiplied by x_{n+1}^m, however this is done to make sure that the two homogeneous polynomials have the same degree.

2.2.4 Local and Discrete Valuation Rings

The contents of this subsection will be based on Fulton (2008)[Sections 2.4 and 2.5]. The results presented will apply to both affine and projective varieties, most of the proofs will however only be given in the affine cases, however the results generalize since $\Bbbk(\mathcal{X})$ and $\Bbbk(\mathcal{X}^*)$ are isomorphic, if $\mathcal{X}$ is an affine variety.

Definition 2.55. Let $\mathcal{X}$ be an affine or projective variety and $P \in \mathcal{X}$, then the ring

$$\mathcal{O}_P(\mathcal{X}) := \{f/g \in \Bbbk(\mathcal{X}) \mid f/g \text{ is defined at } P\}$$

is called *the local ring of* $\mathcal{X}$ *at* P, furthermore we define:

$$\mathfrak{m}_P(\mathcal{X}) := \{f/g \in \mathcal{O}_P(\mathcal{X}) \mid f(P) = 0\}.$$

By identifying $f \in \Bbbk[\mathcal{X}]$ with $f/1 \in \mathcal{O}_P(\mathcal{X})$ we see that $\Bbbk[\mathcal{X}]$ is a subring of $\mathcal{O}_P(\mathcal{X})$. Additionally, it is straight forward to see that $\mathcal{O}_P(\mathcal{X})$ is a subring of $\Bbbk(\mathcal{X})$.

The notion of a local ring R is defined more generally in Lang (2002)[Section 2.4], to be a ring with a unique maximal ideal, in the proposition below we prove that $\mathcal{O}_P(\mathcal{X})$ satisfies this definition.

Proposition 2.56. *Let $\mathcal{X}$ be an affine or projective variety and $P \in \mathcal{X}$, then $\mathfrak{m}_P(\mathcal{X})$ is the unique maximal ideal of $\mathcal{O}_P(\mathcal{X})$*

Proof. Suppose $I \subseteq \mathcal{O}_P(\mathcal{X})$ such that $I \not\subseteq \mathfrak{m}_P(\mathcal{X})$, then there exists $f/g \in I$ such that $f(P) \neq 0$, then f/g is a unit as $(f/g)^{-1} = g/f$, is defined at P, and hence $(f/g)^{-1}(f/g) = 1 \in I$ which in turn implies that $I = \mathcal{O}_P(\mathcal{X})$. ∎

Lemma 2.57. *Let $\mathcal{X}$ be an affine or projective variety and $P \in \mathcal{X}$, then $\mathcal{O}_P(\mathcal{X})$ is a Noetherian domain.*

Proof. Let $I \subseteq \mathcal{O}_P(\mathcal{X})$ be an ideal. We will show that I is finitely generated, consider the ideal $I \cap \Bbbk[\mathcal{X}]$ of $\Bbbk[\mathcal{X}]$, this ring is Noetherian by Proposition 2.22, and thus there exists $f_1, f_2, \ldots, f_m \in \Bbbk[\mathcal{X}]$ which generate $I \cap \Bbbk[\mathcal{X}]$. We will show that $f_1, f_2, \ldots, f_m$ also generates I in $\mathcal{O}_P(\mathcal{X})$. Suppose $\alpha \in I$, then there exists $g, h \in \Bbbk(\mathcal{X})$ such that $\alpha = g/h$ and $h(P) \neq 0$, as such we have $h\alpha \in \Bbbk[\mathcal{X}] \in I \cap \Bbbk[\mathcal{X}]$, now since $I \cap \Bbbk[\mathcal{X}]$ was generated by $f_1, f_2, \ldots, f_m$ there exists $c_1, c_2, \ldots, c_m \in \Bbbk[\mathcal{X}]$ such that $h\alpha = \sum_{i=1}^m c_i f_i$ therefore $\alpha = \sum_{i=1}^m (c_i/h) f_i$. However, since α was chosen arbitrary, we have proven that $\mathcal{O}_P(\mathcal{X})$ is a Noetherian domain. ■

Definition 2.58. A ring R is called a *discrete valuation ring* if there exists an irreducible element $t \in R$, which we shall call a *uniformizing parameter*, such that every $z \in R \setminus \{0\}$ can be written uniquely as $z = ut^m$, where $u \in R$ is a unit and $m \in \mathbb{N}$ is called the *order* of z, which we denote $ord(z)$.

The following theorem will be especially useful, in our treatment of plane algebraic curves.

Theorem 2.59. *If $\mathfrak{m}_P$ is a principal ideal generated by t, then $\mathcal{O}_P(\mathcal{X})$ is a discrete valuation ring with uniformizing parameter t.*

Proof. Suppose $\langle t \rangle = \mathfrak{m}_P$ and that $z \in \mathcal{O}_P$, we will start by showing uniqueness: Suppose $z = ut^m = vt^l$, where u, v are units and $m, l \in \mathbb{N}$, we can without loss of generality assume that $m \geq l$. This implies that $ut^{m-l} = v$ however as t generates $\mathfrak{m}_p$, it is not a unit, hence we must have $m = l$ and $u = v$.

As for the existence of a unit $u \in \mathcal{O}_P(\mathcal{X})$ and $m \in \mathbb{N}$ such that $z = ut^m$: Suppose $z \in \mathcal{O}_P(\mathcal{X})$, we may assume that z is not a unit since if z is a unit we may pick $u = z$ and $m = 0$. Now as z is not a unit we have $z \in \mathfrak{m}_P$ and hence there exists $z_1 \in \mathcal{O}_P(\mathcal{X})$ such that $z = z_1 t$, if z_1 is a unit, then we are finished, otherwise we may similarly write $z_1 = z_2 t$, and so on. As such we construct an infinite chain of ideals $\langle z_1 \rangle \subseteq \langle z_2 \rangle \subseteq \cdots$ since $\mathcal{O}_P(\mathcal{X})$ is Noetherian domain, by Lemma 2.57, the chain must have a maximal member, confer Proposition 2.19. Meaning that there exists $k \in \mathbb{N}$ such that $\langle z_k \rangle = \langle z_{k+1} \rangle$, which implies $z_{k+1} = v z_k$ for some $v \in \mathcal{O}_P(\mathcal{X})$. Combining this with $z_k = z_{k+1} t$ we see that $z_k = v z_k t = (vt) z_k$, thus $vt = 1$. However, this is a contradiction as t generates $\mathfrak{m}_P$ and hence is not a unit. ■

2.3 Algebraic Plane Curves

In this section we will fix a finite field $\mathbb{F}_q$. We will apply the theory of algebraic geometry, to the affine and projective plane. However since $\mathbb{F}_q$ is not algebraically closed, confer Proposition 2.4, we will let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$, as in Proposition 2.8.

Definition 2.60. Let $F \in \mathbb{F}_q[X, Y]$, then the zero set $V(F)$ is called an *affine plane curve* over $\overline{\mathbb{F}}_q$. The equation $F = 0$ is called the *defining equation* of $V(F)$. The points $P \in \mathbb{F}_q^n \cap V(F)$ are called *$\mathbb{F}_q$-rational points* of $V(F)$. The *degree* of $V(F)$ is the degree of F, a curve of degree 1 is called a *line*.

In general the defining equation of an affine plane curve, is not unique, for instance the equations $X = 0$ and $aX = 0$ describe the same curve for all $a \in \mathbb{F}_q^*$. Additionally it is worth highlighting that many of the properties of the curve depend on the particular ground field.

