Algebraic-geometric codes and their decoding algorithm

Shen, B.Z.

DOI:
10.6100/IR381307

Published: 01/01/1992

Document Version
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
• A submitted manuscript is the author's version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Algebraic-Geometric Codes
And Their Decoding Algorithm

Ba-Zhong Shen
Algebraic-Geometric Codes and Their Decoding Algorithm

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof.dr. J.H. van Lint, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op maandag 28 september 1992 om 16.00 uur

door

SHEN, BA-ZHONG

Geboren te Suzhou, Jiangsu, China
Dit proefschrift is goedgekeurd door promotoren prof.dr. J.H. van Lint en prof.dr. G.B.M. van der Geer

coopromotor: dr. G.R. Pellikaan
Preface

This thesis presents the results of the author's research in the period October 1988 to May 1992. He has tried to make the introduction self-contained, so that the reader who has no background of algebraic geometry can also understand it. The rest of the thesis is based upon seven papers written in the period mentioned above. The papers are:


Acknowledgments

Here, I would like to thank all the people, who have had part in making my Ph.D. time a pleasant time. However, in order to keep the number of pages down, I will just mention a few.

First of all I would like to express my gratitude to my supervisor, Prof. dr. Jack H. van Lint, who gave me a great opportunity to carry out my doctorate research in the group of Discrete Mathematics at the Eindhoven University of Technology. It is his guidance and encouragement that led to the completion of this thesis.
Another person who has played a role in my research is my co-supervisor, Dr. Ruud Pellikaan, from whom I learned the theory of algebraic-geometric codes. I am indebted to him for always being ready to discuss problems, for his many advices and many stimulating discussions, and for his rapid critical reading of my manuscripts. Furthermore, my thanks go to my co-authors R. Pellikaan, S.C. Porter and G.J.M. van Wee and my other colleague Iwan Duursma for sharing their research interests with me and the pleasure I had working with them. I want to thank my roommates Jack Kooien and Fengwen Sun for always being ready to discuss with me. I have been fortunate to learn coding theory and combinatorial theory in a land that holds a high concentration of eminent researchers in this field. Special thanks go to Prof. dr. Brouwer and Prof. dr. H.C.A. van Tilborg from whom I followed lectures. I appreciate that Prof. dr. A.E. Brouwer, Prof.dr. G. van der Geer and Prof.dr. T. Heholdt, and, of course, my supervisor and co-supervisor, took the trouble to review this thesis. I feel grateful to F.C. Bussemaker for the enthusiastic way, in which he did the programming for me. To all the other members of the Discrete Mathematics group I owe many thanks for their help of any kind whatsoever I have received during my stay among them. Special thanks go to Ms. J. van Amsterdan and Ms. H. Houben, the former and incumbent secretaries of our group.

It is a great pleasure to mention the enthusiasm shown by my friend, Dr. Louis ten Bosch on reading the manuscript, although the subject of this thesis is outside his research area.

The most important participant in the preparation of this thesis was Qi, my wife. She helped in many ways, physical and psychological, sharing happiness and sadness.

July 1992, Eindhoven

Bazhong SHEN
Contents

Preface ................................ ................................ i
1. Introduction ................................ ..................................... 1
2. Representing Linear Codes by Curves ................................ 13
3. Constructing Asymptotically Good Binary Codes from Curves ........................................ 33
4. Decoding Geometric Goppa Codes ................................ 39
5. Solving a Congruence on a Graded Algebra ......................... 61
6. Codes from Hermitian Curves .......................................... 75
7. A Realization of the Decoding Algorithm ............................ 93
References .................................................................... 109
Nederlandse samenvatting .............................................. 114
Chapter 1

Introduction

In 1981, Goppa [26] introduced the use of algebraic geometry in coding theory. This beautiful discovery came as a result of many years of searching for possible generalizations of Reed-Solomon codes, BCH codes and "classical" Goppa codes. For about a decade, algebraic-geometric codes have been in the spotlight of coding theoretic research. As is well-known, numerous exciting results have been achieved using algebraic curves to construct linear codes. Among them is the result given by Tsfasman, Vladuț and Zink [80] in 1982, which is the most sensational development in the theory of error-correcting codes in the last decade. In this introduction, we will first give a brief introduction of this development and explain what algebraic-geometric codes are. Next, a survey of this thesis will be given.

1.1 Why do algebraic-geometric codes excite people?

In block coding one starts by choosing a so-called alphabet \(Q\), that is, a set of \(q\) distinct symbols. In this thesis, \(q\) is a power of a prime and \(Q\) denotes the finite field \(\mathbb{F}_q\). A code \(C\) with word length \(n\) is a subset of \(Q^n\). Elements of \(Q^n\) are called words, those of \(C\) codewords. The Hamming-distance in \(Q^n\) is defined by

\[
    d(x, y) := \#\{i|1 \leq i \leq n, x_i \neq y_i\}.
\]

For a code \(C\), the minimum distance \(d\) is defined by

\[
    d := \min\{d(x, y)|x \in C, y \in C, x \neq y\}.
\]

A code with word length \(n\), \(M\) elements and minimum distance \(d\) is called an \((n, M, d)\) code. If an \((n, M, d)\) code \(C\) is a linear space over \(\mathbb{F}_q\), we call it an \([n, k, d]\) linear code, where \(k\) is the dimension of \(C\).

One of the most important parameters of a code \(C\) is its so-called information rate \(R\) defined by \(R := (\log_q |C|)/n\). Consider communication over a channel with probability \(p\) that a symbol is received incorrectly. Suppose \(C = \{c_1, \ldots, c_M\}\) is a code over \(\mathbb{F}_q^n\) used on this channel and we use maximum-likelihood-decoding. Let \(p(i)\) be the probability of making an incorrect decision given that \(c_i\) is transmitted. Then the probability of incorrect decoding of a received word is

\[
    P_{\text{err}}^{(n)} := M^{-1} \sum_{i=1}^{M} p(i).
\]
For a given rate \( R \), how small can \( P^{(n)}_{err} \) be made for an \((n, q^{nR})\) code? In 1948, Shannon [68] answered this question by the so-called Shannon channel coding Theorem. To explain this theorem, we need a concept, called channel capacity. Let us consider a binary symmetric channel (BSC) with error probability \( p_e \) (for the other types of channel we refer to [49]). The capacity of this BSC is defined by

\[
C(p_e) := 1 + p_e \log_2 p_e + (1 - p_e) \log_2(1 - p_e).
\]

The Shannon Theorem says:

All rates below capacity \( C(p_e) \) are achievable. Specifically, for every rate \( R < C(p_e) \), there exists a sequence of \((n, 2^{nR})\) codes with \( P^{(n)}_{err} \to 0 \). Conversely, any sequence of \((n, 2^{nR})\) codes with \( P^{(n)}_{err} \to 0 \) must have \( R < C(p_e) \).

Unfortunately, although almost 45 years passed after the discovery of this theorem, people still do not know how to construct such a sequence of codes. Moreover, in practice it is difficult to find \( P_{err} \). So what can we do? We again consider communication over a channel. In a received word the expected number of errors is \( np_e \) and in order to correct these we need \( d \) to be at least \( 2np_e + 1 \). So \( d/n \) should exceed \( 2p_e \) if we are to use these codes successfully for error-correction on the channel. Therefore the relative minimum distance \( d/n \) is used as a more convenient measure of the quality of the code. Here we denote this relative minimum distance by \( \delta := d/n \).

Inspired by the Shannon channel coding theorem, we shall often be interested in a sequence of codes with increasing word length \( n \) and either a fixed rate \( R \) or a fixed relative minimum distance \( \delta \). If we use the notation \( A_q(n, d) \) for the maximal value of \( M \) for which an \((n, M, d)\) code exists, then the following function gives the information rate of good long codes for which \( d/n = \delta \):

\[
\alpha(\delta) := \limsup_{n \to \infty} \frac{\log_q A_q(n, \lfloor \delta n \rfloor)}{n}.
\]

For thirty years, the best lower bound on \( \alpha(\delta) \) was the so-called Gilbert-Varshamov (GV) bound [22, 81] that was found in 1952, that is \( \alpha(\delta) \geq 1 - H_q(\delta) \), where the entropy function \( H_q \) is defined on \([0, (q-1)/q]\) by \( H_q(0) := 0 \) and

\[
H_q(x) := x \log_q(q - 1) - x \log_q x - (1 - x) \log_q(1 - x) \quad \text{for} \quad 0 < x \leq (q - 1)/q.
\]

Moreover, for a long time there was serious doubt whether it is at all possible to give an explicit algebraic construction of a sequence of codes such that both \( R \) and \( \delta \) are bounded away from zero. Such codes are called asymptotically good codes. The so-called explicit construction is in the sense that once the rates of the codes have been computed, the entries of the generator matrices of the codes can be written as closed formulas, and no searching is required. To study a construction of codes from the complexity point of view, we need the following definition, see also [79].

**Definition 1.1** Let \( \{C_i\} \) be a family of codes over \( \mathbb{F}_q \) of increasing length. Let \( G_i \) be a generator matrix of \( C_i \). The family \( \{C_i\} \) is said to have a polynomial construction complexity if and only if there exists an algorithm that constructs matrices \( G_i \) in time complexity which is polynomial in the length of \( C_i \).

For the GV bound (at least in the binary case), people still do not know how to give an explicit or a polynomial construction of a sequence of codes meeting this bound.
For the construction of explicit asymptotically good codes, Justesen [34] succeeded in doing this by using concatenated codes [18] in 1972. For this work Justesen received the Browder J. Thompson Prize Award for the best paper published in any of the IEEE Transactions in 1972 by an author under 30 years of age. But the Justesen codes can only achieve a bound below the GV bound.

In 1982, Tsfasman, Vlăduţ and Zink [80] published a paper with an extremely exciting result, namely the existence of a sequence of polynomially constructive codes over $\mathbb{F}_q$ (with $q$ an even power of a prime) which exceeds the GV bound, whenever $q \geq 49$. In detail, they give a new bound on $\alpha(\delta)$, namely the Tsfasman-Vlăduţ-Zink (TVZ) bound:

$$\alpha(\delta) \geq 1 - (\sqrt{q} - 1)^{-1} - \delta,$$

For $q = p^{2m} \geq 49$ this new bound lies above the GV bound on the interval $(\delta_1, \delta_2)$, where $\delta_1$ and $\delta_2$ are the zeroes of the equation $H_q(\delta) - \delta = (\sqrt{q} - 1)^{-1}$. For this paper the authors received the IEEE Information Theory Group Paper Award in 1983.

This sensational result is due to the use of a new class of codes constructed from curves, namely algebraic-geometric codes.

This is not the whole story about algebraic-geometric codes. In fact, it provides a new method to construct a huge number of linear codes of long length.

1.2 What are algebraic-geometric codes?

Let us consider a linear $[n, k]$ code $C$ over $\mathbb{F}_q$ from a different point of view. Let $A^{(k)}$ be the affine space over $\mathbb{F}_q$ of dimension $k$. Let $G$ be a generator matrix of $C$. Every column of $G$ can be considered as a point in $A^{(k)}$; we denote the family of all these points as $\mathcal{P} = (P_1, \ldots, P_n)$. Let $V$ be a subspace of $A^{(k)}$ generated by the family $\mathcal{P}$ over $\mathbb{F}_q$, and $V^*$ be the space of linear functions from $V$ to $\mathbb{F}_q$. Now the code $C$ can be denoted as follows,

$$C = \{(f(P_1), \ldots, f(P_n)) | f \in V^*\}.$$

To generalize this idea, we can use any kind of linear subspace of functions from $A^{(k)}$ to $\mathbb{F}_q$ instead of $V^*$. Obviously, after this generalization we still get a linear code. For example, let $A^{(1)} = \mathbb{F}_q$ and $\mathcal{P}$ be all the elements of $A^{(1)} \setminus \{0\}$. Let $L$ be the space consisting of all polynomials of degree less than $k$. Then the code $C = \{(f(P_1), \ldots, f(P_n)) | f \in L\}$ is a so-called $[n, k, n - k + 1]$ Reed-Solomon code over $\mathbb{F}_q$.

Instead of an affine space, we also can give the same discussion for a projective space (this will be explained in Section 1.3). Now the construction of a linear code is equivalent to choosing both a family of points and a space of functions either in an affine space or in a projective space. One thing we should always keep in mind is that any such construction should allow the estimation of the dimension and minimum distance of the code. If we choose a family of points from a curve and a space of functions from the field of rational functions of this curve, those estimations can indeed be achieved. The codes constructed in this way are called algebraic-geometric codes. In the rest of this section, we will give a heuristic description of curves, a precise definition of algebraic-geometric codes and the estimations of their parameters. For the details of curves and codes, we refer to [6, 19, 30, 43, 79].
Let $k$ be the algebraic closure of the finite field $F_q$, and let an $n$-dimensional projective space over $k$ be denoted by

$$P^n = \{(x_0 : x_1 : \cdots : x_n) | x_i \in k, i = 0, \ldots, n \text{ and not all } x_i \text{ vanish}\}.$$ 

Let $G_1, \ldots, G_r$ be homogeneous polynomials in $k[x_0, x_1, \ldots, x_n]$. An algebraic set $\mathcal{X}$ in the projective space $P^n$ is defined to be the zero set of $G_1, \ldots, G_r$, that is

$$\mathcal{X} = \{(x_0 : x_1 : \cdots : x_n) \in P^n | G_1(x_0, x_2, \ldots, x_n) = \cdots = G_r(x_0, x_1, \ldots, x_n) = 0\}.$$ 

If we consider all algebraic sets and their complements as closed sets and open sets, respectively, we obtain a topology in $P^n$, the so-called Zariski topology. Furthermore we also can define an induced topology in $\mathcal{X}$ in a similar way. $\mathcal{X}$ may be the union of two of its proper closed subsets. If this is not the case, then $\mathcal{X}$ is called irreducible. As a Zariski topological space, we can define the dimension of $\mathcal{X}$ to be the supremum of all the integers $m$, such that there exists a strictly descending chain of irreducible closed subsets of $\mathcal{X}$, namely, $\mathcal{X} = \mathcal{X}_0 \supset \mathcal{X}_1 \supset \cdots \supset \mathcal{X}_m \neq \emptyset$. Now a projective curve $\mathcal{X}$ is defined to be an irreducible closed set of dimension 1. The field of rational functions on the curve $\mathcal{X}$, denoted by $k(\mathcal{X})$ is the set of functions $f/g \in k(x_0, \ldots, x_n)$ such that $g(P) \neq 0$ for some $P \in \mathcal{X}$, $f$ and $g$ are homogeneous polynomials of the same degree and another ratio $f'/g'$ defines the same function as $f/g$ if and only if $f'g - fg'$ vanishes on $\mathcal{X}$. If a curve $\mathcal{X}$ is defined by a finite number of homogeneous polynomials $G_1, \ldots, G_r$, from $F_q[x_0, x_1, \ldots, x_n]$, we call it an absolutely irreducible curve defined over $F_q$. Similarly, we can also define the field of rational functions of this curve over $F_q$, denoted by $F_q(\mathcal{X})$. Moreover, we have $k(\mathcal{X}) = k \cdot F_q(\mathcal{X})$.

The following theorem makes the following two things possible. One is the using both equivalent languages — algebraic and geometric — to study curves. The other is the constructing codes over a non-algebraic closed field by using curves. The theorem states,

A field $K$ containing a field $F$ (not necessarily algebraically closed) is isomorphic to $F(\mathcal{X})$ for a projective non-singular (see [19, 30, 79]) curve $\mathcal{X}$ if and only if $K$ is of transcendence degree one and finitely generated over $F$. We call $K$ an algebraic function field of one variable.

Let us look at the details of the relations between a curve and its corresponding algebraic function field of one variable, and vice versa. Let $V$ be a proper valuation ring of $F_q(\mathcal{X})$ containing $F_q$, that is a ring $V$ satisfying the condition that $f \notin V$ implies $f^{-1} \notin V$. Let $m_V$ be its maximal ideal. There exists an element $t \in V$, called a local parameter, such that every non-zero element of $V$ can be written uniquely in the form $ut^n$, with $u \in V \setminus m_V$. Both $V$ and $m_V$ determine $s$ points in $\mathcal{X}$, where $s = [V/m_V : F_q]$, these $s$ points are conjugated under the action of the Galois group $Gal(k(F_q))$. Let $Q$ denote the set of these $s$ points. We call both $Q$ and $(V, m_V)$ a place of $F_q(\mathcal{X})$ and $s$ the degree of this place and denote it by $\deg(Q)$. Therefore the place of degree one is exactly a point on the curve such that all the coordinates are in $F_q$. This place is called an $F_q$-rational point. A formal sum $D = \sum_Q n_Q Q$ is called a divisor, where $Q$ runs over all the places of $F_q(\mathcal{X})$, $n_Q \in Z$ and almost all $n_Q = 0$. The degree of a divisor $D$ is defined by $\deg(D) = \sum_Q n_Q \deg(Q)$. The support of a divisor $D$ is defined by $\text{supp}(D) = \{Q | n_Q \neq 0\}$. Let $f$ be a non-zero rational function in $F_q(\mathcal{X})$. For every place $Q$, let $V_Q$ be its corresponding valuation ring with a local parameter $t_Q$. Then $f$ can be expanded into a Laurent series $\sum_{i \geq m} a_i t_Q^{-i}$, where $m$ is an integer and $a_i \in F_q$ with $a_m \neq 0$. We call $m$ the discrete
valuation of $f$ at $Q$ and denote it by $v_Q(f)$. Now the principal divisor $(f)$ is defined by $(f) = \sum Q v_Q(f)Q$, where $Q$ also runs over all the places of $\mathbb{F}_q(X)$. Actually, $v_Q(f)$ can be considered as the multiplicity or minus the multiplicity, respectively of $Q$ for $f$ whenever $Q$ is a zero or pole, respectively, otherwise it is zero. It is a fact that $\deg((f)) = 0$.

Now the precise definition of an algebraic-geometric code can be given as follows.

**Definition 1.2 ((Weakly) Algebraic-Geometric code)** Let $X$ be a projective, nonsingular, absolutely irreducible curve defined over $\mathbb{F}_q$. Let $P_1, P_2, \ldots, P_n$ be $n$ distinct $\mathbb{F}_q$-rational points of $X$ and let $D$ be the divisor $P_1 + \cdots + P_n$. Furthermore, let $G$ be some other divisor that has support disjoint from $D$. Define the linear space $L(G) = \{ \omega \in \mathbb{F}_q(X)^* \mid (\omega) \supseteq -G \} \cup \{0\}$. An (weakly) algebraic-geometric code $C_L(D,G)$ is defined to be

$$\{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L(G)\}.$$ 

To estimate the minimum distance $d$ of this code, we look at the number of zeroes of $\omega$, for any $f \in L(G)^*$. It turns out to be at most $\deg(G)$, since $\deg((f)) = 0$. Therefore $d \geq n - \deg(G)$.

Historically, the codes defined by the above definition are not the first version of Goppa's invention. For Goppa's first construction of algebraic-geometric codes, let us trace back to 1970 and 1971. A very important development in coding theory during these two years was the invention of so-called Goppa code [23, 24] which is defined as follows,

$$\{(e_0, c_1, \ldots, c_{n-d} \in \mathbb{F}_q^m \mid \sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i} \equiv 0 \pmod{g(z)}\},$$

where $\gamma_0, \ldots, \gamma_{n-1} \in \mathbb{F}_q^m$ and $g(z)$ is a polynomial over $\mathbb{F}_q^m$ such that $g(\gamma_i) \neq 0$ for $0 \leq i \leq n - 1$. In this thesis we call it a classical Goppa code. For this, Goppa received the IEEE Information Theory Group Award in 1972. Ten years later after this discovery, by extending this idea to curves, Goppa [26] himself again introduced another new class of codes which turn out to be the dual of the codes defined by Definition 1.2. To explain his construction, we first consider the set of rational differential forms on a curve $X$ over $\mathbb{F}_q$, which is denoted by $\Omega(X)$. $\Omega(X)$ is a one dimensional vector space over $\mathbb{F}_q(X)$, that means $\Omega(X) = \mathbb{F}_q(X) \cdot df$ for any $f \in \mathbb{F}_q(X)^*$, where $d$ is a map from $\mathbb{F}_q(X)$ to an $\mathbb{F}_q(X)$-module such that $d(f + g) = df + dg$, $d(fg) = gdf + fdg$ and $da = 0$ for $f, g \in \mathbb{F}_q(X)$ and $a \in \mathbb{F}_q$. Consider a differential form $\omega \in \Omega(X)$. For every place $P$ of $\mathbb{F}_q(X)$, there exists an $f_P \in \mathbb{F}_q(X)$ such that $\omega = f_P dt_P$, where $t_P$ is a local parameter of $P$. Furthermore, as we mentioned before $f_P$ can be expanded into a Laurent series $\sum_{i \geq m} a_i t_P^i$. A special name is given to the $a_{-1}$, that is the residue of $\omega$ at $P$, which is denoted by $\text{res}_P(\omega)$. Moreover, we can define the canonical divisor (\omega) of $\omega$, that is $(\omega) = \sum_P \text{res}_P(\omega)P$. Let $G$ be a divisor on $\mathbb{F}_q(X)$, the set $\Omega(G)$ defined by $\{ \omega \in \Omega(X)^* \mid (\omega) \supseteq G \} \cup \{0\}$ is a finite dimensional vector space over $\mathbb{F}_q$. A very important invariant of the curve — the genus of the curve — now can be defined by $g = \dim \Omega(0)$. For a non-singular projective curve in $\mathbb{P}^2$ defined by a degree $d$ homogeneous polynomial, its genus can be calculated by the well-known formula $g = (d-1)(d-2)/2$. 

**Chapter 1: Introduction**
Now the definition of Goppa's construction of an algebraic-geometric code can be described as follows.

**Definition 1.3 (Geometric Goppa code)** Let the assumption be as in Definition 1.2. The code \( C_\Omega(D, G) \) of length \( n \) over \( \mathbb{F}_q \) is defined by

\[
C_\Omega(D, G) := \{(\text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega)) | \omega \in \Omega(G - D)\}.
\]

In this thesis we call it a geometric Goppa code.

Furthermore, by the residue theorem which says that \( \sum_P \text{res}_P(\omega) = 0 \), where \( P \) runs over all the places on \( \mathbb{F}_q(\mathcal{X}) \), we have the following duality theorem.

**Theorem 1.1 (Duality Theorem)** The linear code \( C_\Omega(D, G) \) is the dual of the code \( C_L(D, G) \).

The minimum distance of \( C_\Omega(D, G) \) can be estimated by the same method as we described for \( C_L(D, G) \), that is \( d \geq \deg(G) + 2 - 2g \), since every canonical divisor has degree \( 2g - 2 \). However to estimate the dimension of both \( C_L(D, G) \) and \( C_\Omega(D, G) \), one needs the following famous theorem in algebraic geometry, known as the Riemann-Roch theorem.

**Theorem 1.2 (Riemann-Roch Theorem)** Let \( G \) be a divisor on an absolutely irreducible, nonsingular projective curve. Let \( g \) be the genus of the curve. Then

\[
l(G) = \deg(G) - g + 1 + \delta(D),
\]

where \( l(D) := \dim L(D) \) and \( \delta(D) := \dim \Omega(D) \). Moreover, for any canonical divisor \( W \), \( l(W - D) = \delta(D) \).

By using the Riemann-Roch theorem, one can get the following main theorem for algebraic-geometric codes.

**Theorem 1.3** (a) If \( \deg(G) = m < n \), then \( C_L(D, G) \) is a linear \([n, k, d]\) code with \( k \geq m + 1 - g \) and \( d \geq n - m \). We call \( d^* := n - m \) the designed minimum distance. If moreover \( 2g - 2 < m \), then \( k = m + 1 - g \).

(b) If \( \deg(G) = m > 2g - 2 \), then \( C_\Omega(D, G) \) is a linear \([n, k, d]\) code with \( k \geq n - m - 1 + g \) and \( d \geq n + 2 - 2g \). We call \( d^* := m + 2 - 2g \) the designed minimum distance. If moreover \( m < n \), then \( k = n - m - 1 - g \).

### 1.3 What are the contributions of this thesis?

In this thesis, we consider the following problems:

- Can we handle all linear codes by algebraic geometry?
- Can we give an explicit construction with far less complexity (compared to the construction of the codes from modular curves) of asymptotically good binary codes meeting a good bound?
- How to give an efficient encoding and decoding algorithm for algebraic-geometric codes?
In Chapter 2, we present a solution for the first question. This is a part of the joint work [55] with Pellikaan and van Wee.

In the first part of Chapter 2, we show that all linear codes can be described as algebraic-geometric codes. To explain this conclusion, we first make a distinction among all algebraic-geometric codes to weakly algebraic-geometric (WAG), algebraic-geometric (AG) and strongly algebraic-geometric (SAG). A WAG code is a code defined by Definition 1.1 whenever no restriction is imposed on the degree of the divisor used. Consider an \([n, k]\) linear code \(C\) over \(\mathbb{F}_q\) and assume for simplicity that the all-one vector \((1, 1, \ldots, 1)\) is a codeword and every two columns of a generator matrix of \(C\) are linearly independent. Let \(M\) be a generator matrix containing \((1, 1, \ldots, 1)\) as the first row. Let \(V\) be the linear space over \(\mathbb{F}_q\) generated by the columns of this generator matrix. Let \(\mathcal{P}(V)\) be the set of lines in \(V\), that is the set of equivalence classes \(v\) for \(v \in V \setminus \{0\}\), with \(v\) being equivalent to \(\lambda v\) for \(\lambda \in \mathbb{F}_q \setminus \{0\}\). Then \(\mathcal{P}(V)\) is a \(k-1\) dimensional projective space; we can denote it by \(\mathcal{P}^{k-1}\). Then the columns of the generator matrix \(M\) correspond to \(n\) points \(P_1, \ldots, P_n\). Furthermore, these points are distinct and lie in the complement of the hyperplane \(H = \{(x_0 : x_1 : \ldots : x_{k-1}) \in \mathcal{P}^{k-1} | x_0 = 0\}\). Now the code \(C\) can be denoted by

\[
C = \{(f(P_1), \ldots, f(P_n)) | f \in L\},
\]

where \(L\) is a linear space over \(\mathbb{F}_q\), generated by maps from \(\mathcal{P}(V)\) to \(\mathbb{F}_q\), namely \(f_i = x_i/x_0, \ i = 0, \ldots, k-1\). Suppose there exists a nonsingular and absolutely irreducible curve \(X\) over \(\mathbb{F}_q\) which passes through \(P_1, \ldots, P_n\). Let \(G\) be the intersection divisor \(X \cdot H\) and \(D = \sum_{i=1}^n P_i\). Then \(G\) and \(D\) have disjoint supports. Moreover \(\mathcal{P}(V)^* \subseteq L(G)\). In a very special case, one may has \(\mathcal{P}(V)^* = L(G)\), so \(C = C_L(D, G)\). That is to say, \(C\) is WAG.

In [27], Goppa claimed that every linear code is WAG, simply because it is always possible to find a curve in \(\mathcal{P}^{k-1}\) of sufficiently large degree passing through all points \(P_1, \ldots, P_k\). But as we have seen, it is not always true that \(\mathcal{P}(V)^* = L(G)\), in other words, the linear system of hyperplane sections of the curve does not need to be complete. This will only prove that every projective code is a subcode of a WAG code, see Lachaud [40]. In Chapter 2, we show explicitly that indeed there exists such a curve, going though all the \(q^{k-1}\) rational points of \(\mathcal{P}^{k-1}\) outside a hyperplane such that \(\mathcal{P}(V)^* = L(G)\). By this approach we prove that every linear code is WAG.

Unfortunately, up to now no one knows how to figure out the dimension and the minimum distance of a WAG code if one does not impose any condition on the degree of the divisor. Therefore, to give the question more sense, we impose some conditions on the degree of the divisor so that Theorem 1.3 (a) or both (a) and (b) of Theorem 1.1 can be applied, respectively. We call such codes AG or SAG, respectively. In the second part of Chapter 2, we derive some criteria for the existence of these codes. It turns out that many well-known codes, such as the binary Golay code (which is closely connected with other subjects in mathematics, such as Steiner systems and the Leech lattice, etc.), all non trivial Hamming codes, except the binary \([7, 4, 3]\) code, binary quadratic-residue codes and many binary Reed-Muller codes are not AG. This does remind us that it is a very important to figure out properties of WAG codes which are not AG. If it is not possible, we have to generalize those well-known codes by another method so that by the known knowledge one can estimate the parameters of these generalized codes. In [21], van der Geer and van der Vlugt have treated Reed-Muller codes (at least for order two) by their methods of algebraic geometry.
In Chapter 3, we give an answer for the second question by constructing a sequence of asymptotically good binary concatenated codes using curves.

In 1966, Forney [18] introduced the concept of concatenated codes in which the \( m \) information digits of an inner binary code are treated as single digits of an outer code over \( GF(2^m) \). Therefore if one takes a sequence of linear codes \( \{C(k)\}_{k=1}^\infty \), where \( C(k) \) is a \([N, K, D]\) code over \( GF(2^k) \), as the outer codes and for every \( k \) one chooses a binary \([n, k, d]\) code as an inner code, one gets a sequence of binary concatenated codes. In 1971 Zyablov [86] proved that there exists a sequence of concatenated binary codes with the inner code length \( n \to \infty \) and the outer code length \( N \to \infty \), in which the outer code is maximal distance separable (MDS), and which satisfies

\[
\liminf \frac{\text{distance}}{\text{length}} \geq \max_{0 < r \leq 1} \left\{ (1 - \frac{R}{r})H_2^{-1}(1 - r) \right\},
\]

if the overall rate is \( R \). In this paper we call this the Zyablov bound. Zyablov’s construction is not explicit since the inner codes are taken to be codes meeting the GV bound. Therefore it was still in doubt whether it is at all possible to give an explicit algebraic construction of a sequence of asymptotically good binary codes. In 1972, Justesen [34] succeeded in doing this by generalizing Forney’s concept of concatenation to allow variation of the inner code. In this thesis we call such a construction a Justesen construction. By using this construction, in [34] Justesen also proved that for the overall rate not lower than 0.30 the Zyablov bound can be met by a sequence of explicitly constructive codes. Furthermore, the time complexity of the construction of those asymptotically good codes is about \( O(n^2) \), where \( n \) is the overall word length. Later, for low rate, several improvements have been made, see [1], [77] and [83] etc.. But none of them meets the Zyablov bound when the overall rate \( R < 0.30 \). Now the question is, whether it is possible to give an explicit construction for binary concatenated codes which meet the Zyablov bound when the rate is lower than 0.30. MacWilliams and Sloane put this question as a Research Problem (10.3) in their book [50, p. 315].

After the discovery and the sensational application of algebraic-geometric codes, people found that it may be possible to solve the above problem by using algebraic-geometric codes. In 1984, Katsman, Tsfasman and Vlăduţ [38] improved the Zyablov bound for binary concatenated codes, by using a sequence of codes over a fixed field \( GF(2^k) (2^k \geq 49) \), which meet TVZ bound, as outer codes and a fixed \([n, k, d]\) binary inner code. However, since the time complexity of constructing their outer codes is \( O(N^{20}) \) [79, Chapter 4.3], where \( N \) is the outer code length, they hardly can be called constructive from any practical perspective. Therefore it is still a problem to find an explicit construction of binary codes asymptotically meeting or exceeding the Zyablov bound, of low complexity.

In Chapter 3, we use a class of algebraic-geometric codes as outer codes which have somehow similar properties as MDS codes when the code lengths are sufficiently large. We give an explicit Justesen construction of concatenated codes which asymptotically meet the Zyablov bound for rates lower than 0.30, with the complexity of construction \( O(n^2) \). In this way we solve the open problem (10.3) of [50]. Our outer codes are the codes constructed from generalized Hermitian curves which are defined by a homogeneous ideal \( I(l, q) = (X_{i+1}X_0^3 + X_{i+1}X_0 - X_i^{l+1}, i = 1, \ldots, l-1) \).

The last three chapters of this thesis are devoted to solving the third problem.
Chapter 1: Introduction

The algebraic decoding of block codes by the determination of an error-locator polynomial and the subsequent determination of the error locations as its zeroes was presented by Peterson [56] in 1960 for binary BCH codes and extended by Gorenstein and Zierler to q-ary BCH-codes. In 1961, independently, Arimoto [3] also published his decoding method in Japanese. By generalizing their idea to algebraic-geometric codes, Justesen, Larsen, Jensen, Havemose and Høstholdt [35] published the first decoding algorithm for a class of codes on plane curves in 1989. For this paper they received the IEEE Information Theory Society Paper Award in 1991. Later many generalizations and improvements were achieved by Skorobogatov and Vlăduț [71], Krachkovskii [39], Pellikaan [53], Vlăduț [82], Duursma [12], Ehrhard [15], Feng and Rao [16] and Duursma [13]. Remember that we denoted the designed minimum distance of algebraic-geometric codes by \( d^* \). We can classify those results into two classes. The first one can correct up to \( (d^* - 1)/2 - s \) errors with complexity \( O(n^4) \), where \( s \) is the Clifford defect of a set of special divisors defined by Duursma in [12] and \( n \) is the length of the code, see [71, 39, 12]. The second one can correct up to \( [(d^* - 1)/2] \) errors, which is first given by existence proofs in [53, 82] and very recently by explicit algorithms with complexity \( O(n^3) \), independently in [15] and in [16]. The one given in [13] is a generalization of the algorithm of [16] to all geometric Goppa codes. Theoretically, one can generalize this method to all linear block codes as a method of finding an error locating pair, which is proved by Pellikaan [54]. All these decoding algorithms are carried out by solving systems of linear equations. To decrease the complexity, Justesen et al. [36] and Dahl Jensen [8], respectively, gave an attempt to a class of codes constructed from plane curves and a special curve in a 3-dimensional space, respectively. To generalize their method to more general geometric Goppa codes seems difficult.

Around the same time as Justesen et al. [35], by defining the syndrome in a different way, Porter described another decoding algorithm for a certain class of geometric Goppa codes in his Ph.D. thesis [57]. The syndrome he defined is a generalization of the syndrome for a classical Goppa code, which is defined as an element in the ring of polynomials in one variable. One can view the ring of polynomials in one variable as the ring of rational functions on the projective line with only poles at the point at infinity. The ring of polynomials in one variable is replaced by the ring \( K_\infty(P) \) of rational functions on the curve with only poles at a fixed place \( P \), where \( P \) is not equal to one of the rational points used to construct the code. Therefore a decoding algorithm constructed from this syndrome can be carried out in the ring \( K_\infty(P) \). This makes it more likely to decrease the decoding complexity. We will explain this in Chapter 6.

The proofs in the thesis of Porter contain several mistakes and gaps. In Chapter 4, we give a correct account of the results of Porter, in more generality and with a better error correcting capacity. This a joint work with Porter and Pellikaan [58]. We first prove that for every place \( P \) not in the support of \( D \), every geometric Goppa code \( C_D(D,G) \) is isometric to the code \( C_D(D,E - \mu P) \), for some effective divisor \( E \) and positive integer \( \mu \). Then we show that there exist \( n \) independent differentials \( \varepsilon_1, \ldots, \varepsilon_n \in \Omega(-D - \mu P) \) such that for every differential \( \omega \in \Omega(E - \mu P - D) \) we have \( \omega = \sum_{i=1}^n \text{res}_P(\omega)\varepsilon_i \). If we let \( \varepsilon(\mathbf{x}) = \sum x_i \varepsilon_i \), then \( \varepsilon(\mathbf{x}) \in \Omega(E - \mu P - D) \) if and only if \( \mathbf{x} \in C_D(D,E - \mu P) \). In order to represent the syndrome as a rational function we first prove the existence of a particular differential \( \eta \). By using these results we construct the syndrome \( S(\mathbf{x}) \) of a received word \( \mathbf{x} \) in the ring \( K_\infty(P) \). We also show how to decode \( (d^* - 1)/2 - s \) errors, where \( s \) is the Clifford defect, by
solving the key equation \( fS(x) = r + qh \), under a constraint in terms of the degrees of \( f \) and \( r \). In Chapter 5, we will explain how to solve this equation with complexity \( O(n^3) \). In Chapter 6, for a class of codes constructed from Hermitian curves, we show how to solve the corresponding key equation with lower complexity.