Example 2.61. Every line L over $\mathbb{F}_q$ in the affine plane has q $\mathbb{F}_q$-rational points. Consider the general defining equation $aX + bY + c = 0$ of a line where at least one of a, b are non-zero. Then assuming $a \neq 0$ we get that $X = -a^{-1}(bY + c)$, so picking $y \in \mathbb{F}_q$ yields an element $x \in \mathbb{F}_q$ such that (x, y) is a $\mathbb{F}_q$-rational point of L. Conversely if $a = 0$, we see that $bY + c = 0$. Hence we see that $Y = -b^{-1}c$, so $(x, -b^{-1}c)$ where $x \in \mathbb{F}_q$ are the only $\mathbb{F}_q$-rational points on L. □

Definition 2.62. Let $F \in \mathbb{F}_q[X, Y]$ and $P \in \mathbb{A}^n(\overline{\mathbb{F}}_q)$ be a point on the affine plane curve $V(F)$, then P is called *singular* if $F_X(P) = F_Y(P) = 0$, the point P is called *regular* otherwise. If all points $P \in V(F)$ are singular or regular then the curve it self is called singular or regular respectively. Let $P = (a, b)$ be a regular point of the curve $V(F)$, then we define the *tangent line* at P as the affine curve $V\left(F_X(P)(X - a) + F_Y(P)(Y - b)\right)$.

This is one of the properties, which depends strongly on the characteristic of the ground field, we will illustrate this in Example 2.67.

In corollary 2.44 we saw that the affine zero set of irreducible polynomials were affine varieties, we would like to extend the notion of irreducibility to polynomials over $\mathbb{F}_q$, however as we consider the affine zero set over the ground field $\overline{\mathbb{F}}_q$, we are primarily interested in if $F \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ is also irreducible when viewed as a polynomial in $\overline{\mathbb{F}}_q[X_1, X_2, \ldots, X_n]$.

Definition 2.63. Let $F \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$, then F is called *absolutely irreducible* if F is irreducible in $\overline{\mathbb{F}}_q[X_1, X_2, \ldots, X_n]$. That is there exists no $G \in \overline{\mathbb{F}}_q[X_1, X_2, \ldots, X_n]$ with $0 < \deg(G) < \deg(F)$, such that $F = GH$ for some $H \in \overline{\mathbb{F}}_q[X_1, X_2, \ldots, X_n]$.

We will call $V(F)$ an *absolutely irreducible affine plane curve* if $F \in \mathbb{F}_q(X, Y)$ is absolutely irreducible, by Corollary 2.44 we see that every absolutely irreducible affine plane curve is an affine variety.

Definition 2.64. If $F \in \overline{\mathbb{F}}_q[X, Y, Z]$ is a homogeneous polynomial, then $V_{\mathbb{P}}(F)$ is called a *projective plane curve*. A point $P \in V_{\mathbb{P}}(F)$ is called *rational* if there exists a representation $P = [a : b : c]$, where $a, b, c \in \mathbb{F}_q$.

The *defining equation* and *degree* of a projective plane curve are defined similarly to the affine case. Hence we will omit them.

Definition 2.65. Let $F \in \overline{\mathbb{F}}_q[X, Y, Z]$ be a homogeneous polynomial and $P \in V_{\mathbb{P}}(F)$. Then P is called a *singular* if $F_X(P) = F_Y(P) = F_Z(P) = 0$, otherwise P is called *regular*

Remark 2.66. Since the polynomial F is homogeneous we see that F_X, F_Y and F_Z are homogeneous as well. Combining this with the fact that the notion of a root of a homogeneous polynomial at a projective point, is well defined, we see that the notion of a singular and regular point on a projective line is well defined.
However since the value of a homogeneous polynomial at a projective point is not generally well defined, we can not define a tangent line of a projective plane curve.

Let $F \in \mathbb{F}_q[X, Y]$, then $V(F)$ is an affine plane curve and $V(F^*)$ is a projective plane curve, furthermore we say that $V(F^*)$ *corresponds to* $V(F)$.

Similarly to an affine curve, a projective plane curve is a projective variety if the defining polynomial F is absolutely irreducible, by Corollary 2.50.

Example 2.67. Let $F = X^m + Y^m + Z^m$, then the *Fermat curve* of degree m denoted $\mathcal{F}_m$ is the projective plane curve with defining equation $F = 0$. The partial derivatives F was found in Example 2.67, as $mX^{m-1}, mY^{m-1}, mZ^{m-1}$. Assuming $m \geq 2$ and that m is coprime with q then this curve is regular. However if m is not coprime with q, then all points are singular. □

Example 2.68. Let p be a prime, and $\overline{\mathbb{F}}_{p^2}$ be the algebraic closure of $\mathbb{F}_{p^2}$, as noted Remark 2.7 this algebraic closure exists. Let $F := Y^pZ + YZ^p - X^{p+1}$, then the *Hermitian curve* $\mathcal{H}_p$ over $\overline{\mathbb{F}}_{p^2}$ is the projective curve with defining equation $F = 0$. The polynomial F has the following partial derivatives: $F_X = -(p+1)X^p = -X^p$, since $\mathrm{char}(\overline{\mathbb{F}}_{p^2}) = p$, $F_Y = Z^p$ and $F_Z = Y^p$. Hence the Hermitian curve is another example of a smooth curve. □

Lemma 2.69. *Let $\mathcal{X}$ be a regular affine plane curve and $P \in \mathcal{X}$, then the unique maximal ideal $\mathfrak{m}_P \subseteq \mathcal{O}_P(\mathcal{X})$ is a principal ideal.*

Proof. Let $F = 0$ be the defining equation of $\mathcal{X}$. We may assume that $P = (0,0)$, and that the tangent of $\mathcal{X}$ at P has defining equation $Y = 0$[1]. Furthermore we have that $\mathfrak{m}_P = \langle x, y\rangle$, by Hilbert Nullstellensatz (Theorem 2.35). It follows that all monomials of F have degree greater than or equal to 2, as $\mathcal{X}$ is regular and the tangent line has defining equation $Y = 0$. Hence one can write

$$F(X,Y) = Y + YG(Y) + XH(X,Y) \tag{2.3}$$

where $G(0) = 0$ and $H(0,0) = 0$. Now $F(x,y) = 0$ implies that $y = -xH(x,y)(1+G(y))^{-1}$, by Equation (2.3). From this it follows that $H(x,y) \in \mathcal{O}_P(\mathcal{X})$ as $G(0) = 0$. Therefore $y \in \langle x\rangle$ and hence $\mathfrak{m}_P = \langle x, y\rangle = \langle x\rangle$. ■

Remark 2.70. If $\mathcal{X}$ is a projective plane curve we likewise have that $\mathcal{O}_P(\mathcal{X})$ is a prinicipal ideal, as $\mathcal{O}_P(\mathcal{X})$ is isomorphic to $\mathcal{O}_P(\mathcal{X}_*)$, confer Remark 2.54.

In many examples we will need a way to compute the uniformizing parameter at a point of a projective plane curve. Hence we state the next proposition from Giulietti (2003)[Chapter 3] without proof as we will exclusively be using it in examples.

Proposition 2.71. *Let $\mathcal{X}$ be a smooth projective plane curve, and $P = [a : b : c] \in \mathcal{X}$ such that $c \neq 0$. Then $f = L_1/L_2 \in \mathfrak{m}_P$ is a uniformizing parameter at P if* $\deg(L_1) = \deg(L_2) = 1$, *$L_2(P) \neq 0$ and L_1 is not a constant multiple of $F_X(P)X + F_Y(P)Y + F_Z(P)Z$.*

Remark 2.72. It is actually sufficient that one of a, b, c is non zero.[2]

Suppose that $\mathcal{X}$ is an affine or projective regular plane curve then, by Lemma 2.69 or Remark 2.70, there exists $t \in \mathcal{O}_P(\mathcal{X})$ such that $\mathfrak{m}_P(\mathcal{X}) = \langle t\rangle$. By Theorem 2.59 We see that $\mathcal{O}_P(\mathcal{X})$ is a discrete valuation ring and that t is a uniformizing parameter. We will denote the order of $f \in \mathcal{O}_P(\mathcal{X})$ as $ord_P(f)$.