In Chapter 5, we discuss the more general problem of solving a congruence in a graded algebra (for the definition we refer to [30, 52]). Consequently, solving key equations, defined in Chapter 4 is just an application.

Let \( F[X] \) be a polynomial ring over a field \( F \), that is an \( N \)-graded algebra over \( F \), where \( N \) is the monoid of all nonnegative integers. Let \( f, g \in F[X] \). By using Euclid’s algorithm one can solve for \( a \) and \( b \) the congruence \( af \equiv b \pmod{g} \) such that \( \deg(b) \) is less than a given integer and \( a \) has the minimal degree among all such solutions. This was proved by Sugiyama, Kasahara, Hirasawa and Namekawa in [76] where they also applied it to decode BCH codes and classical Goppa codes. For solving such a congruence on an \( N^r \)-graded algebra \( F[X_1, \ldots, X_n] \), methods were given by Sakata [62] and Fitzpatrick and Flynn [17], respectively. As applications, they showed how to find minimal linear recurring relations for an \( n \)-dimensional array and how to decode Hensel codes, respectively. Unfortunately the ring \( K_\infty(P) \) given in Chapter 4, is not of the above two kinds of graded algebras if the genus of the curve used is not zero. In fact it is a \( \Gamma \)-graded algebra, where the grading monoid \( \Gamma \) is a proper submonoid of \( N \). So one cannot use the above two methods to solve a congruence in this \( \Gamma \)-graded algebra.

In Chapter 5, by generalizing a subresultant sequence (see [5, 7, 45] for the definition) in a \( \Gamma \)-graded algebra with a \( \Gamma \)-basis, we give an algorithm to solve the congruence \( af \equiv b \pmod{g} \) on this algebra, such that \( \deg(b) - \deg(a) \) is less than a given integer and \( a \) has the minimal degree among all such solutions. The idea of using subresultant sequences comes from Porter’s Ph.D. thesis [57]. But by using his generalization, one may get a wrong solution. In Chapter 5 a counter-example is given. The complexity of the improved algorithm we give is \( O((m + n)^3) \), where \( m = \deg(f) \) and \( n = \deg(g) \).

A very good explicit example of algebraic-geometric codes are the codes constructed from Hermitian curves, introduced by Goppa [28]. If we consider communication over a given channel, van Lint [44] remarked that these codes are usually better than the corresponding Reed-Solomon codes with the same rate. Tiersma [78], Stichtenoth [73] and Yang and Kumar [84] studied these codes in more detail. It looks more urgent to give efficient encoding and decoding algorithms for these codes. Chapter 6 is devoted to this. There we give a complete encoding and decoding scheme for these codes.

The encoding scheme we give is somewhat like the encoding scheme of Reed-Solomon codes, see [50, Ch.10.§7], which can be separated into two parts. One is to transfer message symbols to codewords and the other is to recover message symbols from codewords.

To decode these codes we use the decoding method given in Chapter 4. To fulfil this, the first task is to construct syndromes which are given only by a non-constructive existence proof in Chapter 4. Before doing this, we give a detailed description of the code \( C_\Omega(D, l(q + 1)P_\infty, \Delta P_\infty) \), which is isometric to the code \( C_\Omega(D, mP_\infty) \), where \( P_\infty \) is a point at infinity, \( n = \deg(D) = q^2 - 1 \) and \( m = l(q + 1) - \delta \). This description is different from the one given by Tiersma [78] and Stichtenoth [73], since our discussion is concentrated on the subspace of differential
forms while theirs is on the dual codes. After that, an explicit construction of syndromes for these codes is given. To solve the key equation of the received word for these codes, we transfer it to finding a minimal recurrence relation for a non-gap subscript sequence of size $m+1$, rather than using the method given in Chapter 5. Thus the decoding complexity is reduced.

At the end of Chapter 6, we show how to compute the residues explicitly by a given database.

The last chapter is the most technical part of this thesis.

A non-gap subscript sequence discussed in Chapter 6 is a sequence of elements of $F_q$, subscripted by a proper submonoid $N(q)$ of $N$. In Chapter 7, we denote it by $(U_i)_{N(q)}$. To find a minimal recurrence relation for $(U_i)_{N(q)}$, we give an iterative algorithm in Chapter 7. The main idea of this algorithm comes from Sakata's algorithm [62] which generalizes the Berlekamp-Massey algorithm [4, 47] to more than one variable. In brief, suppose for $\{U_i|i < n\}$, we already have a minimal recurrence relation, say $f_n$, a minimal recurrence relation $f_{n+}$ for $\{U_i|i < n^+\}$ is obtained by $f_n$ and another auxiliary relation given by the algorithm in one of the previous steps, where $n^+$ is the successor of $n$ in $N(q)$ under the normal order in $N$.

The difference between this method and the method given in Chapter 5 for decoding the same code is that the first one does use the knowledge of $\{f_i|i \leq n\}$ to find $f_{n^+}$ while the second one does not. Therefore the complexity of the first method is less than the second one. At the end of Chapter 7, we calculate the complexity of the iterative algorithm explicitly.
Chapter 2

Representing Linear Codes by Curves

In this chapter we discuss which linear codes are algebraic-geometric.

In Section 2.1 we define weakly algebraic-geometric (WAG), algebraic-geometric (AG), and strongly algebraic-geometric (SAG) codes. Furthermore, we also explain what we mean by a WAG, AG or SAG representation of a code. At the end of Section 2.1 we introduce the notion of a minimal representation. We prove that every WAG, AG or SAG code of dimension at least two has a minimal WAG, AG or SAG representation, respectively. This is useful in Section 2.3. Section 2.2 is devoted to prove that every linear code is WAG. In Section 2.3 we derive several conditions on linear codes to be AG. Special attention is paid to Reed-Muller codes, Hamming codes and the binary Golay code and its extension.

In this chapter, we use the terminology of scheme. For this and its properties, we refer to [30, Chapter II]. Some of the notations in this chapter were already introduced in Chapter 1. The following notations are new. The group of divisors on $\mathcal{X}$ is denoted by $\text{Div}(\mathcal{X})$. If $\varphi: \mathcal{X} \to \mathcal{X}'$ is a morphism of curves, then we denote by $\varphi^*$ both the induced homomorphism $k(\mathcal{X}') \to k(\mathcal{X})$ and the induced homomorphism $\text{Div}(\mathcal{X}') \to \text{Div}(\mathcal{X})$, see [30, p.137]. If $P$ is a place of $k(\mathcal{X})$ over $k$, that is, $P$ is a discrete valuation ring of $k(\mathcal{X})$ over $k$, then we denote by $v_P$ the discrete valuation function at $P$. In the literature the notation $\text{ord}_P$ is also customary. If $D_1$ and $D_2$ are divisors on a curve $\mathcal{X}$, then we denote by $D_1 \sim D_2$ that $D_1$ and $D_2$ are linearly equivalent. By $[D]$ we denote the linear equivalence class of $D$, that is, the set consisting of all the divisors on $\mathcal{X}$ linearly equivalent with $D$. The complete linear system associated to $D$ is denoted by $|D|$. This is the set of all effective divisors in $[D]$. If $C$ is a linear code, we denote by $d(C)$ its minimum distance.

2.1 Algebraic-geometric codes and representations

Let $\mathcal{X}$ be a projective, nonsingular, absolutely irreducible curve defined over $\mathbb{F}_q$. The genus of $\mathcal{X}$ is denoted by $g(\mathcal{X})$, or simply by $g$, if it is clear which curve is meant. Let $P_1, \ldots, P_n$ be $n$ distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$. We denote both the $n$-tuple $(P_1, \ldots, P_n)$ and the divisor $P_1 + \ldots + P_n$ by $D$ (the order of the $P_i$ is fixed).
Let \( G \) be a divisor on \( X \) of degree \( m \) with support disjoint from the support of \( D \). Define the map \( \alpha_L : L(G) \rightarrow \mathbb{F}_q^n \) by
\[
\alpha_L(f) = (f(P_1), \ldots, f(P_n)),
\]
and the map \( \alpha_{\Omega} : \Omega(G - D) \rightarrow \mathbb{F}_q^n \) by,
\[
\alpha_{\Omega}(\omega) = (\text{resp}_{P_1}(\omega), \ldots, \text{resp}_{P_n}(\omega)).
\]

Define
\[
C_L(X, D, G) = \text{Image}(\alpha_L) \quad \text{and} \quad C_{\Omega}(X, D, G) = \text{Image}(\alpha_{\Omega}).
\]

Then \( C_L(X, D, G) \) and \( C_{\Omega}(X, D, G) \) are those codes defined by Definition 1.2 and 1.3, respectively, but here we indicate the curve from which the codes are constructed.

**Definition 2.1** We call a \( q \)-ary linear code \( C \) weakly algebraic-geometric (WAG) if there exists a projective, nonsingular, absolutely irreducible curve \( X \) defined over \( \mathbb{F}_q \) of genus \( g \), and \( n \) distinct rational points \( P_1, \ldots, P_n \) on \( X \) and a divisor \( G \) with support disjoint from the support of \( D \), where \( D = P_1 + \ldots + P_n \), such that \( C = C_L(X, D, G) \). We call the triple \((X, D, G)\) a weakly algebraic-geometric representation (WAG representation), or shortly, a representation of \( C \).

An algebraic-geometric representation (AG representation) is a representation \((X, D, G)\) with \( \deg(G) < n \). We call a code algebraic-geometric (AG) if it has an AG representation. A strongly algebraic-geometric representation (SAG representation) is a representation \((X, D, G)\) with \( 2g - 2 < \deg(G) < n \). A code is called strongly algebraic-geometric (SAG) if it has a SAG representation.

**Remark 2.1** There exists a differential form \( \omega \) with a simple pole at each \( P_i \) and such that \( \text{resp}_{P_i}(\omega) = 1 \) for \( i = 1, \ldots, n \). We have \( C_{\Omega}(X, D, G) = C_L(X, D_1(\omega) - G + D) \), see [74, Corollary 2.6] or [43, Lemma 3.5]. As a consequence we have that \( C \) is WAG if and only if \( C = C_{\Omega}(X, D, G) \) for some curve \( X \) and divisors \( D \) and \( G \) (without the constraints on the degree of \( G \)). The code \( C \) is AG if moreover \( 2g - 2 < \deg(G) < n \). The code \( C \) is SAG if moreover \( 2g - 2 < \deg(G) < n \). In view of Theorem 1.1 we therefore have the following corollary.

**Corollary 2.1** If \( C \) is WAG or SAG, then \( C^\perp \) is WAG or SAG, respectively.

**Remark 2.2** There exist codes which are AG while the dual is not. For an example, see Remark 2.10.

**Definition 2.2** Let \( n > 1 \). Let \( \pi_i : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-1} \) be the projection defined by deleting the \( i^{th} \) coordinate. If \( C \) is a code in \( \mathbb{F}_q^n \) then define \( C_i \) by \( C_i = \pi_i(C) \). We say that \( C_i \) is obtained from \( C \) by puncturing at the \( i^{th} \) coordinate.

**Lemma 2.1** If \( C \) is WAG then \( C_i \) is WAG.

**Proof:** Suppose that \( C = C_L(X, D, G) \) for some curve \( X \), where \( D = (P_1, \ldots, P_n) \). By setting \( D_i = (P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n) \), we immediately have \( C_i = C_L(X, D_i, G) \).
\[\Box\]

**Remark 2.3** If \( C \) is AG or SAG, then \( C_i \) need not be AG or SAG, respectively, see Remark 2.15.
Chapter 2: Representing Linear Codes by Curves

Definition 2.3 Let $C$ be a linear code in $\mathbb{F}_q^n$ and $\sigma$ a permutation of $\{1, \ldots, n\}$. Define
\[
\sigma C = \{(x_\sigma(1), \ldots, x_\sigma(n)) | (x_1, \ldots, x_n) \in C\}.
\]
Two linear codes $C_1$ and $C_2$ in $\mathbb{F}_q^n$ are called equivalent if $C_2 = \sigma C_1$ for some permutation $\sigma$ of $\{1, \ldots, n\}$. Let $\lambda = (\lambda_1, \ldots, \lambda_n)$ be an $n$-tuple of non-zero elements in $\mathbb{F}_q$. Define
\[
\lambda C = \{ (\lambda_1 x_1, \ldots, \lambda_n x_n) | (x_1, \ldots, x_n) \in C\}.
\]
The codes $C_1$ and $C_2$ are called generalized equivalent or isometric if there is an $n$-tuple $\lambda = (\lambda_1, \ldots, \lambda_n)$ of nonzero elements in $\mathbb{F}_q$ and a permutation $\sigma$ such that $C_2 = \lambda \sigma C_1$.

Lemma 2.2 If $C_1$ and $C_2$ are isometric codes and $C_1$ is WAG, AG or SAG, then $C_2$ is WAG, AG, SAG, respectively.

Proof: Suppose $C_1 = C_L(X, D, G)$ and $C_2 = \lambda \sigma C_1$ for some non-zero elements $\lambda_1, \ldots, \lambda_n$ in $\mathbb{F}_q$ and a permutation $\sigma$. There exists a rational function $f$ such that $f(P_{\sigma(i)}) = \lambda_i$ for all $i$, by the independence of valuations, see [6, p.11]. Let $\sigma D = (P_{\sigma(1)}, \ldots, P_{\sigma(n)})$. Then the divisor $G - (f)$ has disjoint support with $\sigma D$, since all the $\lambda_i$ are nonzero. We have $C_2 = C_L(X, \sigma D, G - (f))$ and $C_2$ is WAG. The degrees of $G$ and $G - (f)$ are equal. So, if $C_1$ is AG or SAG, then $C_2$ is AG or SAG, respectively. □

Definition 2.4 We call a $q$-ary linear $[n, k]$ code projective if every two columns of a generator matrix of $C$ are linearly independent; Thus if we view the columns of a generator matrix as points in the $(k - 1)$-dimensional projective space $\mathbb{P}^{k-1}$, expressed in homogeneous coordinates, then we get $n$ distinct points. Obviously, this definition is independent of the generator matrix chosen. By $S(r, q)$ we denote any $q$-ary projective code of dimension $r$ and length $(q^r - 1)/(q - 1)$. Such a code is called a Simplex code. By $H(r, q)$ we denote the dual of $S(r, q)$. This is a $q$-ary Hamming code of redundancy $r$. If all the $n$ points of a projective code lie in the complement of a hyperplane then we call the code affine.

From the above definition, we can easily derive the following simple properties. If $n \geq 3$, then a code $C$ is projective if and only if $d(C^L) \geq 3$. The code $C$ is affine if and only if $C$ is projective and there exists a codeword with its weight equal to the word length. The maximal word length of a projective code of dimension $r$ is $(q^r - 1)/(q - 1)$. For fixed $r$ and $q$ all $q$-ary Simplex codes of dimension $r$ are isometric. The same holds for Hamming codes. The maximal possible word length of an affine code of dimension $r$ is $q^{r-1}$. For fixed $q$ and $r$ all affine $q$-ary codes of dimension $r$ and word length $q^{r-1}$ are isometric and are called $q$-ary first order Reed-Muller codes.

Remark 2.4 Let $C$ be a $q$-ary projective code $C$ of dimension at least 2. Suppose $C = C_L(X, D, G)$ for some curve $X$ and divisors $D$ and $G$. If $L(G) = L(G - P)$ for some point $P$ of $X$, then $P$ is not in the support of $D$. Otherwise $P = P_i$ for some $i \in \{1, \ldots, n\}$, so all the codewords have a zero at place $i$, contradicting the assumption that $C$ is projective. Thus $G - P$ has disjoint support with $D$ and $C = C_L(X, D, G - P)$. Repeating this procedure we may assume without loss of generality that $G$ is a divisor such that $L(G) \neq L(G - P)$ for all points $P$, that is
to say, \( G \) has no base points. Let \( l(G) = l \) and let \( f_0, \ldots, f_{l-1} \) be a basis of \( L(G) \). Consider the morphism

\[ \varphi_G : \mathcal{X} \rightarrow \mathbf{P}^{l-1}, \]

given by the collection of morphisms \( \{ \varphi_j : \mathcal{X} \setminus \text{supp}(G_j) \rightarrow \mathbf{P}^{l-1} \}_{j=0}^{l-1} \), where \( G_j = G + (f_j) \), and \( \varphi_j \) is defined by

\[ \varphi_j(P) = \left( \frac{f_0(P)}{f_j}, \ldots, \frac{f_{l-1}(P)}{f_j} \right), \]

for \( P \in \mathcal{X} \setminus \text{supp}(G_j) \), see [33, p.128]. Then \( \varphi_G(P) = (f_0(P) : \ldots : f_{l-1}(P)) \), for \( P \in \mathcal{X} \setminus \text{supp}(G) \). This holds in particular for the \( P_i \). The morphism \( \varphi_G \) depends only on the linear equivalence class of \( G \), and on the choice of the basis \( f_0, \ldots, f_{l-1} \) of \( L(G) \). A different choice of a basis of \( L(G) \) gives a morphism which differs by an automorphism of \( \mathbf{P}^{l-1} \) (see [30, p.158]). Let \( \mathcal{X}_0 \) be the reduced image of \( \mathcal{X} \) under the morphism \( \varphi_G \). Then \( \mathcal{X}_0 \) is not a single point. Even stronger, \( \mathcal{X}_0 \) is not contained in any hyperplane. This follows from the fact that \( f_0, f_1, \ldots, f_{l-1} \) are linearly independent. Hence \( \varphi_G \) is a finite dominant morphism \( \mathcal{X} \rightarrow \mathcal{X}_0 \) of curves. Since \( \mathcal{X} \) is absolutely irreducible, so is \( \mathcal{X}_0 \). Finally, we have

\[ \deg(G) = \deg(\varphi_G) \cdot \deg(\mathcal{X}_0), \]

since \( G \) has no base points, see [33, p. 213].

**Definition 2.5** Let \( C \) be a projective code of dimension at least 2. If \( (\mathcal{X}, D, G) \) is a \((WAG, \text{AG} \text{ or SAG})\) representation of \( C \) and \( G \) is a divisor without base points and \( \deg(\varphi_G) = 1 \), then we call \((\mathcal{X}, D, G)\) a minimal \((WAG, \text{AG} \text{ or SAG})\) representation of \( C \) (respectively).

**Proposition 2.1** Suppose \( C \) is a projective \( WAG \) code of dimension at least two. If \( (\mathcal{X}, D, G) \) is a representation of \( C \), with \( G \) base point free, then there exists a minimal representation \((\mathcal{X}_0, D', G')\) of \( C \) and a finite morphism \( \varphi : \mathcal{X} \rightarrow \mathcal{X}_0 \) with the following properties:

i) \( D' = (\varphi(P_1), \ldots, \varphi(P_n)) \).

ii) \( \varphi^*(G) \sim G \), where \( \varphi^*(G) \) is the pull back of \( G \) under \( \varphi \).

iii) \( \deg(\varphi) = \deg(\varphi_G) \).

iv) \( \deg(G) = \deg(G') / \deg(\varphi) \leq \deg(G) \).

v) \( g(\mathcal{X}_0) \leq g(\mathcal{X}) \), with equality if and only if \( \deg(\varphi) = 1 \).

vi) If \( (\mathcal{X}, D, G) \) is an \( \text{AG} \) representation, then so is \((\mathcal{X}_0, D, G)\).

vii) If \( (\mathcal{X}, D, G) \) is a \( \text{SAG} \) representation, then so is \((\mathcal{X}_0, D, G)\).

**Proof:** Let \( l(G) = l \). The kernel of the linear map \( \alpha_L \) is \( L(G - D) \). We have \( k = \dim(C) = l(G) - l(G - D) \). Let \( f_0, \ldots, f_{l-1} \) be a basis of \( L(G) \) such that \( f_k, \ldots, f_{l-1} \) is a basis of \( L(G - D) \). Let \( A \) be the \((l \times n)\)-matrix \( (f_j(P_i))_{i=0, \ldots, l-1; j=1, \ldots, n} \). The first \( k \) rows of \( A \) form a generator matrix of \( C \). The remaining \( l-k \) rows have only zero entries. Let the morphism \( \varphi_G \) be defined by this basis of \( L(G) \). The reduced image \( \mathcal{X}_0 \) of \( \mathcal{X} \) under \( \varphi_G \) is possibly singular. Let \( n : \mathcal{X}_0 \rightarrow \mathcal{X}_0 \) be the normalization of \( \mathcal{X}_0 \). Then \( n \) is a birational morphism. Hence we have a rational map \( \tilde{\varphi}_G : \mathcal{X} \rightarrow \mathcal{X}_0 \) such that \( n \circ \tilde{\varphi}_G = \varphi_G \). The curve \( \mathcal{X} \) is nonsingular, hence \( \tilde{\varphi}_G \) is a morphism. The \( n \) points \( \tilde{\varphi}_G(P_i) \) \( (i = 1, \ldots, n) \) are rational and we claim that they are all distinct. Indeed, if \( \tilde{\varphi}_G(P_i) = \tilde{\varphi}_G(P_j) \) then \( \varphi_G(P_i) = \varphi_G(P_j) \). But \( \varphi_G(P_i) \)
corresponds to the \( s^{th} \) column of the matrix \( A \), and \( C \) is projective, hence \( s = t \). Put \( P_i = \phi_G(P_i) \) and \( \tilde{D} = (P_1, \ldots, P_n) \). For \( j = 0, \ldots, l - 1 \), we denote by \( g_j \) the function \( x_j/x_0 \), which is a rational function on \( X_0 \) such that \( f_j/f_0 = g_j \circ \phi_G \). We denote \( g_j \circ n \) by \( \tilde{g}_j \). Let \( H \) be the hyperplane in \( \mathbb{P}^{l-1} \) with equation \( x_0 = 0 \) and let \( H \cdot X_0 \) be the intersection divisor of \( H \) with \( X_0 \). Define \( G_0 := G + (f_0) \). The pull back \( \phi_G^*(H \cdot X_0) \) is equal to \( G_0 \). Let \( \tilde{G}_0 = n^*(H \cdot X_0) \). Then \( \phi_G \) induces an injective map \( \tilde{\phi}_G \) from the function field of \( \tilde{X}_0 \) into the function field of \( X \), and maps \( L(\tilde{G}_0) \) injectively into \( L(G_0) \). This map is also surjective since \( \phi_G^*(\tilde{g}_j) = f_j/f_0 \), for \( j = 0, \ldots, l - 1 \), and \( f_1/f_0, \ldots, f_{l-1}/f_0 \) is a basis of \( L(G_0) \). Let \( \phi_{\tilde{G}_0} \) be defined by the basis \( \tilde{g}_0, \ldots, \tilde{g}_{l-1} \) of \( L(\tilde{G}_0) \). Note that \( \phi_{\tilde{G}_0} \) is equal to the normalization map \( n \). There exists a divisor \( \tilde{G} \) which is linearly equivalent with \( \tilde{G}_0 \) and has disjoint support with \( iJ \), by the theorem of independence of valuations, see [6, p.11]. We have \( \phi_{\tilde{G}} = \phi_{\tilde{G}_0} \), where \( \phi_{\tilde{G}} \) is defined by a suitable choice of a basis of \( L(\tilde{G}) \). Hence \( \phi_{\tilde{G}}(P_i) = n^* \phi_G(P_i) = \phi_G(P_i) \), for \( i = 1, \ldots, n \). All these points have their last \( l - k \) coordinates equal to zero. Thus there is an \( n \)-tuple \( \lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_q^n \), with all \( \lambda_i \neq 0 \), such that \( C_L(\tilde{X}_0, \tilde{D}, \tilde{G}) = \lambda C_L(X, D, G) \). As we see from the proof of Lemma 2.2, we may assume without loss of generality that \( C_L(\tilde{X}_0, \tilde{D}, \tilde{G}) = C_L(X, D, G) \). In the proposition choose \( \phi = \phi_{\tilde{G}} \). We have \( \deg(\phi_{\tilde{G}}) = \deg(n) = 1, \deg(\phi) = \deg(\phi_G) \) and

\[
\deg(\tilde{G}) = \deg(\tilde{G}_0) = \frac{\deg(G_0)}{\deg(\phi)} = \frac{\deg(G)}{\deg(\phi_G)} \leq \deg(G),
\]

see Remark 2.4. Since \( G \) is base point free and \( \phi^* \) restricts to an isomorphism from \( L(\tilde{G}_0) \) to \( L(G_0) \), \( \tilde{G} \) is base point free too. Since \( \phi^* \) preserves linear equivalence and \( \tilde{G} \sim \tilde{G}_0 \), we have \( \phi^*(\tilde{G}) \sim \phi^*(\tilde{G}_0) = G_0 \sim G \). This proves everything in the proposition, except \( v),vi) \) and \( vii) \). Note that \( vi) \) is an immediate consequence of \( iv) \). Part \( v) \) and part \( vii) \) will follow by the genus formula of Zeuthen-Hurwitz, see [43, p.52] or [30, p.301]. First we prove that \( \varphi \) is separable. The morphism \( \varphi : X \to \tilde{X}_0 \) factorizes into \( \varphi = \varphi_s \circ \varphi_i \), where

\[
\varphi_i : X_i \to X_i
\]
is purely inseparable and

\[
\varphi_s : X_i \to \tilde{X}_0
\]
is separable, see [30, p. 303, Example 2.5.4]. The morphism \( \varphi_i \) induces an inclusion

\[
\varphi_i^* : \mathbb{F}_q(X_i) \hookrightarrow \mathbb{F}_q(X),
\]

and the image is equal to

\[
\{ f^r \mid f \in \mathbb{F}_q(X) \} = \mathbb{F}_q(X)^{\varphi_i},
\]

where \( p = \deg(\varphi_i) \), \( p \) is the characteristic of \( \mathbb{F}_q \) and \( r \) is some nonnegative integer. The curve \( X_i \) is isomorphic with \( X_i \), see [30, p. 302, Prop. 2.5]. Let \( \psi : X_i \to X \) be the isomorphism (of curves) which induces the isomorphism (of function fields)

\[
\psi^* : \mathbb{F}_q(X) \to \mathbb{F}_q(X_i), f \to f^{\varphi_i^*},
\]

Put \( G_i := \varphi_s^*(\tilde{G}_0) \). Define the divisor \( G_i' \) on \( X \) by \( \psi^*(G_i') = G_i \). Then \( G_0 = \varphi^*(\tilde{G}_0) = \varphi_s^*(\varphi_i^*(\tilde{G}_0)) = \varphi_i^*(G_i') = p^r G_i' \). The map \( \varphi_i^* \) maps \( L(G_i) \) injectively into \( L(G_0) \). The morphism \( \varphi_s \) induces an inclusion

\[
\varphi_s^* : \mathbb{F}_q(\tilde{X}_0) \hookrightarrow \mathbb{F}_q(X_i).
\]
and \( \varphi_\ast \) maps \( L(\tilde{G}_0) \) injectively into \( L(G_i) \). Thus \( l(\tilde{G}_0) \leq l(G_i) \leq l(G_0) \). But, as we saw earlier in the proof of this proposition, \( l(G_0) = l(\tilde{G}_0) \), hence \( l(G_i) = l(G_0) \).

Now suppose that \( \deg(\varphi_i) > 1 \), that is to say \( r > 0 \). Let \( P \in \text{supp}(G'_i) \). Then

\[
G'_i \leq (p^r - 1)G'_i \leq p^r G'_i - P = G_0 - P \leq G_0.
\]

Hence

\[
L(G'_i) \subseteq L(G_0 - P) \subseteq L(G_0).
\] (1)

On the other hand, \( \psi^* \) restricts to an isomorphism \( L(G_i) \rightarrow L(G'_i) \), hence \( l(G_i) = l(G'_i) \), and by (1), \( l(G_0) = l(G'_i) \). This implies that the inclusions in (2) are equalities, and hence that \( P \) is a basepoint of \( G_0 \), a contradiction. Thus \( \deg(\varphi_i) = 1 \), and \( \varphi \) is separable. So we can apply the genus formula of Zeuthen-Hurwitz to \( \varphi \):

\[
2g(X) - 2 = (2g(\tilde{X}_0) - 2)\deg(\varphi) + \deg(R),
\]

where \( R \) is the ramification divisor of \( \varphi \), which is effective. As shown in [30, p. 303, Example 2.5.4], it follows that \( g(X) \geq g(\tilde{X}_0) \). Note that if \( \deg(\varphi) = 1 \), then \( R = 0 \). One easily verifies that \( g(X) = g(\tilde{X}_0) \) if and only if \( \deg(\varphi) = 1 \), or \( g(X) = 0 \), or \( g(X) = 1 \) with \( \varphi \) unramified. However, in our situation, the second and the third case are included in the first. Namely, suppose that \( g(X) = g(\tilde{X}_0) =: g \leq 1 \). We have \( 2 \leq k \leq l(G) = l(\tilde{G}_0) \), hence \( \deg(G) > 0 \geq 2g - 2 \) and \( \deg(G_0) > 0 \geq 2g - 2 \), and by Riemann-Roch

\[
l(G_0) = \deg(G) + 1 - g,
\]

\[
l(\tilde{G}_0) = \deg(\tilde{G}_0) + 1 - g.
\]

Since \( l(G_0) = l(\tilde{G}_0) \), we get \( \deg(G_0) = \deg(\tilde{G}_0) = \deg(G_0)/\deg(\varphi) \), hence \( \deg(\varphi) = 1 \). This proves v). Finally, if \( \deg(G) > 2g(X) - 2 \), then

\[
\deg(\tilde{G}) = \frac{\deg(G)}{\deg(\varphi)} \geq \frac{2g(X) - 2}{\deg(\varphi)} \geq 2g(\tilde{X}_0) - 2.
\]

This proves vii) and completes the proof of the proposition. \( \square \)

**Corollary 2.2** Suppose that \( (X, D, G) \) is a WAG representation of a projective code \( C \) of dimension at least two, with \( G \) base point free, and such that \( g(X) \) is minimal, that is to say, for all WAG representations \( (X', D', G') \) of \( C \) we have \( g(X) \geq g(X') \). Then \( (X, D, G) \) is a minimal WAG representation of \( C \). This corollary is also true if ‘WAG’ is replaced by ‘AG’ everywhere, or by ‘SAG’.

**Proof:** Let \( (\tilde{X}_0, \tilde{D}, \tilde{G}) \) be a minimal WAG representation of \( C \) with the properties as in Proposition 2.1 By the assumption on \( g(X) \), and by Proposition 2.1 (v), we have \( g(\tilde{X}_0) = g(X) \), and hence \( \deg(\varphi_0) = \deg(\varphi) = 1 \), by Proposition 2.1 (iii). Since \( G \) is base point free, moreover, \( (X, D, G) \) is minimal. The two assertions in the second part of the corollary are proved similarly, using Proposition 2.1 (vi) and 2.1 (vii), respectively. \( \square \)
2.2 All linear codes are weakly algebraic-geometric

In [31], Hansen and Stichtenoth considered the curve $\mathcal{X}$ in $\mathbb{P}^2$ defined by the homogeneous equation

$$x^{q_0}(x^q + xz^{q-1}) = x^{q_0}(y^q + yz^{q-1}),$$

where $q_0 = 2^m$ and $q = 2^{2n+1}$. This curve is absolutely irreducible, has exactly one (singular) point $P_\infty$ at the line $z = 0$, and goes through all the rational points outside the line $z = 0$. The linear system of hyperplane sections of this curve is complete. Inspired by their result we consider the following series of curves.

Definition 2.6 Let $p$ be a prime number and $q$ a power of $p$. Let $\mathcal{X}(l, q)$ be the closed subscheme over $\mathbb{F}_q$ in $\mathbb{P}^l$ defined by the homogeneous ideal

$$I(l, q) = (x_i^{q+1} - x_i^2 x_0^{q-1} + x_{i+1} x_0^q - x_{i+1} x_0, i = 1, \ldots, l-1)$$

in $\mathbb{F}_q[x_0, \ldots, x_l]$.

Proposition 2.2 The scheme $\mathcal{X}(l, q)$ is a projective, absolutely irreducible, reduced curve over $\mathbb{F}_q$. It has exactly one point $P_\infty$ at the hyperplane $H$ with equation $x_0 = 0$, the curve is nonsingular outside $P_\infty$ and goes through all the $q^l$ rational points of $\mathbb{P}^l$ outside the hyperplane $H$.

Proof: The scheme $\mathcal{X}(l, q)$ is defined by $l-1$ equations, hence all the irreducible components are at least one-dimensional (cf. [85, p.196]). So the dimension of $\mathcal{X}(l, q)$ is at least one. $P_\infty = (0 : \ldots : 0 : 1)$ is the only point in the intersection with $H$, which follows directly from the equations. Let

$$f_i = y_i^{q+1} - y_i^2 + y_{i+1} - y^{q}_{i+1} \quad \text{for} \quad i = 1, \ldots, l-1.$$

Then $f_1 = \ldots = f_{l-1} = 0$ are the equations of $\mathcal{X}(l, q)$ on the complement of $H$, which is isomorphic with affine $l$-space with coordinates $y_1, \ldots, y_l$, denoted by $\mathcal{X}(l, q)_*$, where $y_i = x_i/x_0$. Let $\psi : \mathcal{X}(l, q)_* \to A^1$ (a one-dimensional affine space), such that $\psi(y_1, \ldots, y_l) = y_l$. Then $\psi$ is a morphism and $\psi^{-1}(y)$ is the set of $q^{l-1}$ elements $y = (y_1, \ldots, y_l)$ in $\mathbb{F}_q^l$ as well as in $\mathbb{F}_q^l$ of the equations $f_1, \ldots, f_{l-1} = 0$. This implies that the dimension of $\psi^{-1}(y)$ is zero. Thus $\dim \mathcal{X}(l, q)_* \leq \dim A^1 + \dim \psi^{-1}(y) = 1$ (cf. [30, p. 95, Exe. 3.22]). Hence $\mathcal{X}(l, q)$ has dimension one and codimension (see [30, p. 86]) $l-1$. Let $f = (f_1, \ldots, f_{l-1})$. Computing the derivative of $f$ yields

$$df = \begin{pmatrix} y_1^q - 2y_1 & 1 & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & y_{l-1}^q - 2y_{l-1} & 1 \end{pmatrix}$$

Hence $df$ has maximal rank at all points not equal to $P_\infty$ of $\mathcal{X}(l, q)$ over $\bar{\mathbb{F}}_q$. Thus the scheme is nonsingular outside $P_\infty$. Let $H_i$ be a subscheme defined by the ideal $(x_i^{q+1} - x^2 x_0 + x_{i+1} x_0^q - x_{i+1} x_0)$. It is a locally principal subscheme of codimension 1. Furthermore, $\mathcal{X}(l, q) = H_1 \cap H_2 \cap \cdots \cap H_{l-1}$. This proves that $\mathcal{X}(l, q)$ is a complete intersection (cf. [30, p. 118]). By the nonsingularity of the scheme for every place $P(\neq P_\infty)$, we have that the local ring defined by $P$ is a discrete valuation ring which has no nilpotent element. Thus $\mathcal{X}(l, q)$ is reduced outside $P_\infty$ (cf. [30, p. 82]).
Moreover, it is reduced since it is a complete intersection (cf. [30, p. 186] and [48, p. 110]). Therefore there is a normalization of $X(l,q)$. Let 

$$n : \tilde{X}(l,q) \longrightarrow X(l,q)$$

be the normalization of $X(l,q)$ and $\tilde{P}_\infty$ any point in $n^{-1}(P_\infty)$. Let $v_\infty$ be the discrete valuation at $\tilde{P}_\infty$. Let $z_1 = y_1 \circ n$. Then $z_1, \ldots, z_i$ are rational functions on $\tilde{X}(l,q)$ and have no poles outside $n^{-1}(P_\infty)$. Furthermore $z_i^{i+1} - z_i^2 = z_{i+1} - z_{i+1}$. Thus

$$(q+1)v_\infty(z_i) = qv_\infty(z_{i+1}).$$

Now $z_i$ has a pole at $\tilde{P}_\infty$, hence $v_\infty(z_i)$ is negative. Hence by induction one shows that there exists a positive integer $a$ such that $v_\infty(z_i) = -aq^{i-1}(q+1)^{i-1}$. Consider the map $\varphi : \tilde{X}(l,q) \rightarrow \mathcal{Y}$, which is the projection of the curve in $\mathbb{P}^l$ with center with equations $x_0 = x_1 = 0$, onto the line $\mathcal{Y}$ defined by the equations $x_0 = \ldots = x_l = 0$. Then $t = x_0/x_1$ is a local parameter of the point $Q_\infty = (0 : 1 : 0 : \ldots : 0)$ in $\mathcal{Y}$. Let the map $\tilde{\varphi} : \tilde{X}(l,q) \rightarrow \mathcal{Y}$ be defined by $\tilde{\varphi} = \varphi \circ n$. Then $\tilde{P}_\infty$ is a point of $\tilde{\varphi}^{-1}(Q_\infty)$ and $v_\infty(t) = aq^{l-1}$, so the ramification index $e_{P_\infty}$ of $\tilde{\varphi}$ at $\tilde{P}_\infty$ is at least $q^{l-1}$. For every other point $Q$ of $\mathcal{Y}(\tilde{F}_q)$ not equal to $Q_\infty$, the inverse image $\tilde{\varphi}^{-1}(Q)$ consists of exactly $q^{l-1}$ points over $\tilde{F}_q$, all with ramification index one, since the map

$$d\tilde{\varphi} : T_Q(\tilde{X})(l,q) \longrightarrow T_Q(\mathcal{Y})$$

between the tangent spaces, is surjective, as one sees from the derivative $df$ of $f$. Thus $\deg(\tilde{\varphi}) = q^{l-1} \leq e_{P_\infty}$. Therefore $\tilde{X}(l,q)$ is absolutely irreducible and $n^{-1}(P_\infty) = \{\tilde{P}_\infty\}$, by the following lemma, and thus $X(l,q)$ is absolutely irreducible. 

\[\square\]

**Lemma 2.3** Let $X$ and $\mathcal{Y}$ be projective, nonsingular curves over an algebraically closed field. Suppose $\mathcal{Y}$ is irreducible. Let $\varphi : X \rightarrow \mathcal{Y}$ be a finite morphism. Suppose there exist points $P_\infty$ in $X$ and $Q_\infty$ in $\mathcal{Y}$ such that $\varphi(P_\infty) = Q_\infty$ and the ramification index $e_{P_\infty}$ of $\varphi$ at $P_\infty$ is at least $\deg(\varphi)$. Then $\deg(\varphi) = e_{P_\infty}$ and $X$ is irreducible and $\{P_\infty\} = \varphi^{-1}(Q_\infty)$.