[1] If this is not the case, then there exists an affine change of coordinates such that this is the case.

[2] As we can apply a projective change of cordinates otherwise, for instance if $b \neq 0$, then we may swap Y and Z.

Definition 2.73. Let $\mathcal{X}$ be an regular plane curve, the function $v_P : \mathcal{O}_P(\mathcal{X}) \to \mathbb{N} \cup \{\infty\}$, defined as:

$$v_P(f) = \begin{cases} \infty & \text{if } f = 0 \\ ord_P(f) & \text{otherwise.} \end{cases}$$

Let $f \in \mathcal{O}_P(\mathcal{X})$, then P is called a *zero* of order $v_P(f)$ if $v_P(f) > 0$.

Remark 2.74. The function v_P, can be extended to the domain $\overline{\mathbb{F}}_q(\mathcal{X})$ and codomain $\mathbb{Z} \cup \{\infty\}$, since $\mathcal{O}_P(\mathcal{X})$ is a subring of $\overline{\mathbb{F}}_q(\mathcal{X})$, by setting $v_P(f) = v_P(g) - v_P(h)$, where $f = g/h \in \overline{\mathbb{F}}_q(\mathcal{X})$. If $v_P(f) < 0$, then f is said to have a *pole* at P of order $-v_P(f)$.

We will now show that the map $v_P : \mathcal{O}_P(\mathcal{X}) \to \mathbb{N} \cup \{\infty\}$, that is the non extended version, is a *discete valuation*, meaning that it satisfies properties (i)-(v) in the theorem below. However the map $v_P : \overline{\mathbb{F}}_q(\mathcal{X}) \to \mathbb{Z} \cup \{\infty\}$, have properties similar to (iii) and (iv) albeit for $f, g \in \overline{\mathbb{F}}_q(\mathcal{X})$.

Theorem 2.75. *The function $v_P : \mathcal{O}_P(\mathcal{X}) \to \mathbb{N} \cup \{\infty\}$, satisfies the following properties hold for all $f, g \in \mathcal{O}_P(\mathcal{X})$:*

(i) $v_P(f) = \infty$ *if and only if* $f = 0$.

(ii) $v_P(\lambda f) = v_P(f)$ *for all* $\lambda \in \overline{\mathbb{F}}_q^*$.

(iii) $v_P(f + g) \geq \min\{v_P(f), v_P(g)\}$.

(iv) $v_P(fg) = v_P(f) + v_P(g)$.

(v) *If* $v_P(f) = v_P(g)$, *where* $f, g \in \mathcal{O}_P(\mathcal{X}) \setminus \{0\}$ *then there exists a unit* $\lambda \in \overline{\mathbb{F}}_q$ *such that* $v_P(f - \lambda g) > v_P(g)$

Proof. Assertions (i) and (ii) follow directly from Definitions 2.58 and 2.73. Next we will show that v_P satisfies Assertion (iii): Let $t \in \mathcal{O}_P(\mathcal{X})$ be the uniformizing parameter. Suppose $f = 0$ this implies that $v_P(f + g) = v_P(g) = \min\{v_P(f), v_P(g)\}$ as $v_P(f) = \infty$. A similar argument holds when $g = 0$. Hence we may assume $f \neq 0$ and $g \neq 0$, furthermore we can assume without loss of generality that $v_P(g) \geq v_P(f)$. Since $f \neq 0$ and $g \neq 0$ there exists units u, v such that $f = ut^{v_P(f)}$ and $g = vt^{v_P(g)}$, then:

$$f + g = (u + vt^{v_P(g) - v_P(f)})t^{v_P(f)}.$$

Hence $v_P(f + g) \geq v_P(f) = \min\{v_P(f)v_P(g)\}$ as $(u + vt^{v_P(g)-v_P(f)})$ is a unit in $\mathcal{O}_P(\mathcal{X})$ since

$$(u + vt^{v_P(g)-v_P(f)})(P) = u(P) + v(P)t^{v_P(g)-v_P(f)}(P) = u(P) \neq 0$$

because $u \in \mathcal{O}_P(\mathcal{X})^*$. Continuing with Assertion (iv), we are once again able to assume that $f \neq 0$ and $g \neq 0$, then $fg = ut^{v_P(f)} \cdot vt^{v_P(g)} = uv \cdot t^{v_P(f)+v_P(g)}$, and hence $v_P(fg) = v_P(f) + v_P(g)$. Finishing the proof with Assertion (v), we consider the polynomial $f - \lambda g \in \mathcal{O}_P(\mathcal{X})[\lambda]$, then:

$$f - \lambda g = ut^{v_P(f)} + \lambda vt^{v_P(g)} = (u + \lambda v)t^{v_P(f)}$$

However when $\lambda = -uv^{-1}$ then $(u + \lambda v) = 0$, and hence $v_P(f - \lambda g) = \infty$. ∎

2.3.1 Bézout's Theorem and It's Applications

The contents of this subsection is based on Fulton (2008)[Section 5.3] or Pellikaan et al. (2018)[Subsection 11.1.4]

Definition 2.76. Let $\mathcal{X}$ and $\mathcal{Y}$ be regular projective plane curves of degrees m and l, and defining equations $F = 0$ and $G = 0$ respectively. Assume that $\mathcal{X} \not\subseteq \mathcal{Y}$, and let $P \in \mathcal{X}$ and H be a homogeneous linear polynomial such that $H(P) \neq 0$. Then the *intersection multiplicity* $I(P, \mathcal{X}, \mathcal{Y})$ of $\mathcal{X}$ and $\mathcal{Y}$ at the point P is defined to be $v_P(g/h^m)$, where g and h are the classes of G and H modulo $I(\mathcal{X})$ respectively.

The intersection multiplicity is well defined: Suppose H_0 is another homogeneous linear polynomial such that $H_0(P) \neq 0$ and h_0 is the class of H_0 modulo $I(\mathcal{X})$, then $h/h_0 \in \mathcal{O}_P(\mathcal{X})$ is a unit. From this it follows that:

$$\begin{aligned} v_P(g/h^m) &= v_P(g) - v_P(h^m) + (v_P(h_0^m) - v_P(h_0^m)) \\ &= v_P(g) - v_P(h^m h_0^m) - v_P(h_0^m) = v_P(g) - v_P(h_0^m) = v_P(g/h_0^m) \end{aligned}$$

since $v_P(f) = 0$ for all units $f \in \mathcal{O}_P(\mathcal{X})$, as f can be written as ft^0, where t is a uniformizing parameter in $O_P(\mathcal{X})$. Next we state the strong version of Bézout's theorem, without proof. The theorem is proved in Fulton (2008)[Section 5.3].

Theorem 2.77. *Let $\mathcal{X}$ and $\mathcal{Y}$ be regular projective plane curves, with defining equations $F = 0$ and $G = 0$ respectively. If F and G have no common factors, then*

$$\sum_{P \in \mathcal{X} \cap \mathcal{Y}} I(P, \mathcal{X}, \mathcal{Y}) = \deg(F) \deg(G)$$

Meaning that $\mathcal{X}$ and $\mathcal{Y}$ intersect at exactly $\deg(F)\deg(G)$ points, assuming the points are counter with multiplicity.

This is a pretty powerfull result, which has many interesting consequences, for instance the following corollary follows naturally:

Corollary 2.78. *If $\mathcal{X}$ and $\mathcal{Y}$ are regular plane projective curves with strictly positive degree, then they intersect in at least one point.*

Finally we obtain the following usefull result, which will help us to determine which plane projective curves are varieties.