**Proof:** Suppose $X_1, \ldots, X_s$ are the irreducible components of $X$. Let $\varphi_i$ be the restriction of $\varphi$ to $X_i$. Then

$$\deg(\varphi) = \sum_{i=1}^s \deg(\varphi_i) = \sum_{P \in e_{\varphi^{-1}}(Q)} e_P,$$

for every point $Q$ of $\mathcal{Y}$. Suppose $P_\infty \in X_1$. Then

$$\deg(\varphi) \geq \deg(\varphi_1) \geq e_{P_\infty} \geq \deg(\varphi).$$

Thus $\deg(\varphi) = \deg(\varphi_1) = e_{P_\infty}$. So $\{P_\infty\} = \varphi^{-1}(Q_\infty)$ and $X_1$ is the only irreducible component of $X$, that is to say $X$ is irreducible. \[\square\]

**Proposition 2.3** The normalization of $X(l,q)$ has genus $g(l,q)$, where

$$g(l,q) = \frac{1}{2} \left\{ \sum_{i=1}^{l-1} q^{i+1-i}(q+1)^{i-1} - (q+1)^{i-1} + 1 \right\}$$
Chapter 2: Representing Linear Codes by Curves

Proof: It follows from the proof of Proposition 2.2 that \( v_\infty(z_i) = -q^{i-1}(q+1)^{i-1} \) and \( n^{-1}(P_\infty) \) consists of exactly one point \( \tilde{P}_\infty \). Let

\[
u = \prod_{i=1}^{l} z_i^{\binom{l-1}{i-1}}(-1)^{i-1}.
\]

Then \( \nu \) is a local parameter of \( \tilde{P}_\infty \), since

\[
u_\infty(\nu) = \sum_{i=1}^{l} \binom{l-1}{i-1}(-1)^{i-1-i} v_\infty(z_i) = \sum_{i=0}^{l-1} \binom{l-1}{i}(-q)^{i-1-i} (q+1)^i = [-q + (q+1)]^{i-1} = 1.
\]

Differentiating the equation

\[z_{i+1} - z_i^q = z_i^{q+1} - z_i^2 \quad \text{for} \quad 1 \leq i \leq l - 1,
\]

with respect to \( z_i \) gives

\[rac{dz_{i+1}}{dz_i} = 2z_i - z_i^q.
\]

Hence we get by the chain rule and induction

\[rac{dz_j}{dz_1} = \prod_{i=1}^{j-1} (2z_i - z_i^q).
\]

Let \( t = z_1^{-1} \). Then \( t \) is a local parameter of \( Q_\infty \) in \( \mathcal{Y} \). Thus

\[rac{du}{dt} = -z_1^2 \frac{du}{dz_1} = -z_1^2 \left\{ \prod_{i=1}^{l} \left[ z_i^{\binom{l-1}{i-1}}(-1)^{i-1-i} \right] \left( \frac{dz_i}{dz_1} \right) \right\}.
\]

Now

\[
u_\infty(z_1^{-1} \frac{dz_i}{dz_1}) = q^{i-1}(q+1)^{i-1} - \sum_{j=1}^{i-1} q^{i-j}(q+1)^{j-1} > v_\infty(z_1^{-1} \frac{dz_{i+1}}{dz_1}).
\]

Therefore

\[
u_\infty(\frac{du}{dt}) = \nu_\infty(z_1^2 u z_i^{-1} \frac{dz_i}{dz_1}).
\]

And we conclude

\[
u_\infty(\frac{dt}{du}) = \sum_{i=1}^{l-1} q^{i+1-i}(q+1)^{i-1} + 2q^{i-1} - 1 - (q+1)^i.
\]

The map \( \phi \) is separable, has degree \( q^{-1} \) and is only ramified at \( \tilde{P}_\infty \). Let \( g = g(l, q) \). Then

\[2g - 2 = -2\deg(\phi) + \nu_\infty(\frac{dt}{du}),
\]

by the theorem of Hurwitz-Zeuthen, see [43]. Thus

\[g = \frac{1}{2} \left\{ \sum_{i=1}^{l-1} q^{i+1-i}(q+1)^{i-1} - (q+1)^{i-1} + 1 \right\}.
\]
Remark 2.5 (See [19].) Let \( P \) be a point on a nonsingular, absolutely irreducible curve \( X \) of genus \( g \) over a field. Let \( N_n = \dim(L(nP)) \) for \( n \in \mathbb{N} \). Then \( 1 = N_0 \leq N_1 \leq \ldots \leq N_{2g-1} = g \), so there are exactly \( g \) numbers \( 0 < n_1 < \ldots < n_g < 2g \) such that \( L(n,P) = L((n_i-1)P) \). These \( n_i \) are called Weierstrass gaps of \( P \). Furthermore, if \( m \in \mathbb{N} \) then

\[
N_n = \#\{m \in \mathbb{N} | m \leq n \text{ and } m \text{ is not a gap at } P\}.
\]

Definition 2.7 Let \( G(l,q) = \{n_1, n_2, \ldots, n_g\} \) be the set of all gaps of \( \hat{P}_\infty \) on the curve \( \hat{X}(l,q) \) of genus \( g = g(l,q) \).

Definition 2.8 Let

\[
\mathcal{P}(l,q) = \{\sum_{i=1}^{l} k_i q^{l-i}(q+1)^{i-1} | k_i \in \mathbb{Z} \text{ and } k_i \geq 0\}.
\]

Proposition 2.4 \( G(l,q) = \mathbb{N} \setminus \mathcal{P}(l,q) \).

To prove this proposition we need the following lemmas.

Lemma 2.4 For every \( m \in \mathbb{Z} \), there are unique \( u, v \in \mathbb{Z} \), such that

\[ m = uq + v(q+1)^{l-1} \quad \text{and} \quad 0 \leq v < q. \]

Moreover, \( m \in \mathcal{P}(l,q) \) if and only if \( u \in \mathcal{P}(l-1,q) \).

Proof: Since

\[ 1 = -\left(\sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1}\right)q + (q+1)^{l-1}, \]

we have that

\[ m = -m\left(\sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1}\right) + m(q+1)^{l-1}, \]

for every \( m \in \mathbb{N} \), furthermore there exist \( a, b \in \mathbb{N} \) such that \( m = aq + b \) and \( 0 \leq b < q \), so

\[ m = \{a(q+1)^{l-1} - m\sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1}\}q + b(q+1)^{l-1}. \]

Let

\[ u = a(q+1)^{l-1} - m\sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1} \quad \text{and} \quad v = b, \]

then \( m = uq + v(q+1)^{l-1} \) and \( 0 \leq v < q \). If there were another \( u_1, v_1 \in \mathbb{Z} \), such that \( m = u_1q + v_1(q+1)^{l-1} \) and \( 0 \leq v_1 < q \) then we can assume without loss of generality that \( u_1 \geq u \), thus \( (u_1 - u)q + (v_1 - v)(q+1)^{l-1} = 0 \), so \( q \) would divide \( (v_1 - v) \), so \( v_1 = v \), and \( u_1 = u \) as well. Therefore such \( u \) and \( v \) are unique.

Now suppose \( m = uq + v(q+1)^{l-1} \) and \( 0 \leq v < q \).

If \( m \in \mathcal{P}(l,q) \), then \( m = \sum_{i=1}^{l} k_i q^{l-i}(q+1)^{i-1} \) where \( k_i \) is a non negative integer for \( i = 1, \ldots, l \). But \( k_i = aq + b \), where \( a, b \in \mathbb{N} \) and \( 0 \leq b < q \), so

\[
m = \{\sum_{i=1}^{l-1} k_i q^{l-i}(q+1)^{i-1} + a(q+1)(q+1)^{l-2}\}q + b(q+1)^{l-1},
\]
hence \( u = \sum_{i=1}^{l-1} j_i q^{l-1-i}(q+1)^{i-1} \), by the uniqueness of \( u \), where \( j_i = k_i \) for \( i = 1, \ldots , l-2 \) and \( j_{l-1} = k_{l-1} + a(q+1) \). Thus \( u \in P(l-1,q) \).

If \( u \in P(l-1,q) \) then \( u = \sum_{i=1}^{l-1} j_i q^{l-1-i}(q+1)^{i-1} \) for some nonnegative integers \( j_1, \ldots , j_{l-1} \) so

\[
m = \left\{ \sum_{i=1}^{l-1} j_i q^{l-1-i}(q+1)^{i-1} \right\} q + v(q+1)^{l-1} \in P(l,q) .
\]

**Lemma 2.5** \( \#(N \setminus P(l,q)) = g(l,q) \).

**Proof:** By induction on \( l \).

(i) We have that \( P(2,q) = \{ iq + j(q+1) \mid i, j \in \mathbb{N} \} \), so

\[
N \setminus P(2,q) = \bigcup_{k=0}^{q-2} \left\{ kq + (k+1), kq + (k+1) + 1, \ldots , (k+1)q - 1 \right\},
\]

which is a union of mutually disjoint sets, hence

\[
\#(N \setminus P(2,q)) = (q-1) + (q-2) + \ldots + 2 + 1 = \frac{1}{2} q(q-1),
\]

which satisfies the conclusion.

(ii) Assume the conclusion is true for \( l-1 \). By Lemma 2.4 we have that

\[
N = \{ uq + v(q-1)^{l-1} \mid u < 0, 0 \leq v < q \} \cup \{ uq + v(q+1)^{l-1} \mid u \geq 0, 0 \leq v < q \},
\]

where the two sets are disjoint. We denote the first set by \( N_1 \), and the second one by \( N_2 \). Then

\[
N \setminus P(l,q) = (N_1 \setminus P(l,q)) \cup (N_2 \setminus P(l,q)).
\]

1) For each \( uq + v(q-1)^{l-1} \in N_2 \setminus P(l,q) \), we have \( u \in N \setminus P(l-1,q) \) by Lemma 2.4, so

\[
\#(N_2 \setminus P(l,q)) = \#(N \setminus P(l-1,q)) = \frac{1}{2} q \left\{ \sum_{j=1}^{l-2} q^{l-j}(q+1)^{j-1} - (q+1)^{l-2} + 1 \right\}.
\]

2) For each \( uq + v(q-1)^{l-1} \in N_1 \setminus P(l,q) \), we have \( u < 0 \) and \( 0 \leq v < q \). Hence

\[
uq + v(q+1)^{l-1} \geq 1 \Leftrightarrow -uq \leq v(q+1)^{l-1} - 1
\]

\[
\Leftrightarrow -uq \leq v \left( \sum_{i=1}^{l-1} \binom{l-1}{i} q^i \right) + v - 1 \Leftrightarrow -u \leq v \sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1},
\]

since \( v - 1 < q - 1 \). Hence

\[
\#(N_1 \setminus P(l,q)) = \sum_{v=1}^{q-1} \sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1} = \frac{1}{2} q(q-1) \sum_{i=1}^{l-1} \binom{l-1}{i} q^{i-1} = \frac{1}{2} \left( q(q+1)^{l-1} - (q+1)^{l-1} - q + 1 \right).
\]
Combining 1) and 2) gives
\[ \#(N \setminus P(l, q)) = \frac{1}{2} \sum_{j=1}^{l-2} q^{j+1-j}(q + 1)^{j-1} - q(q + 1)^{j-2} + q \]
\[ + q(q + 1)^{j-1} - (q + 1)^{j-1} - q + 1 \]
\[ = \frac{1}{2} \sum_{i=1}^{l-1} q^{i+1-i}(q + 1)^{i-1} - (q + 1)^{i-1} + 1 \]
\[ = g(l, q). \]

**Proof of Proposition 2.4:** If \( m \in P(l, q) \) then \( m = \sum_{i=1}^{l} k_i(q^{l-i}(q + 1)^i) \), where \( k_i \) is a non-negative integer for \( i = 1, \ldots, l \). Now
\[ \nu_\infty(z_1^{k_1} z_2^{k_2} \cdots z_l^{k_l}) = - \sum_{i=1}^{l} k_i(q^{l-i}(q + 1)^i) = -m, \]

since \( \nu_\infty(z_i) = -q^{l-i}(q + 1)^{i-1} \) for \( i = 1, \ldots, l \). So \( z_1^{k_1} z_2^{k_2} \cdots z_l^{k_l} \) is an element of \( L(m \tilde{P}_\infty) \) and not of \( L((m-1) \tilde{P}_\infty) \), hence \( m \) is not a gap of \( P_\infty \), so \( G(l, q) \subset N \setminus P(l, q) \). But by Lemma 2.5 we have that \( \#G(l, q) = g(l, q) = \#(N \setminus P(l, q)) \). Therefore \( G(l, q) = N \setminus P(l, q) \). \( \square \)

**Proposition 2.5** The vector space \( L(m \tilde{P}_\infty) \) is generated by
\[ \{ z_1^{k_1} z_2^{k_2} \cdots z_l^{k_l} \mid \sum_{i=1}^{l} k_i(q^{l-i}(q + 1)^i) \leq m \}. \]

**Proof:** This follows from Proposition 2.4 and Remark 2.5.

**Corollary 2.3** If \( 2q^{l-1} > q^{l-i}(q + 1)^{i-1} \) then \( 1, z_1, \ldots, z_i \) is a basis of \( L(q^{l-i}(q + 1)^{i-1} \tilde{P}_\infty) \).

**Proof:** It follows from Proposition 2.5 and the assumption that \( 1, z_1, \ldots, z_i \) generate the vector space we consider. The valuations at \( P_\infty \) of these \( i + 1 \) elements are mutually distinct, so they are independent. \( \square \)

**Corollary 2.4** A \( q \)-ary first order Reed-Muller code of dimension 3 is AG.

**Proof:** A \( q \)-ary first order Reed-Muller code of dimension 3 can be represented by \( (\mathcal{V}(2, q), D, G) \), by Corollary 2.3, where \( P_1, \ldots, P_q \) are the \( q^2 \) rational points of the complement in \( P^2 \) of the line with equation \( x_0 = 0 \), and \( D = \sum_{i=1}^{q^2} P_i \) and \( G = (q + 1) \tilde{P}_\infty \). The divisor \( G \) has degree \( q + 1 \) which is smaller than \( q^2 \). \( \square \)

**Proposition 2.6** If \( C \) is a \( q \)-ary linear code which has a codeword of weight equal to the word length, then \( C \) is WAG.

**Proof:** Let \( C \) have dimension \( k \). We may assume that the all-one vector is a codeword, by Lemma 2.2. Choose a generator matrix of \( C \) such that the all one vector is the first row. Let \( Q_1, \ldots, Q_n \) be the points of \( P^{k-1} \) corresponding to the \( n \) columns of the generator matrix. Define
\[ s = \max\{ t \mid \text{there exist } i_1 < \ldots < i_t \text{ such that } Q_{i_1} = \ldots = Q_{i_t} \}. \]
Let \( l = [k + \log_q s] \). Then \( s \leq q^{l-k+1} \) and there are \( n \) distinct points \( P_1, \ldots, P_n \), rational over \( \mathbb{F}_q \), in \( \mathbb{P}^l \) such that \( \pi(P_i) = Q_i \), where \( \pi : \mathbb{P}^l \setminus H \to \mathbb{P}^{k-1} \) is defined by \( \pi(x_0 : \ldots : x_l) = (x_0 : \ldots : x_{k-1}) \) and \( H \) is the hyperplane with equation \( x_0 = 0 \), since the fibres of \( \pi \) are isomorphic with \( \mathbb{A}^{l-k+1} \). Choose a power \( q_0 \) of \( q \) such that \( 2q_0^{l-1} > q_0^{l-k}(q_0 + 1)^{k-1} \). Let \( X = \tilde{X}(l, q_0) \) and \( G = q_0^{l-k}(q_0 + 1)^{k-1} \hat{P}_\infty \) and \( D = P_1 + \ldots + P_n \). Then \( C = C_L(X, D, G) \) by Corollary 2.3 and \( C \) is WAG.

**Theorem 2.1** Every linear code is WAG.

*Proof:* Let \( C \) be a linear code. Then the dual of the extended code \( \overline{C} \) of \( C \), has word length \( n + 1 \) and the all one vector is an element of \( (\overline{C})^\perp \). Thus \( (\overline{C})^\perp \) is WAG by Proposition 2.6, so \( C \) is WAG by Corollary 2.1. But \( C \) can be obtained from \( \overline{C} \) by puncturing at the last coordinate. Therefore \( C \) is WAG, by Lemma 2.1.

### 2.3 Criteria for linear codes to be algebraic-geometric

We first mention a few well-known theorems (Theorems 2.2, 2.3, 2.4) and bounds on the genus of a curve.

**Definition 2.9** For any divisor \( D \) on a nonsingular, absolutely irreducible curve \( X \) over a field we define \( l(D) = \dim L(D) \) and \( \delta(D) = \dim \mathfrak{m}(D) \).

**Remark 2.6** If \( \deg(D) < 0 \) then \( l(D) = 0 \). If \( \deg(D) > 2g - 2 \) then \( \delta(D) = 0 \), where \( g \) is the genus of the curve. The Riemann-Roch Theorem states that

\[
l(D) = \deg(D) + 1 - g + \delta(D).
\]

So it gives a lower bound on \( l(D) \) in terms of the degree of \( D \). The following theorem gives an upper bound.

**Theorem 2.2 (Clifford)** (see [30]) If \( l(D) > 0 \) and \( \delta(D) > 0 \), then

\[
l(D) \leq \frac{\deg(D)}{2} + 1.
\]

**Remark 2.7** A hyperelliptic curve is an absolutely irreducible, nonsingular curve of genus at least two, which has a morphism of degree two to the projective line. The pull back under this morphism of a point of degree one on the projective line is called a hyperelliptic divisor. A hyperelliptic curve over \( \mathbb{F}_q \) has at most \( 2q + 2 \) rational points. We have equality in Clifford's theorem if and only if \( D \) is a principal or a canonical divisor or the curve is hyperelliptic and the divisor \( D \) is linearly equivalent with a multiple of a hyperelliptic divisor, see [30, p.343].

**Definition 2.10** Let \( N_q(g) \) be the maximal number of rational points on a nonsingular, absolutely irreducible curve, over \( \mathbb{F}_q \) of genus \( g \).

**Theorem 2.3 (Serre's bound)** (see [66])

\[
N_q(g) \leq q + 1 + g[2\sqrt{q}].
\]

Furthermore, \( N_q(g) \leq 0.83g + 5.35 \).
Remark 2.8 Table I gives some exactly determined values of \( N_4(g) \). See [43, p. 34], [66] and [67].

\[
\begin{array}{cccccccccccc}
g & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 15 & 19 & 21 & 39 & 50 \\
N_2(g) & 3 & 5 & 6 & 7 & 8 & 9 & 10 & 10 & 11 & 12 & 17 & 20 & 21 & 33 & 40 \\
N_3(g) & 4 & 7 & 8 & 10 \\
N_4(g) & 5 & 9 & 10 & 14 \\
\end{array}
\]

Theorem 2.4 (Castelnuovo’s bound). Let \( l \geq 1 \). If \( \mathcal{X} \) is an absolutely irreducible curve, over \( \mathbb{F}_q \), in \( \mathbb{P}^l \) and not contained in any hyperplane, then \( g(\mathcal{X}) \leq \pi(m, l) \). Here \( m \) is the degree of \( \mathcal{X} \) in \( \mathbb{P}^l \), and \( \pi(m, l) \) is defined by \( \pi(m, 1) = 0 \) and

\[
\pi(m, l) = \frac{t(l-1)}{2}(l-1) + t\varepsilon, \text{ if } l > 1,
\]

where \( t \) is an integer such that \( m - 1 = t(l-1) + \varepsilon \) and \( 0 \leq \varepsilon < l-1 \).

Proof: See [2], where the proof is given for curves over the complex numbers. In [30] the proof is given in arbitrary characteristic for \( l = 3 \). One can easily make a proof for arbitrary \( l \) and in any characteristic, by a combination of [2] and [30]. □

Remark 2.9 It is easily verified that \( \pi(m, l) \leq \pi(m', l) \), if \( m \leq m' \).

The following proposition is hidden in a remark of Katsman and Tsfasman, see [37].

Proposition 2.7 Let \( C \) be an \([n, k]\) code. If \( C \) is AG, then \( 2k \leq n + d^\perp - 1 \), where \( d^\perp = d^\perp(C) \) is the minimum distance of \( C^\perp \).

Proof: If \( C^\perp \) is MDS then \( d^\perp = k + 1 \), hence \( 2k \leq n + d^\perp - 1 \). So we may assume that \( C^\perp \) is not MDS, that is to say \( d^\perp \leq k \). If \( C \) is an AG code, then \( C = C_L(D, G) \) for some divisor \( G \) of degree \( m < n \) and \( k = l(G) \). Now \( C^\perp = C_{\Omega}(D, G) \), so there exist \( d^\perp \) distinct indexes \( i_1, \ldots, i_{d^\perp} \) and a differential \( \omega \in \Omega(G - D) \), such that \( res_{P_j}(\omega) \neq 0 \) for \( j = 1 \ldots d^\perp \), and \( res_{P_i}(\omega) = 0 \) for \( i \not\in \{i_1, \ldots, i_{d^\perp}\} \). Put \( D_1 = \sum_{j=1}^{d^\perp} P_j \). Then \( \omega \) is an element of \( \Omega(G - D_1) \) and not of \( \Omega(G) \). But \( \Omega(G - D_1) \) contains \( \Omega(G) \), so

\[
\delta(G - D_1) \geq \delta(G) + 1 > 0.
\]

Hence

\[
l(G - D_1) = m - d^\perp + 1 - g + \delta(G - D_1) \geq m + 1 - g + \delta(G) - d^\perp + 1 = k - d^\perp + 1 > 0,
\]

using the Riemann-Roch Theorem twice. We have

\[
k - d^\perp + 1 \leq l(G - D_1) \leq 1 + \frac{m - d^\perp}{2},
\]

by Clifford’s Theorem. Therefore \( 2k \leq m + d^\perp \leq n + d^\perp - 1 \), since \( m \leq n - 1 \). □
Remark 2.10 The q-ary first order Reed-Muller code \( C \) of dimension 3 has length \( q^2 \) and minimum distance \( q(q-1) \), see [10]. By Corollary 2.4 this code is AG. If \( q \geq 7 \), then \( C^\perp \) is not AG, by Proposition 2.7, since \( 2(q^2 - 3) > q^2 + q(q-1) - 1 \) if \( q \geq 7 \). Thus we have examples of codes \( C \) such that \( C \) is AG and \( C^\perp \) is not AG (see Remark 2.2).

Definition 2.11 Let \( g_q(n) \) be the minimal genus of a nonsingular, absolutely irreducible curve \( \mathcal{X} \) over \( \mathbb{F}_q \), with at least \( n \) rational points.

Remark 2.11 Serre's bound implies \( n \leq q + 1 + g_q(n)[2\sqrt{q}] \), for all \( n \).

Proposition 2.8 Suppose \( (\mathcal{X}, D, G) \) is an AG representation of a q-ary \([n, k]\) code and let \( m = \deg(G) (< n) \).

a) If \( m \leq 2g - 2 \), then \( k \leq [(n+1)/2] \). b) If \( m > 2g - 2 \), then \( g_q(n) \leq g \leq n - k \).

Proof: a) If \( k = 0 \), then there is nothing to prove. So assume \( k > 0 \), hence \( l(G) = k > 0 \).

If \( g \leq n - k \), then
\[
k = l(G) = m + 1 - g + \delta(G) \leq g - 1 + \delta(G) \leq n - k - 1 + \delta(G),\]
hence \( 2k \leq n - 1 + \delta(G) \). It follows that \( \delta(G) > 0 \) or \( k \leq (n - 1)/2 \).

If \( g > n - k \), then
\[
k = l(G) = m + 1 - g + \delta(G) < m + 1 - n + k + \delta(G) \leq k + \delta(G),\]
hence \( \delta(G) > 0 \).

If \( \delta(G) > 0 \), then \( k = l(G) \leq m/2 + 1 \leq (n + 1)/2 \), by Clifford's Theorem. Thus in every case \( k \leq [(n + 1)/2] \).

b) If \( m > 2g - 2 \), then \( \delta(G) = 0 \). Hence \( k = m + 1 - g \leq n - g \). □

Corollary 2.5 There exists a q-ary \([n, k]\) SAG code if and only if
\[
g_q(n) \leq \min\{k, n-k\} \]

Proof: If a q-ary \([n, k]\) code has a SAG representation, then \( g_q(n) \leq n - k \), by Proposition 2.8.b. The dual of this code is a SAG \([n, n-k]\) code, by Corollary 2.1. Hence, again by Proposition 2.8.b, \( g_q(n) \leq k \). Conversely, by definition, there exists a nonsingular, absolutely irreducible curve \( \mathcal{X} \) over \( \mathbb{F}_q \) of genus \( g = g_q(n) \), having (at least) \( n \) distinct rational points, \( P_1, \ldots, P_n \) say. Put \( D = P_1 + \ldots + P_n \). There exists a divisor \( G \) of degree \( k + g - 1 \) and with disjoint support with \( D \), by the theorem of independence of valuations [6, p.11]. Now \( 2g - 2 < \deg(G) = k + g - 1 < n \), since \( g \leq k \) and \( g \leq n - k \). Thus \( (\mathcal{X}, D, G) \) represents a SAG \([n, k]\) code. □

Corollary 2.6 If there exists a q-ary \([n, k]\) AG code, then
\[
k \leq \left[ \frac{n+1}{2} \right] \text{ if } g_q(n) > n - k \]
and
\[
k \leq \left[ \frac{(2\sqrt{q}) - 1)n + q + 1}{2\sqrt{q}} \right] \text{ if } g_q(n) \leq n - k.\]
Proof: Suppose \((X, D, G)\) is an AG representation of a \(q\)-ary \([n, k]\) code. Let \(m = \deg(G)\). If \(g_q(n) > n - k\), then \(m \leq 2g - 2\), by Proposition 2.8.b. Thus \(k \leq [(n + 1)/2]\), by Proposition 2.8.a. If \(g_q(n) \leq n - k\) then
\[
n \leq q + 1 + g_q(n)[2\sqrt{q}] \leq q + 1 + (n - k)[2\sqrt{q}],
\]
by Serre's bound, so
\[
k \leq \left[\frac{([2\sqrt{q}] - 1)n + q + 1}{2\sqrt{q}}\right].
\]

In the following, we shall investigate which Hamming codes \(H(r, q)\) are AG. The code \(H(r, q)\) is only determined up to isometries (see Definition 2.3), but this question makes sense anyway, by Lemma 2.2.

\textbf{Corollary 2.7} If \(r \geq 3\) and the Hamming code \(H(r, q)\) is AG then \((r, q) = (3, 2)\).

\textbf{Proof:} Let \(r \geq 3\), \(n = (q^r - 1)/(q - 1)\) and \(k = n - r\). Then \(H(r, q)\) is an \([n, k]\) code, see Definition 2.3. The minimum distance of its dual is \(q^{r-1}\). If \(H(r, q)\) is AG then Proposition 2.7 implies that
\[
2(\frac{q^r - 1}{q - 1} - r) \leq \frac{q^r - 1}{q - 1} + q^{r-1} - 1,
\]
so
\[
\frac{q^{r-1} - 1}{q - 1} < 2r.
\]
This is only possible in case the pair \((r, q)\) is equal to \((3, 2)\), \((4, 2)\), \((3, 3)\) or \((3, 4)\). To exclude the last three possibilities, observe that \(g_2(15) > 4\), \(g_3(13) > 3\) and \(g_4(21) > 3\), by Table 1, hence \(g_q(n) > r = n - k\) in these three cases, and apply Corollary 2.6. Since in all three cases \(k > [(n + 1)/2]\), we get a contradiction. \(\Box\)

\textbf{Remark 2.12} In [55, Section V], it was proved that \(H(1, q)\) and \(H(2, q)\) are SAG, for every \(q\), and that \(H(3, 2)\) is SAG.

\textbf{Proposition 2.9} Let \(k \geq 2\). Let \((X, D, G)\) be a minimal representation of a projective \(q\)-ary \([n, k]\) code. Let \(l = l(G)\). Then
\[
g_q(n) \leq g(X) \leq \pi(\deg(G), l - 1).
\]
In particular, if \((X, D, G)\) is AG, moreover, then
\[
g_q(n) \leq g(X) \leq \pi(\deg(G), k - 1).
\]

\textbf{Proof:} By assumption, the divisor \(G\) has no base points and the morphism \(\varphi_G : X \to \mathbb{P}^{l-1}\) has degree one. Hence \(\deg(X_0) = \deg(G)\), where \(X_0\) is the reduced image of \(X\) under \(\varphi_G\) (see Remark 2.4). Since \(X\) has at least \(n\) rational points, we have \(g_q(n) \leq g(X)\). Since \(\deg(\varphi_G) = 1\), we have \(g(X) = g(X_0)\) by Proposition 2.1.v. The result now follows from Castelnuovo's bound, applied to the curve \(X_0\), which is absolutely irreducible and does not lie in any hyperplane. The second part of the proposition follows from the fact that \(\deg(G) < n\) implies \(l = k\). \(\Box\)

\textbf{Corollary 2.8} Let \(k \geq 2\). If there exists a \(q\)-ary projective AG \([n, k]\) code, then
\[
g_q(n) \leq \pi(n - 1, k - 1).
\]
Chapter 2: Representing Linear Codes by Curves

29

Proof: If a q-ary projective AG \([n, k]\) code exists, then there exists a minimal AG representation \((X_0, \tilde{D}, \tilde{G})\) of this code, by Proposition 2.1. The result now follows from Proposition 2.9, applied to this minimal representation, and Remark 2.9, using \(\deg(\tilde{G}) \leq n - 1\). □

**Proposition 2.10** If there exists a binary projective AG \([n, k]\) code, then

a) If \(n \geq 14\) or \(n = 12\) then \(k < \lfloor n/2 \rfloor\), b) If \(n = 11\) or \(n = 13\) then \(k < n/2\).

**Proof:** If \(k < \lfloor n/2 \rfloor\), then there is nothing to prove. Suppose \(k \geq \lfloor n/2 \rfloor\) then

\[
\begin{align*}
 g_2(n) &\leq n - k \\
 &\leq 0.83(n - \lfloor \frac{n}{2} \rfloor) + 5.35,
\end{align*}
\]

by Serre’s bound, which implies \(n < 10\). Suppose \(n \geq 10\). Then \(g_2(n) > n - k\). So by Corollary 2.6, we have

\[
\left\lfloor \frac{n}{2} \right\rfloor \leq k \leq \left\lfloor \frac{n+1}{2} \right\rfloor.
\]

There are the following possibilities, a priori:

i) \(k \geq 5\) and \(n = 2k\), ii) \(k \geq 5\) and \(n = 2k + 1\), iii) \(k \geq 6\) and \(n = 2k - 1\).

In the first case \(t(n - 1, k - 1) = k + 2\). Hence \(g_2(n) \leq k + 2\), by Corollary 2.8. So \(2k \leq 0.83(k + 2) + 5.35\), by Serre’s bound. Thus \(k \leq 5\), and \(n \leq 10\), and there is nothing to prove. Similarly we get \(k \leq 6, n \leq 13\) in the second case, but now \(k < n/2\). Finally, we get \(k \leq 5, n \leq 9\) in the third case, which therefore cannot occur. Combining these inequalities we get the desired result. □

**Corollary 2.9** The binary Golay code and its extension are not AG.

**Proof:** As we know, the minimal distances of the dual codes of the binary Golay code and its extension exceed 3, see [50]. The binary Golay code is a \([23,12]\) code and its extension is a \([24,12]\) code, so they are not AG, by Proposition 2.10. □

**Remark 2.13** Our results do not yield a similar result concerning the ternary Golay code and its extension. The problem whether these codes are AG is still unsolved.

**Corollary 2.10** For every \(t \geq 2\), \(r \geq t\), and \(\varepsilon \in \{0,1\}\), the \(r\)-th order binary Reed-Muller code \(RM(r, 2t + \varepsilon)\) of length \(2^{2t+\varepsilon}\) is not AG.

**Proof:** Let \(r > 1\) and \(m = 2t + \varepsilon\), where \(t \geq 2\) and \(\varepsilon \in \{0,1\}\). The code \(RM(m - r - 1, m)\) is the dual code of \(RM(r, m)\). The length of the codewords of \(RM(r, m)\) is \(n = 2^m\), the dimension of \(RM(r, m)\) is \(1 + \binom{m}{1} + \cdots + \binom{m}{r}\) and the minimum distance of \(RM(r, m)\) is \(2^m - r\), see [10] and [50]. So \(d_L(RM(r, m)) = 2^{r+1} > 3\). If \(RM(r, m)\) is AG then, since \(n \geq 16\),

\[
\dim RM(r, m) \leq \left\lfloor \frac{n}{2} \right\rfloor - 1 = 2^{m-1} - 1,
\]

by Proposition 2.10. However, if \(m = 2t\) or \(m = 2t + 1\), and \(r \geq t\), then

\[
\dim RM(r, m) = 1 + \binom{m}{1} + \cdots + \binom{m}{r} \geq 2^{m-1} > 2^{m-1} - 1,
\]

which gives a contradiction. □
Remark 2.14 Let $p$ be a prime such that 2 is a quadratic residue modulo $p$. Let $Q$ denote the set of quadratic residues modulo $p$ and $N$ the set of nonresidues. Define

$$q(x) := \prod_{\alpha \in Q} (x - \alpha^r) \quad \text{and} \quad n(x) := \prod_{\alpha \in N} (x - \alpha^r),$$

where $\alpha$ is a primitive $p^{th}$ root of unity in some field containing $F_2$. Then the binary quadratic-residue codes $Q, Q', N, N'$ are cyclic codes with generator polynomials

$$q(x), \quad (x-1)q(x), \quad n(x), \quad (x-1)n(x)$$

respectively. Furthermore, the length of all these codes is $p$, the dimension of both $Q$ and $N$ is $(p + 1)/2$ and the dimension of both $Q'$ and $N'$ is $(p - 1)/2$, and the minimum distances of all these codes are not less than $\sqrt{p}$, see [50]. Therefore, if $p > 13$, the codes $Q, Q', N, N'$ are not AG codes, and if $p = 11, 13$ the codes $Q$ and $N$ are not AG codes, by Proposition 2.10.