Corollary 2.79. *Let $F = 0$ be the defining equation of a regular projective plane curve, then F is absolutely irreducible.*

Proof. Suppose for the sake of contradiction that F factors into GH, with $\deg(G), \deg(H) \geq 1$, then

$$F_X = GH_X + HG_X$$

Hence $F_X \in \langle G, H \rangle$ similarly for the other partial derivatives. Hence $V(G) \cap V(H)$ is a subset of $V(F_X), V(F_Y), V(F_Z)$ and $V(F)$. However by Corollary 2.78, the curves with defining equations $G = 0$ and $H = 0$ intersect in at least one point, and hence $V(G) \cap V(H) \neq \emptyset$. However the points in $V(G) \cap V(H)$ are all singular, meaning F did have a singular point after all. ■

The following example is based on Pellikaan et al. (2018)[Example 11.1.38].

Example 2.80. The *Klein quadratic* $\mathcal{K}$ is the curve with defining equation $X^3Y + Y^3Z + Z^3X = 0$, consider the projective line $\mathcal{L}$ with defining equation $X = 0$, then $\mathcal{K}$ and $\mathcal{L}$ intersects at the points $P_1 = [0 : 1 : 0]$ and $P_2 = [0 : 0 : 1]$. We will start by considering the point $P_1 = [0 : 1 : 0]$, applying Proposition 2.71 we see that $t = X/Y$ is a unifomzing parameter of $\mathcal{O}_{P_1}(\mathcal{X})$ as X is not a constant multiple of $\mathcal{K}_X(P_1)X+\mathcal{K}_Y(P_1)Y+\mathcal{K}_Z(P_1)Z$. We see that $I(P_1, \mathcal{K}, \mathcal{L}) = v_{P_1}(X/Y^4) = v_{P_1}(X) - v_{P_1}(Y^4)$. Computing using the uniformizing parameter we get that $v_{P_1}(Y^4) = 0$ since Y^4 is a unit in $\mathcal{O}_{P_1}(\mathcal{X})$, and hence $Y^4 = Y^4(X/Y)^0$. Similarly we have $v_{P_1}(X) = 1$ as Y is a unit in $\mathcal{O}_{P_1}(\mathcal{X})$ and $X = Yt^1$. Thus $I(P_1, \mathcal{K}, \mathcal{L}) = 1$. This in turn implies that $I(P_2, \mathcal{K}, \mathcal{L}) = 3$, by Bézuotz Theorem 2.77. □

2.3.2 Divisors and the Reimann Roch Theorem

The following subsection will be based on Fulton (2008)[Chapter 8], Tsfasman et al. (2007)[Section 2.1.3] and Pellikaan et al. (2018)[Subsection 11.1.5]. We will let $\mathcal{X}$ be an absolutely irreducible regular projective plane curve, over $\overline{\mathbb{F}}_q$.

Before we can introduce our main object of study in this section, we need to introduce the notion of a formal sum. A formal sum is informally defined to be a sum which we do not assign a meaning, for instance the formal sum $1 + 4$ is simply the sum, it does not attain the value 5. In this way formal sums are simply a way of specifying elements in a set, this is exactly their usage, in the following definition:

Definition 2.81. A *divisor* D on $\mathcal{X}$, is defined as a formal sum $\sum_{P\in\mathcal{X}} n_P P$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but a finite number of points $P \in \mathcal{X}$. The set of divisors on $\mathcal{X}$ will be denoted $Div(\mathcal{X})$, furthermore each n_P will be refereed to as the *weight* associated with P. The *support* of a divisor D, denoted $\text{supp}(D)$, is defined as the set of points P where $n_P \neq 0$. The divisor D is called *effective* if $n_P \geq 0$ for all $P \in \mathcal{X}$. Finally, the *degree* of the divisor D is defined as $\deg(D) := \sum_{P\in\mathcal{X}} n_P$.

The divisors $Div(\mathcal{X})$ form an abelian group with respect to *addition of divisors*, mainly if $D = \sum_{P\in\mathcal{X}} n_P P$ and $D' = \sum_{P\in\mathcal{X}} m_P P$ are both divisors on $\mathcal{X}$, then $D \pm D' = \sum_{P\in\mathcal{X}}(n_P \pm m_P)P$, the neutral element of $Div(\mathcal{X})$, will be denoted 0. Using this addition of divisors we can introduce a partial ordering $\geq$ on $Div(\mathcal{X})$, where $D \geq D'$ if and only if $D - D'$ is effective.

One of the applications of divisors is to keep track of the locations where a rational function has zeros and poles and their respective orders. This is exactly the idea of the following definition:

Definition 2.82. Let $f \in \overline{\mathbb{F}}_q[\mathcal{X}] \setminus \{0\}$, then we define the *divisor of zeros* and *divisor of poles* of f, is defined as the formal sums:

$$(f)_0 := \sum_{v_P(f)>0} v_P(f)P \text{ and } (f)_\infty := \sum_{v_P(f)<0} -v_P(f)P.$$

Finally, we define the *principal divisor* of f as

$$(f) := \sum_{P\in\mathcal{X}} v_P(f)P = (f)_0 - (f)_\infty.$$

Two divisors D and D' are called *linearly equivalent*, denoted $D \sim D'$, if there exists $g \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\}$ such that $D - D' = (g)$.

Notice that we used the extension of the discrete valuation $v_P : \mathcal{O}_P(\mathcal{X}) \to \mathbb{N}$ to the domain $\overline{\mathbb{F}}_q[\mathcal{X}] \setminus \{0\}$, as described in Remark 2.74.

Next we will show that these principal divisors are well-defined, meaning that they have a finite number of weights which are non-zero. This by extension shows that $(f)_0$ and $(f)_\infty$ are well-defined, since they do not share any weights.

Proposition 2.83. *Let* $f \in \overline{\mathbb{F}}_q[\mathcal{X}] \setminus \{0\}$*, then* $\deg((f)) = 0$.

Proof. Suppose $\mathcal{X}$ has degree n, then f can be represented as g/g', where G, G' are homogeneous polynomials of the same degree m. Then let $\mathcal{Y} = V(G)$ and $\mathcal{Z} = V(G')$, notice that $f = g/g' = (g/h^m)(g'/h^m)^{-1}$, where h is the class of a homogenus linear polynomial H such that $H(P) \neq 0$. Hence we have $v_P(f) = I(P, \mathcal{X}, \mathcal{Y}) - I(P, \mathcal{X}, \mathcal{Z})$, from this it follows by Bézout's Theorem 2.77 that:

$$\deg((f)) = \sum_{P \in \mathcal{X}} v_P(f)P = \sum_{P \in \mathcal{X}} I(P, \mathcal{X}, \mathcal{Y}) - \sum_{P \in \mathcal{X}} I(P, \mathcal{X}, \mathcal{Z}) = nm - nm = 0 \qquad \blacksquare$$

Let $D = \sum_{i=1}^{k} n_i P_i - \sum_{j=1}^{l} m_j Q_j$, where $P_i, Q_j \in \mathcal{X}$ and $n_i, m_j > 0$, be a divisor. We could be interested in keeping track of which rational functions that have zeros of order at least n_i at the points P_i and have no poles except those found at Q_j, with order at most m_j. This is precisely the key to understanding the following definition:

Definition 2.84. Let D be a divisor on $\mathcal{X}$ then we define the set

$$L(D) := \left\{ f \in \overline{\mathbb{F}}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \text{ is effective} \right\} \cup \{0\}.$$

The set $L(D)$ forms a vector space over $\overline{\mathbb{F}}_q$ and we define $\ell(D) := \dim_{\overline{\mathbb{F}}_q}(L(D))$.

Remark 2.85. If $D \sim D'$, meaning there exists $g \in \overline{\mathbb{F}}_q(\mathcal{X})$ such that $D - D' = (g)$, then $L(D)$ and $L(D')$ are isomorphic, which can be seen as follows: Suppose $D = \sum_{P \in \mathcal{X}} n_P P$ and $D' = \sum_{P \in \mathcal{X}} n'_P P$ then $f \in L(D)$ implies that $fg \in L(D')$. Since the weight m_P of a point P in the divisor $(fg) + D'$, satisfies:

$$m_P = n'_P + v_P(fg) = n'_P + v_P(f) + v_P(g) = n_P + v_P(f) > 0.$$

The last equality follows from the fact that $D - D' = (g)$ implies that $n_P + v_P(g) = n_P$ and the last inequality from the fact that $D + (f)$ is an effective divisor. A similar argument can be made to show that $f \in L(D')$ implies $fg^{-1} \in L(D)$. The rest follows from the fact that $f \mapsto fg$ is a linear map.