Lemma 2.6 Suppose $(X, D, G)$ is an AG representation of an $[n, k]$ code. Then

$$\deg(G) \leq k + g - 1. \quad \text{If} \quad k \neq 0 \quad \text{and} \quad \deg(G) < k + g - 1, \quad \text{then} \quad \deg(G) \geq 2k - 2.$$

Proof: By the Riemann-Roch Theorem, $k = l(G) \geq \deg(G) - g + 1$, so $\deg(G) \leq k + g - 1$. If $\deg(G) \neq k + g - 1$, then by Clifford's Theorem $k \leq \deg(G)/2 + 1$, since $l(G) = k - \deg(G) + g - 1 > 0$. Thus $\deg(G) \geq 2k - 2$. □

Corollary 2.11 If $(X, D, G)$ is an AG representation of an $[n, k]$ code, and $g \leq n - k$ and $k > [n/2]$, then $\deg(G) = k + g - 1$.

Proof: If $\deg(G) \neq k + g - 1$ then $2k - 2 \leq \deg(G) < k + g - 1 \leq n - 1$, by Lemma 2.6, so $k \leq [n/2]$. This contradicts the assumption on $k$. □

Proposition 2.11 (See Table II). Let $C$ be a binary $[n, k]$ code with $4 \leq n \leq 10$. Let $k_0$ and $k'$ be given by Table II.

a) If $k > k_0$, then $C$ is not AG.

b) Suppose that $C$ is AG and projective, and that $k = k'$. Let $(X, D, G)$ be a minimal AG representation of $C$. Let $g$ be the genus of $X$ and let $m = \deg(G)$. Then $(g, m) = (g', m')$ for one of the pairs $(g', m')$ given in the last column.

Table II.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$k_0$</th>
<th>$k'$</th>
<th>$(g', m')$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>5</td>
<td>5</td>
<td>(6, 9) (7, 9)</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>5</td>
<td>(5, 8)</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>4</td>
<td>(4, 6) (4, 7) (5, 7) (6, 7)</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>4</td>
<td>(3, 6) (4, 6)</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>4</td>
<td>(2, 5)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>(2, 4) (3, 4) (3, 5) (4, 5) (5, 5) (6, 5)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
<td>(1, 4)</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>(1, 3) (2, 4) (3, 4)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>3</td>
<td>(1, 3)</td>
</tr>
</tbody>
</table>

Proof: a) For every $n$, the proof goes as follows. If $k > k_0$, then $k > [(n + 1)/2]$, while $n - k < n - k_0 \leq g_2(n)$, by Table I. By Corollary 2.6, $C$ cannot be AG.
b) We shall only give the proof for the case \( n = 6, k = 3 \). The proofs in the other cases are analogous, and sometimes simpler. So let \( n = 6 \) and \( k = 3 \). By Table I, \( g_2(6) = 2 \), hence \( g \geq 2 \). We have \( m < n = 6 \). If \( m = 5 \), then \( 2 \leq g \leq \pi(5,2) = 6 \), by Proposition 2.9. The case \( (g,m) = (2,5) \) is excluded by Lemma 2.6. If \( m = 4 \), then \( 2 \leq g \leq \pi(4,2) = 3 \), by Proposition 2.9. Since \( \pi(3,2) = 1 < 2 \leq g \), it is not possible that \( m \leq 3 \), by Proposition 2.9 and Remark 2.8.

**Remark 2.15** In Proposition 2.11.b we do not claim that for every pair \( (g',m') \) given in the table a minimal AG representation with \( (g,m) = (g',m') \) actually exists. As a matter of fact, in the next section we shall prove that for \( n = 7, k' = 4 \), the case \( (g',m') = (4,6) \) is impossible!

**Proposition 2.12** There exists a binary SAG code of length \( n \) if and only if \( n \leq 8 \).

**Proof:** By Proposition 2.10, SAG codes of length \( n \geq 11 \) do not exist, since a SAG code is AG and its dual is too, but they cannot both have dimension \( < n/2 \). The cases with \( n \leq 10 \) are dealt with by Corollary 2.5 and Table I: only for \( n \leq 8 \) there exists a \( k \) such that \( g_2(n) \leq \min\{k,n-k\} \).

**Remark 2.16** (See Remark 2.3) There exists a binary SAG [5,4] code, by Corollary 2.5, since \( g_2(5) = 1 \), by Table I. This code is a fortiori AG. Puncturing this code gives a binary [4,4] code, which is not AG (and not SAG), by Proposition 2.11.
Chapter 3

Constructing Asymptotically Good Binary Codes from Curves

In this chapter, an explicit construction of a sequence of binary codes which asymptotically meet the Zyablov bound for rate lower than 0.30 is given by using Justesen’s construction of concatenation (see Chapter 1). The Zyablov bound can be described as follows.

There exists a sequence of concatenated binary codes with inner code length \( n \to \infty \) and outer code length \( N \to \infty \), in which the outer code is maximum distance separable (MDS), and which satisfy

\[
\liminf \frac{\text{distance}}{\text{length}} \geq \max_{0 \leq r \leq 1} \{(1 - \frac{R}{r})H_2^{-1}(1 - r)\},
\]

if the overall rate is \( R \), where \( H_2^{-1} \) is defined in Chapter 1.

In Section 3.1 we define the generalized Hermitian curves. By using these curves, we construct the outer codes of our concatenated codes and give the properties of the outer codes. In Section 3.2 we define the ensemble of the inner codes. Finally, in Section 3.3 the sequences of concatenated binary codes, which meet the Zyablov bound for lower rate, is constructed.

3.1 The construction of the outer codes

Recall the definition of a Justesen code. Its outer code is taken to be a \([2^m - 1, k, 2^m - 1 - k + 1]\) Reed-Solomon code over \( GF(2^m) \) which is MDS. So it has the maximal minimum distance among all the \([2^m - 1, k]\) codes over \( GF(2^m) \). Its inner codes exhaust all \( 2^m - 1 \) distinct binary codes in Wozencraft’s ensemble of randomly shifted codes described by Massey [46, p.21]. The reason that Justesen codes cannot meet the Zyablov bound for rate lower than 0.30 is that the construction requires a good ensemble of inner codes with at most \( 2^m - 1 \) (the length of a Reed-Solomon code) codes and such an ensemble for rates less than \( 1/2 \) cannot be constructively specified. Therefore if we can construct outer codes over the same field but with length \( N \) much larger than \( 2^m - 1 \), such that they behave almost like MDS codes when the code length becomes sufficiently large, then the specification of an ensemble with \( N \) codes for rates lower than \( 1/2 \) becomes possible. Fortunately, the algebraic geometry
method again provides a possibility to construct such an outer code. Over every field \( GF(2^{2n}) \), the outer code we will construct in this section is a \( [2^{2n(l+1)} - 1, K, D] \) code, where \( l \) is an integer greater than 1 and \( D \geq (2^{2n(l+1)} - 1) - K + 1 - g \). Therefore if \( g \) is relatively small the code behaves almost like a MDS code. In fact \( g \) is the genus of the curve used and is approximately \( 1/2(l - 1)2^{2n} \). Thus \( g/2^{2n(l+1)} \) tends to 0 for \( n \rightarrow \infty \). In the rest of this section we will give the details of this construction.

**Definition 3.1** Let \( q = 2^n \). Let \( \mathbb{F}_{q^2} \) be a finite field with \( q^2 \) elements. Let \( PG(l, q^2) \) be an \( l \) dimensional projective space over \( \mathbb{F}_{q^2} \). Let \( \mathcal{H}(l, q) \) be a closed subscheme over \( \mathbb{F}_2 \) in \( PG(l, q^2) \) defined by the homogeneous ideal

\[
I(l, q) = (X_{i+1} + X_{i+1}X_0^q + X_iX_0, \quad i = 1, \ldots, l - 1)
\]
in \( \mathbb{F}_2[X_0, \ldots, X_l] \).

**Proposition 3.1** The scheme \( \mathcal{H}(l, q) \) is a projective, absolutely irreducible, reduced curve over \( \mathbb{F}_2 \). It has exactly one point \( P_{\infty} \) at the hyperplane \( H \) with equation \( X_0 = 0 \). The curve is nonsingular outside \( P_{\infty} \) and goes through \( q^{l+1} \) rational points of \( PG(l, q^2) \) outside the hyperplane \( H \). The genus of this curve is

\[
g(l, q) = \frac{1}{2} \left( \sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1 \right).
\]

**Proof.** The proof is the same as the proof of Proposition 2.2 and 2.3 in Chapter 2. \( \Box \)

The function field of \( \mathcal{H}(l, q) \) is \( K(l, q^2) := \mathbb{F}_{q^2}(x_1, \ldots, x_l) \) with defining equations

\[
x_i^{q+1} = x_{i+1} + x_i^q, \quad i = 1, \ldots, l - 1.
\]

It is the function field of a Hermitian curve over \( \mathbb{F}_{q^2} \) when \( l = 2 \), see [73] and [78]. Therefore we call the curve \( \mathcal{H}(l, q) \) a generalized Hermitian curve. This generalized Hermitian curve is an example of so called Artin-Schreier extensions, see [41]. Some of its properties are described in that paper. This curve was mentioned in [35, Example 7] too, but there it was not proved that this curve is absolutely irreducible.

**Proposition 3.2** If \( a \in \mathbb{F}_{q^2} \), then the equations

\[
x_1 = a; \quad x_{i+1}^q + x_{i+1} = x_i^{q+1} \quad \text{for } i = 1, \ldots, l - 1
\]

have their all solutions in \( \mathbb{F}_{q^2} \). Furthermore, they have exactly \( q^{l-1} \) solutions.

**Proof.** We follow the proof of [20, §1 Lemma].

Suppose \( b \) is a solution of \( Y^q + Y = a^{q+1} \), that is \( b^q + b = a^{q+1} \). Raising to the \( q \)-th power and using the fact that \( a^{q(q+1)} = a^{q+1} \), we have \( b^{q^2} + b^q = a^{q+1} = b^{q+1} + b \). From this we conclude that \( b \in \mathbb{F}_{q^2} \). Therefore every solution of the equations is in \( \mathbb{F}_{q^2} \). This proves the first claim of the proposition. The second claim of the proposition is a consequence of the first conclusion and the fact that a polynomial of degree \( q \) has at most \( q \) zeroes. \( \Box \)

By the above proposition, we know that the \( q^{l+1} + 1 \) rational points of the curve \( \mathcal{H}(l, q) \) are the following: the common pole \( P_{\infty} \) of \( x_i \) for \( i = 1, \ldots, l \), and for any \( a_1 \in \mathbb{F}_{q^2} \) and any \( a_i \) such that \( a_i^q + a_i = a_{i-1}^{q+1} \) for \( i = 2, \ldots, l \), the common zero \( P = P_{a_1, \ldots, a_l} \) of \( x_i - a_i \) for \( i = 1, \ldots, l \).
Definition 3.2 (The outer code) Let $D$ be a divisor of $K(l, q^2)$ defined by $D = \sum_{i=1}^{N} P_i$, where $0 < N \leq q^{l+1} - 1$ and $P_1, \ldots, P_N$ are different and chosen from rational points of $H(l, q)$ such that $P_i \notin \{P_\infty, P_0, \ldots, 0\}$. Let $m$ be any nonnegative integer. Then the outer code is defined to be the algebraic-geometric code $C_L(D,mP_\infty)$ (see Definition 1.2).

Theorem 3.1 If $m < N$, then $C_L(D,mP_\infty)$ is a linear $[N,K,D]$ code over $F_{q^2}$ with

$$K \geq m + 1 - g(l, q) \quad \text{and} \quad D \geq N - m.$$ 

Therefore

$$D \geq N - K + 1 - g(l, q).$$

Furthermore, $K = m + 1 - g(l, q)$ if $m > 2g(l, q) - 2$. Moreover if we take $N = q^{l+1} - 1$ then $g(l, q)/N \rightarrow 0$, $(q \rightarrow \infty)$.

Proof. The theorem follows from Theorem 1.3.a. □

3.2 The ensemble of the inner codes

Let $r$ be a positive rational number less than 1/2. Then we always can write $r = nt/(nt + n_2)$, where $n_1$ and $n_2$ are positive integers, $n_2 \geq n_1$ and $(n_1, n_2) = 1$. The aim of this section is to construct an ensemble of binary codes with rate $r$, such that the number of the distinct codes in this ensemble is $2^{n_2} - 1$ and the intersection of every two distinct codes is $\{(0, \ldots, 0)\}$. In Section 3.4, we use this ensemble as our inner codes to construct a concatenated code.

Let $n$ be a positive integer. Then every element in the finite field $F_{2^n}$ can be written as an element in $F_2[x]/(f)$, where $(f)$ is the ideal in $F_2[x]$ generated by $f$, an irreducible polynomial of degree $n$ in $F_2[x]$. Let $n_1, n_2$ be positive integers, such that $n_2 \geq n_1$. We have

$$F_{2^{n_1}} = \{\alpha(x) + (f) | \alpha(x) \in F_2[x] \text{ and } \deg(\alpha(x)) < n_1\}$$

and

$$F_{2^{n_2}} = \{\beta(x) + (f) | \beta(x) \in F_2[x] \text{ and } \deg(\beta(x)) < n_2\},$$

where $f_i, i = 1, 2$ are irreducible polynomials of degree $n_i$ in $F_2[x]$.

Definition 3.3 For every $\beta \in F_{2^{n_2}}$, define a map $\phi_\beta$ from $F_{2^{n_1}}$ to $F_{2^{n_2}}$ by

$$\phi_\beta(\alpha) = \gamma(x) + (f_2) \quad \text{with} \quad \deg(\gamma(x)) < n_2,$$

where $\gamma(x) \equiv \beta(x)\alpha(x) \mod f_2$ for $\beta(x) + (f_2) = \beta$ with $\deg(\beta(x)) < n_2$ and $\alpha = \alpha(x) + (f_1) \in F_{2^{n_1}}$ with $\deg(\alpha(x)) < n_1$.

It is easy to see that $\phi_\beta$ is well defined and $\phi_\beta(\alpha_1 + \alpha_2) = \phi_\beta(\alpha_1) + \phi_\beta(\alpha_2)$ for $\alpha_1, \alpha_2 \in F_{2^{n_1}}$.

Furthermore, we define a map $\nu_n$ from $F_{2^n} = F_2[x]/(f)$ to $F_2^n$ by

$$\nu_n(\alpha) := (a_0, \ldots, a_{n-1}),$$

for every $\alpha = \sum_{i=0}^{n-1} a_i x^i + (f) \in F_{2^n}$. It is easy to see that $\nu_n$ is injective and linear over $F_2$. Now we can define our ensemble of binary codes.
Definition 3.4 (The inner code) For every $\beta \in \mathbb{F}_{2^{n_2}}^*$, the binary code $C_\beta$ of length $n_3 = n_1 + n_2$ is defined by

$$C_\beta := \{ (\nu_{n_1}(\alpha), \nu_{n_2}(\phi_\beta(\alpha))) | \alpha \in \mathbb{F}_{2^{n_1}} \}.$$ 

For the convenience of explanation in Section 3.4 we can describe this code as a map $\varphi_\beta$ from $\mathbb{F}_{2^{n_1}}$ to $\mathbb{F}_{2^{n_3}}$ defined by

$$\varphi_\beta(\alpha) := (\nu_{n_1}(\alpha), \nu_{n_2}(\phi_\beta(\alpha))),$$

for every $\alpha \in \mathbb{F}_{2^{n_1}}$.

Proposition 3.3 For every $\beta \in \mathbb{F}_{2^{n_2}}^*$, $C_\beta$ is a binary $[n_1 + n_2, n_3]$ linear code. For every two distinct $\beta, \beta' \in \mathbb{F}_{2^{n_2}}^*$, $C_\beta \cap C_{\beta'} = \{(0, \ldots, 0)\}$. Therefore there are $2^{n_3} - 1$ distinct codes in the ensemble.

In other words, If $c_1, \ldots, c_T$ are nonzero elements in $\mathbb{F}_{2^{n_1}}$ and $\beta_1, \ldots, \beta_T$ are distinct elements in $\mathbb{F}_{2^{n_2}}^*$. Then $\varphi_{\beta_1}(c_1), \ldots, \varphi_{\beta_T}(c_T)$ are also different.

Proof. This follows immediately from Definition 3.3 and Definition 3.4.

3.3 The concatenated codes

In this section we construct the sequence of binary concatenated codes, and prove that these codes meet the Zyablov bound for rate lower than 0.30. Some of the notations in this section were introduced already in the previous sections.

Definition 3.5 Let $l$ be an integer such that $l \geq 2$ and $0 < t \leq 1$ such that $t = t_1/t_2$ for some positive integers $t_1$ and $t_2$. Let $n = t_2 k$ and $q = 2^n$, where $k$ is a positive integer. Let $N = q^l - 1$. Then from Section 3.1 one gets a linear code $C_L(D, m P_\infty)$ with the support of $D$ containing $N$ rational points. Furthermore, let $n_1 = 2n$, $n_2 = (l + t)n$ and $n_3 = n_1 + n_2 = (2 + l + t)n$. A binary concatenated code $C_c(l, t, k, m)$ of length $M := (2 + l + t)nN$ is defined by

$$\{(\varphi_{\beta_1}(c_1), \ldots, \varphi_{\beta_N}(c_N)) | (c_1, \ldots, c_N) \in C_L(D, m P_\infty) \},$$

where $\{\beta_1, \ldots, \beta_N\} = \mathbb{F}_{q^{l+t}}^*$ and $\varphi_{\beta_i}$ is the map from $\mathbb{F}_{2^{n_1}}$ to $\mathbb{F}_{2^{n_3}}$ defined by Definition 3.4. We call $C_L(D, m P_\infty)$ the outer code of the code $C_c(l, t, k, m)$.

Proposition 3.4 Let $l$ be an integer $\geq 2$. Let $\{t_{1k}\}$ and $\{t_{2k}\}$ be two sequences of integers such that $t_k := t_{1k}/t_{2k} \to t$ ($k \to \infty$) for some $0 < t \leq 1$. Let $r_k := 2/(2 + l + t_k)$ and $r := 2/(2 + l + t)$. Finally, let $R_k, d_k$ and $M_k$ be the rate, minimum distance and length, respectively, of the code $C_c(l, t, k, m_k)$. Suppose $\liminf R_k = R$ ($k \to \infty$), Then

$$\liminf_{k \to \infty} d_k/M_k \geq (1 - R/r)H_2^{-1}(1 - r).$$

Proof. Suppose the outer code $C_L(D_k, m_k P_\infty)$ is a $[N_k, K_k, D_k]$ code. Then $D_k \geq N_k - K_k + 1 - g(l, q_k)$ by Theorem 3.1, where $q_k = 2^n$ with $n_k = t_{2k} k$, and

$$R_k = \frac{2n_k K_k}{(2 + l + t_k)n_k N_k} = R_k \frac{K_k}{N_k}.$$ 

Hence we have

$$D_k \geq N_k(1 - R_k/r_k - g(l, q_k)/N_k) = (q_k^{l(t_k)} - 1)\{1 - R_k/r_k + o(1)\}, \quad (k \to \infty),$$

where $R_k/r_k \to R$ as $k \to \infty$.


Chapter 3: Constructing Asymptotically Good Binary Codes from Curves

since \( N_k = q_k^{(l + t_k)} - 1 \), 
\[ g(l, q_k) = \{ \Sigma_{i=1}^{l-1} q_k^{l+1-i} (q_k + 1)^{i-1} - (q_k + 1)^{l-1} + 1 \} / 2, \]
and \( t_k n_k \to \infty \).

Now let \( L_k = (2 + l + t_k)n_k, \delta_k = (l + t_k)/(2 + l + t_k) = 1 - r_k \), and \( M_k L_k = D_k \). Then

\[ 2^{-L_k} \delta_k M_k L_k \geq 2^{-(l + t_k)k} \{ 2^{(l + t_k)k} - 1 \} \{ 1 - R_k / r_k + o(1) \} = 1 - R_k / r_k + o(1). \]

Now by Proposition 3.3 and the following Lemma 3.1, we have

\[ d_k \geq (1 - R_k / r_k) \{ 2^{(l + t_k)k} \{ H_2^{-1}(1 - r_k) + o(1) \} \}, \quad (k \to \infty). \]

Therefore

\[ \liminf_{k \to \infty} d_k / M_k \geq (1 - R / r) H_2^{-1}(1 - r). \]

□

**Lemma 3.1** Let \( \gamma, \delta \in (0, 1) \). Let \( (M_L)_{L \in \mathbb{N}} \) be a sequence of natural numbers with the property \( M_L \cdot 2^{-L} = \gamma + o(1) \) \( (L \to \infty) \). Let \( W \) be the sum of the weights of \( M_L \) distinct words in \( F_2^L \). Then

\[ W \geq \gamma L 2^L \{ H_2^{-1}(\delta) + o(1) \}, \quad (L \to \infty). \]

**Proof.** See [34]. □

**Theorem 3.2** For overall rate \( R \) satisfying \( 0 < R < 0.30 \), the Zyablov bound can be achieved by a sequence of concatenated codes \( \{ C_c(l, t_k, k, m_k) \}_{k=1}^\infty \), where \( t_k = t_{1k} / t_{2k} \leq 1 \) and \( l, t_{1k}, t_{2k} \) and \( m_k \in \mathbb{N}^* \).

**Proof.** Let \( r_0 \in [0, 1] \) such that

\[ (1 - R / r_0) H_2^{-1}(1 - r_0) = \max_{0 \leq r \leq 1} \{ (1 - R / r) H_2^{-1}(1 - r) \}. \]

Then we know that \( r_0 < 1/2 \) (see [50, p.314]) and \( r_0 > R \). It is easy to see that there exists an integer \( l \geq 2 \) and a real number \( t \in (0, 1) \) such that \( 2 / (2 + l + t) = r_0 \). Let \( \{ t_k \} \) be a sequence of rational numbers such that \( t_k \to t \) \( (k \to \infty) \). Denote \( r_k := 2 / (2 + l + t_k) \), then \( \lim_{k \to \infty} r_k = r_0 \). Then we get a sequence of concatenated codes \( C_c(l, t_k, k, m) \) for every \( m > 0 \). Now choose \( m_k \) such that the rate \( R_k \) of \( C_c(l, t_k, k, m_k) \) satisfies:

\[ \liminf_{k \to \infty} R_k = \liminf_{k \to \infty} \frac{2n_k K_k}{(2 + l + t_k)n_k N_k} = R, \]

where \( n_k = t_{2k} k \) \( (t_{1k} / t_{2k} := t_k) \) and \( K_k = m_k + 1 - g(l, q_k) \) and \( N_k = 2^{(l + t_k)k} - 1 \) denote the dimension and minimum distance, respectively, of the outer code \( C_L(D_k, m_k P_\infty) \) (This always can be done by Theorem 3.1).

Now by Proposition 3.4, for the sequence of concatenated codes \( C_c(l, t_k, k, m_k) \) with the minimum distance \( d_k \) and the length \( M_k \), we have

\[ \liminf_{k \to \infty} d_k / M_k \geq (1 - R / r_0) H_2^{-1}(1 - r_0). \]

This proves the theorem. □
Remark 3.1 By using the dual code of $C_L(D, mP_{\infty})$ as the outer code, we also can get the same result as the above theorem. For the details of the dual code $C_L(D, mP_{\infty})^\perp$ we refer to [73, 78] and Chapter 6.

Remark 3.2 (Complexity) Let us consider the number of binary computations involved in the construction of a generator matrix of the code $C_c(l, t, k, m)$, where the length of the code is $M = (2+l+t)n(2^{n(l+t)} - 1)$. In order to find all the rational points of $H(l, q)$ ($q = 2^n$), we need to solve the equations given by Proposition 3.1. For this we need at most $O((q^3 + q^{2(l-1)})m^2)(\sim O(M^2))$ binary calculations. By Proposition 2.5 we know that $L(mP_{\infty})$ can be generated by

$$\{x_1^{k_1} \cdots x_i^{k_i} | (k_1, \ldots, k_i) \in N^l, \sum_{i=1}^{l} k_i q^{l-i}(q + 1)^{i-1} \leq m\},$$

where $N$ is the set of all nonnegative integers. Thus to construct the generator matrix of the outer code we need at most $Km/q^{l-1}$ calculations over $F_{q^2}$, where $K$ is the dimension of the outer code. Hence to construct the generator matrix of the concatenated code we need at most $O([((l+t)n)^2KM/q^{l-1}])$ binary calculations, which is $O(M^2)$ since $K = m + 1 - g(l, q)$ and $m < q^{l+t} - 1$. Therefore, the total complexity of the construction of these binary concatenated codes is $O(M^2)$. 
Chapter 4

Decoding Geometric Goppa Codes

In this chapter, we present a decoding algorithm for geometric Goppa codes $C_{\Omega}(D,G)$ by using an extra place—a place which is not in the support of $D$. In fact, the decoding algorithm is reduced to solving a key congruence on an affine ring.

In Section 4.1 the ring $K_{\Omega}(P)$ is defined. We also give a division theorem for this ring. In Section 4.2, we show how to derive a decoding algorithm of a code from a decoding algorithm for a code isometric to the first one. Furthermore, we prove that for every place $P$ not in the support of $D$, every geometric Goppa code $C_{\Omega}(D,G)$ is isometric to the code $C_{\Omega}(D,E-\mu P)$, for some effective divisor $E$ and positive integer $\mu$. It is shown in Section 4.3 that there exist $n$ independent differentials $\epsilon_1, \ldots, \epsilon_n \in \Omega(-D-\mu P)$ such that for every differential $\omega \in \Omega(E-\mu P-D)$ one has $\omega = \sum \text{res}_{P_i}(\omega)\epsilon_i$. If we let $\epsilon(\mathbf{x}) = \sum x_i \epsilon_i$, then

$$\epsilon(\mathbf{x}) \in \Omega(E-\mu P-D)$$

This generalizes the description of classical Goppa codes as follows. Let $L$ be a subset of $\mathbb{F}_q$ and $h$ a Goppa polynomial. Let $L = \{\alpha_1, \ldots, \alpha_n\}$. Suppose $h$ does not vanish at $\alpha_i$, for all $i$. The classical Goppa code $\Gamma(L,h)$ is defined by

$$\Gamma(L,h) = \{\mathbf{x} | \sum \frac{x_i}{X-\alpha_i} \equiv 0 \pmod{h}\}.$$ 

If we let $\epsilon_i = 1/(X-\alpha_i)dX$, and take for $P$ the point at infinity on the projective line and for $E$ the divisor of zeros of $h$, then $\Gamma(L,h) = C_{\Omega}(D,E-P)$ and

$$\mathbf{x} \in \Gamma(L,h)$$

if and only if

$$\sum \frac{x_i}{X-\alpha_i}dX \in \Omega(E-P-D).$$

In Section 4.4, the definition of the syndrome of a received word is given. In order to represent the syndrome as a rational function, we first prove the existence of a particular differential $\eta$. For a Goppa polynomial $h$, the syndrome $S(\mathbf{x})$ of a received word $\mathbf{x}$ is now defined as follows.

$$S(\mathbf{x})\eta = \sum x_i \frac{h(P_i) - h}{h(P_i)} \epsilon_i.$$ 

The syndrome is an element of the ring $K_{\Omega}(P)$, and if $E$ is the divisor of zeros of $h \in K_{\Omega}(P)$, then

$$\mathbf{x} \in C_{\Omega}(D,E-\mu P)$$

if and only if $S(\mathbf{x}) \equiv 0 \pmod{h}$. 

39
In Section 4.5 we show how to decode \((d^* - 1)/2 - s\) errors, where \(d^*\) is the designed minimum distance of the code (see Theorem 1.3) and \(s\) is the Clifford defect, by solving the key equation \(fS(x) = r + qh\), under a constraint in terms of the degrees of \(f\) and \(r\). In Section 4.6, we give a decoding algorithm for a class of codes which are isometric to \(C_\mathbb{F}(D, mP)\). Finally in Section 4.7 we give an example showing that in this way one cannot in general decode more than the above mentioned number of errors.

We will use the notations defined in Chapter 1 and add the following notations in this chapter. \(X\) is always a projective, non-singular, absolutely irreducible curve defined over a finite field \(\mathbb{F}\), \(P_1, \ldots, P_n\) are \(n\) distinct \(\mathbb{F}\)-rational points on \(X\), and \(D\) is the divisor \(P_1 + \cdots + P_n\). Let \(G = \sum mQ\) be a divisor on \(X\), denote \(G_0 := \sum_{m > 0} mQ\) and \(G_\infty := \sum_{m < 0} mQ\). If \(f\) is a rational function and the principal divisor (\(f\)) = \(\sum v_0(f)Q\), then (\(f\))_0 := \(\sum v_0(f) > 0 v_0(f)Q\) and (\(f\))_\infty := \(\sum v_0(f) < 0 v_0(f)Q\). Let \(O\) be a finite set of places on \(X\), then we denote (\(f\))_O := \(\sum_{Q \in O} v_0(f)Q\). Let \(G_1\) and \(G_2\) be divisors on \(X\). If there exists a rational function \(f\) such that \(G_1 = G_2 + (f)\), then we say that \(G_1\) and \(G_2\) are linearly equivalent and denote this by \(G_1 \sim G_2\).

4.1 The affine ring \(K_\infty(P)\)

Definition 4.1 Let \(P\) be a place of \(X\), define

\[K_\infty(P) = \{f \in \mathbb{F}(X) | \text{supp}((f)_\infty) \subseteq \{P\}\},\]

we call \(K_\infty(P)\) the affine ring with respect to \(P\).

Since our decoding algorithm will work on \(K_\infty(P)\), it is worth to know some details about this ring. In the following, we will give the construction of \(K_\infty(P)\) and a division theorem for \(K_\infty(P)\), in the case that \(P\) is a place of degree one, that is, a rational point.

Definition 4.2 Let \(P\) be a place of \(X\) of degree one, let \(n\) be a non-negative integer. If \(l(nP) = l((n-1)P)\), then \(n\) is called a (Weierstrass) gap of \(P\).

Proposition 4.1 \cite{19} Let \(X\) be a curve of genus \(g \geq 1\) and let \(P\) be a place of degree one of \(X\), then

a) \(1 = l(0) \leq l(P) \leq \cdots \leq l((2g-1)P) = g\). So there are exactly \(g\) gaps of \(P\).

b) Let \(m \in \mathbb{N}\). Then \(m\) is a non-gap of \(P\) if and only if there exists an \(f \in L(mP)\), such that \(v_0(f) = -m\).

c) If \(m_1\) and \(m_2\) are non-gaps of \(P\), then \(m_1 + m_2\) is also a non-gap of \(P\).

Lemma 4.1 If \(r\) is a gap of \(P\), then there exists an integer \(t\) with \(1 \leq t \leq [(2g + 1 - r)/2]\), such that \(2g + 1 - t\) and \(r + t\) are both non-gaps.

Proof. Let \(n_1, \ldots, n_g\) be all gaps of \(P\). For all \(s \in \{1, \ldots, [r/2]\}\) either \(s = r\) or \(r - s\) is a gap by Proposition 4.1.c, since \(r\) is a gap. Suppose \(1 \leq s \leq r/2\) then \(r/2 \leq r - s < r\), so if \(s_1, s_2 \in \{1, \ldots, [r/2]\}\) and \(s_1 \neq s_2\), then \(r - s_1 \neq s_2\). Thus

\[\#\{n_i < r|1 \leq i \leq g\} \geq \left\lfloor \frac{r}{2} \right\rfloor.\]
Chapter 4: Decoding Geometric Goppa Codes

If the assertion of this lemma is not true, then for all \( t \in \{1, \ldots, \lfloor (2g+1-r)/2 \rfloor \} \) either \( 2g+1-t \) or \( r+t \) is a gap. Suppose \( 1 \leq t \leq (2g+1-r)/2 \) then \( (2g+1+r)/2 \leq 2g+1-t \leq 2g \) and \( r+1 \leq r+t \leq (2g+1+r)/2 \). So if \( t_1, t_2 \in \{1, \ldots, \lfloor (2g+1-r)/2 \rfloor \} \) and \( t_1 \neq t_2 \), then \( 2g+1-t_1 \neq r+t_2 \). Thus

\[
\# \{ n_i > r | 1 \leq i \leq g \} \geq \left\lfloor \frac{2g+1-r}{2} \right\rfloor.
\]

Therefore, by the above and the assumption that \( r \) is also a gap, one gets

\[
g \geq \left\lceil \frac{r}{2} \right\rceil + \left\lfloor \frac{2g+1-r}{2} \right\rfloor + 1 = g + 1,
\]

a contradiction. □

**Proposition 4.2** Let \( 0 = m_0 < m_1 < \cdots < m_{g-1} < m_g = 2g < m_{g+1} = 2g + 1 \) be all the non-gaps of \( P \) between 0 and \( 2g + 1 \). If \( m \in \mathbb{N} \) is a non-gap of \( P \), then

\[
m = \sum_{i=0}^{g+1} k_im_i,
\]

where \( k_i \in \mathbb{N} \) for all \( i \).

**Proof.** If \( 0 \leq m \leq 2g + 1 \) then the result is trivial. Now we consider the case that \( m \geq 2g + 2 \). Let \( m = k(2g+1+r) \), where \( 0 \leq r \leq 2g \) and \( k \geq 1 \), then

i) if \( r \) is a non-gap, then there is an \( i \) such that \( r = m_i \). Thus \( m = m_i + km_{g+1} \).

ii) if \( r \) is a gap, then by Lemma 4.1 there exists a \( t \in \mathbb{N} \) with \( 1 \leq t \leq \lfloor (2g+1-r)/2 \rfloor \), such that \( 2g-t+1 \) and \( r+t \) are non-gaps of \( P \). So there exist \( i, j \) with \( 1 \leq i, j \leq g+1 \) such that \( r+t = m_i \) and \( 2g+1-t = m_j \). Thus \( 2g+1+r = r+t+2g+1-t = m_i+m_j \). Therefore \( m = (k-1)(2g+1) + (2g+1+r) = (k-1)m_{g+1} + m_i + m_j \).

□

**Proposition 4.3** Let \( 0 = m_0 < m_1 < \cdots < m_{g-1} < m_g = 2g < m_{g+1} = 2g + 1 \) be all the non-gaps of \( P \) between 0 and \( 2g + 1 \). Let \( f_i \in L(m_iP) \) with \( vP(f_i) = -m_i \). Then for every \( m \in \mathbb{N} \), the vector space \( L(mP) \) is generated by

\[
\left\{ \prod_{i=0}^{g+1} f_{i}^{k_i} \middle| \sum_{i=0}^{g+1} k_im_i \leq m, \text{ with } k_i \in \mathbb{N} \text{ for all } i \right\},
\]

**Proof.** If \( m \) is a gap of \( P \), then there exists an \( m_i \) such that \( L(mP) = L(m_iP) \) by the definition of a gap. So we may assume that \( m \) is a non-gap of \( P \).

We first rearrange all the non-gaps ascending order, that is \( 0 = m_0 < m_1 < m_2 < \cdots < m_{g-1} < m_g = 2g < m_{g+1} = 2g + 1 < \cdots < m_{g+l} = 2g + l < \cdots \). For every \( k \in \mathbb{N} \), let the vector space generated by

\[
\left\{ \prod_{i=0}^{g+1} f_{i}^{k_i} \middle| \sum_{i=0}^{g+1} k_im_i \leq m_k, \text{ with } k_i \in \mathbb{N} \text{ for all } i \right\},
\]

be denoted by \( L_k \), in particular \( L_k \subseteq L(m_kP) \).

Now we prove the proposition by induction on \( k \).

1) If \( k = 0 \), then \( m_0 = 0 \), so \( L(m_0P) = L(0) = F = L_0 \).
2) Suppose \( L(m_kP) = L_k \). Then \( L(m_{k+1}P) \supseteq L_{k+1} \supseteq L_k = L(m_kP) \), by the induction hypothesis. Now we consider the dimension of \( L_{k+1} \). Since \( m_{k+1} \) is a non-gap, there exist non-negative integers \( k_0, \ldots, k_{g+1} \) such that \( m_{k+1} = \sum_{i=0}^{g+1} k_im_i \), by Proposition 4.2. Put \( f = \prod_{i=0}^{g+1} f_i^{k_i} \), then \( \nu_p(f) = -m_{k+1} \). Thus \( f \in L_k \) but \( f \notin L(m_kP) \), therefore

\[
\dim(L_{k+1}) \geq \dim(L_k) + 1.
\]

But \( \dim(L_{k+1}) \leq \dim(L_k) + 1 \) by the definition of the sequence \( \{m_k\}_{k=0}^{\infty} \). So \( \dim(L_{k+1}) = \dim(L_k) + 1 \). Thus finally \( L(m_{k+1}P) = L_{k+1} \).

**Theorem 4.1** Let \( m_0 < \cdots < m_{g+1} \) be all the non-gaps of \( P \) between 0 and \( 2g+1 \), let \( f_i \in L(m_iP) \) such that \( \nu_p(f_i) = -m_i \) for \( i = 0, \ldots, g+1 \). Then

\[
K_\infty(P) = F[f_1, f_2, \ldots, f_{g+1}].
\]

So that

\[
K_\infty(P) \cong F[X_1, \ldots, X_{g+1}]/I,
\]

where \( I \) is some ideal of the polynomial ring \( F[X_1, \ldots, X_{g+1}] \).

**Proof.** One has \( K_\infty(P) = \bigcup_{m=0}^{\infty} L(mP) \), which is generated by the elements \( \prod_{i=0}^{g+1} f_i^{k_i} \), by Proposition 4.3 and \( f_0 \in F \). Thus \( K_\infty(P) \subseteq F[f_1, f_2, \ldots, f_{g+1}] \). On the other hand, \( F[f_1, \ldots, f_{g+1}] \subseteq K_\infty(P) \) since \( f_i \in K_\infty(P) \) for all \( i = 1, \ldots, g+1 \) and \( K_\infty(P) \) is a ring. Therefore \( K_\infty(P) = F[f_1, f_2, \ldots, f_{g+1}] \).

**Example 4.1** The projective line \( P^1 \) over \( F \). If \( P = (1 : 0) \) and \( 1/x \) is a local parameter at \( P \), then \( K_\infty(P) = F[x] \).

**Example 4.2** The Hermitian curve \( H(q) \) is defined by the equation

\[
U^{q+1} + V^{q+1} + W^{q+1} = 0
\]

over \( GF(q^2) \) (for the details we refer to [72, 78] and Chapter 6). Let \( a, b \in GF(q^2) \) such that \( a^2 + a = b^{q+1} = -1 \) and \( P = (1 : b : 0) \). The set of non-gaps of \( P \) is \( \{iq+j(q+1):i,j \in \mathbb{N}\} \). Let \( x = U/W \) and \( y = V/W \). Define \( x = b/(v-bu) \) and \( y = ux - a \). Hence we have \( K_\infty(P) = F[x,y] \), where \( x^{q+1} = y^q + y \).

**Example 4.3** In Chapter 2, we have defined the curve \( X(l,q) \) in \( P^1 \), see Definition 2.6 of Chapter 2. From Proposition 2.5 we know that \( L(m\tilde{P}_\infty) \) is generated by the set

\[
\{z_1^{k_1} \cdots z_l^{k_l} | \sum_{i=1}^{l} k_0q^{i-1}(q+1)^{i-1} \leq m\},
\]

where \( z_i = y_i \circ n \), and \( n \) is the normalization of \( X(l,q) \) and \( \tilde{P}_\infty \) is the unique rational point of \( n^{-1}(P_\infty) \), and \( y_i = X_i/X_0 \). Hence \( K_\infty(P_\infty) = F[z_1, \ldots, z_l] \).

**Definition 4.3** Define the map \( \deg : K_\infty(P) \rightarrow \mathbb{N} \) by \( \deg(f) = -\nu_p(f) \) and \( \deg(f) = -\infty \) if and only if \( f = 0 \).

**Remark 4.1** Notice that we now have an abuse of notation: \( \deg \) is a map on the set of divisors and on \( K_\infty(P) \). If \( f \) is a rational function, then

\[
\deg(f) = 0 \quad \text{and} \quad \deg(f)_0 = \deg(f)_\infty.
\]

Hence for every \( f \in K_\infty(P) \), \( \deg(f) = \deg(f)_\infty = \deg(f)_0 \).
Remark 4.2 If $P$ is a rational point, then $\mathbb{N} \setminus \text{Image}(\text{deg}) = \{n_1, \ldots, n_g\}$ is the set of gaps of $P$.

Lemma 4.2 If $f, h \in K_{\infty}(P)$ then
i) $\text{deg}(fh) = \text{deg}(f) + \text{deg}(h)$;
ii) $\text{deg}(f + h) \leq \max\{\text{deg}(f), \text{deg}(h)\}$ if $f + h \neq 0$, furthermore $\text{deg}(f + h) = \text{deg}(f)$ if $\text{deg}(f) > \text{deg}(h)$.

Proof. This follows immediately from the corresponding properties of the discrete valuation $\nu_P$. □

Remark 4.3 If $P$ is a rational point and the genus is not zero, then $K_{\infty}(P)$ with the map $\text{deg}$ is not an Euclidean domain. In fact, given an $f \in K_{\infty}(P)$ with $\text{deg}(f) > 0$, there exists a gap $n$ such that $\text{deg}(f) + n$ is not a gap. Hence $\text{deg}(f') = \text{deg}(f) + n$. Suppose $K_{\infty}(P)$ is an Euclidean domain, then there exist $q, r \in K_{\infty}(P)$ such that $f' = qf + r$ with $0 \leq \text{deg}(r) < \text{deg}(f)$. Hence $q \neq 0$ and $\text{deg}(f') = \text{deg}(q) + \text{deg}(f)$. Thus $n = \text{deg}(q)$ is not a gap, which is a contradiction.

Although $K_{\infty}(P)$ with the map $\text{deg}$ is not an Euclidean domain when $P$ is a rational point and the genus is not zero, we still can prove a division theorem. We need a lemma and a definition first.

Lemma 4.3 Let $P$ be a rational point. Suppose $f, h \in K_{\infty}(P)$, and $n = \text{deg}(f) = \text{deg}(h)$, then there exists a unique $\alpha \in \mathbb{F}$, such that $\text{deg}(f - \alpha h) < n$.

Proof. The vector space $L(nP)/L((n-1)P)$ is at most one-dimensional. $f$ and $h$ are elements of $L(nP)$ but not of $L((n-1)P)$, since $\text{deg}(f) = \text{deg}(h) = n$. Hence $f + L((n-1)P), h + L((n-1)P)$ are linearly dependent and not equal to $L((n-1)P)$. Thus there exists a unique $\alpha \in \mathbb{F}$ such that $f - \alpha h \in L((n-1)P)$. Therefore $\text{deg}(f - \alpha h) < n$. □

Definition 4.4 Let $P$ be a rational point. Let $m \in \mathbb{N}$. Define

$$\text{gap}(m) = \{0, 1, \ldots, m-1, m+n_1, \ldots, m+n_g\},$$

where $n_1, \ldots, n_g$ are the gaps of $P$. For a non-zero element $h$ of $K_{\infty}(P)$ we define

$$\text{gap}(h) = \text{gap}(\text{deg}(h)).$$

Theorem 4.2 (Division Theorem) Let $P$ be a rational point. For every two elements $f, h \in K_{\infty}(P)$ with $h \neq 0$, there exist $q, r \in K_{\infty}(P)$, such that $f = qh + r$ and $r = 0$ or $\text{deg}(r) \in \text{gap}(h)$. Moreover, $\text{deg}(r)$ is unique, that is, if there are another $q', r' \in K_{\infty}(P)$ such that $f = q'h + r'$, and $r' = 0$ or $\text{deg}(r') \in \text{gap}(h)$, then $\text{deg}(r') = \text{deg}(r)$ or $r = r' = 0$.

Proof. We prove the existence by induction on $\text{deg}(f)$.

1) If $f = 0$ then take $q = r = 0$.
2) If $\text{deg}(f) \in \text{gap}(h)$, then take $q = 0$ and $r = f$.
3) If $\text{deg}(f) \notin \text{gap}(h)$, then $\text{deg}(f) \geq \text{deg}(h)$ and $\text{deg}(f) - \text{deg}(h)$ is not a gap. Hence there exists a $q_0 \in K_{\infty}(P)$ such that $\text{deg}(q_0) = \text{deg}(f) - \text{deg}(h)$, so $\text{deg}(f) = \text{deg}(q_0h)$. Hence $\text{deg}(f - \alpha q_0h) < \text{deg}(f)$ for some $\alpha \in \mathbb{F}$, by Lemma 4.3.
By the induction hypothesis there exist \( q_1, r \in K_\infty \) such that \( f - \alpha q_0 h = q_1 h + r \), and \( \deg(r) \in \text{gap}(h) \). Therefore \( f = q h + r \) where \( q = q_1 + \alpha q_0 \) and \( \deg(r) \in \text{gap}(h) \), or \( r = 0 \).

Now we prove the uniqueness. If there are another \( q', r' \in K_\infty(P) \) such that \( f = q'h + r' \) with \( r' = 0 \) or \( \deg(r') \in \text{gap}(h) \), then \( (q - q')h = r' - r \). If \( r = 0 \) but \( r' \neq 0 \) (or \( r' = 0 \) but \( r \neq 0 \)) then \( \deg(r') = \deg(h) + \deg(q - q') \) which is not an element of \( \text{gap}(h) \), since \( \deg(q - q') \) is not a gap, a contradiction. Thus \( r = 0 \) if and only if \( r' = 0 \).

Next we prove the uniqueness. If there are another \( q', r' \in K_\infty(P) \) such that \( f = q'h + r' \) with \( r' = 0 \) or \( \deg(r') \in \text{gap}(h) \), then \( (q - q')h = r' - r \). If \( r = 0 \) but \( r' \neq 0 \) (or \( r' = 0 \) but \( r \neq 0 \)) then \( \deg(r') = \deg(h) + \deg(q - q') \) which is not an element of \( \text{gap}(h) \), since \( \deg(q - q') \) is not a gap, a contradiction. Thus \( \deg(r) = \deg(r') \).

### 4.2 Isometric geometric Goppa codes

**Definition 4.5** Let \( \Omega \) be the vector space of rational differential forms on \( \mathcal{X} \) over \( F \). Define the map \( \alpha : \Omega \to F^n \) by

\[
\omega \mapsto (\res_1(\omega), \ldots, \res_n(\omega)).
\]

Let \( G \) be a divisor on \( \mathcal{X} \) such that \( \text{supp}(G) \cap \text{supp}(D) = \emptyset \). By Definition 1.3, we have that \( \text{Image}(\alpha|_{\Omega(G-D)}) \) is a geometric Goppa code \( C_\Omega(D,G) \).

We rewrite Theorem 1.3.b in the following form.

**Theorem 4.3** If \( m = \deg(G) \geq 2g - 1 \), then the restriction of \( \alpha_\Omega \) to \( \Omega(G-D) \) is injective, and \( C_\Omega(D,G) \) is a linear \([n,k,d] \) code with

\[
k \geq n - m - 1 + g, \quad \text{and} \quad d \geq m - 2g + 2,
\]

If moreover \( m < n \), then \( k = n - m - 1 + g \). We call \( m - 2g + 2 \) the designed minimum distance of \( C_\Omega(D,G) \) and denote it by \( d^* \). Furthermore, if \( \omega_1, \ldots, \omega_k \) is a basis of \( \Omega(G-D) \), and

\[
A = \begin{pmatrix}
\res_1(\omega_1) & \cdots & \res_n(\omega_1) \\
\vdots & \ddots & \vdots \\
\res_1(\omega_k) & \cdots & \res_n(\omega_k)
\end{pmatrix},
\]

then \( A \) has rank \( k \) and is a generator matrix of \( C_\Omega(D,G) \).

**Remark 4.4** Recall the definition of isometry in Chapter 2, we have that codes \( C_1 \) and \( C_2 \) are isometric if there is an \( n \)-tuple \( \lambda = (\lambda_1, \ldots, \lambda_n) \) of nonzero elements in \( F \) and a permutation \( \sigma \) such that \( C_2 = \lambda \sigma C_1 \). We call \( \lambda \) the scaling factor. We can view \( \lambda \sigma \) as a linear map of \( F^n \) which leaves the Hamming metric invariant. Note that a linear map of \( F^n \) leaves the Hamming metric invariant if and only if it is of the form \( \lambda \sigma \).

**Definition 4.6** Let \( C_1 \) and \( C_2 \) be two isometric codes in \( F^n \), that is \( C_2 = \lambda \sigma C_1 \) for some permutation \( \sigma \) and scaling factor \( \lambda \). Suppose \( A(C_1) \) is a decoding algorithm of \( C_1 \), the induced decoding algorithm \( \lambda \sigma A(C_1) \) is defined as follows,

1. input \( x \);
2. \( y := \sigma^{-1}(x_1/\lambda_1, \ldots, x_n/\lambda_n) \);
3. run \( A(C_1) \) with input \( y \) to get \( c' \in C_1 \);
4. output \( c := \lambda \sigma c' \);
5. stop.
Chapter 4: Decoding Geometric Goppa Codes

The following proposition follows immediately from the above definition.

**Proposition 4.4** Let $C_1$ and $C_2$ be isometric codes in $F^n$, that is $C_2 = \lambda \sigma C_1$ for some permutation $\sigma$ and scaling factor $\lambda$. Suppose the algorithm $A(C_1)$ decodes $C_1$ up to $e$ errors. Then the induced algorithm $\lambda \sigma A(C_1)$ decodes $C_2$ up to $e$ errors as well.

**Remark 4.5** By the above definition and Proposition 4.4, we see that, as soon as a decoding algorithm of one of the codes in an isometry class is given, all the decoding algorithms of the codes in this class are given by the induced algorithms and they correct the same number of errors. In the rest of this section, we will give a special class leader of every isometry class for which a decoding algorithm will be given later. First, the following proposition gives a sufficient condition for two geometric Goppa codes to be isometric.

**Proposition 4.5** Let $G_1$ and $G_2$ be two linear equivalent divisors such that $G_i$ and $D$ have disjoint support, where $i = 1, 2$. Suppose there is a rational function $f$ with disjoint support with $D$, such that $G_1 = G_2 + (f)$. Then

$$C_{\Omega}(D, G_2) = \lambda C_{\Omega}(D, G_1),$$

where $\lambda = (f(P_1), \ldots, f(P_n))$.

**Proof.** See [75]. $\Box$

**Proposition 4.6** Let $H$ be an effective divisor such that $\mathcal{H} \cap \{P_1, \ldots, P_n\} = \emptyset$, where $\mathcal{H} = \text{supp}(H)$. Let $P$ be a place of $\mathcal{X}$ which is not in $\mathcal{H} \cup \{P_1, \ldots, P_n\}$. Then there exists an $h \in K_{\infty}(P)$, such that $(h)_{\mathcal{H}} = H$ and $\text{supp}((h)) \cap \{P_1, \ldots, P_n\} = \emptyset$.

**Proof.** Suppose $H = \sum_{i=1}^{m} b_i Q_i$, where $b_i \geq 0$ for $i = 1, \ldots, m$, so $\mathcal{H} = \{Q_1, \ldots, Q_m\}$. Define $Q_{m+i} = P_i$ for $i = 1, \ldots, n$, and define $b_i = b_i + 1$ if $i = 1, \ldots, m$ and $b_i = 1$ if $i = m + 1, \ldots, m + n$. Now choose an integer $k$, such that

$$k \deg(P) - \sum_{i=1}^{m+n} b_i \deg(Q_i) \geq 2g - 1.$$

So

$$k \deg(P) - \sum_{i=1}^{m+n} b_i \deg(Q_i) + \deg(Q_j) > 2g - 1,$$

for every $j$. Hence

$$l(kP - \sum_{i=1}^{m+n} b_i Q_i + Q_j) = l(kP - \sum_{i=1}^{m+n} b_i Q_i) + \deg Q_j,$$

for every $j$, by the Riemann-Roch Theorem. Therefore $L(kP - \sum_{i=1}^{m+n} b_i Q_i + Q_j)$ contains $L(kP - \sum_{i=1}^{m+n} b_i Q_i)$ as a proper subspace. Thus for every $j$ there exists an $h_j$ in the first mentioned space and not in the last one. So $h_j \in K_{\infty}(P)$, and $v_{Q_i}(h_j) = b_j - 1$ and $v_{Q_j}(h_j) \geq b_j$ if $i \neq j$. Now define $h = \sum_{j=1}^{m+n} h_j$, then $h \in K_{\infty}(P)$ and

$$(h)_{\mathcal{H'}} = \sum_{i=1}^{m+n} (b_i - 1) Q_i = \sum_{i=1}^{m+n} b_i' Q_i = H$$

where $\mathcal{H'} = \{Q_1, \ldots, Q_{m+n}\}$. 


Hence \( (h)_{\mathcal{H}} = H \) and \( v_{P_i}(h) = v_{Q_m}(h) = 0 \) for \( i = 1, \ldots, n \), that is
\[
\text{supp}(h) \cap \{P_1, \ldots, P_n\} = \emptyset.
\]

Lemma 4.4 Let \( G \) be a non-zero divisor such that \( G \) and \( D \) have disjoint support. Let \( P \) be a place not in \( \{P_1, \ldots, P_n\} \). Then there exists a rational function \( f \), such that \( G' \) and \( D + P \) have disjoint support, \( G' = G + (f) \) is a non-effective divisor and \( v_{P_i}(f) = 0 \) for \( i \in \{1, \ldots, n\} \).

Proof. Suppose \( v_P(G) = v \). Choose a place \( Q \), such that \( Q \notin \{P_1, \ldots, P_n, P\} \cup \text{supp}(G) \). There exists a rational function \( f \) such that \( v_Q(f) = -v \) and \( v_{P_i}(f) = 0 \) for all \( i = 1, \ldots, n \), by the independence of valuations, see [6, p.11]. Hence \( G' := G + (f) \) is a non-effective divisor since \( v_Q(G + (f)) = v_Q(f) = -1 \) and \( \text{supp}(G') \cap \{P_1, \ldots, P_n, P\} = \emptyset \). \( \square \)

Proposition 4.7 Let \( P \) be an extra place, that is a place not in \( \{P_1, \ldots, P_n\} \). Let \( G \) be a divisor such that \( G \) and \( D \) have disjoint support. Then there exist an effective divisor \( E \) and a positive integer \( \mu \), such that \( C_\Omega(D, G) \) and \( C_\Omega(D, E - \mu P) \) are isometric.

Proof. First there exists a rational function \( f \) such that if we define \( G' = G + (f) \), then \( G'_{\infty} \neq 0 \), \( \text{supp}(G') \cap \{P_1, \ldots, P_n, P\} = \emptyset \) and \( v_{P_i}(f) = 0 \) for \( i \in \{1, \ldots, n\} \) by Lemma 4.4. Hence \( f(P_i) \) exists and is not equal to zero for every \( i \in \{1, \ldots, n\} \). Now by Proposition 4.6, there exists an \( h \in K_\infty(P) \) such that \( (h)_{\mathcal{H}} = G'_{\infty} \), where \( \mathcal{H} = \text{supp}(G'_{\infty}) \) and \( \text{supp}(h) \cap \{P_1, \ldots, P_n\} = \emptyset \). Thus \( h(P_i) \) exists and \( h(P_i) \neq 0 \) for all \( i = 1, \ldots, n \). Now define \( E = G' + (h)_0 \), then \( E \geq G'_0 - G'_{\infty} + (h)_{\mathcal{H}} \geq 0 \), this means that \( E \) is an effective divisor. Moreover \( E \) and \( D \) have disjoint support, since \( \text{supp}(E) \subseteq \text{supp}(G') \cup \text{supp}((h)_0) \) and \( G' \) and \( (h)_0 \) have disjoint support with \( D \). Take \( \mu = -v_P(h) \), then \( \mu \geq \deg(G'_{\infty}) > 0 \) and
\[
E - \mu P = G' + (h)_0 - (h)_{\infty} = G + (fh),
\]
since \( h \in K_\infty(P) \). Therefore \( C_\Omega(D, G) \simeq C_\Omega(D, E - \mu P) \) by Proposition 4.5. This proves our proposition. \( \square \)

Proposition 4.8 Let \( P \) be an extra place. Let \( m \) be an integer. Then there exists an \( h \in K_\infty(P) \) and a positive integer \( \mu \), such that \( C_\Omega(D, mP) \) and \( C_\Omega(D, (h)_0 - \mu P) \) are isometric.

Proof. By Proposition 4.6, there exists an \( h \in K_\infty(P) \) such that \( (h) \) and \( D \) have disjoint support and \( \deg(h) > m \). Let \( \mu = \deg(h) - m \), then \( \mu \) is a positive integer and
\[
(h)_0 - \mu P = (h) + mP.
\]
Therefore \( C_\Omega(D, (h)_0 - \mu P) \) and \( C_\Omega(D, mP) \) are isometric by Proposition 4.5. \( \square \)
4.3 The residue representation of differentials

Before we define the syndrome of the code \( C_0(D, E - \mu P) \), in this section we will give the representation of every differential \( \omega \in \Omega(E - \mu P - D) \) by its residues at the points \( P_1, \ldots, P_n \).

**Proposition 4.9** Let \( P \) be a place not in \( \{ P_1, \ldots, P_n \} \) and let \( \mu \) be a positive integer. Then

\[
\Omega(-D - \mu P)/\Omega(-\mu P) \cong \mathbb{F}^n.
\]

*Proof.* The restriction of \( \alpha_0 \) to \( \Omega(-D - \mu P) \) is an homomorphism from \( \Omega(-D - \mu P) \) to \( \mathbb{F}^n \) with kernel \( \Omega(-\mu P) \). Furthermore, by the Riemann-Roch Theorem we have that the difference between the dimensions of \( \Omega(-D - \mu P) \) and \( \Omega(-\mu P) \) is \( n \).

**Proposition 4.10** Let \( P \) be a place not in \( \{ P_1, \ldots, P_n \} \) and let \( \mu \) be a positive integer. Then for every \( i \in \{ 1, \ldots, n \} \) there exists an \( \varepsilon_i \in \Omega(-P_i - \mu P) \) such that \( \text{res}_{P_i}(\varepsilon_i) = 1 \). Therefore \( \{ \varepsilon_i := \varepsilon_i + \Omega(-\mu P) \}_{i=1}^n \) is a basis of \( \Omega(-D - \mu P)/\Omega(-\mu P) \), and for every \( \omega \in \Omega(-D - \mu P) \),

\[
\overline{\omega} := \omega + \Omega(-\mu P) = \sum_{i=1}^n \text{res}_{P_i}(\omega)\varepsilon_i.
\]

*Proof.* By Proposition 4.9, we have

\[
\Omega(-P_i - \mu P)/\Omega(-\mu P) \cong \mathbb{F},
\]

where \( i = 1, \ldots, n \). Hence there exists an \( \omega_i \in \Omega(-P_i - \mu P) \) such that \( \omega_i \notin \Omega(-\mu P) \), so \( \nu_{P_i}(\omega_i) = -1 \). Now define the differential \( \varepsilon_i = \omega_i/\text{res}_{P_i}(\omega_i) \), then \( \varepsilon_i \in \Omega(-P_i - \mu P) \) and \( \text{res}_{P_i}(\varepsilon_i) = 1 \).

Now suppose there exist \( a_1, a_2, \ldots, a_n \in \mathbb{F} \) such that \( \sum_{i=1}^n a_i\varepsilon_i = 0 \), that is \( \sum_{i=1}^n a_i\varepsilon_i \in \Omega(-\mu P) \). We claim that all \( a_i \) are zero. Otherwise there exists a \( j \in \{ 1, \ldots, n \} \), such that \( a_j \neq 0 \). So \( \nu_{P_j}(\sum_{i=1}^n a_i\varepsilon_i) = -1 \), hence \( \sum_{i=1}^n a_i\varepsilon_i \notin \Omega(-\mu P) \), a contradiction. Thus \( \varepsilon_1, \ldots, \varepsilon_n \) are linearly independent. Hence it is a basis of \( \Omega(-D - \mu P)/\Omega(-\mu P) \), since this last mentioned space has dimension \( n \), by Proposition 4.9. Therefore, for every \( \omega \in \Omega(-D - \mu P) \), there exist \( a_1, \ldots, a_n \in \mathbb{F} \) such that

\[
\overline{\omega} = \sum_{i=1}^n a_i\varepsilon_i.
\]

This means that there exists an \( \omega' \in \Omega(-\mu P) \), such that

\[
\omega = \sum_{i=1}^n a_i\varepsilon_i + \omega'.
\]

After calculating the residue of \( P_i \) on both sides, we get \( \text{res}_{P_i}(\omega) = a_i \). Thus

\[
\overline{\omega} = \sum_{i=1}^n \text{res}_{P_i}(\omega)\varepsilon_i.
\]
Proposition 4.11 Let $P$ be a place not in $\{P_1, \ldots, P_n\}$. Let $E$ be an effective divisor and let $\mu$ be a positive integer, such that $E$ and $D$ have disjoint support and $\deg(E - \mu P) \geq 2g - 1$. Then there exist $n$ differentials $\varepsilon_1, \ldots, \varepsilon_n$, which are independent modulo $\Omega(-\mu P)$, such that $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\res_{P_i}(\varepsilon_i) = 1$, and for every $\omega \in \Omega(E - \mu P - D)$

$$\omega = \sum_{i=1}^{n} \res_{P_i}(\omega) \varepsilon_i.$$

If moreover $\mu = 1$, then $(\varepsilon_i)_\infty = P_i + P$ for all $i$.

Proof. By Proposition 4.10, there exist $\eta_1, \ldots, \eta_n \in \Omega(-D - \mu P)$, such that $\eta_i \in \Omega(-P_i - \mu P)$ and $\res_{P_i}(\eta_i) = 1$ for $i = 1, \ldots, n$, and $\eta_1, \ldots, \eta_n$ is a basis of $\Omega(-D - \mu P)/\Omega(-\mu P)$. Now let $\omega_1, \omega_2, \ldots, \omega_k$ be a basis of $\Omega(E - \mu P - D)$, which is a subset of $\Omega(-\mu P - D)$. Thus

$$\omega_i = \sum_{j=1}^{n} \res_{P_j}(\omega_i) \eta_j$$

for $i = 1, \ldots, k$,

by Proposition 4.10. Define $A = (\res_{P_j}(\omega_i))_{k \times n}$, we have $W = AT$, where $W = (\omega_1, \ldots, \omega_k)^t$ and $T = (\eta_1, \ldots, \eta_n)^t$. Let $l = g + \mu - 1$, then $l$ is the dimension of $\Omega(-\mu P)$. Let $\beta_1, \ldots, \beta_l$ be a basis of $\Omega(-\mu P)$, then there exists a $(k \times l)$-matrix $Y$ over $F$ such that

$$W - AT = YB,$$

where $W = (\omega_1, \ldots, \omega_k)^t$, $T = (\eta_1, \ldots, \eta_n)^t$ and $B = (\beta_1, \ldots, \beta_l)^t$. Now rank($A$) = $k$ by Theorem 4.3, since $\deg(E - \mu P) \geq 2g - 1$. Hence there exists an $(n \times l)$-matrix $X$ over $F$ such that $AX = YB$ Thus $W = A(T + XB)$. Define

$$\varepsilon_i = \eta_i + \sum_{j=1}^{l} x_{ij} \beta_j$$

for $i = 1, \ldots, n$.

where $x_{ij}$ is entry of matrix $X$ in row $i$ and column $j$. Then $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\res_{P_i}(\varepsilon_i) = 1$ and

$$\omega_i = \sum_{j=1}^{n} \res_{P_j}(\omega_i) \varepsilon_j$$

for $i = 1, \ldots, k$.

Finally, for every $\omega \in \Omega(E - \mu P - D)$

$$\omega = \sum_{j=1}^{n} \res_{P_j}(\omega) \varepsilon_j.$$

by the linearity of $\res_{P_j}$ and since the corresponding statement is true for the basis $\omega_1, \ldots, \omega_k$ of $\Omega(E - \mu P - D)$. Clearly $(\varepsilon_i)_\infty = P_i + P$ if $\mu = 1$. □

Remark 4.6 In case $X$ is the projective line, e.g. for classical Goppa codes with $n + 1$ distinct rational points $P_1, \ldots, P_n, P_\infty$, where $P_i = (a_i : 1)$ and $P_\infty = (1 : 0)$, and Goppa polynomial $h$, which is not zero at the points $P_i$, we can take for the differentials $\varepsilon_i = 1/(X - a_i) dX$. For an arbitrary curve it is not so easy to find these differentials $\varepsilon_i$ explicitly, see e.g. Chapter 6 in case of the Hermitian curve.
Definition 4.7 Let the assumptions be as in Proposition 4.11. For code $C_\Omega(D, E - \mu P)$, define the map

$$\varepsilon : \mathbb{F}^n \rightarrow \Omega \text{ by } \varepsilon(x) = \sum_{i=1}^{n} x_i \varepsilon_i,$$

where $\varepsilon_1, \ldots, \varepsilon_n$ are given by Proposition 4.11.

Remark 4.7 The restriction of $\varepsilon$ to $C_\Omega(D, E - \mu P)$ is the inverse map of $\alpha_\Omega$ restricted to $\Omega(E - \mu P - D)$, as we will see in the following corollary.

Corollary 4.1 Let the assumptions be as in Proposition 4.11. Let $\varepsilon_1, \ldots, \varepsilon_n$ be the differentials given by Proposition 4.11. Then

$$\varepsilon(c) \in \Omega(E - \mu P - D) \text{ if and only if } c \in C_\Omega(D, E - \mu P).$$

Proof. By Proposition 4.11, there exist independent differentials $\varepsilon_1, \ldots, \varepsilon_n$ with $\varepsilon_i \in \Omega(-P_i - \mu P)$ and $\text{res}_{P_i}(\varepsilon_i) = 1$, such that for every $\omega \in \Omega(E - \mu P - D)$

$$\omega = \sum_{i=1}^{n} \text{res}_{P_i}(\omega) \varepsilon_i.$$

Let $c \in C_\Omega(D, E - \mu P)$, then there exists an $\omega \in \Omega(E - \mu P - D)$ such that

$$c = (\text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega)),$$

so

$$\varepsilon(c) = \sum_{i=1}^{n} \text{res}_{P_i}(\omega) \varepsilon_i = \omega \in \Omega(E - \mu P - D).$$

Conversely, let $\varepsilon(c) \in \Omega(E - \mu P - D)$, then one has $\text{res}_{P_j}(\varepsilon(c)) = c_j$ for every $j = 1, \ldots, n$, so $c = \alpha_\Omega(\varepsilon(c)) \in C_\Omega(D, E - \mu P)$ by the definition of $\alpha_\Omega$. □

4.4 The syndrome

In [35], [71] and [53], for the code $C_\Omega(D, G)$, the syndrome of $x \in \mathbb{F}^n$ is defined by a map from $L(F)$ to $\mathbb{F}$, namely by $s(x, f) = \sum_{i=1}^{n} x_i f(P_i) g(P_i)$, where $g \in L(G - F)$ and $F$ is a divisor. But here we give a different definition of the syndrome of $x$, namely as an element of $K_\infty(P)$, which is a generalization of the syndrome of classical Goppa codes. In this section, we will give the definition only for codes of the form $C_\Omega(D, E - \mu P)$. This is not a restriction since every geometric Goppa code is isometric with a code of this type, by the discussion in Section 4.2. First we need some preliminaries.

Definition 4.8 [6, I.7] Let $B$ be a divisor on $\mathcal{X}$. The rational functions $f_1$ and $f_2$ are said to be congruent to each other modulo $B$ under a set of places $O$, if we have $v_Q(f_1 - f_2) \geq v_Q(B)$ for every $Q \in O$. We shall write

$$f_1 \equiv_O f_2 \text{ (mod } B).$$

In particular,

1) If $O$ is the set of all places of $\mathcal{X}$, then we write $f_1 \equiv f_2 \text{ (mod } B);$  
2) If $O$ is the support of a divisor $E$ on $\mathcal{X}$, then we write $f_1 \equiv_E f_2 \text{ (mod } B).$
3) If $B = (f)$, where $f$ is a rational function, then we write $f_1 \equiv_O f_2 \text{ (mod } f).$
Lemma 4.5 Let \( \langle h \rangle \) be the principal ideal of \( K_\infty(P) \) generated by \( h \in K_\infty(P) \). Let \( E = \langle h \rangle \). Then

\[
\{ f \in K_\infty(P) | f \equiv_0 (\text{mod } h) \} = \langle h \rangle.
\]

Therefore for \( f \in K_\infty(P) \), \( f \equiv_0 (\text{mod } h) \) if and only if there exists a \( q \in K_\infty(P) \) such that \( f = qh \), that is \( f \equiv_0 (\text{mod } h) \) in the ring \( K_\infty(P) \).

Proof. Let \( f \in \langle h \rangle \), then there is a \( q \in K_\infty(P) \) such that \( f = qh \). Thus

\[
v_Q(f) = v_Q(q) + v_Q(h) \geq v_Q(h)
\]

for \( Q \in \text{supp}(E) \), hence \( f \equiv_0 (\text{mod } h) \) by definition.

Conversely, let \( f \in K_\infty(P) \) and \( f \equiv_0 (\text{mod } h) \). Then by the Division Theorem 4.2, there exist \( q, r \in K_\infty(P) \) such that \( f = qh + r \) where \( r = 0 \) or \( \deg(r) \in \text{gap}(h) \). We claim \( r = 0 \), therefore \( f \in \langle h \rangle \). If it is not true, then for every \( Q \neq P \) we have

\[
v_Q(r) = v_Q(f - qh) \geq \min\{v_Q(f), v_Q(q) + v_Q(h)\} \geq v_Q(h),
\]

since if \( Q \not\in \text{supp}(\langle h \rangle) \) then \( v_Q(h) = 0 \) and if \( Q \in \text{supp}(h) \) then \( v_Q(f) \geq v_Q(h) \). So \( r/h \in K_\infty(P) \) and \( r/h \neq 0 \). Thus \( \deg(r) - \deg(h) = \deg(r/h) \) is not a gap of \( P \), that is \( r \not\in \text{gap}(h) \) which is a contradiction. \( \square \)

Definition 4.9 Let \( W \) be a divisor on \( \mathcal{X} \) and \( P \) be a rational point on \( \mathcal{X} \), such that \( P \) is not in the support of \( W \). Define \( K_\infty(P, W) \) by

\[
K_\infty(P, W) = \{ f \in K_\infty(P) | f = 0 \text{ or } f \equiv_W 0 (\text{mod } W) \}
\]

Lemma 4.6 \( K_\infty(P, W) \) is an ideal in \( K_\infty(P) \).