We will briefly discuss how $L(D)$ forms a vector space over $\overline{\mathbb{F}}_q$: Suppose $D = \sum_{P\in\mathcal{X}} n_P P$ and $f = g/h, f' = g'/h' \in L(D)$. Then

$$(\lambda f) + D = \sum_{P\in\mathcal{X}} (n_P + v_P(\lambda f))P = \sum_{P\in\mathcal{X}} (n_P + v_P(f))\, P = (f) + D$$

for all $\lambda \in \overline{\mathbb{F}}_q^*$, where the last equality followed from Assertion (ii) of Theorem 2.75. This combined with the fact that $0 \in L(D)$ imply that $\lambda f \in L(D)$ for all $f \in L(D)$ and $\lambda \in \overline{\mathbb{F}}_q$. Secondly we have

$$(f + f') + D = \sum_{P\in\mathcal{X}} \left(n_P + v_P\left(\frac{gh' + g'h}{hh'}\right)\right) P$$

Instead of looking at the entirety of the formal sum, we will focus on the weight of a single point $P \in \mathcal{X}$, as we only need to show that this is non-negative, to show that $(f + f') + D$ is effective. We have:

$$\begin{aligned} n_P + v_P\left(\frac{gh' + g'h}{hh'}\right) &= n_P + v_P(gh' + g'h) - v_P(hh') \\ &= n_P + \min\left\{v_P(g) + v_P(h'), v_P(g') + v_P(h)\right\} - (v_P(h) + v_P(h')) \end{aligned}$$

Where the last equality follows by applying Assertions (iii) and (iv) from Theorem 2.75. However, as $n_P + \min\{v_P(g) + v_P(h'), v_P(g') + v_P(h)\} - (v_P(h) + v_P(h'))$ is either $n_P + v_P(g) - v_P(h)$ or $n_P + v_P(g') - v_P(h')$ depending on which of $v_P(g) + v_P(h')$ and $v_P(g') + v_P(h)$ is smaller, we get that each weight is non-negative, since $(f) + D$ and $(f') + D$ are both effective, and hence $f + f' \in L(D)$ whenever $f, f' \in L(D)$.

Example 2.86. Let $\mathcal{X}$ be the projective line, defined by $X - Y = 0$, consider the divisor $D = [1 : 1 : 0]$, then $L(D)$, consists of all rational functions $\alpha \in \overline{\mathbb{F}}_q(\mathcal{X})$ such that α has a root at $[1 : 1 : 0]$ and no poles. □

Lemma 2.87. *Let D be the zero divisor on $\mathcal{X}$, then $L(D) = \overline{\mathbb{F}}_q$.*

Proof. Since $\mathcal{X}$ is a projective plane curve, then $f \in L(D)$, implies that f has no poles, however Proposition 2.83 implies that the number of poles equals the number of zeros of f, each counted with multiplicity. Hence, f can not have any zeros or poles, meaning $f \in \overline{\mathbb{F}}_q$. Combining this with the fact that every constant polynomial has no poles, we get $L(D) = \overline{\mathbb{F}}_q$. ■

Next we show some properties of the vector space $L(D)$, combining these facts we see that $L(D)$ is finite dimensional for all $D \in Div(\mathcal{X})$.

Proposition 2.88. *Let D be a divisor on $\mathcal{X}$, then:*

(i) $\deg(D) < 0$ *implies that* $\ell(D) = 0$.

(ii) *If D is an effective divisor then* $\ell(D) \leq 1 + \deg(D)$.

Proof. We start by proving Assertion (i). Let $\deg(D) < 0$, then for any $f \in \overline{\mathbb{F}}_q(\mathcal{X})$, we have

$$\deg((f) + D) = \deg((f)) + \deg(D) < 0$$

by Proposition 2.83, meaning $f \notin L(D)$. Since $f \in \overline{\mathbb{F}}_q(\mathcal{X})$ was arbitrary we see that $L(D) = \{0\}$.

Next we prove Assertion (ii) by induction on $\deg(D)$. If $\deg(D) = 0$ then D being effective implies that $D = 0$, then Lemma 2.87 implies that $\ell(D) = \dim_{\overline{\mathbb{F}}_q} \overline{\mathbb{F}}_q = \deg(D) + 1$. Now suppose that $\deg(D) > 0$, then there exists $P \in \mathcal{X}$ such that the weight of P satisfies $n_P > 0$. Let $D' = D - P$. Since $n_P > 0$, we have that $D' \geq 0$ and $\deg(D') = \deg(D) - 1$, hence we can apply our induction hypothesis, to obtain $\ell(D') = \deg(D)$.

If we can represent $L(D')$ as the kernel of a linear transformation ϕ from $L(D)$ into $\overline{\mathbb{F}}_q$, then

$$\ell(D) = \dim_{\overline{\mathbb{F}}_q} L(D) = \dim_{\overline{\mathbb{F}}_q} \ker(\phi) + \dim_{\overline{\mathbb{F}}_q} \text{image}(\phi) \leq \ell(D') + \dim_{\overline{\mathbb{F}}_q} \text{image}(\phi).$$

However as $\text{image}(\phi)$ is a subspace of $\overline{\mathbb{F}}_q$ we get that $\ell(D) \leq \deg(D) + 1$. Hence, it is sufficient to construct a linear transformation $\phi : L(D) \to \overline{\mathbb{F}}_q$ such that $\ker(\phi) = L(D')$. Let t be the uniformizing parameter of $\mathcal{O}_P(\mathcal{X})$, then we define $\phi(f) = (t^{n_P} f)(P)$. The transformation ϕ is well-defined since $v_P(t^{n_P} f) = n_P + v_P(f) \geq 0$, implies that $t^{n_P} f$ is defined at P. Clearly ϕ is linear, moreover $f \in \ker(\phi)$ if and only if P is a zero of $t^{n_P} f$, meaning $v_P(t^{n_P} f) > 0$. However this is equivalent to $v_P(f) + n_P > 0$ by Assertion (iv) of Theorem 2.75, which is in turn equivalent to $(f) + D' \geq 0$, so $f \in L(D')$. ■

Definition 2.89. Let $\mathcal{X}$ be a projective smooth plane curve of degree m, then the *genus* g of $\mathcal{X}$ is defined as $g = (m-1)(m-2)$.

This is not the standard definition of the genus of a curve, but rather a way to compute the genus of a smooth projective plane curve, which was proved by the German mathematician Julius Plücker. However, it is sufficient for our purposes.

Definition 2.90. Let $\mathcal{X}$ be a smooth projective plane curve, with genus g, then a divisor W on $\mathcal{X}$ with $\deg(W) = 2g - 2$ is called a *canonical* divisor.

We now reach the main result of this section or arguably even the main result of this chapter. But we will omit it's proof, which can be found in Fulton (2008)[Section 8.6]

Theorem 2.91 (Reimann Roch Theorem)**.** *Let $\mathcal{X}$ be a regular projective plane curve of genus g, and D be a divisor on $\mathcal{X}$, then for all canonical divisors W we have*

$$\ell(D) - \ell(W - D) = \deg(D) - g + 1$$

Next we show the following corollary, which have numerous applications, one of these is determining the minimum distance of algebraic geometry codes.

Corollary 2.92. *Let $\mathcal{X}$ be a regular projective plane curve of genus g and let $\deg(D) > 2g-2$, then $\ell(D) = \deg(D) - g + 1$.*

Proof. We have $\deg(W - D) = \deg(W) - \deg(D) < \deg(W) - (2g - 2) < 0$, since W is a canonical divisor and hence by Assertion (i) of Proposition 2.88, we have that $\ell(W - D) = 0$. The rest follows from the Reimann Roch Theorem 2.91. ■

Example 2.93. Let $\mathcal{X}$ be the projective plane curve with defining equation $Y = 0$ over $\overline{\mathbb{F}}_q$. Let $G = (k-1)P_\infty$ where $P_\infty = [1:0:0]$. Finally let

$$V = \left\{ F(X,Z)/Z^{k-1} \mid F(X,Y) \in \overline{\mathbb{F}}_q[X,Z], \text{ homogeneous with } \deg(F) \leq k-1 \right\}$$

We will show that $L(G) = V$. Since every $f = F(X,Z)/Z^{k-1} \in V$ has the property that F is homogeneous we may write $f = \sum_{i=0}^{k-1} a_i f_i$, where $f_i = (X/Z)^i$. Then $t = Z/X$ is an uniformizing parameter of $\mathcal{O}_{P_\infty}(\mathcal{X})$ by Proposition 2.71. Hence,

$$v_{P_\infty}(f) = v_{P_\infty}\left(\sum_{i=1}^{k-1} a_i f_i \right) = \max\left\{ v_{P_\infty}(a_i f_i) \mid 1 \leq i \leq k-1 \right\} = -\max\left\{ i \mid a_i \neq 0 \right\}.$$

Where the second equality follows from Theorem 2.75 and the third equality from the fact that $a_i f_i = a_i t^{-i}$. Since f is defined at all points, except P_∞ we have that $(f)_\infty = -v_{P_\infty}(f) P_\infty$, and since $v_{P_\infty} \leq k-1$ we have $f \in L(G)$.

From this it follows that it is sufficient to prove that $\dim(V) = \ell(G)$, as we have shown that $V \subseteq L(G)$. Clearly $\dim(V) = k$ as $f_0, f_1, \ldots, f_{k-1}$, forms a basis of V, however we also have that $\ell(G) = k$, by Corollary 2.92 since $\mathcal{X}$ has genus 0. □

3 Algebraic Geometry Codes

The following chapter is based on Pellikaan et al. (2018)[Section 11.2] and Giulietti (2003)[Chapter 4]. We introduce the codes constructed on curves, we will introduce some new notation. An affine or projective curve $\mathcal{X}$ with defining equation $F = 0$ is said to be a curve over $\mathbb{F}_q$ if $F \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ is absolutely irreducible. Furthermore, if $\mathcal{X}$ is an affine or projective curve over $\mathbb{F}_q$ then we will let $I(\mathcal{X})$ by the ideal consisting of all polynomials in $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ which vanish on $\mathcal{X}$. This ideal is prime both in $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ but also in $\overline{\mathbb{F}}_q[X_1, X_2, \ldots, X_n]$, since F being absolutely irreducible implies that F is prime in $\mathbb{F}[X_1, X_2, \ldots, X_n]$ and $\overline{\mathbb{F}}_q[X_1, X_2, \ldots, X_n]$. The coordinate ring $\mathbb{F}[\mathcal{X}]$ is defined as $\mathbb{F}_q[X_1, X_2, \ldots, X_n]/I(\mathcal{X})$, and the function field $\mathbb{F}(\mathcal{X})$ is defined as the quotient field of $\mathbb{F}_q[\mathcal{X}]$.[1]

Recall the Frobenius map $\mathbb{F}_q \ni x \mapsto x^q \in \mathbb{F}_q$. The *extended Frobenius map* ψ is simply the Frobenius map extended coordinate wise, to either the n dimensional affine or projective space. We notice that $G(x_1, x_2, \ldots, x_n)^q = G(x_1^q, x_2^q, \ldots, x_n^q)$ for all $G \in \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ and $x_1, x_2, \ldots, x_n \in \mathbb{F}_q$ by freshman's dream. Hence, if $\mathcal{X}$ is an affine or projective curve defined over $\mathbb{F}_q$ then $P \in \mathcal{X}$, implies $\psi(P) \in \mathcal{X}$.

A divisor $D \in Div(\mathcal{X})$ is called rational if the weight of P and $\psi(P)$ is the same for all $P \in \mathcal{X}$. The vector space $L(D)$ will only consist of rational divisors and is otherwise defined as before, albeit with the restriction of the rational functions to $\mathbb{F}_q(\mathcal{X})$. However, even with these changes the Reimann Roch Theorem 2.91 remains true, confer both of the sources listed earlier.

Finally, let $\mathcal{P} := (P_1, P_2, \ldots, P_m)$ be a tuple of points, then we define the *evaluation map* as in Example 1.21 to be the map as $\mathrm{Ev}_{\mathcal{P}}(F) = (F(P_1), F(P_2), \ldots, F(P_m))$. The domain of $\mathrm{Ev}_{\mathcal{P}}$ will either be a subset of $\mathbb{F}_q(\mathcal{X}) \setminus \{0\}$ or $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$.

[1] Notice that it is a subring and field respectively of the usual coordinate ring and function field of $\mathcal{X}$.

3.1 Codes Constructed on Affine Plane Curves

We will start by considering codes constructed from affine plane curves, as this is the simplest case to understand. Our proof of the following proposition will be based on the proof of Pellikaan et al. (2018)[Proposition 11.2.1].

Proposition 3.1. *Let F be an absolutely irreducible polynomial in $\mathbb{F}_q[X,Y]$, of degree m, and let $\mathcal{X}$ be the curve with defining equation $F=0$. Furthermore let $P_1, P_2, \ldots, P_n \in \mathcal{X}$ be n distinct rational points and $\mathcal{P} := (P_1, P_2, \ldots, P_n)$. Finally consider the linear code:*

$$E(l) = \{\mathrm{Ev}_{\mathcal{P}}(G) \mid G \in \mathbb{F}_q[X,Y], \deg(G) \leq l\}.$$

Then if $lm < n$, then the minimum distance d and dimension k of $E(l)$ satisfies:

$$d \geq n - lm$$
$$k = \begin{cases} \binom{l+2}{2} & \text{if } l < m \\ lm + 1 - \binom{m-1}{2} & \text{otherwise} \end{cases}$$

Proof. Let $V_l \subseteq \mathbb{F}_q[X,Y]$ be the $\mathbb{F}_q$ vector space of polynomials with degree at most l, notice that $\mathrm{Ev}_{\mathcal{P}}(V_l) = E(l)$. Then the monomials X^iY^j, with $i+j = 0, 1, \ldots, l$ form a basis of V_l. Since there is $\binom{l+2}{2}$ of these the vector space V_l has dimension $\binom{l+2}{2}$.
Let $G \in V_l$, if F factors G, then $\mathrm{Ev}_{\mathcal{P}}(G) = 0$. Conversely, if $\mathrm{Ev}_{\mathcal{P}}(G) = 0$, then the projective curves with defining equations $F^* = 0$ and $G^* = 0$, have degrees $\deg(G) \leq l$ and m respectively but intersect at n points namely $\phi(P_1), \phi(P_2), \ldots, \phi(P_n)$, where $\phi(x_1, x_2, \ldots, x_n) = [x_1 : x_2 : \cdots : x_n : 1]$. This is a contradiction since $\deg(G)m \leq lm < n$ and Bézout's Theorem 2.77 implies that they intersect in at most $\deg(G)m$ points. Hence F and G must have a common factor; meaning G is divisible by F as F is irreducible. Hence, $\mathrm{Ev}_{\mathcal{P}}$ restricted to V_l have kernel FV_{l-m}. Now if $l < m$, then FV_{l-m} has dimension 0 and hence:

$$k = \dim_{\mathbb{F}_q}(E(l)) = \dim_{\mathbb{F}_q}(V_l) - \dim_{\mathbb{F}_q}(FV_{l-m}) = \binom{l+2}{2}$$

since $\mathrm{Ev}_{\mathcal{P}}$ is a linear map. Conversely if $l \geq m$ we obtain:

$$k = \binom{l+2}{2} - \binom{l-m+2}{2} = \frac{-m^2 - 2lm + 3m}{2} = lm + 1 - \binom{m-1}{2}$$

Finally by a similar argument as earlier, by Bézouts Theorem 2.77 a nonzero codeword has at most lm zeros. Hence the minimum weight of $E(l)$ is at least $n - lm$. ■

The results of Proposition 3.1 indicate that if we want $E(l)$ to have a high minimum distance, we should choose F and l such that $\deg(F)$ and l are as small as possible, while maximizing the number of rational points on $\mathcal{X}$.
Conversely if we want to maximize the dimension of $E(l)$ then we should choose F and l such that $\deg(F)$ and l are as large as possible, albeit such that $l\deg(F)$ is strictly less than the number of rational points on $\mathcal{X}$.