Proof. Let \( f_1, f_2 \in K_\infty(P, W) \), then for every \( Q \in \text{supp}(W) \), we have \( v_Q(f_1) \geq v_Q(W) \) for \( i = 1, 2 \), so

\[
v_Q(f_1 + f_2) \geq \min\{v_Q(f_1), v_Q(f_2)\} \geq v_Q(W).
\]

Let \( f \in K_\infty(P, W) \) and \( h \in K_\infty(P) \), then for every \( Q \in \text{supp}(W) \), we have \( v_Q(f) \geq v_Q(W) \) and \( v_Q(h) \geq 0 \), since \( Q \neq P \). Hence \( v_Q(fh) \geq v_Q(W) \). Therefore \( fh \in K_\infty(P, W) \), so \( K_\infty(P, W) \) is an ideal in \( K_\infty(P) \). \( \square \)

Proposition 4.12 Let \( P \) be a place not in \( \{P_1, \ldots, P_n\} \). Let \( E \) be an effective divisor. Then there exists a differential form \( \eta \) such that

\[
\text{supp}(\eta_0) \subseteq \{P\} \text{ and supp}(\eta) \cap \{P_1, \ldots, P_n\} \cup \text{supp}(E) = \emptyset,
\]

If moreover \( g > 1 \), then \( \text{supp}(\eta_0) = \{P\} \).

Proof. Suppose \( \text{supp}(E) = \{Q_1, \ldots, Q_m\} \). Let \( \omega' \) be any non-zero differential form. By the independence of valuations, see [6, p. 11], there exists a rational function \( f_0 \) such that \( v_P(f_0) = -v_P(\omega') \), \( v_P(f_0) = -v_P(\omega') \) for \( i = 1, \ldots, n \) and \( v_Q(f_0) = -v_Q(\omega') \) for \( i = 1, \ldots, m \). Define \( \omega = f_0 \omega' \), then \( \omega \neq 0 \) and \( \text{supp}(\omega) \cap \{P, P_1, \ldots, P_n, Q_1, \ldots, Q_m\} = \emptyset \). Now by Proposition 4.6, there exists an \( f \in K_\infty(P) \) such that \( (f) \omega = (\omega)_0 \), where \( \omega = \text{supp}(\omega)_0 \). Define \( \eta = \omega f^{-1} \), then \( \eta \neq 0 \) and \( (\eta) = (\omega) - (f) \leq -v_P(\omega) \). Hence \( \text{supp}(\eta_0) \subseteq \{P\} \) and \( \text{supp}(\eta) \cap \{P_1, \ldots, P_n, Q_1, \ldots, Q_m\} = \emptyset \). If \( g > 1 \), then \( 2g - 2 > 0 \), hence \( \eta_0 \neq 0 \), so \( \text{supp}(\eta_0) = \{P\} \) and \( \text{supp}(\eta) \cap \{P, P_1, \ldots, P_n\} \cup \text{supp}(E) = \emptyset \). \( \square \)

In the following three examples, such an \( \eta \) is explicitly given with the additional property \( \text{supp}(\eta) = (2g - 2)P \).
Example 4.4 The projective line $\mathbb{P}^1$ over $F$, see Example 4.1.
If $P_\infty = (1 : 0)$ and $\eta = dX$, then $\eta = (-X^2)d(1/X)$. Hence $(\eta) = -2P_\infty$. If $P = (\alpha : 1)$ and $\eta = d(1/(X - \alpha))$, then $(\eta) = -2P$.

Example 4.5 Hermitian Curve $H(q)$, see Example 4.2.
If $\eta = dx$, then $(\eta) = (2g - 2)P_\infty$, see [72, Satz 1 (f)].

Example 4.6 Let $\mathcal{X}(l, q)$ be the curve as in Example 4.3.
The genus of this curve is $\{1 : i : i = q^{l+1-i}(q+1)^{i-1} - (q+1)q^{l-1} + 1\}/2$ and this curve goes through all the $q^i$ places of degree one, outside the hyperplane with equation $x_0 = 0$. The number $2g - 1$ is a gap of $P_\infty$, see Chapter 2. Thus there exists an $\eta \in \Omega$ such that $(\eta) = (2g - 2)P_\infty$ by [57, Theorem 4.4.1] and [63, Lemma 1.1].

Remark 4.8 All these examples have the property that there exists a differential with support concentrated at at most one place. Other examples are rational, elliptic and hyperelliptic curves, see [57]. See Delgado [9] and Sathaye [63] for a characterization of such curves. It would be interesting to know how large the class of such curves is, in particular whether there exists a family of curves such that the ratio of the number of rational points divided by the genus does not tend to zero, whereas the number of rational points tends to infinity.

Over an algebraically closed field of characteristic zero the situation is as follows. The moduli variety $M_g$, parametrizing all isomorphism classes of curves of genus $g$, has dimension $3g - 3$, if $g > 1$. The subvariety $P_g$ of $M_g$, of curves with a differential with support at one point, has dimension $2g - 1$, see [60].

In the following we give an example of a curve without such a differential. The Klein quartic in characteristic two is also such a curve.

Example 4.7 A curve of genus 3, which is not hyperelliptic, has a plane model of degree 4. Effective canonical divisors are intersection divisors of this plane curve with a line. So there exists a differential $\eta$ such that $(\eta) = 4P$ if and only if the plane model has a tangent line, which intersects the curve in $P$ with multiplicity 4. The plane curve $\mathcal{X}$ defined over $GF(2)$ with equation: $XY(X + Y)(X + Z) + XZ^2(X + Z) + Y^2Z(Y + Z) = 0$, see [55], has not such a differential. In fact, this curve has seven places of degree one, say $P_1, P_2, \ldots, P_7$. Every line $L$ in $\mathbb{P}^2$, defined over $GF(2)$, has intersection $L \cdot \mathcal{X} = 2P_1 + P_2 + P_k$, where $i, j$ and $k$ are mutually different. Therefore there does not exist a differential form such that its divisor is $(2g - 2)P$ for some point $P$ on $\mathcal{X}$.

Theorem 4.4 Let $P$ be a rational point not in $\{P_1, \ldots, P_n\}$. Let $E$ be an effective divisor and $\mu$ a positive integer, such that $\deg(E - \mu P) \geq 2g - 1$. Then by the results of the previous sections and the above proposition, we have the following conclusions:
1) (Proposition 4.6). There exists an $h \in K_\infty(P)$, such that $(h)_\epsilon = E$ where $E = \supp(E)$.
2) (Proposition 4.11). There exist $n$ differentials, namely $\epsilon_1, \ldots, \epsilon_n$, such that $\epsilon_i \in \Omega(-P_i - \mu P)$ and $\res_{P_i}(\epsilon_i) = 1$ for $i = 1, \ldots, n$. Moreover, for every $\omega \in \Omega(E - \mu P - D)$,
$$\omega = \sum_{i=1}^n \res_{P_i}(\omega)\epsilon_i.$$ 
3) (Proposition 4.12). There exists a differential $\eta$, such that $(\eta)_0 = lP$ and
$$\supp((\eta)_\infty) \cap (\{P, P_1, \ldots, P_n\} \cup \supp(E)) = \emptyset.$$
Definition 4.10 The syndrome of the code $C_\Omega(D, E - \mu P)$ is defined by the map $S$ from $F^n$ to $F(\mathcal{X})$, such that for every $x \in F^n$,

$$S(x) \eta = \sum_{i=1}^{n} x_i \frac{h(P_i) - h}{h(P_i)} \varepsilon_i,$$

$S(x)$ is called the syndrome of $x$.

Remark 4.9. The syndrome is well defined, since for every differential $\sigma$ on $\mathcal{X}$ there is a unique $s \in F(\mathcal{X})$ such that $\sigma = s \eta$. It follows immediately from the definition that $S$ is a linear map over $F$.

Proposition 4.13 For every $x \in F^n$, $S(x) \in K_\infty(P, W)$, where $W = (\eta)_\infty$.

Proof. For every $i = 1, \ldots, n$, we have

$$v_Q\left(\frac{h(P_i) - h}{h(P_i)} \varepsilon_i\right) \geq 0 \text{ if } Q \not\subset \{P, P_i\}$$

and

$$v_{P_i}\left(\frac{h(P_i) - h}{h(P_i)} \varepsilon_i\right) \geq 1 + v_{P_i}\left(\varepsilon_i\right) \geq 0,$$

since $h \in K_\infty(P)$ and $\varepsilon_i \in \Omega(-P_i - \mu P)$. Thus $v_Q(S(x) \eta) \geq 0$ for $Q \neq P$. Hence

$$v_Q(S(x)) = v_Q(S(x) \eta) - v_Q(\eta) \geq -v_Q(\eta) \text{ for } Q \neq P.$$

Therefore $S(x) \in K_\infty(P, W)$.

The name syndrome $S(x)$ of $x$ is justified by the following theorem.

Theorem 4.5 Under the assumptions of Theorem 4.4 we have that

$$c \in C_\Omega(D, E - \mu P) \text{ if and only if } S(c) \equiv 0 \pmod{h}.$$

If moreover $E = (h)_0$, then

$$c \in C_\Omega(D, E - \mu P) \text{ if and only if } S(c) \equiv 0 \pmod{h} \text{ in } K_\infty(P).$$

Proof. If $c \in C_\Omega(D, E - \mu P)$, then there is an $\omega \in \Omega(E - \mu P - D)$ such that

$$c = (res_{P_1}(\omega), \ldots, res_{P_n}(\omega)),$$

so

$$S(c) \eta = \sum_{i=1}^{n} res_{P_i}(\omega) \frac{h(P_i) - h}{h(P_i)} \varepsilon_i = \omega - h \sum_{i=1}^{n} \frac{c_i}{h(P_i)} \varepsilon_i,$$

by Proposition 4.11. Let $Q \in \supp(E)$, then:

i) $v_Q(\omega) \geq v_Q(E) = v_Q(h)$;

ii) $v_Q(h \sum_{i=1}^{n} c_i \varepsilon_i / h(P_i)) \geq v_Q(h)$;

iii) $v_Q(\eta) = 0$ since $\supp(\langle \eta \rangle) \cap \supp(E) = \emptyset$.

Hence

$$v_Q(S(c)) = v_Q(\omega - h \sum_{i=1}^{n} \frac{c_i}{h(P_i)} \varepsilon_i) - v_Q(\eta) \geq v_Q(h).$$
Chapter 4: Decoding Geometric Goppa Codes

Thus $S(c) \equiv 0 \pmod{h}$.

Conversely, suppose $c \in \mathbb{F}^n$, then

$$S(c) \eta = \varepsilon(c) - h \sum_{i=1}^{n} \frac{c_i}{h(P_i)} \xi_i.$$ 

Let $S(c) \equiv 0 \pmod{h}$. Then for $Q \in \text{supp}(E)$,

$$v_Q(\varepsilon(c)) \geq \min\{v_Q(S(c)) + v_Q(\eta) + v_Q\left(\sum_{i=1}^{n} \frac{c_i}{h(P_i)} \xi_i\right)\} \geq v_Q(h).$$

For all other places, we have $\sum_{Q \in \text{supp}(E)} v_Q(\varepsilon(c)) \geq -D - \mu P$. Combining these two facts, we have $\varepsilon(c) \in \Omega(E - \mu P - D)$. Hence $c = \alpha_Q(\varepsilon(c)) \in C_0(D, E - \mu P)$, by Corollary 4.1. If moreover $E = (h)_0$, then the conclusion follows from the above and Lemma 4.5. □

4.5 Decoding by solving the key congruence

Let $P$ be an extra place, that is not in $\{P_1, \ldots, P_n\}$. Let $E$ be an effective divisor with disjoint support with $D$ and $P$, Let $\mu$ be a positive integer, such that deg($E - \mu P$) $\geq 2g - 1$. By the discussion in Section 4.2, we know that, to decode all geometric Goppa codes it is sufficient to give a decoding algorithm for codes of the form $C_0(D, E - \mu P)$.

**Definition 4.11** Let $S(x)$ be the syndrome of $x \in \mathbb{F}^n$ with respect to $(D, E, P)$. Let $h \in K_\infty(P)$ and $\eta \in \Omega$ be given in Theorem 4.4 for the code $C_0(D, E - \mu P)$. Let $W = (\eta)_\infty$ and $l = \deg(\eta)_\infty$.

1) If $f \in K_\infty(P)$ and $r \in K_\infty(P, W)$ are such that $fS(x) \equiv r \pmod{h}$, then we say that $(f, r)$ satisfies the key congruence of $x$ with respect to $(D, E, P)$.

If moreover $\deg(r) - \deg(f) \leq l + \mu$, then the pair $(f, r)$ is called a valid solution of the key congruence.

If furthermore $(f, r)$ is a valid solution and $\deg(f)$ is minimal among all the degrees of $f'$ such that $(f', r')$ is a valid solution, then $(f, r)$ is called a minimal valid solution of the key congruence.

2) If $E = (h)_0$ and $f \in K_\infty(P)$ and $r \in K_\infty(P, W)$ such that $fS(x) = r + qh$ for some $q \in K_\infty(P, W)$, then we say that $(f, r)$ satisfies the key equation of $x$ with respect to $(D, E, P)$.

Similarly as in 1) we define what a (minimal) valid solution of the key equation is.

**Definition 4.12** The Clifford defect of the pair $(E, P)$ is defined by

$$s = \max\{\frac{\deg(E - kP)}{2} - (l(E - kP) - 1)|k \in \mathbb{N}\}.$$ 

For the details of the Clifford defect we refer to Duursma [12].

**Remark 4.10** Suppose $g$ is the genus of the curve used. Then it is easy to see that

$$s = \max\{\frac{\deg(E - kP)}{2} - (l(E - kP) - 1)|\deg(E) - 2g + 1 \leq k \deg(P) \leq \deg(E)\},$$

and $s \leq g/2$. 
**Definition 4.13** Let $I$ be a subset of $\{1, \ldots, n\}$. Let $Q = \sum_{i \in I} P_i$. Define

$$K_I(P) = \bigcup_{k \in \mathbb{N}} L(kP - Q).$$

Let $b_I$ be the smallest integer for which $l(b_I P - Q) \neq 0$.

**Proposition 4.14** Let $I \subseteq (d^*-\deg(P))/2-s$, where $d^* = \deg(E) - \mu \deg(P) - 2g + 2$ (see Theorem 4.3) and $s$ is the Clifford defect of $(E, P)$. Then

$$\Omega(E - (\mu + b_I)P - Q) = \{0\},$$

where $Q = \sum_{i \in I} P_i$.

**Proof.** Let $t$ be the number of elements of $I$. Assume

$$\Omega(E - (\mu + b_I)P - Q) \neq \{0\}.$$

Then there exists a nonzero differential $\omega$ and an effective divisor $E^*$ such that

$$(\omega) - E + (\mu + b_I)P + Q \sim E^*,$$

hence

$$\deg(E^*) = 2g - 2 - \deg(E) + (\mu + b_I)\deg(P) + t.$$ 

Therefore

$$(b_I - 1)P - Q \sim K - E + (\mu + 2b_I - 1)P - E^*,$$

where $K$ represents the canonical divisor class. Now by the assumption of $b_I$ we have

$$l(K - E + (\mu + 2b_I - 1)P - E^*) = 0,$$

and therefore $\deg(E^*) \geq l(K - E + (\mu + 2b_I - 1)P)$. By the Riemann-Roch Theorem

$$l(K - E + (\mu + 2b_I - 1)P) = l(E - (\mu + 2b_I - 1)P) - \deg(E) + (\mu + 2b_I - 1)\deg(P) + g - 1.$$ 

Hence by the above and the definitions $t$ and the Clifford defect $s$, we have

$$\deg(E^*) \geq \frac{(\deg(E) - (\mu + 2b_I - 1)P)/2 - s + 1}{\deg(E) + (\mu + 2b_I - 1)\deg(P) + g - 1} \geq t - \deg(E) + 2g - 2 + (\mu + b_I)\deg(P) + 1 = \deg(E^*) + 1,$$

which is a contradiction. \(\square\)

**Theorem 4.6 (Decoding Theorem)** Let $x \in \mathbb{F}^n$ with $x = c + e$, where $c$ is a code word of $C_\Omega(D, E - \mu P)$ and $e$ is an error vector. Let $\eta$ be given by Theorem 4.4. Then

**Existence:** There exists a valid solution $(f, r)$ of the key congruence of $x$ with respect to $(D, E, P)$, such that

$$\frac{r}{f} \eta \in \Omega(-D - \mu P) \quad \text{and} \quad \alpha_\Omega(\frac{r}{f} \eta) = e.$$ 

**Uniqueness:** Let $t = (d^* - \deg(P))/2 - s$, where $d^*$ is the designed minimum distance and $s$ is Clifford defect of this code. Suppose $wt(e) \leq t$. If $(f, r)$ is a minimal valid solution of the key congruence of $x$ with respect to $(D, E, P)$, then

$$\frac{r}{f} \eta \in \Omega(-D - \mu P) \quad \text{and} \quad \alpha_\Omega(\frac{r}{f} \eta) = e.$$
Proof. Let \( I = \{ i | e_i \neq 0, 1 \leq i \leq n \} \), where \((e_1, \ldots, e_n) = e\).

Existence: The vector space of differentials on \( X \) is one dimensional over \( \mathbb{F}(X) \), so \( \eta \) is a basis of \( \Omega \). Hence for every \( i \in \{1, \ldots, n\} \), there exists an \( u_i \in \mathbb{F}(X) \) such that \( \varepsilon_i = u_i \eta \), where \( \varepsilon_i \), for \( i = 1, \ldots, n \), are given by Theorem 4.4. Therefore by the definitions of \( \eta \) and \( \varepsilon_i \), one has

1) \( v_R(u_i) = v_R(\varepsilon_i) - v_R(\eta) \geq -l - \mu; \)
2) \( v_P(u_i) = v_P(\varepsilon_i) - v_P(\eta) = \delta_{ij} \), where \( \delta_{ij} = 1 \) if \( i = j \) and 0 otherwise.
3) \( v_R(u_i) = v_R(\varepsilon_i) - v_R(\eta) \geq 0 \), if \( R \notin \{ P_1, \ldots, P_n, P \} \).

Let \( f_0 \) be a nonzero element of \( K_f(P) \), then \( v_R(f_0) \geq 1 \) and therefore \( f_0u_i \in K_\infty(P) \) for every \( i \in I \). Define \( r_0 = f_0 \sum_{i \in I} e_i u_i \). Then \( r_0 \in K_\infty(P) \) and \( (r_0/f_0)\eta = \varepsilon(e) \), so \( \alpha_\Omega((r_0/f_0)\eta) = e \), and also

\[
v_R(r_0) = v_R(f_0) + v_R(\varepsilon(e)) - v_R(\eta) \geq -v_R(\eta),
\]

for all places \( R \) not in \( \{ P_1, \ldots, P_n, P \} \), thus \( r_0 \in K_\infty(P, W) \).

Now by the definition of the syndrome we have

\[
f_0S(x)\eta = f_0 \sum_{i=1}^{n} \frac{h(P_i)}{h(P_i)} \varepsilon_i = f_0\varepsilon(e) + f_0S(\varepsilon)\eta - F \sum_{i \in I} e_i \varepsilon_i = (r_0 + f_0S(\varepsilon) - F \sum_{i \in I} e_i u_i)\eta,
\]

where \( h \in K_\infty(P) \) is given by Theorem 4.4, that is \( h) = E \). Thus \( f_0S(x) \equiv_E r_0 \) (mod \( h \)) since \( S(e) \equiv_0 0 \) (mod \( h \)) by theorem 4.5, and

\[
\deg(r_0) - \deg(f_0) = -v_R(r_0) + v_R(f_0) = -v_R(\varepsilon(e)) + v_R(\eta) \leq l + \mu.
\]

This proves the existence.

Uniqueness: Now \( \omega(t(e)) \leq t \), hence \( \Omega(I) \leq t \). By the assumption we have \( \deg(f) \leq b_I \). Let \( Q = \sum_{i \in I} P_i \). We claim that

\( r\eta - f\varepsilon(e) \in \Omega(E - (\mu + b_I)P - Q) \),

and therefore \( r\eta - f\varepsilon(e) = 0 \), by Proposition 4.4. Thus \( (r/f)\eta = \varepsilon(e) \in \Omega(-D - \mu P) \) and \( \alpha_\Omega((r/f)\eta) = e \).

Now we prove our claim. Let us consider the valuation of \( r\eta - f\varepsilon(e) \) at every place of the curve.

Since \( r \in K_\infty(P, W) \), we have

\[
v_R(r\eta - f\varepsilon(e)) \geq 0
\]

for every \( R \notin \{ P_1, \ldots, P_n, P \} \). Now look at the valuation of \( r\eta - f\varepsilon(e) \) at \( R \) such that \( R \in \text{supp}(E) \). First by the assumption, we have \( v_R(fS(x)\eta - r\eta) \geq v_R(h) \), that is

\[
v_R(r\eta - f\varepsilon(e) - f[S(x)\eta - \varepsilon(e)]) \geq v_R(h).
\]

Moreover, we have

\[
S(x)\eta - \varepsilon(e) = \sum_{i=1}^{n} (x_i - h x_i / h(P_i) - e_i) \varepsilon_i
\]

\[
= \varepsilon(c) - h \sum_{i=1}^{n} x_i / h(P_i) \varepsilon_i.
\]
Hence $v_R(f(S(x)\eta - \varepsilon(e))) \geq v_R(h)$ since $\varepsilon(e) \in \Omega(E - \mu P - D)$. Therefore we can conclude that, for every $R \in \text{supp}(E)$,

$$v_R(r\eta - f\varepsilon(e)) \geq v_R(h).$$

(2)

For the rational points $P_i$, $i = 1, \ldots, n$, we have

$$v_{P_i}(r\eta - f\varepsilon(e)) \geq \begin{cases} -1 & \text{if } i \in I, \\ 0 & \text{if } i \notin I. \end{cases}$$

(3)

At last, we have

$$v_{P}(r\eta - f\varepsilon(e)) = v_{P}(f([r/f]\eta - \varepsilon(e)))$$

$$\geq -\deg(f) + \min\{-\deg(r) + \deg(f) + l, -\mu\}$$

$$\geq -b_I - \mu,$$

(4)

since $\deg(r) - \deg(f) \leq l + \mu$.

Combining (1), (2), (3) and (4) gives

$$r\eta - f\varepsilon(e) \geq E - Q - (b_I + \mu)P,$$

hence $r\eta - f\varepsilon(e) \in \Omega(E - (b_I + \mu)P - Q)$. This proves our claim. □

4.6 Decoding codes isometric with $C_{\Omega}(D, mP)$

In this section we assume that the code length is smaller than the number of rational points, so there exists a rational point $P$ not in $\{P_1, \ldots, P_n\}$. We know that $C_{\Omega}(D, mP)$ is isometric with $C_{\Omega}(D, (h_0) - \mu P)$ for some $h \in K_\infty(P)$. Hence it is sufficient to give a decoding theorem of the code $C_{\Omega}(D, (h_0) - \mu P)$. First let us look at the details of the Clifford defect of this class.

**Proposition 4.15** The Clifford defect $s$ of $((h_0), P)$ is

$$s = \max\{k/2 - l(kP) + 1|0 \leq k \leq 2g - 1\},$$

**Proof.** Since $h \in K_\infty(P)$, hence $(h_0) \sim \deg(h)P$. Therefore $l((h_0) - kP) = l((\deg(h) - k)P)$. Thus by the definition of Clifford defect we immediately have the desired result. □

**Proposition 4.16** Let $H(q)$ be the Hermitian curve over $F = GF(q^2)$ with the function field $F(x, y)$, where $x^{q + 1} = y^q + y$. Let $P$ be the common pole of $x$ and $y$ (for the details of this curve we refer to [72] and Chapter 6). Then the Clifford defect of $((h_0), P)$ is

$$s = \begin{cases} (q - 1)^2/8 + 1/2 & \text{if } q \equiv 1 \pmod{2}; \\ (q - 2)^2/8 + 1/2 & \text{if } q \equiv 0 \pmod{2}. \end{cases}$$

**Proof.** See also Duursma [12]. It is easy to see that the non-gaps of $P$ between 0 to $2g - 1$ are

$$iq + j(q + 1), 0 \leq i \leq q, 0 \leq j \leq q - i - 2,$$
and the gaps of $P$ are $j(q + 1) + 1, \ldots, (j + 1)q - 1, 0 \leq j \leq q - 2$. For the details of this conclusion we refer to Chapter 6. Then we have

$$l((iq + j(q + 1))P) = \frac{(i + j)(i + j + 1)}{2} + j + 1,$$

where $0 \leq i \leq q$ and $0 \leq j \leq q - i - 2$, and

$$l((j(q + 1) + k)P) = l((j + 1)qP) - 1,$$

for $1 \leq k \leq q - j - 1$, where $0 \leq j \leq q - 2$. Let $s(k) = k/2 - l(kP) + 1$. It is easy to prove that

$$s(iq + j(q + 1)) \leq \begin{cases} (q - 1)^2/8 & \text{if } q \equiv 1 \pmod{2}; \\ (q - 2)^2/8 & \text{if } q \equiv 0 \pmod{2}, \end{cases}$$

and the equality holds if

$$(i, j) = \begin{cases} ((q - 1)/2, 0) & \text{if } q \equiv 1 \pmod{2}; \\ ((q - 2)/2, 0) & \text{if } q \equiv 0 \pmod{2}. \end{cases}$$

Furthermore

$$s(j(q + 1) + k) \leq s((j + 1)q) + \frac{1}{2},$$

where $\leq q - j - 1$, and the equality holds if $l = q - j - 1$. Therefore our proposition follows immediately from the above two inequalities.

As a special case of the Decoding Theorem in Section 4.5, the following theorem gives method to decode geometric Goppa codes isometric with $C_G(D, mP)$.

**Theorem 4.7** Let $x \in \mathbb{F}^n$ with $x = c + e$, where $c$ is a code word of $C_G(D, (h)_0 - \mu P)$ and $e$ is an error vector. Let $\eta$ be given by Theorem 4.4. Then

Existence: There exists a valid solution $(f, r)$ of the key equation of $x$ with respect to $(D, (h)_0, P)$, such that

$$r \neq \frac{1}{f} \eta \in \Omega(-D - \mu P) \quad \text{and} \quad \alpha(t^{r/f} \eta) = e.$$

Uniqueness: Let $t = (d^* - 1)/2 - s$, where $d^*$ is the designed minimum distance and $s$ is Clifford defect of this code. Suppose $\omega(t(e)) \leq t$. If $(f, r)$ is a minimal valid solution of the key equation of $x$ with respect to $(D, (h)_0, P)$, then

$$r \neq \frac{1}{f} \eta \in \Omega(-D - \mu P) \quad \text{and} \quad \alpha(t^{r/f} \eta) = e.$$

**Proof.** By using the Lemma 4.5, this theorem is a special case of Theorem 4.6, since $\deg(P) = 1$. □

**Remark 4.11** By the above theorem, we see that we can decode $C_G(D, mP)$ if we can solve the key equation. In Chapter 5, we will give an algorithm for solving the key equation using the subresultant sequence, a generalization of the Euclidean algorithm, so that the algorithm can correct up to $(d^* - 1)/2 - s$ errors with complexity $O(n^3)$. In Chapter 6, for the Hermitian curves $H(q)$ we will give a more efficient algorithm for solving the key equation, which is a generalization of the Berlekamp-Massey decoding algorithm.
4.7 This method may not correct more than \((d^* - 1)/2 - s\) errors

Let \(\mathcal{H}(3)\) be the Hermitian curve \(U^4 + V^4 + W^4 = 0\) over \(F = GF(9)\). Then the function field of \(\mathcal{H}(3)\) is \(F(x, y)\), where the defining equation is \(x^4 = y^3 + y\). The genus of this curve is 3, see \([72]\). Let \(\alpha\) be a primitive element of \(GF(9)\) such that

\[
\alpha^2 = \alpha + 1, \quad \alpha^3 = 2\alpha + 1, \quad \alpha^4 = 2\alpha, \quad \alpha^5 = 2\alpha, \quad \alpha^6 = 2\alpha + 2, \quad \alpha^7 = \alpha + 2, \quad \alpha^8 = 1.
\]

All the rational points of \(\mathcal{H}\) are the following,

(1) a point at infinity \(P\) and

(2)

\[
\begin{align*}
P_0 &= (0, 0), & P_1 &= (\alpha, 1), & P_2 &= (\alpha^3, 1), & P_3 &= (\alpha^5, 1), & P_4 &= (\alpha^7, 1) \\
P_5 &= (\alpha^2, \alpha), & P_6 &= (2, \alpha), & P_7 &= (\alpha^6, \alpha), & P_8 &= (1, \alpha), & P_9 &= (0, \alpha^2), \\
P_{10} &= (\alpha^2, \alpha^3), & P_{11} &= (2, \alpha^3), & P_{12} &= (\alpha^6, \alpha^3), & P_{13} &= (1, \alpha^3), & P_{14} &= (\alpha^2, 2), \\
P_{15} &= (2, 2), & P_{16} &= (\alpha^6, 2), & P_{17} &= (1, 2), & P_{18} &= (\alpha, \alpha^5), & P_{19} &= (\alpha^3, \alpha^5), \\
P_{20} &= (\alpha^5, \alpha^3), & P_{21} &= (\alpha^7, \alpha^3), & P_{22} &= (0, \alpha^3), & P_{23} &= (\alpha, \alpha^7), & P_{24} &= (\alpha^3, \alpha^7), \\
P_{25} &= (\alpha^5, \alpha^7), & P_{26} &= (\alpha^7, \alpha^7),
\end{align*}
\]

and \(K_\infty(P) = F[x, y]\), for the details we refer to \([72]\) and Chapter 6.

Let \(D = \sum_{i=1}^{26} P_i\) and \(E = (y^4)_0 = 16P_0\). In this section we will consider the code \(C_\Omega(D, E - P)\) which is isometric to the code \(C_\Omega(D, 15P)\). Denote \(P_i = (\alpha_i, \beta_i)\) for \(i = 1, \ldots, 26\), then we have \((\varepsilon_i)_\infty = P_i + P\) and \(\omega = \sum_{i=1}^{26} \text{res}_{P_i}(\omega) \varepsilon_i\) for every \(\omega \in C_\Omega(D, E - P)\). Let \(\eta = dx\). Hence the syndrome of \(x \in \mathbb{F}^{26}\) (see Chapter 6 for detail) is

\[
S(x) = \sum_{i=1}^{26} x_i \beta_i^{-1} \left( \sum_{k=0}^{3} \sum_{j=0}^{3} \alpha_k \beta_j \alpha^{3-k} \beta^{3-j} \right) + \sum_{k=0}^{1} \sum_{\nu=0}^{k} \alpha_k^{k+2} \beta_\nu \beta^{3-\nu} x^{1-k} y^\nu \pmod{y^4}.
\]

By Theorem 4.3 and Proposition 4.16, we know that the designed minimum distance is \(d^* = 11\) and the Clifford defect is 1. Therefore one can correct up to 4 errors by solving the key equation, see Theorem 4.7. The following example shows that one cannot always correct 5, which is equal to \((d^* - 1)/2\), errors.

**Example 4.8** Suppose the error vector \(e\) has nonzero values at the locations \(P_1, P_2, P_3, P_4\) and \(P_5\) (for the reason of this choice we refer to \([12, \text{Proposition 5}]\)), hence we can suppose the received word is \(x = (1111000010 \cdots 0)\). Then the syndrome of \(x\) is

\[
S(x) = \sum_{i=1}^{4} \left( \sum_{k=0}^{3} \sum_{j=0}^{3} \alpha_k \beta_j \alpha^{3-k} \beta^{3-j} + \sum_{k=0}^{1} \sum_{\nu=0}^{k} \alpha_k^{k+2} \beta_\nu \beta^{3-\nu} \right) x^{1-k} y^\nu + x^3 y^3 + \alpha^3 x^3 y^2 + \alpha^4 x^3 y + \alpha^5 x^3 \pmod{y^4} = 2x^3 y^3 + \alpha^7 x^3 y^2 + 2\alpha x^3 \pmod{y^4}.
\]
Furthermore we have
\[ xS(x) \equiv (y^3 + y)(2y^3 + \alpha^7y^2 + 2\alpha) \pmod{y^4} \]
\[ \equiv 2y^3 + 2\alpha y \pmod{y^4}; \]  
(6)
\[ yS(x) \equiv (\alpha^7x^3y^3 + 2\alpha x^3y) \pmod{y^4}; \]  
(7)
\[ x^2S(x) \equiv 2xy^3 + 2\alpha xy \pmod{y^4}; \]
(8)
and
\[ xyS(x) \equiv 2\alpha y^2 \pmod{y^4}. \]  
(9)

Now let \( f = Ax^2 + By + Cx + D \neq 0 \), where \( A, B, C, D \in GF(9) \). Then
\[ fS(x) \equiv B\alpha^7x^3y^3 + 2x^3y + 2Axy^3 + 2xy + 2Cy^3 + \\
+2y + 2Dx^3y^3 + \alpha^7Dx^3y^2 + 2x^3 \pmod{y^4} \]
by (5),(6),(7),(8) and (9). Therefore, if there exists an \( r \in K_\infty(P) \) such that
\[ fS(x) \equiv r \pmod{y^4} \]  
and \( \deg(r) - \deg(f) \leq 2g - 1 \),
then \( A = B = C = D = 0 \), which is a contradiction to \( f \neq 0 \).

Hence the minimal degree of \( f \) which satisfies \( \deg(fS(x) \pmod{y^4}) - \deg(f) \leq 2g - 1 = 5 \) is at least 7. But there exist at least two independent solutions, namely \( f_1 = xy \) and \( f_2 = xy - x \), where
\[ f_1S(x) \equiv 2\alpha y^2 \pmod{y^4} \]  
and \( f_2S(x) \equiv y^3 + 2\alpha y^2 + \alpha y \pmod{y^4} \).
Moreover, let \( r_1 = 2\alpha y^2 \), then \( \text{res}_{P_1}(r_1dx/f_1), \ldots, \text{res}_{P_{26}}(r_1dx/f_1) \neq e \).
Hence, we conclude that by finding a minimal valid solution of the key equation, in particular by using the subresultant sequence, we may not get the right error vector \( e \) when \( \text{wt}(e) > (d^* - 1)/2 - s \).
Chapter 5

Solving a Congruence on a Graded Algebra

In this chapter, we will use a subresultant sequence to solve for $a$ and $b$ the congruence $af \equiv b \pmod{g}$ such that $\deg(b) - \deg(a)$ is less than a given integer and $a$ has the minimal degree among all such solutions, where $a, b, f$ and $g$ are elements of a non-Euclidean graded algebra. By using this result, we show how the decoding algorithm given by Chapter 4 is fulfilled.

In Section 5.1, we give definitions of $\Gamma$-graded algebra, $\Gamma$-basis and a minimal valid solution of a congruence, respectively. In Section 5.2, we construct a subresultant sequence of two elements of $\Gamma$-graded algebra. In Section 5.3, we show how to find a minimal valid solution for a congruence by using a subresultant sequence. We also give an algorithm to do this. Section 5.4 calculates the complexity of the algorithm. Finally, we show in Section 5.5 how to use the algorithm to decode geometric Goppa codes. In Section 5.6, a decoding example is given, which is also a counter-example to the method given by Porter [57].

5.1 Graded algebra and a minimal valid solution of a congruence

The following definition is a special case of the definition of a graded ring [30, p.9] and [52, pp.113f].

Definition 5.1 Let $K$ be an algebra over a field $F$. Let $\Gamma$ be a submonoid of $\mathbb{N}$. If

$$K = \bigoplus_{\gamma \in \Gamma} K^\gamma$$

and $K^\gamma K^{\gamma'} \subseteq K^{\gamma + \gamma'}$, where $K^\gamma$ is a subgroup of the additive group of $K$, then we call $K$ a $\Gamma$-graded algebra and $\Gamma$ a grading monoid. In other words, any non-zero element $f \in K$ has a unique decomposition $f = \sum_{\gamma \in \Gamma} f_\gamma$, $f_\gamma \in K^\gamma$ and $f_\gamma \neq 0$, see also [51]. Therefore there is a degree map defined by $\deg(f) = \gamma$ such that $\deg(fg) = \deg(f) + \deg(g)$.

Definition 5.2 We say that a linearly independent set $B$ of $K$ is a $\Gamma$-basis of $K$, if and only if 1) there is a bijective map from $B$ to $\Gamma$ such that $\Gamma = \{\deg(f)|f \in B\}$, 2) any $f \in K$ has a $\Gamma$-representation

$$f = \sum_{i=1}^{r} \alpha_i f_i, \quad \alpha_i \in F, f_i \in B, i = 1, \ldots, r,$$
such that deg(f) ≥ deg(f_{i+1}) ≥ deg(f_i) for i = 1, ..., r - 1. In [51], the definition of a Γ-basis is given for a finitely generated module.