Example 3.2. If we pick $F = Y - 1$ and let $\mathcal{X}$ be the affine plane curve with defining equation $F = 0$. Then the set of rational points of $\mathcal{X}$ consist of the points $P = (a, 1)$ where $a \in \mathbb{F}_q$. Let $G \in \mathbb{F}_q[X,Y]$ such that $\deg(G) \leq l$ then $G(X, 1)$ is an univariate polynomial of degree less than or equal to l. Hence the linear code $E(l)$, where $l \in \mathbb{N}$, corresponds to the Reed-Solomon code of degree $l+1$. □

3.2 Goppa Codes

In this section we will introduce codes on constructed projective algebraic curves (not necessarily in the protective plane) and show some results on the parameters of these.

Definition 3.3. Let $\mathcal{X}$ be an absolutely irreducible regular projective curve over $\mathbb{F}_q$ and $P_1, P_2, \ldots, P_n \in \mathcal{X}$ be n distinct rational points. Let $D = \sum_{i=1}^{n} P_i$ and $G \in Div(\mathcal{X})$ such that $\text{supp}(D) \cap \text{supp}(G) = \emptyset$, then the linear code $C_{D,G} := \text{Ev}_{\mathcal{P}}(L(G))$, where $\mathcal{P} := (P_1, P_2, \ldots, P_n)$, is called an *algebraic geometry code* or a *Goppa code*.

As noted in Section 1.2, the family of Reed-Solomon codes (see Example 1.21), are a subfamily of the family of algebraic geometry codes. We will show this in the following example which is based on Giulietti (2003)[Exercise 4.2].

Example 3.4. Let $1 \leq k \leq n \leq q$, let $\mathcal{X}$ be the projective plane curve with defining equation $Y = 0$ and divisors $D = \sum_{i=1}^{n} P_i$ and $G = (k-1)P_\infty$ where $P_i = [i : 0 : 1]$ and $P_\infty = [1 : 0 : 0]$. From Example 2.93 we have that:

$$L(G) = \left\{ F(X,Z)/Z^{k-1} \mid F(X,Y) \in \overline{\mathbb{F}}_q[X,Z], \text{ homogeneous with } \deg(F) \leq k-1 \right\}$$

Consider the codeword $c = (f(P_1), f(P_2), \ldots, f(P_n)) \in \mathcal{C}_{D,G}$, where $f(X,Y,Z) = \frac{F(X,Z)}{Z^{k-1}}$, such that $\deg(F) \leq k-1$ and F is homogeneous, then $f \in L(G)$. Then writing $F = \sum_{i=0}^{\deg(F)} a_i X^i Z^{\deg(F)-i}$ and letting $F_*(X) := F(X,1) = \sum_{i=0}^{\deg(F)} a_i X^i$ we see that c equal to the codeword $(F_*(1), F_*(2), \ldots, F_*(n))$ of the Reed-Solomon code of degree k, since $\deg(F) \leq k-1$. □

Clearly since every Reed-Solomon code is a MDS code, Goppa codes with good parameters can be constructed. One of the advantages of Goppa codes is that we can obtain good lower bounds for their minimum distance, this is along with other things what we will show in the following theorem:

Theorem 3.5. *Let $C_{D,G}$ be a $[n,k,d]_q$ code. Then*

(i) $k = \ell(G) - \ell(G-D)$.

(ii) $d \geq n - \deg(G)$.

Proof. We start by proving Assertion (i). The map $\text{Ev}_{\mathcal{P}}$ is a surjective linear map from $L(G)$ to $C_{G,D}$. Hence,

$$k = \dim_{\mathbb{F}_q}(\text{image}(\text{Ev}_{\mathcal{P}})) = \ell(G) - \dim_{\mathbb{F}_q}(\ker(\text{Ev}_{\mathcal{P}})) = \ell(G) - \ell(G-D)$$

where the last equality follows as $\ker(\text{Ev}_{\mathcal{P}}) = L(G-D)$. This equality can be seen as follows: If $f \in L(G)$ and $\text{Ev}_{\mathcal{P}}(f) = 0$, then $v_{P_i}(f) \geq 1$ for all $i = 1, 2, \ldots, n$, and hence $(f) + G - D$ is effective meaning $f \in L(G-D)$, conversely if $f \in L(G-D)$, then f vanishes at every $P \in \text{supp}(D)$ as $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. This means that $f \in \ker(\text{Ev}_{\mathcal{P}})$.

Continuing with Assertion (ii). Suppose $c \in \mathcal{C}_{G,D}$ then there exists $f \in \mathbb{F}_q(\mathcal{X})$ such that $c = (f(P_1), f(P_2), \ldots, f(P_n))$. Assuming $\text{wt}(c) = d$, then f vanishes at $n-d$ points, say

$P_{i_1}, P_{i_2}, \ldots, P_{i_{n-d}}$. This in turn implies that $f \in L\left(G - \sum_{j=1}^{n-d} P_{i_j}\right)$ as $G - \sum_{j=1}^{n-d} P_{i_j} + (f)$ are effective because $v_{P_{i_j}}(f) \geq 1$ for all $j = 1, 2, \ldots, n-d$. Hence,

$$\deg\left(G - \sum_{j=1}^{n-d} P_{i_j}\right) \leq \deg((f)) = 0$$

by Proposition 2.83. However, as $\deg\left(G - \sum_{j=1}^{n-d} P_{i_j}\right) = \deg(G) - n + d$ this yields the desired result. ■

Imposing extra conditions on the degree of G yields further results on the dimension of $\mathcal{C}_{D,G}$, these results are stated and proved in the following corollary.

Corollary 3.6. *Suppose $\mathcal{X}$ be an absolutely irreducible regular projective curve over $\mathbb{F}_q$ of genus g. Let $\mathcal{C}_{D,G}$ be a $[n,k,d]_q$ Goppa code on $\mathcal{X}$. Then the following assertions hold:*

(i) *If $\deg(G) < n$, then $k = \ell(G)$. Furthermore if $f_1, f_2, \ldots, f_k$ is an $\mathbb{F}_q$-basis of $L(G)$, then a generator matrix of $\mathcal{C}_{G,D}$ is given by:*

$$M := \begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{bmatrix}$$

(ii) *If $2g - 2 < \deg(G) < n$, then $k = \deg(G) - g + 1$.*

Proof. We start by proving the first claim of Assertion (i). Notice that $\deg(G - D) = \deg(G) - \deg(D) < n - n = 0$ implies that $\ell(G - D) = 0$ by Proposition 2.88.
Next we show that M is a generator matrix of $\mathcal{C}_{D,G}$. It is sufficient to show that the rows $m_1, m_2, \ldots, m_k$ of M are $\mathbb{F}_q$-linearly independent since all k of them are codewords. Suppose $\sum_{i=1}^{k} a_i m_i = 0^T$ with $a_1, a_2, \ldots, a_k \in \mathbb{F}_q$, then $\sum_{i=1}^{k} a_i f_i(P_j) = 0$ for $j = 1, 2, \ldots, n$. Letting $g := \sum_{i=1}^{k} a_i f_i$ we see that g vanishes at $P_1, P_2, \ldots, P_n$ and hence $g \in L(G - D) = \{0\}$, meaning $a_1 = a_2 = \cdots = a_k = 0$.