**Remark 5.1** The following properties can be easily proved by the definition of a Γ-graded algebra.

1. deg(α) = 0 if α ∈ F^* (by using [52, Theorem 21,p.114]);
2. Let f, g ∈ K. deg(f + g) ≤ max{deg(f), deg(g)}, moreover, if deg(f) > deg(g) then deg(f + g) = deg(f).

Furthermore, suppose f_1, ..., f_n ∈ K such that deg(f_1), ..., deg(f_n) are mutually different. Then deg(f_1 + · · · + f_n) = max{deg(f_i)}.

For convenience we will define deg(f) = -∞ if f = 0.

**Example 5.1** Let K = F[X] be a polynomial ring. Then it is an N-graded algebra with an N-basis {X^i|i ∈ N}. Here the grading monoid is the whole set of nonnegative integers. Furthermore, K is a Euclidean domain, so one can use Euclid’s algorithm on F[X].

**Example 5.2** Let K∞(P) be defined as in Definition 4.1 of Chapter 4. Then it is also a Γ-graded algebra with a Γ-basis (see Proposition 5.5 in Section 5.5), where Γ ⊆ N. But Γ ≠ N if the genus of the curve is not zero. In fact Γ is the set of all non Weierstrass gaps (see Definition 4.2). Therefore K∞(P) is not a Euclidean domain (see Remark 4.3).

**Proposition 5.1** Suppose K is a Γ-graded algebra over a field F, where Γ ⊆ N. Then the following statements are equivalent:

1. For two elements f, g ∈ K, if deg(f) = deg(g) = n, then there exists an α ∈ F such that deg(f - αg) < n;
2. K has a Γ-basis.

**Proof.** (1)→(2) For every i ∈ Γ, choose an element ψ_i from K of degree i. In particular, if i = 0 then choose ψ_0 = 1. We claim B := {ψ_i|i ∈ Γ} is a Γ-basis of K. Obviously the first condition for a Γ-basis is satisfied. Now we use induction on deg(f) to prove the second condition.

1°) If f = 0, then it is obvious.

2°) If deg(f) = k ∈ Γ, then there exists an element α ∈ F such that deg(f - αψ_k) < k by the assumption. That means that either (i) f - αψ_k = 0, or (ii) deg(f - αψ_k) = l ∈ Γ for some l < k. In case (i), take a_k = α so that f = a_kψ_k; In case (ii), by the induction hypothesis there exists an (a_0, ..., a_l) ∈ F^{l+1} such that f - αψ_k = ∑_{i=0}^{l} a_i ψ_i. Now take a_i = a_i for i = 0, ..., l, and a_i = 0 for i = l + 1, ..., k - 1 and a_k = α; then f = ∑_{i=0}^{k} a_i ψ_i.

Now we prove the independence of B. Assume there exist k elements of B, namely ψ_{i_1}, ..., ψ_{i_k}, such that ∑_{j=1}^{k} a_j ψ_{i_j} = 0, where (a_1, ..., a_k) ∈ F^k is a nonzero vector. Then by Remark 5.1, we have

-∞ = deg(0) = deg(∑_{j=1}^{k} a_j ψ_{i_j}) = max{i_j|j ∈ {1, ..., k} and a_j ≠ 0},

which is a contradiction. Therefore B is a Γ-basis of K.

(2)→(1) is trivial. □

In the following, we always denote by K a Γ-graded algebra as defined in Definition 5.1, and by L a nonzero ideal of K. Moreover, we define Γ_L = {deg(f)|f ∈ L}.
Chapter 5: Solving a Congruence on a Graded Algebra

Remark 5.2 It is easy to prove that $\Gamma_L$ is also a submonoid of $\mathbb{N}$ and the statement (1) of Proposition 5.1 is satisfied in $L$. Therefore there is a $\Gamma_L$-basis $B_L$ for $L$. Moreover we can find a $\Gamma$-basis $B$ for $K$ such that $B_L \subseteq B$ (this can be easily proved by a method similar to the proof of Proposition 5.1). Furthermore, for $n \in \Gamma$ and $m \in \Gamma_L$, we have $m + n \in \Gamma_L$.

Definition 5.3 Let $f \in L$ and $g \in K$. Let $s$ be a positive integer. If $0 \neq p \in K$ and $r \in L$ is a solution of the congruence $pf \equiv r \pmod{g}$ such that $\text{deg}(r) - \text{deg}(p) \leq s$, then we say that $(p, r)$ is a valid solution of $(f, g, s)$. A minimal valid solution $(p, r)$ of $(f, g, s)$ such that $\text{deg}(p) \leq \text{deg}(p')$ for all valid solutions $(p', r')$ of $(f, g, s)$.

To find a minimal valid solution of a congruence is the core of this chapter. The next two sections will be devoted to this problem. For convenience of the discussion we give some notations in the rest of this section. Firstly, we denote $\{\text{deg}(f)\mid f \in K\}$ and $\{\text{deg}(f)\mid f \in L\}$ by $\{m_i\mid i = 0, 1, \ldots \}$ and $\{n_i\mid i = 0, 1, \ldots \}$, respectively, where $n_i < n_j$ and $m_i < m_j$ if $i < j$.

Definition 5.4 Let $f \in L$ and $g \in K$ such that $\text{deg}(f) > 0$ and $\text{deg}(g) > 0$. Define $I(f, g) = \{k \in \mathbb{N} \mid m - k - 1 \in \Gamma$ and $n - k - 1 \in \Gamma_L\}$.

Then for every $k \in I(f, g)$, there exist $u_k, v_k, w_k \in \mathbb{N}$ such that $m - k - 1 = m_{u_k}$, $n - k - 1 = n_{w_k}$, $m + n - k - 1 = n_{u_k}$, where $m_{u_k} \in \Gamma$ and $n_{w_k}, n_{u_k} \in \Gamma_L$. Now denote $\{(u_k, v_k, w_k) \in \mathbb{N}^3 \mid k \in I(f, g)\}$ by $U(f, g)$.

Suppose $\#I(f, g) = l \neq 0$. Enumerate $I(f, g)$ by the decreasing sequence $k_1, \ldots, k_l$, that is $I(f, g) = \{k_1, \ldots, k_l\}$, where $k_i > k_{i+1}$ for $i = 1, \ldots, l - 1$. Then we denote $(u_{k_i}, v_{k_i}, w_{k_i})$ by $(u(i), v(i), w(i))$ for every $i \in \{1, \ldots, l\}$.

Remark 5.3 By the definition of $u(i), v(i)$ and $w(i)$, respectively, we immediately have $0 \leq u(1) < \cdots < u(l)$, $0 \leq v(1) < \cdots < v(l)$ and $0 \leq w(1) < \cdots < w(l)$ respectively.

Lemma 5.1 \{m_j + n|u(i) + 1| + 1 \leq j \leq u(i + 1)\} \cap \{n_j + m|v(i) + 1| + 1 \leq j < v(i + 1)\} = \emptyset, \text{ where } 0 \leq i < l.$

Proof. Suppose there exist some $j_1$ and $j_2$ with $u(i) + 1 \leq j_1 \leq u(i + 1)$ and $v(i) + 1 \leq j_2 < v(i + 1)$ respectively, such that $m_{j_1} + n = n_{j_2} + m$. By this assumption we also have $n > n_{j_2}$ and $m > m_{j_1}$. Now take $k = n - n_{j_2} - 1 = m - m_{j_1} - 1$, then $k \in I(f, g)$. So $k = k_j$ for some $j \in \{1, \ldots, l\}$. Hence $n_{j_2} = n - k_j - 1 = n_{v(i)}$ by the definition, thus $v(i) < j_2 = v(j) < v(i + 1)$, this implies that $k_i > k_j > k_{i+1}$ which is a contradiction. $\Box$

Definition 5.5 Let the assumption be as in Definition 5.4. For every $k_i \in I(f, g)$, define $P_i(f, g) = \{(p, r) \in K \times L \mid r \equiv pf \pmod{g}, \text{deg}(p) = m_{u(i)} \text{ and } \text{deg}(r) < n_{w(i)}\},$ and $J_i(f, g) = \{\text{deg}(r)|(p, r) \in P_i(f, g)\}$.

In the following section we shall construct a subresultant sequence $\{sre_i(f, g)\}$. Then in Section 5.3, we shall prove that $P_i(f, g)$ contains a minimal valid solution $(p, r)$ of $(f, g, s)$, such that $r = sre_i(f, g)$ and $\text{deg}(r) = \min J_i(f, g)$.
5.2 The construction of a subresultant sequence

Let $K$ be a $\Gamma$-graded algebra over $F$, such that $\Gamma \subseteq \mathbb{N}$ and there exists a $\Gamma$-basis. Let $L$ be a nonzero ideal of $K$, therefore $L$ is a $\Gamma_L$-graded algebra. Let $B_L := \{ \psi_i | i \in \mathbb{N}, \deg(\psi_i) = n_i \in \Gamma_L \}$ be a $\Gamma_L$-basis of $L$ such that $\psi_0 = 1$ if $n_0 = 0$, and $B := \{ \varphi_i | i \in \mathbb{N}, \deg(\varphi_i) = m_i \in \Gamma \}$ be a $\Gamma$-basis of $K$, such that $\varphi_0 = 1$ and $\varphi_i = \psi_i$ if $m_i \in \Gamma_L$.

Let $f \in L$ with $\deg(f) = n > 0$ and $g \in K$ with $\deg(g) = m > 0$. Then we have two sets $I(f, g)$ and $U(f, g)$ defined in Section 5.1. In the following we shall define the resultant matrix of $f, g$ at every $k \in I(f, g)$.

**Definition 5.6** Let $k \in I(f, g)$ and denote $(u, v, w) := (u_k, v_k, w_k) \in U(f, g)$. Suppose $\varphi_i f = \sum_{j=0}^{u} a_{ij} \psi_j$ for $i = 0, \ldots, u$, where $a_{ij} = 0$ if $n_j > \deg(\varphi_i f)$, and $\psi_j g = \sum_{j=0}^{v} b_{ij} \psi_j$ for $i = 0, \ldots, v$, where $b_{ij} = 0$ if $n_i > \deg(\psi_j g)$. Define an $(u + v + 2) \times (w + 1)$ matrix $M(f, g; k)$ by:

\[
\begin{bmatrix}
\varphi_u f & \psi_w & \cdots & \psi_1 & \psi_0 \\
\varphi_0 g & & & \cdots & \\
\varphi_v g & & & \cdots & \\
\end{bmatrix}
\]

That is, the entry in the row corresponding to $\varphi_i f$ and the column corresponding to $\psi_j$ is $a_{ij}$; the entry in the row corresponding to $\psi_j g$ and the column corresponding to $\varphi_i$ is $b_{ij}$. We call this matrix a resultant matrix of $f$ and $g$ at $k$. The row vector corresponding to $\varphi_i f$ ($\psi_j g$) is called the coefficients representation of $\varphi_i f$ ($\psi_j g$).

The degree of the column corresponding to $\psi_j$ is defined by $\deg(\psi_j) = n_j$. For convenience, sometimes we also denote $M(f, g; k)$ as follows

\[M(f, g; k) = (\alpha_u \alpha_{u-1} \cdots \alpha_0),\]

where $\alpha_i$ is a column vector.

Now we have a sequence of resultant matrices, namely $M(f, g; k_1), \ldots, M(f, g; k_t)$ for $I(f, g) = \{k_1, \ldots, k_t\}$. We abbreviate them by $M_1, \ldots, M_t$, if it is clear which $f, g$ are meant.

By using resultant matrices we shall construct a subresultant sequence in the rest of this section. First we will study a resultant matrix in detail. In the following, the number of rows and the number of columns of matrix $M$ are denoted by $r(M)$ and $c(M)$, respectively.

**Corollary 5.1** $c(M(f, g; k)) \geq r(M(f, g; k))$.

**Proof.** By the definition of $M(f, g; k)$, we have

\[c(M(f, g; k)) = \#(\Gamma_L \cap \{0, \ldots, n + m - k - 1\}),\]

and

\[r(M(f, g; k)) = \#(\psi_0 g, \ldots, \psi_v g) + \#(\varphi_u f, \ldots, \varphi_0 f)\]

\[\leq \#(\Gamma_L \cap \{0, \ldots, n - k - 1\}) + \#(\Gamma_L \cap \{n, \ldots, n + m - k - 1\}).\]

Hence $c(M(f, g; k)) \geq r(M(f, g; k))$ since $n - 1 \geq n - k - 1$. \(\square\)
Definition 5.7 Let

\[ D(M(f, g; k)) = \{ \text{all the degrees of the columns in } M(f, g; k) \}. \]

If \( I \subseteq D(M(f, g; k)) \), then let \( M(f, g; k)[I] \) be the submatrix of \( M(f, g; k) \) consisting of those columns of \( M(f, g; k) \) which have their degrees in \( I \). The degree of a column in \( M(f, g; k)[I] \) is defined as the degree of the the same column in \( M(f, g; k) \).

Definition 5.8 Let \( I \) be a subset of \( D(M(f, g; k)) \) such that \( \#(I) = r(M(f, g; k)) - 1 \). For every \( n_i \in D(M(f, g; k)) \setminus I \), define a square matrix

\[ M(f, g; k)[I](i) = (M(f, g; k)[I], \alpha_i), \]

where \( \alpha_i \) is the column of degree \( n_i \) in \( M(f, g; k) \). The determinant element of \( M(f, g; k) \) with respect to \( I \) is defined by

\[ \text{detel}(M(f, g; k), I) = \sum_{n_i \in D(M(f, g; k)) \setminus I} \text{det}(M(f, g; k)[I](i)) \psi_i, \]

where \( \text{det}(M) \) is the determinant of a square matrix \( M \). We call this element a subresultant with respect to \( I \).

Lemma 5.2 Let \( X \) be a \( r(M(f, g; k)) \times r(M(f, g; k)) \) nonsingular matrix over \( F \), then

\[ \text{detel}(M(f, g; k), I) = \frac{1}{\text{det}(X)} \text{det}(XM(f, g; k), I). \]

Proof. The proof follows immediately from the identity \( \text{det}(XM) = \text{det}(X) \text{det}(M) \), for two square matrices \( X \) and \( M \) of the same size. \( \Box \)

In the following, we will first define a set \( I_i \) for every \( M(f, g, k_i) \). Then for this particular \( I_i \) we define the \( i \)th subresultant of \( f \) and \( g \) by using Definition 5.8.

Definition 5.9 For every \( i \in \{1, \ldots, \#(I(f, g))\} \), we have \( (u(i), v(i), w(i)) \) defined by Definition 5.4 and resultant matrix \( M_i \). Now define \( I_i \) as follows:

1°: for \( i = 1 \) define \( I_1 = \{ m_{u(1)} + n, \ldots, m_0 + n, n_0 + m, \ldots, n_{u(1)-1} + m \} \).

2°: for \( i > 1 \), suppose \( I_{i-1} \subseteq D(M_{i-1}) \) has been defined, such that \( \#(I_{i-1}) \neq 0 \) and its degree is equal to \( n_{t(i-1)} \), moreover,

\[ \#(I_{i-1}) = r(M_{i-1}) - 1. \]

Define \( I_i = A_i \cup I_{i-1} \cup \{ n_{t(i-1)} \} \), where

\[ A_i = \{ m_j + n|u(i-1) + 1 \leq j \leq u(i) \} \cup \{ n_j + m|v(i-1) + 1 \leq j \leq v(i) - 1 \}. \]

Furthermore if there exists a \( j \leq l \) such that \( I_j \) is defined and

\[ \text{detel}(M_j, I_j) = 0 \text{ but } \text{detel}(M_{j-1}, I_{j-1}) \neq 0, \]

then define \( i(f, g) := j \), otherwise define \( i(f, g) := l \).

Lemma 5.3 For every \( i \in \{1, \ldots, i(f, g)\} \), \( I_i \subseteq D(M_i) \) and \( \#(I_i) = r(M_i) - 1. \)
Proof. By the definition of $I_1$ and Lemma 5.1, we immediately have $\#(I_1) = u(1) + v(1) + 1 = r(M_1) - 1$ and $I_1 \subseteq \mathcal{D}(M_1)$. Now consider the case $i > 1$. Suppose the lemma is true for $I_{i-1}$. Then for every $n_j \in I_{i-1}$, we have $n_j \leq n_{w(i-1)} = m_{u(i-1)} + n = n_{w(i-1)} + m$. Hence $I_{i-1} \cap A_i = \emptyset$. Moreover, since $\det(M_{i-1}, I_{i-1}) \neq 0$ by $i - 1 < i(f,g)$, we have that the degree of $\det(M_{i-1}, I_{i-1})$, $n_{t(i-1)}$, is not in $I_{i-1}$ and $n_{t(i-1)} \leq n_{w(i-1)}$ by the definition of $M_{i-1}$. Hence $n_{t(i-1)} \notin A_i$. Thus

$$\#(I_i) = \#(A_i) + \#(I_{i-1}) + 1 = u(i) + v(i) + 1 = r(M_i) - 1$$

by Lemma 5.1. Furthermore, we have $I_i \subseteq \mathcal{D}(M_i)$, since $\mathcal{D}(M_{i-1}) \subseteq \mathcal{D}(M_i)$, $A_i \subseteq \mathcal{D}(M_i)$ and $n_{t(i-1)} \in \mathcal{D}(M_{i-1})$. \[\square\]

**Lemma 5.4** Let $u(0) = -1$ and $v(0) = -1$. Then for $i \geq 0$, the rows corresponding to

$$\varphi_{u(i+1)}f, \ldots, \varphi_{u(i)+1}f, \psi_{v(i)+1}g, \ldots, \psi_{v(i+1)-1}g$$

in $M_{i+1}[A_{i+1}]$ are linearly independent, where $A_{i+1}$ is defined by Definition 5.9.

**Proof.** Suppose $\alpha_i f = \sum_{j=0}^{u(i)} a_{ij} \psi_j$ for $u(i) + 1 \leq l \leq u(i) + 1$ and $\psi_i g = \sum_{j=0}^{v(i)} b_{ij} \psi_j$, for $v(i) + 1 \leq l \leq v(i) + 1 - 1$. If the lemma is not true, then by Definition 5.6 there exist $u(i+1) = u(i) + v(i+1) - v(i) - 1$ elements of $F$, namely $\alpha_{u(i)+1}, \ldots, \alpha_{u(i)+1}$, $\beta_{v(i)+1}, \ldots, \beta_{v(i)+1}$ which are not all zero, such that

$$u(i+1) \sum_{l=u(i)+1}^{v(i)+1} \alpha_l a_{il} + \sum_{l=v(i)+1}^{v(i+1)} \beta_l b_{il} = 0$$

for all $n_j \in A_{i+1}$. Thus

$$u(i+1) \sum_{l=u(i)+1}^{v(i)+1} \alpha_l \varphi_l f + \sum_{l=v(i)+1}^{v(i+1)} \beta_l \psi_l g = \sum_{n_j \in \mathcal{D}(M_{i+1}) \setminus A_{i+1}} \left( \sum_{l=u(i)+1}^{u(i+1)} \alpha_l a_{il} + \sum_{l=v(i)+1}^{v(i+1)} \beta_l b_{il} \right) \psi_j.$$  

Hence the degree of $\sum_{l=u(i)+1}^{v(i+1)} \alpha_l \varphi_l f + \sum_{l=v(i)+1}^{v(i+1)} \beta_l \psi_l g$ is not in $A_{i+1}$. On the other hand, if we define

$$J_1 = \{ m_j + n | u(i) + 1 \leq j \leq u(i) + 1 \text{ and } \alpha_j \neq 0 \},$$

$$J_2 = \{ n_j + m | v(i) + 1 \leq j \leq v(i) + 1 - 1 \text{ and } \beta_j \neq 0 \},$$

then $J_1 \cup J_2 \subseteq A_{i+1}$. Hence

$$\deg\left( \sum_{l=u(i)+1}^{u(i+1)} \alpha_l \varphi_l f + \sum_{l=v(i)+1}^{v(i+1)} \beta_l \psi_l g \right) = \max(J_1 \cup J_2) \in A_{i+1}$$

by Lemma 5.1 and Remark 5.1, which is a contradiction. This proves the lemma. \[\square\]

**Proposition 5.2** For every $i \in \{1, \ldots, i(f,g)\}$, the first $u(i) + v(i) + 1$ rows of $M_i[I_i]$ are linear independent, and the same hold for the last $u(i) + v(i) + 1$ rows of $M_i[I_i]$, where $I_i$ is defined by Definition 5.9.
Proof. We prove the first part of the proposition by induction on $i$. The second part goes similarly.

1°) Since $I_1 = \{m_{u(1)} + n, \ldots, m_0 + n, n_0 + m, \ldots, n_{v(1) - 1} + m\}$ and all the rows in $M_1[I_1]$, except the last row, are the coefficients representations of $\varphi_{u(1)}f, \varphi_{0}f, \psi_{0}g, \ldots, \psi_{v(1) - 1}g$ respectively, so they are linearly independent by Lemma 5.4.

2°) By the definition of $M_{i+1}[I_{i+1}]$, we can write

$$M_{i+1}[I_{i+1}] = \begin{pmatrix} Z_1 & X \\ \emptyset & M_i[I_i](t(i)) \\ Z_2 & Y \end{pmatrix},$$

where the set of all degrees of columns in $Z_j$ ($j = 1, 2$) is $A_{i+1}$, the set of all degrees of the columns in $X$ is $I_i \cup \{n_{u(0)}\}$. Furthermore the rows in $Z_1$ together with the rows in $Z_2$, except the last one, correspond to

$\varphi_{u(i+1)}f, \ldots, \varphi_{u(i+1)}f, \psi_{v(i+1)}g, \ldots, \psi_{v(i+1)}g,$

hence they are linearly independent by Lemma 5.4. Thus the first $u(i+1) - u(i)$ rows and the last $v(i+1) - v(i)$ rows, except the row corresponding to $\psi_{v(i+1)}g$, in $M_{i+1}[I_{i+1}]$ are linearly independent and none of them can be a linear combination of the rows corresponding to the rows in $M_i[I_i](t(i))$. Now the rows in $M_{i+1}[I_{i+1}]$ corresponding to the rows of $M_i[I_i](t(i))$ are linearly independent, since $M_i[I_i](t(i))$ is a nonsingular matrix. Therefore all the rows, except the last row which corresponds to $\psi_{v(i+1)}g$, are linearly independent. $\square$

Corollary 5.2 \( \text{rank}(M_i[I_i]) = r(M_i[I_i]) - 1 = c(M_i[I_i]) \) for $i = 1, \ldots, i(f, g)$.

Proof. By Lemma 5.3 and Proposition 5.2, we have

$$\text{rank}(M_i[I_i]) \geq r(M_i[I_i]) - 1 = r(M_i) - 1 = \#(I_i) = c(M_i[I_i]),$$

thus equality holds. $\square$

Definition 5.10 For every $1 \leq i \leq i(f, g)$, the $i^{th}$ subresultant of $f$ and $g$ is defined by

$$\text{sre}_i(f, g) = \text{det}(M_i, I_i).$$

We call $\text{sre}_1(f, g), \ldots, \text{sre}_{i(f, g)}(f, g)$ a subresultant sequence of $f$ and $g$

5.3 Solving for a minimal valid solution of a congruence

Let a $\Gamma$-graded algebra $K$ over $\mathbb{F}$ be defined as in Definition 5.1 and with a $\Gamma$ basis $B$. Let $L$ be its nonzero ideal. Let $f \in L$ and $g \in K$ with $\text{deg}(f) = m$ and $\text{deg}(g) = n$. Then we have sets $I(f, g)$ and $U(f, g)$, and have $P_i(f, g)$ and $J_i(f, g)$ for every $k_i \in I(f, g)$ defined in Section 5.1, moreover we have a subresultant sequence $\{\text{sre}_i(f, g)\}_{i=1}^{i(f, g)}$. In this section we shall first prove, that for every $i \in \{1, \ldots, i(f, g)\}$, there exists a $p \in K$ such that $(p, \text{sre}_i(f, g)) \in P_i(f, g)$ and $\text{deg}(\text{sre}_i(f, g)) = \min J_i(f, g)$. After that we will give an algorithm to find a minimal valid solution of $(f, g, s)$ by using $\{\text{sre}_i(f, g)\}_{i=1}^{i(f, g)}$. First we need the following notation.
Definition 5.11 Suppose \( f = \sum_{j=0}^{l} a_j \psi_j \in L \) where \( a_j \in F \) for \( 0 \leq j \leq l \). Define the coefficient support of \( f \) by

\[
csupp(f) = \{ n_j = \deg(\psi_j) | a_j \neq 0 \text{ for } 0 \leq j \leq l \}.
\]

Proposition 5.3 For every \( i \in \{1, \ldots, i(f,g)\} \), there exist \( (p_i, r_i) \in P_i(f, g) \) such that \( \text{src}_i(f, g) = r_i \), \( \deg(p_i) = m_{u(i)} \) and \( \deg(\text{src}_i(f, g)) < n_{w(i)} \). Furthermore,

\[
csupp(\text{src}_i(f, g)) \cap I_i = \emptyset,
\]

where \( I_i \) is defined by Definition 5.9.

Proof. By Corollary 5.2, there exists an \( r(M_i[I_i]) \times r(M_i[I_i]) \) nonsingular matrix \( X \) over \( F \) such that

\[
XM_i[I_i] = \begin{pmatrix}
1 & & & \\
1 & \ast & & \\
& \ddots & \ddots & \\
0 & & 1 & \\
0 & & & 0
\end{pmatrix}
\]

(1)

Denote \( u = u(i) \) and \( v = v(i) \) and \( w = w(i) \), and let \( (x_u, \ldots, x_0, y_0, \ldots, y_v) \) be the last row of \( X \). Then \( x_u \neq 0 \) and \( y_v \neq 0 \) by Proposition 5.2. Let \( (z_w, \ldots, z_0) \) be the last row of \( XM_i \). Then we have \( z_j = 0 \) if \( n_j \in I_i \) by (1), and

\[
\sum_{j=0}^{w} z_j \psi_j = \sum_{j=0}^{u} x_j \varphi_j f + \sum_{j=0}^{v} y_j \psi_j g,
\]

by the definition of \( M_i \). Thus

\[
detel(XM_i[I_i]) = \sum_{j=0}^{u} x_j \varphi_j f + \sum_{j=0}^{v} y_j \psi_j g.
\]

That is

\[
\text{src}_i(f, g) = \text{detel}(M_i[I_i]) = \text{detel}(XM_i[I_i]) / \det(X)
\]

\[
= (\sum_{j=0}^{u} x_j \varphi_j f + \sum_{j=0}^{v} y_j \psi_j g) / \det(X),
\]

by Lemma 5.2. Now let \( p_i = (\sum_{j=0}^{u} x_j \varphi_j) / \det(X) \in K \) and \( r_i = (\sum_{j=0}^{w} z_j \psi_j) / \det(X) \) is in \( L \). Then \( \text{src}_i(f, g) = r_i \), and \( \deg(p_i) = m_{u(i)} \) and \( \deg(r_i) < n_{w(i)} \) since \( x_u \neq 0 \) and \( y_v \neq 0 \). Furthermore, by the definition of \( \text{detel}(M_i[I_i]) \), we have \( csupp(\text{src}_i(f, g)) \subseteq D(M_i[I_i]) \cap I_i \), that is \( csupp(\text{src}_i(f, g)) \cap I_i = \emptyset \). \( \square \)

Corollary 5.3 For every \( i \in \{1, \ldots, i(f,g)\} \), if \( n_t \in I_i \), \( n_t \neq n_{u(i)} \), then there exist \( p \in K \) and \( r \in L \) such that \( r \equiv pf \pmod{g} \), and \( \deg(p) < m_{u(i)} \) and \( n_t = \deg(r) \).

Proof. If \( i = 1 \), this is obvious. For \( i > 1 \), suppose the corollary is proved for \( i - 1 \). (i) If \( n_t \in A_i \cup I_{i-1} \setminus \{n_{w(i)}\} \), then by the definition of \( A_i \) and the induction hypothesis, the conclusion is also obvious. (ii) If \( n_t = n_{u(i-1)} = \deg(\text{src}_{i-1}(f, g)) \), then by Proposition 5.3, there exist \( p = p_{i-1} \) and \( r = r_{i-1} \) such that \( n_t = \deg(r) \), where \( \deg(p) = m_{u(i-1)} < m_{u(i)} \). \( \square \)
Lemma 5.5 There exists a pair \((p, r) \in P_i(f, g)\) such that \(\deg(r) = \min J_i(f, g)\) and \(\text{csupp}(r) \cap I_i = \emptyset\).

Proof. By Proposition 5.3, \(P_i(f, g)\) is not empty. Now assume that for every pair \((p, r) \in P_i(f, g)\), if \(\deg(r) = \min J_i(f, g)\), then \(\text{csupp}(r) \cap I_i \neq \emptyset\). Take a pair \((p^*, r^*)\) from \(P_i(f, g)\) with \(\deg(r^*) = \min J_i(f, g)\), such that

\[
\begin{align*}
n_i &:= \max\{\text{csupp}(r^*) \cap I_i\} \\ &\leq \min\{\max\{\text{csupp}(r) \cap I_i\} | (p, r) \in P_i(f, g), \deg(r) = \min J_i(f, g)\}.
\end{align*}
\]

Then \(n_i \leq \deg(r^*)\) so \(n_i < n_{w(i)}\). Hence for such an \(n_i\) there exist \(p^* \in K\) and \(r^* \in L\) with \(\deg(p^*) < m_{w(i)}\), such that \(\deg(r^*) = n_i\) by Corollary 5.3. Now we can write \(r^*, r^* \in L\) as follows:

\[
r^* = \sum_{j=0}^{s} a_j \psi_j \text{ and } r^* = \sum_{j=0}^{t} b_j \psi_j,
\]

where \(a_j \neq 0\) and \(b_i \neq 0\). Now define

\[
p'' = p^* - \frac{a_i}{b_i} p' \text{ and } r'' = r^* - \frac{a_i}{b_i} r'.
\]

Then \((p'', r'') \in P_i(f, g)\) and \(n_i \notin \text{csupp}(r'')\), moreover, since \(\deg(r') \leq \deg(r^*)\), we have \(\deg(r'') \leq \deg(r^*) = \min J_i(f, g)\), that is \(\deg(r'') = \min J_i(f, g)\), since \((p'', r'') \in P_i(f, g)\). Thus by the assumption, we have \(\text{csupp}(r'') \cap I_i \neq \emptyset\), moreover

\[
\max\{\text{csupp}(r'') \cap I_i\} < n_i,
\]

by the definition of \(r''\). This is a contradiction to the definition of \(n_i\). \(\square\)

Proposition 5.4 For every \(i \in \{1, \ldots, i(f, g)\}\), \(\deg(\text{src}_i(f, g)) = \min(J_i(f, g))\).

Proof. By Proposition 5.3, we have \(\text{src}_i(f, g) = r_i\) such that \(r_i \equiv pf \mod g\) and \((p_i, r_i) \in P_i(f, g)\). So \(P_i(f, g) \neq \emptyset\) and \(J_i \neq \emptyset\), for every \(i \in \{1, \ldots, i(f, g)\}\). Hence there exists a pair \((p, r) \in P_i(f, g)\) such that \(\deg(r) = \min J_i(f, g)\) and \(\text{csupp}(r) \cap I_i = \emptyset\) by Lemma 5.5. Suppose \(r = pf + qg\) for some \(q \in L\) and \(\deg(q) = n_{v(i)}\). Now write \(p = \sum_{i=0}^{w(i)} a_i \psi_i\) and \(q = \sum_{i=0}^{v} b_i \psi_i\), respectively, where \(a_w(i) \neq 0\) and \(b_v \neq 0\). Moreover, since \(pf + qg = 0\) or \(\deg(pf + qg) < n_{w(i)} = n_{w(i)} + n\), we conclude that \(n_v + m = m_{w(i)} + n\), that is \(v = v(i)\). Now let \(X\) be a nonsingular matrix such that:

\[
X = \begin{pmatrix}
1 & \cdots & 0 \\
& \ddots & \vdots \\
& \vdots & \ddots & 0 \\
& & & \ddots & 0 \\
& & & & \ddots & 0 \\
& & & & & \ddots & 1 \\
& & & & & & \cdots & 0 \\
0 & a_{u(i)} & \cdots & a_0 & b_0 & \cdots & b_{v(i)-1} & b_{v(i)}
\end{pmatrix}
\]

Multiplying \(X\) by \(M_i\), we see that the last row of \(XM_i[I_i]\) is the coefficient representation of \(r\). Moreover the last row of \((XM_i[I_i])_{k_i}\) is a zero vector since \(r = 0\) or \(\text{csupp}(r) \cap I_i = \emptyset\). Thus \(\det(XM_i[I_i]) = \alpha r\), where \(\alpha = \det(A)\), \(A\) is the nonsingular matrix obtained by deleting the last row of \((XM_i[I_i])\), which is not zero by \(\text{rank}(M_i[I_i]) = \text{rank}(XM_i[I_i]) = c(XM_i[I_i])\) and Corollary 5.2. Thus \(\text{src}_i(f, g) = \alpha r/b_{v(i)}\). Therefore

\[
\deg(\text{src}_i(f, g)) = \deg(r) = \min(J_i(f, g)). \square
\]
Algorithm 5.1:
Step 0: Input \((f,g,s)\);
Step 1: If \(\deg(f) \leq s\) then \(p = 1, r = f\) goto step 7;
Step 2: Compute \(I(f,g) = \{k_1, \ldots, k_i\}\), where \(k_i > k_{i+1}\);
Step 3: \(i = 1\);
Step 4: Compute \(r = \text{sre}_i(f,g)\);
Step 5: if \(\deg(r) - (\deg(g) - k_i - 1) > s\) then \(i = i + 1\) goto step 4;
Step 6: Compute \(p\) and \(q\) such that \(p \in K, q \in L, \deg(p) = \deg(g) - k_i - 1, \deg(q) = \deg(f) - k_i - 1\) and \(pf + qg = r\) (by means of Proposition 5.3);
Step 7: Output \((p,r)\) and stop.

We denote this algorithm by \(A(f,g,s) = (p,r)\).

Remark 5.4 To realize Step 4, we will give an explicit method in Section 5.4 where we compute the complexity of Algorithm 5.1.

Theorem 5.1 Let \(f \in L\) and \(g \in K\) and \(s\) be a positive integer. If there exists a valid solution of \((f,g,s)\), then \(A(f,g,s) = (p,r)\) is a minimal valid solution of \((f,g,s)\).

Proof. Let \(n = \deg(f)\) and \(m = \deg(g)\). If \(n \leq s\), then already \((1,f)\) is a minimal valid solution of \((f,g,s)\). So we may assume \(n > s\). Let \((p',r')\) be a valid solution of \((f,g,s)\). Then there exists a \(q' \in L\) such that \(p'f + q'g = r'\) and \(\deg(r') - \deg(p') \leq s\). Now \(\deg(p') + n = \deg(q') + m\), otherwise

\[
\deg(r') = \max\{\deg(p') + n, \deg(q') + m\} \geq \deg(p') + n \geq \deg(p') + s,
\]

which is a contradiction. Let \(k = n - \deg(q') - 1\). Then \(k = m - \deg(p') - 1\) and \(k \in I(f,g)\). So there exists a \(j\) such that \(1 \leq j \leq \ell\) and \(k = k_j\). For every \(t, 1 \leq t \leq i(f,g)\), there exists a pair \((p_t, r_t)\) such that \(p_t \in K, r_t = \text{sre}_t(f,g)\) and \(\deg(p_t) = m - k_t - 1\), by Proposition 5.3. If \(i(f,g) < j\), then \(r_{i(f,g)}\) is zero and has degree \(-\infty\), so that the algorithm stops at \(i \leq i(f,g)\). If \(j \leq i(f,g)\), then \(\deg(r_j) \leq \deg(r')\), by Proposition 5.4. Hence

\[
\deg(r_j) - \deg(p_j) \leq \deg(r') - \deg(p') \leq s.
\]

So in both cases the algorithm stops at \(i, i \leq j\). Now we claim that \(\deg(p_i) \leq \deg(p')\). Otherwise \(\deg(p_i) > \deg(p')\), so \(n - k_i - 1 > n - k_j - 1\), that is \(k_i < k_j\). Hence \(i > j\) which is a contradiction. Thus \((p_i, r_i)\) is a minimal valid solution of \((f,g,s)\). □

5.4 The complexity of the algorithm

To analyze Algorithm 5.1, we have to give more details about the Step 4 where \(\text{sre}_i(f,g)\) is computed. In the following we will using Gaussian elimination to calculate \(\text{sre}_i(f,g)\).