Assertion (ii), follows from Assertion (i) as $k = \ell(G)$, when $\deg(D) < n$. This along with the fact that $2g - 2 < \deg(G)$ imply that $\ell(G) = \deg(D) - g + 1$ by Corollary 2.92, yielding the desired result. ■

Remark 3.7. Assertion (i) of Corollary 3.6, says that $k = \ell(G)$, combining this with the Reimann Roch Theorem 2.91 we see that $k = \ell(G) \geq \deg(G) - g + 1$, combining this with Assertion (i) of Theorem 3.5, we see that $d + k \geq (n - \deg(G)) + (\deg(G) - g + 1) = n - g + 1$. Recall that the Singleton Bound, Corollary 1.18, states that every $[n,k,d]_q$ code satisfies $d - 1 \leq n - k$. Combining these facts we see that: $n - g + 1 \leq d + k \leq n + 1$ and in particular if $\mathcal{C}_{D,G}$ is constructed on a curve of genus 0, then $\mathcal{C}_{D,G}$ is a MDS code.

3.2.1 Constructing Good Goppa Codes

Let $\mathcal{X}$ be a projective curve and $C_{D,G}$ be a Goppa code constructed on $\mathcal{X}$. If $C_{D,G}$ is a $[n,k,d]_q$ code, then $k+d \geq n-g+1$ by Remark 3.7. If we divide by n we see that the transmission rate R and relative minimum distance δ of $C_{D,G}$ satisfy the following inequality:

$$R+\delta \geq 1-\frac{g-1}{n}. \tag{3.1}$$

Hence in order to construct Goppa codes with good parameters, we need to maximize the ratio $N_q(\mathcal{X})/g(\mathcal{X})$, where $N_q(\mathcal{X})$ is the number of rational points on $\mathcal{X}$ and $g(\mathcal{X})$ is the genus of $\mathcal{X}$.

We state the following result, which where proved by Tsfasman Vlăduţ and Zink without proof.

Theorem 3.8. *Let $q=p^2$ where p is a prime. Let $N_q^*(g)$ be the maximum number of $\mathbb{F}_q$-rational points on an absolutely irreducible smooth projective curve over $\mathbb{F}_q$ with a genus less than or equal to g. Then:*

$$\limsup_{g\to\infty} \frac{N_q^*(g)}{g} \leq \sqrt{q}-1.$$

Theorem 3.8 implies the existence of a sequence $\{\mathcal{X}_g\}_{g\in\mathbb{N}}$ of smooth projective curves over $\mathbb{F}_q$, where $\mathcal{X}_g$ has genus g, such that $\limsup_{g\to\infty} \frac{N_q(\mathcal{X}_g)}{g} \leq \sqrt{q}-1$, and hence $\limsup_{g\to\infty} \frac{g}{N_q(\mathcal{X}_g)} \geq \frac{1}{\sqrt{q}-1}$. Combining this with equation (3.1) we see that there exists a sequence of Goppa codes $\left\{\mathcal{C}_{D_g,G_g}\right\}_{g\in\mathbb{N}}$ where $\mathcal{C}_{D_g,G_g}$ is constructed on $\mathcal{X}_g$ such that:

$$\limsup_{g\to\infty} R(\mathcal{C}_{D_g,G_g}) + \delta(\mathcal{C}_{D_g,G_g}) \geq 1-\frac{1}{\sqrt{q}-1} \tag{3.2}$$

The inequality in equation (3.2) is called the *Tsfasman–Vlăduţ–Zink bound*. If $q \geq 49$, then this bound exceeds the asymptotic Gilbert-Varshaomov bound, meaning $1-\frac{1}{\sqrt{q}-1} > 1-H_q(\delta)+\delta$ albeit only in a certain range of transmission rates / relative minimum distances, see Figure 3.1. However since $R=k/n$ we can construct Goppa codes with parameters in this range, confer Assertion (ii) of Corollary 3.6.

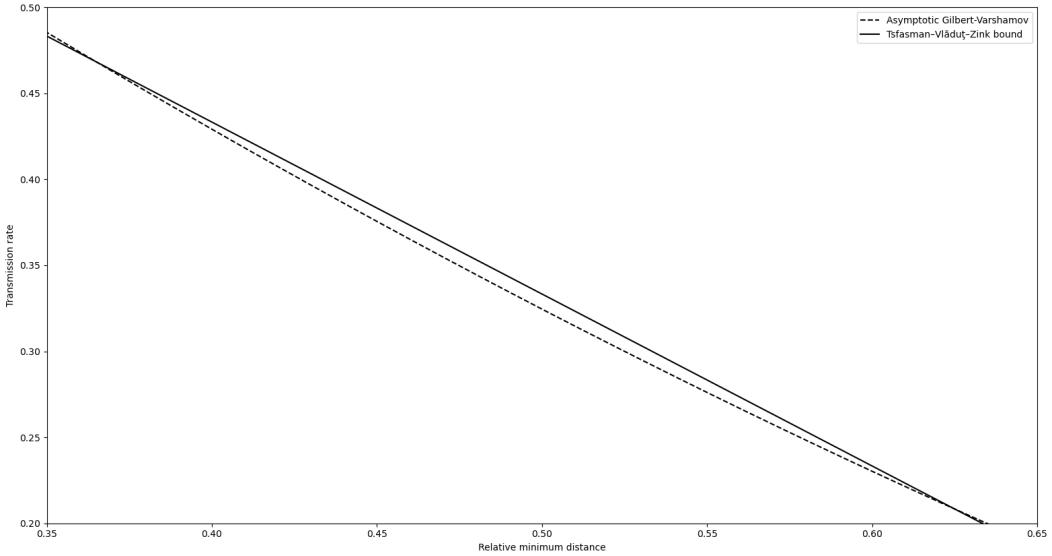

Figure 3.1: *The Asymtotic Gilbert-Varshamov bound versus the Tsfasman–Vlăduţ–Zink bound for* $q = 49$.

The fact that one is able to construct sequences of Goppa codes with parameters that exceed the asymptotic Gilbert-Varshamov bound, was in fact one of the reasons for the initial interest in algebraic geometry codes.

Bibliography

W. Fulton. Algebraic curves: An introduction to algebraic geometry, 2008.

M. Giulietti. Notes on algebraic-geometric codes, 2003. Lecture notes from a series of lectures, given in May 2003.

W. C. Huffman and V. Pless. *Fundementals of Error-Correcting Codes*. Cambrige University Press, 1st edition, 2003. ISBN 9780521131704.

J. Lahtonen. Covering distance for a linear code, 2023. url: https://math.stackexchange.com/q/4653336.

S. Lang. *Algebra*. Springer, 3rd edition, 2002. ISBN 03879585X.

N. Lauritzen. *Concrete Abstract Algebra: From Numbers to Gröbner Bases*. Cambridge University Press, 1st edition, 2003. ISBN 9780521534109.

R. Pellikaan, X.-W. Wu, S. Bulygin, and R. Jurrius. *Codes, Cryptology and Curves with Computer Algebra*. Cambrige University Press, 1st edition, 2018. ISBN 9780521520362.

K. Shum and B. Zhang. The singleton bound and reed-solomon code, 2016. url: https://piazza.com/class_profile/get_resource/isgy6spmwwm3ba/itzo5as3bbw7kk.

M. Tsfasman, S. Vlăduţ, and D. Nogin. *Algebraic Geometry Codes: Basic Notations*. American Mathematical Society, 1st edition, 2007. ISBN 9780821843062.

S. H. Weintraub. *Galois Theory*. Springer, 2nd edition, 2020. ISBN 9780387875743.