Definition 5.12 Let \(A = (a_{ij})_{s \times t}\) be a \(s \times t\) matrix over \(F\). A Gaussian elimination is an algorithm which reduces \(A\) to the following form by elementary row operations:

\[
\begin{pmatrix}
\alpha'_{11} & \alpha'_{12} & \cdots & \alpha'_{1s} & \cdots & \alpha'_{1t} \\
0 & \alpha'_{22} & \cdots & \alpha'_{2s} & \cdots & \alpha'_{2t} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \alpha'_{st} & \cdots & \alpha'_{st}
\end{pmatrix}
\]
where we suppose \( t \geq s \). We denote this matrix by \( G(A) \). Furthermore, the complexity of Gaussian elimination of an \( s \times t \) matrix is about \( t^3 \) (suppose \( t \geq s \)). For the details on Gaussian eliminations we refer to [59] and [64].

**Definition 5.13** Let \( M_i \) and \( I_i \) be defined as in Section 5.1. Suppose \( P_i \) is the product of \( \#(I_i) \) elementary matrices, such that \( M_i P_i = (M_i[I_i], *) \), that is \( P_i \) is a column transform which moves the submatrix \( M_i[I_i] \) of \( M_i \) to the front part. A Gaussian elimination of \( M_i \) with respect to \( I_i \) is an algorithm defined by the following steps:

1. Do \( M_i P_i \) (move the submatrix \( M_i[I_i] \) of \( M_i \) to the front by elementary column transformation);
2. Do a Gaussian elimination on \( M_i P_i \) to get \( G(M_i P_i) \);
3. Do \( G(M_i P_i) P_i^{-1} \) (that is to change back the columns of \( G(M_i P_i) \)).

We denote the matrix obtained from this algorithm by \( G(M_i, I_i) \).

The following corollary follows immediately from the above definitions.

**Corollary 5.4** \( \det G(M_i, I_i) = \alpha \det G(M_i, I_i)(J) \), where \( \alpha \) is a nonzero element of \( F \). Moreover \( G(M_i, I_i)(I_i)(j) \) is a triangle matrix for every \( j \in D(M_i) \setminus I_i \).

In the following we also denote \( \alpha \text{ sre}(f, g) \) by \( \text{sre}(f, g) \) for any \( \alpha(\neq 0) \in F \), since we are only interested in the degree of \( \text{sre}(f, g) \).

Now we can write Step 4 of Algorithm 5.1 in the following sub-steps:

**Step 4.1:** Compute \( M_i \) from \( \varphi_i f \) and \( \psi_i g \);

**Step 4.2:** Operate Gaussian elimination of \( M_i \) with respect to \( I_i \), and to get \( G(M_i, I_i) \);

**Step 4.3:** Compute \( \det G(M_i, I_i)(I_i)(j) \) for all \( j \in D(M_i) \setminus I_i \), get

\[
\text{sre}(f, g) = \sum_{j \in D(M_i) \setminus I_i} \det G(M_i, I_i)(I_i)(j) \psi_j.
\]

**Theorem 5.2** The complexity of Algorithm 5.1 is \( O((m+n)^3) \), where \( m = \deg(g) \) and \( n = \deg(f) \).

**Proof.** From the algorithm we immediately have that the total complexity of the first three steps and Step 5 is \( O(m+n) \).

Now let us consider Step 4. Since one can get the linear representation of every \( \varphi_s \cdot \varphi_t \), where \( s, t \in N \) beforehand, the total complexity of Step 4.1 from \( i = 1 \) to \( i = i(f, g) \) is at most \( O((m+n)^3) \). Suppose we already have \( G(M_i, I_i) \). Then to get \( G(M_{i+1}, I_{i+1}) \), it is enough to do elementary row operations on the rows which correspond to \( \varphi_j f \) and \( \psi_j g \) respectively, where \( u(i) + 1 \leq j \leq u(i+1) \) and \( v(i) + 1 \leq k \leq v(i+1) \) respectively. Therefore, the total complexity of Step 4.2 from \( i = 1 \) to \( i = i(f, g) \) is the same as removing the columns of matrix \( M_{i(f, g)} \) and operating Gaussian elimination of \( M_{i(f, g)} \), that is \( O((m+n)^3) \). Since \( \text{rank}(M_{i[I_i]}) = \#(I_i) - 1 \), \( G(M_i, I_i)(I_i)(j) \) is a triangle matrix for every \( j \in D(M_i) \setminus I_i \). Hence, to get \( \det G(M_i, I_i)(I_i)(j) \) one needs at most \( \#(I_i) \) multiplications. Thus, the complexity of getting \( \text{sre}(f, g) \) is at most \( \#(I_i)(m+n) \). Therefore, the total complexity of Step 4.3 is \( \sum_{i=1}^{i(f, g)} \#(I_i)(m+n) \leq (m+n)^2 \).

Finally, for a given \( i \), getting \( p_i \) and \( q_i \) is equivalent to operating Gaussian elimination to \( XM_i \) (see the proof of Proposition 5.3). Hence, the complexity of Step 6 is \( O((m+n)^3) \).

Now the theorem follows immediately from the above conclusions.
5.5 An application to decoding geometric Goppa codes

Recall the definition of geometric Goppa codes (Definition 1.3) defined on a projective, non-singular and absolutely irreducible curve $X$ of genus $g$. Let $P$ be a rational point not in the support of $D$. In this section we will only interested in a class of geometric Goppa codes defined by $C_0(D, mP)$, where $m \geq 2g$. In Chapter 4, we proved that decoding this kind of codes can be reduced to finding a minimal degree solution of a key congruence on an affine ring, see Theorem 4.7. In the following, we will use Algorithm 5.1 given in Section 5.4 to find a minimal degree solution of a key congruence.

In Chapter 4, we defined the affine ring $K_0(P)$ with the degree map $\deg(f) = -v_P(f)$. Now let $\Gamma$ be defined by \{deg($f$) | $f \in K_0(P)$\}, we have the following proposition.

**Proposition 5.5** $K_\infty(P)$ is a $\Gamma$-graded algebra over $F$. Furthermore, let $f, g \in K$ such that $\deg(f) = \deg(g) = n$. Then there exists an $\alpha \in F$ such that $\deg(f - \alpha g) < n$, that means that $K_\infty(P)$ has a $\Gamma$-basis.

**Proof.** From Theorem 4.1 of Chapter 4, we know that $K_\infty(P) = F[f_1, \ldots, f_{g+1}]$, where $g$ is the genus of the curve and $f_i \in K_\infty(P)$ with $\deg(f_i) = m_i \in \Gamma$. Moreover, we have $\Gamma = \{\sum_{i=1}^{g+1} k_i m_i | k_i \in \mathbb{N}\}$, see Proposition 4.2. Therefore $\Gamma$ is a submonoid of $\mathbb{N}$ and $K_\infty(P)$ is a $\Gamma$-graded algebra such that

$$K_\infty(P) = \bigoplus_{\gamma \in \Gamma} K^\gamma,$$

where $K^\gamma$ is the subgroup of the additive group $K_\infty(P)$, generated by

$$\{af_1^{k_1} \cdots f_{g+1}^{k_{g+1}} | a \in F, k_j \in \mathbb{N} \text{ and } \sum_{j=1}^{g+1} k_j m_{ij} = \gamma\},$$

see Proposition 4.3.

The second conclusion is proved in Lemma 4.3 of Chapter 4. □

**Remark 5.5** It is shown in Remark 4.5 that $K_\infty(P)$ is not an Euclidean domain with $\deg = -v_P$, if the genus of $X$ is not zero.

In Chapter 4, it was proved that there exist $h \in K_\infty(P)$ and a positive integer $\mu$ such that decoding the code $C_0(D, mP)$ is equivalent to decoding the code $C_0(D, (h) - \mu P)$ up to the same errors, where $h$ has disjoint support with $D$. Hence in the following we will only consider the code $C_0(D, (h) - \mu P)$. For every received word $x$ one gets a syndrome $S(x) \in K_\infty(P, W)$, where $K_\infty(P, W)$ is a non zero ideal of $K_\infty(P)$, see Definition 4.9 and Proposition 4.13. Moreover by the Decoding Theorem 4.7, decoding the code $C_0(D, (h) - \mu P)$ can be reduced to finding a minimal valid solution of $(S(x), h, l + \mu)$ for some integer $l > 0$

**Remark 5.6** To find this solution in the case that there exists a differential form $\eta$ on the curve, such that $(\eta) = (2g - 2)P$ and $\mu = 1$, Porter [57] used his generalized subresultant sequence on $K_\infty(P)$. But as we will see in Section 5.6, his method cannot correct the errors for some codes.
Chapter 5: Solving a Congruence on a Graded Algebra

We give our decoding algorithm for the code $C_\Omega(D, (h)_0 - \mu P)$ as follows.

Algorithm 5.2:

1. **Step 1:** Input a received word $x$;
2. **Step 2:** Compute $S(x)$;
3. **Step 3:** Operate Algorithm 5.1 to $S(x)$ and $h$, get $A(S(x), h, l + \mu) = (f, g, r)$;
4. **Step 4:** compute $e = (\text{res}_P((r/f)\eta), \ldots, \text{res}_P((r/f)\eta))$;
5. **Step 5:** stop.

**Theorem 5.3** Algorithm 5.2 decodes $C_\Omega(D, (h)_0 - \mu P)$ up to $(d^* - 1)/2 - s$ errors. Furthermore, the complexity of this algorithm is $O(n^3)$.

**Proof.** The first part of the theorem follows from Theorem 5.1 and Theorem 4.7. The complexity of the first three steps is $O(n^3)$ by Theorem 5.2. The complexity of Step 4 is $O(n^2)$, see [15, §2.5]. □

5.6 An example

Let $X$ be the Hermitian curve $x^5 - y^4 - y = 0$ over $k = \mathbb{F}_{16}$. The genus of this curve is 6. Let

$$\mathcal{H}^*(k) = \{((\alpha, \beta)) \in k \times k | x \in k, \beta^4 + \beta = \alpha^5 \text{ and } (\alpha, \beta) \neq (0, 0)\}.$$ 

Let $D = \sum_{(\alpha, \beta) \in \mathcal{H}^*(k)} P_{\alpha, \beta}$, where $P_{\alpha, \beta}$ is the common zero of $x - \alpha$ and $y - \beta$, and $P_{\infty}$ be a common pole of $x$ and $y$. see [73]. Then $K_{\infty}(P_{\infty}) = k[x, y]$ by Theorem 4.1. Consider the code $C_\Omega(D, 25P_0 - P_{\infty})$. Then the length of the code is 63.

The following facts will be proved in Chapter 6. For every $(\alpha, \beta) \in \mathcal{H}^*(k)$, let

$$e_{\alpha, \beta} = \left(\frac{(y + \beta)^3 + 1}{x + \alpha} + U(\alpha, \beta)\right) dx,$$

where $U(\alpha, \beta) = \alpha^2 \beta^{-1}x^2 + \alpha^3(\beta^{-1}x + \beta^{-2}xy) + \alpha^4(\beta^{-1} + \beta^2y + \beta^{-3}y^2)$. Since

$$y + \beta = \frac{x^5 + \alpha^5}{(y + \beta)^3 + 1},$$

the syndrome of $x = (x_{\alpha, \beta})_{(\alpha, \beta) \in \mathcal{H}^*(k)}$ is

$$S(x)dx = \sum_{(\alpha, \beta) \in \mathcal{H}^*(k)} x_{\alpha, \beta} \frac{y^5 + \beta^5}{\beta^5 - e_{\alpha, \beta}}\ dx$$

$$= \sum_{(\alpha, \beta) \in \mathcal{H}^*(k)} x_{\alpha, \beta} \beta^{-5}(x^4 + \alpha x^3 + \alpha^2 x^2 + \alpha^3 x + \alpha^4)(y^4 + \beta y^3 + \beta^2 y^2 + \beta^3 y + \beta^4)$$

$$+ \ U(\alpha, \beta)(y^5 + \beta^5)\ dx.$$ 

Let $\xi$ be a primitive root of unity of $k$. Suppose we received the word with 3 errors $x = (1, \xi^5, \xi^{10}, 0 \ldots 0)$. This means that, for all $(\alpha, \beta) \in \mathcal{H}^*(k)$, except $(\alpha, \beta) = (0, 1), (0, \xi^5)$ and $(0, \xi^{10})$, $x_{\alpha, \beta} = 0$. Hence $S(x) = x^4y^3 + x^4$.

1. Use Algorithm 5.1 to decode.
Let \( m = \deg(h) = 25 \) and \( n = \deg(S(x)) = 31 \). Then \( m_u(1) = 4 \) and \( n_v(1) = 10 \). Hence

\[
M_1 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 
\end{pmatrix}
\]

where the columns correspond to \((y, y^2, \ldots, y, x, 1)\) and the rows correspond to \((y^2h, xyh, x^2h, yh, xh, h, S(x), xS(x))\)\(^T\), and \(I_1 = \{25, 29, 30, 31, 33, 34, 35\}\). Hence \(sre_1(S(x), h) = y\). This means that \(xS(x) = y + y^2h\). Hence the error function is \(ydx/x\), which fits the solution.

(II) Porter’s method (we refer to [57, Definition 3.3.4 and p.72])

The matrix \(A\) is

\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\end{pmatrix}
\]

where the columns correspond to \((y^8, \ldots, y, x, 1)\) and the rows correspond to \((y^2h, x^2y, x^3h, y^2h, xyh, x^2h, yh, xh, x, S(x), xS(x), yS(x), x^2S(x), xyS(x))\)\(^T\), since \(\deg(f) \leq e + g = 9\).

First consider matrix \(A_{35} = M_1\) which has 8 rows, the degree of the 8th column is 28. Then according to his method, one defines \(A_{35}^{(r)}\), for \(r \leq 28\) and \(r\) is not a gap, in the following way: \(A_{35}^{(r)}\) consisting of all columns of \(A_{35}\) of degree greater than 28 and the column of degree \(r\), that is

\[
A_{35}^{(r)} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\end{pmatrix}
\]

where \(a^r\) is the column of degree \(r\) in \(A_{35}\). Hence \(\det(A_{35}^{(r)}) = 0\), therefore

\[
\detpol(A_{35}) = \sum \det(A_{35}^{(r)}) \phi_r = 0
\]

where \(r\) is taken form the set \(\{0 \leq r \leq 28|r\text{ is not a gap}\}\). By the same reason one also get that \(\detpol(A_{39}) = 0\) and \(\detpol(A_{40}) = 0\).

Conclusion: Using Porter’s method, one cannot solve the congruence \(fS(x) \equiv r \pmod{h}\), neither the error vector for \(x\).
Chapter 6

Codes from Hermitian Curves

In this chapter, we consider the code $C_{D, l(q + 1)P_0, \delta P_\infty}$ from Hermitian curves, which is isometric to the code $C_{\mathcal{H}(D, mP_\infty)}$, where $P_\infty$ is a point at infinity, $\deg(D) = q^3 - 1$ and $m = l(q + 1) - \delta$. We give an explicit construction of syndromes of the code as well as encoding and decoding schemes.

In Section 6.1, a detailed description of the codes is given, which is different from the one given by Tiersma [78] and Stichtenoth [73]. Section 6.2 gives an explicit construction of syndromes. In Section 6.3, an encoding scheme of the codes is given. In Section 6.4, we transfer the decoding method given by Chapter 4 to the method of finding a minimal recurrence relation for a non-gap subscript sequence constructed from a syndrome. The details of finding a minimal recurrence relation will be given in Chapter 7. In Section 6.5, by constructing a database, we show how to compute the residues explicitly.

6.1 The construction of codes

Throughout this chapter, let $k = GF(q^2)$ denote the finite field, where $q$ is a power of some prime. Let $\mathbb{N}$ denote the set of all nonnegative integers and $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Let $m \in \mathbb{N}$ such that $q^2 - q \leq m \leq q^3 + q^2 - q - 3$, and let $l, \delta \in \mathbb{N}^*$ such that $1 \leq \delta \leq q + 1$.

6.1.1 Hermitian curves and their properties

The Hermitian curve $\mathcal{H}(q)$ is defined by the equation $u^{q+1} + v^{q+1} + w^{q+1} = 0$ over $k$. The function field of the Hermitian curve $\mathcal{H}(q)$ is $\mathbb{F}_k(u, v)$, where the defining equation is $u^{q+1} + v^{q+1} + 1 = 0$. Now let

$$x = \frac{b}{v - bu}, \quad y = ux - a, \quad a^q + a = b^{q+1} = -1.$$ 

Then $F = k(x, y)$, where $y^q + y = x^{q+1}$, see [73]. The genus of $\mathcal{H}(q)$ is $g = q(q-1)/2$, and $\mathcal{H}(q)$ has exactly $q^3 + 1$ places of degree one, namely the following (see [73]): (1) the common pole $P_\infty$ of $x$ and $y$; (2) for any $\alpha \in k$ and any $\beta$ such that $\beta^q + \beta = \alpha^{q+1}$, the common zero $P_{\alpha, \beta}$ of $x - \alpha$ and $y - \beta$. Denote $H(\alpha) = \{\beta \in k|\beta^q + \beta = \alpha^{q+1}\}$ for every $\alpha \in k$, and denote $H^{-1}(\beta) = \{\alpha \in k|\alpha^{q+1} = \beta^q + \beta\}$ for every $\beta \in k$. 

75
Furthermore, we denote $\mathcal{H}^*(k) = \{(\alpha, \beta) | \alpha \in k, \beta \in H(\alpha) \} \setminus \{(0, 0)\}$. Then for any $\alpha, \beta \in k$, the principle divisors of $x - \alpha$ and $y - \beta$ are:

$$(x - \alpha) = \sum_{\beta \in H(\alpha)} P_{\alpha, \beta} - qP_\infty$$

and

$$(y - \beta) = \begin{cases} (q + 1)P_{0, \beta} - (q + 1)P_\infty & \text{if } \beta^q + \beta = 0 \\ \sum_{\alpha \in H^{-1}(\beta)} P_{\alpha, \beta} - (q + 1)P_\infty & \text{if } \beta^q + \beta \neq 0, \end{cases}$$

respectively, see [73].

**Proposition 6.1** $(dx) = (2g - 2)P_\infty$, where $(dx)$ is the canonical divisor of $dx$ on $F$.

**Proof.** See [72, Satz 1(f)]. □

By Definition 4.1 of Chapter 4, we have an affine ring $K_\infty(P_\infty)$ with the degree map $\deg$. In this chapter, we abbreviate it by $K_\infty$. From Example 4.2, we know that $K_\infty = k[x, y]$ with the defining equation $x^{q+1} = y^q + y$.

**Remark 6.1** In the following, $k[x, y]$ always means the $k$-algebra generated by $x$ and $y$ with the defining equation $x^{q+1} = y^q + y$, while $k[X, Y]$ denotes the polynomial ring of two variables over $k$.

### 6.1.2 Subspaces of differential forms

For convenience, we enumerate $\mathcal{H}^*(k)$ to $\{(\alpha_i, \beta_i) | i = 1, \ldots, n\}$, where $n = q^3 - 1$, and abbreviate $P_{\alpha_i, \beta_i}$ by $P_i$ for every $i \in \{1, \ldots, n\}$. Moreover, we denote the divisor $P_1 + \cdots + P_n$ by $D$. Furthermore, we denote $\Sigma := N \times N$.

**Definition 6.1** For every $i = (i_1, i_2) \in \Sigma$, define

$$\omega(i) = \frac{x^{i_1}y^{i_2}}{x^{q^3} - x} dx.$$ 

**Definition 6.2** Define $\theta_\alpha(x) = \prod_{\gamma \in k \setminus \{\alpha\}} (x - \gamma)$, where $\alpha \in k$. It is easy to prove that

$$\theta_\alpha(\gamma) = \begin{cases} -1 & \text{if } \gamma = \alpha, \\ 0 & \text{if } \gamma \in k \setminus \{\alpha\}. \end{cases}$$

**Proposition 6.2** For every $j \in \{1, \ldots, n\}$ and every $i \in \Sigma$, $\res_{P_j}(\omega(i)) = -\alpha_j^{i_1} \beta_j^{i_2}$.

**Proof.** After replacing $x$ and $y$ by $x - \alpha_j + \alpha_j$ and $y - \beta_j + \beta_j$, respectively in $\omega(i)$, we have

$$\omega(i) = \left(\frac{\alpha_j^{i_1} \beta_j^{i_2}}{\theta_{\alpha_j(\alpha_j)}} \frac{1}{x - \alpha_j} + W_j(x, y)\right) dx(x - \alpha_j),$$

where $\theta_{\alpha_j}$ is defined by the Definition 6.2, and $W_j(x, y) = \sum_{k \in \Sigma} w_k(x - \alpha_j)^{k_1}(y - \beta_j)^{k_2}$ with $w_k \in k$. Hence

$$\res_{P_j}(\omega(i)) = \frac{\alpha_j^{i_1} \beta_j^{i_2}}{\theta_{\alpha_j(\alpha_j)}} = -\alpha_j^{i_1} \beta_j^{i_2},$$

since $x - \alpha_j$ is a local parameter of $P_j$ and $P_j$ is a zero of $y - \beta_j$. □

In the following, we will show that the space $\Omega((q + 1)P_{0,0} - \delta P_\infty - D)$ can be generated by some of the differential forms $\omega(i)$. 

---

76
Chapter 6: Codes from Hermitian Curves

Definition 6.3 Define a map \( Q : \Sigma \rightarrow \mathbb{N} \) by \( Q(i) = i_1q + i_2(q + 1) \), where \( i = (i_1, i_2) \in \Sigma \).

Definition 6.4 Let \( \Sigma(q) \) be a subset of \( \Sigma \) defined by \( \Sigma(q) = \{ i \in \Sigma | i_1 \leq q \} \). For every \( k \in \mathbb{N} \), define \( \Sigma^k(q) = \{ i \in \Sigma(q) | Q(i) < k \} \). Furthermore, we denote \( N(q) = Q(\Sigma(q)) \), and for any element \( n \in \mathbb{N} \) we call \( n \) a gap if \( n \not\in N(q) \) and a non-gap otherwise.

The following lemmas give some properties of \( N(q) \) and \( \Sigma^k(q) \), respectively, where \( \#(S) \) is the cardinality of the set \( S \).

Lemma 6.1 \( \#(N \setminus N(q)) = g \), so that \( N(q) = Q(\Sigma(q)) \cup \{ n \in \mathbb{N} | n \geq 2g \} \).

Proof. See Lemma 2.5. \( \square \)

Remark 6.2 The following statements are easily proved:

1. The restriction of \( Q \) on \( \Sigma(q) \) is an injective map and \( N(q) = Q(\Sigma) \). Furthermore, \( N(q) \) is a submonoid of \( \mathbb{N} \).

2. \( N \setminus N(q) = \{ j(q + 1) + i | 0 \leq j \leq q - 2, 1 \leq i \leq q \} \).

Lemma 6.2 \( \#(\Sigma^{2g-1}(q)) = g \) and \( \Sigma^{2g-1}(q) = \Sigma^{2g}(q) \).

Proof. For every \( i \in \Sigma^{2g-1}(q) \), we have \( 0 \leq i_1 \leq q - 2 \) and

\[
0 \leq i_2 \leq \left\lfloor \frac{q(q - 1) - 2 - i_1q}{q + 1} \right\rfloor = q - i_1 - 2.
\]

Thus \( \#(\Sigma^{2g-1}(q)) = \sum_{i=1}^{q-2}(q - i - 1) = q(q - 1)/2 = g \). It is easy to see that there is no \( i \in \Sigma(q) \) such that \( Q(i) = q(q - 1) - 1 \). This proves the last conclusion. \( \square \)

Definition 6.5 Suppose \( m = l(q + 1) - \delta \) such that \( l, \delta \in \mathbb{N}^* \) and \( 1 \leq \delta \leq q + 1 \). Let \( \rho(m) = q^3 - 1 + 2g - m \). Define

\[
\Sigma(q, m) = \{ i + (0, l) | i \in \Sigma^{\rho(m)}(q) \setminus \{(0, 0)\} \}.
\]

Proposition 6.3 Let the assumption be as in the above definition. Then

(a) \( \{ \omega(i) | i \in \Sigma(q, m) \} \) is a basis of \( \Omega(l(q + 1)P_{0,0} - \delta P_{\infty} - D) \);

(b) \( \{ x^iy^i | (i_1, i_2) \in \Sigma^{2g+i-1}(q) \} \) is a basis of \( \Omega(-\delta P_{\infty}) \).

Proof. (a) Since for every \( i \in \Sigma(q, m) \), \( Q(i) \leq q^3 - 1 + 2g + \delta - 1 \) and \( i_1 + i_2(q + 1) \geq l(q + 1) + 1 \), and \( (x^q - x) = D + P_{0,0} - q^3P_{\infty} \), we have

\[
(\omega(i)) \geq (i_1 + i_2(q + 1) - 1)P_{0,0} - (Q(i) - 2g + 2 - q^3)P_{\infty} - D
\]

\[
\geq l(q + 1)P_{0,0} - \delta P_{\infty} - D.
\]

Thus \( \omega(i) \in \Omega(l(q + 1)P_{0,0} - \delta P_{\infty} - D) \). Because \( v_{P_{0,0}}(\omega(i)) \) are all different for \( i \in \Sigma(q, m) \), all those differential forms are linearly independent. Furthermore we have

\[
\#(\{ \omega(i) | i \in \Sigma(q, m) \}) = q^3 + g - m - 2 + \dim L((m - q^3)P_{\infty})
\]

\[
= \dim \Omega(l(q + 1)P_{0,0} - \delta P_{\infty} - D),
\]

where the first equality follows from Lemma 6.3, and the last one follows from the fact \( D + P_{0,0} \) and \( q^3P_{\infty} \) being linearly equivalent as are \( l(q + 1)P_{0,0} - \delta P_{\infty} \) and \( mP_{\infty} \), Lemma 6.4 and Riemann-Roch Theorem.

The proof of (b) is the same as the above proof. We leave it to the reader. \( \square \)
Lemma 6.3 \(\#(\Sigma(q, m)) = q^3 + g - m - 2 + \text{dim} L((m - q^3)P_\infty).\)

**Proof.** By the definition of \(\Sigma(q, m)\), we have \(\#(\Sigma(q, m)) = \#(\Sigma^{\rho(m)}(q)) - 1.

(i) If \(m \leq q^3 - 1\) then we have

\[
Q(\Sigma^{\rho(m)}(q)) = \{n \in \mathbb{N} | 2g \leq n < \rho(m)\} \cup Q(\Sigma^2(q)),
\]

by Lemma 6.1. Thus \(\#(\Sigma^{\rho(m)}(q)) = \rho(m) - 2g + g\) by Lemma 6.2. This proves the conclusion since \(\text{dim} L((m - q^3)P_\infty) = 0\) in this case.

(ii) If \(m \geq q^3\). Let \(A\) be a set defined by \(\{k \in \mathbb{N} | N(q)|k < 2g - m + q^3 - 1\}\). Then we have \(\Sigma^{\rho(m)}(q) = \rho(m) - \#(A)\). Now by Remark 6.2(1) and Lemma 6.2, we have \(2g - 1 - Q(i) \in A\) for every \(i \in \Sigma^2(q)\) with \(m - q^3 + 1 \leq Q(i)\). On the other hand, for every \(k \in A\), \(2g - 1 - k\) is in \(N(q)\) and greater than \(m - q^3\), by Remark 6.2(2). Hence \(\#(A) = \#\{i \in \Sigma^2(q) | m - q^3 + 1 \leq Q(i)\}\). On the other hand, by Proposition 4.3, we have

\[
\text{dim} L((m - q^3)P_\infty) = \#(\Sigma^2(q)) - \#\{i \in \Sigma^2(q) | m - q^3 + 1 \leq Q(i)\}.
\]

Thus

\[
\Sigma^{\rho(m)}(q) = \rho(m) - g + \text{dim} L((m - q^3)P_\infty).
\]

This proves the conclusion. \(\square\)

**Lemma 6.4** Let \(0 \leq s \leq 2g - 2\), then \(L(sP_\infty + P_{0,0}) = L(sP_\infty).\)

**Proof.** It is obvious that \(L(sP_\infty + P_{0,0}) \supseteq L(sP_\infty).\) Now suppose there exists an \(f\) belonging to \(L(sP_\infty + P_{0,0}) \setminus L(sP_\infty)\). By the result of Section 6.1.1, we have \(xf \in L((s + q)P_\infty)\). Therefore \(xf = g_1(y) + xg_2(x, y)\) with \(v_{P_\infty}(g_1(y)) \neq v_{P_\infty}(g_2(x, y))\) by Proposition 4.3, where \(g_1(X) \in k[X]\) and \(g_2(X, Y) \in k[X, Y]\). Furthermore \(g_1(X) \neq 0\) since \(f \notin L(sP_\infty)\). Hence \(g_1(y) \in \mathcal{L}((s + q)P_\infty + P_{0,0})\). Thus for every \(P \in \{P_{0,0}, \beta^3 + \beta = 0\}\) and \(\beta \neq 0\), \(v_P(g_1(y)) \geq 1\). This means that \(g_1(\beta) = 0\) if \(\beta^3 + \beta = 0\) and \(\beta \neq 0\). Thus the degree of the polynomial \(g_1(X)\) is at least \(q - 1\). This implies that \(v_{P_\infty}(g_1(y)) \leq -(q - 1)(q + 1) < -s - q\). Thus \(v_{P_\infty}(xf) < -s - q\) which is a contradiction. This proves the lemma. \(\square\)

**6.1.3 The Codes**

**Proposition 6.4** Suppose \(m = l(q + 1) - \delta \geq 2g\), where \(l\) and \(\delta\) are defined as before. Then \(\{(\alpha_1^i \beta_1^{i_1}, \ldots, \alpha_n^i \beta_n^{i_n}) | i \in \Sigma(q, m)\}\) is a basis of the code \(C_\Omega(D, l(q + 1)P_{0,0} - \delta P_\infty)\) and the dimension of the code is \(q^3 + g - m - 2 + \text{dim} L((m - q^3)P_\infty)\). Furthermore, if \(m \leq n\), the minimum distance \(d\) of the code satisfies

\[
m - 2g + 2 \leq d \leq m - 2g + 2 + \delta.
\]

We call \(d^* = m - 2g + 2\) the designed minimum distance.

**Proof.** By Proposition 6.3(a), Proposition 6.2 and Definition 1.3, we have

\[
C_\Omega(D, l(q + 1)P_{0,0} - \delta P_\infty) = \{(\alpha_1^i \beta_1^{i_1}, \ldots, \alpha_n^i \beta_n^{i_n}) | i \in \Sigma(q, m)\}.
\]

For the dimension of the code, we have

\[
\text{dim} C_\Omega(D, l(q + 1)P_{0,0} - \delta P_\infty) = \text{dim} \Omega(l(q + 1)P_{0,0} - \delta P_\infty - D) = q^3 + g - m - 2 + \text{dim} L((m - q^3)P_\infty),
\]
where the first equality follows from Theorem 1.3(b), and the last equality follows from Proposition 6.3(a).

For the minimum distance \( d \), we have \( d \geq m - 2g + 2 \), by Theorem 1.3(b). Now suppose \( m \leq n \) and let \( t = l - q - 2 \), we have \( t \leq q^2 - q \). Thus we can choose \( t \) different elements of \( k \), namely \( \beta_1, \ldots, \beta_t \), such that \( \beta_i^2 + \beta_i \neq 0 \). Define the differential form

\[
\omega = \frac{y^l}{\prod_{i=1}^{l}(y - \beta_i)}dx.
\]

It is easy to see that \( \omega \in \Omega(l(q+1)P_{0,0} - \delta P_\infty - D) \) and \( \text{res}_{\alpha,0}(\omega) \neq 0 \) for every \( \alpha \in H^{-1}(\beta_i) \), where \( i = 1, \ldots, t \). Furthermore, for any \( P_{\alpha,0} \) such that \( \beta \notin \{\beta_1, \ldots, \beta_t\} \), \( \text{res}_{\alpha,0}(\omega) = 0 \). Therefore, if we define \( c = (\text{res}_{P_1}(\omega), \ldots, \text{res}_{P_n}(\omega)) \), then \( c \) is a codeword of the code and \( \text{weight}(c) = t(q + 1) \). This means that \( d \leq t(q + 1) = m - 2g + 2 - \delta \). \( \square \)

To complete this section, we show the isometry of the codes \( C_\Omega(D, l(q+1)P_{0,0} - \delta P_\infty) \) and \( C_\Omega(D, mP_\infty) \).

**Proposition 6.5** Let \( m = l(q+1) - \delta \). Then \( C_\Omega(D, mP_\infty) \) and \( C_\Omega(D, l(q+1)P_{0,0} - \delta P_\infty - D) \) are isometric.

**Proof.** By the facts given in Section 6.1.1, we have \( mP_\infty - D + (y^l) = l(q+1)P_{0,0} - \delta P_\infty - D \). Therefore

\[
\Omega(mP_\infty - D) = \{\omega/y^l | \omega \in \Omega(l(q+1)P_{0,0} - \delta P_\infty - D)\}.
\]

Thus for every \( \omega \in \Omega(mP_\infty - D) \), we have \( \text{res}_{P_i}(\omega) = \text{res}_{P_i}(\omega')/\beta_i^l \) since \( \text{supp}((y^l)) = \{P_{0,0}, P_\infty\} \) and \( P_i \neq P_{0,0} \). Therefore \( C_\Omega(D, mP_\infty) = (\beta_i^{-1}, \ldots, \beta_n^{-1})C_\Omega(D, l(q+1)P_{0,0} - \delta P_\infty - D) \). This proves the proposition, see Definition 2.3. \( \square \)

By Proposition 4.4, we know that decoding the code \( C_\Omega(D, mP_\infty) \) is equivalent to decoding the code \( C_\Omega(D, l(q+1)P_{0,0} - \delta P_\infty) \). Therefore in the rest of this chapter, we only consider the code \( C_\Omega(D, l(q+1)P_{0,0} - \delta P_\infty) \) and denote it by \( C_\Omega(D, mP_\infty) \).

**6.2 The syndromes**

In this section, for the code \( C_\Omega(D, mP_\infty) \) we will give an explicit construction of the syndrome of a received word. First, We will define a set of differential forms \( \{\eta_i | i = 1, \ldots, n\} \) such that \( \{\eta_i + \Omega(\delta P_\infty) | i = 1, \ldots, n\} \) is a basis of \( \Omega(-\delta P_\infty - D)/\Omega(-\delta P_\infty) \). Then by repairing this set we will construct a set of differential forms \( \{\varepsilon_i(\delta)\} \), such that \( \omega = \sum_{i=1}^{n} \text{res}_{P_i}(\omega)\varepsilon_i(\delta) \) for every \( \omega \in \Omega(l(q+1)P_{0,0} - \delta P_\infty - D) \).

**Definition 6.6** For every \( i \in \{1, \ldots, n\} \), define

\[
\eta_i = \frac{(y - \beta_i)^{q-1} + 1}{x - \alpha_i}dx,
\]

where \( (\alpha_i, \beta_i) \in \mathcal{H}^*(k) \) = \{\( (\alpha_i, \beta_i) \) | \( j = 1, \ldots, n \) \}.

**Proposition 6.6** \( (\eta_i)_\infty = P_i + P_\infty \) and \( \text{res}_{P_i}(\eta_i) = 1 \), where \( (\eta_i)_\infty \) means the divisor of the poles of \( \eta_i \).
Proof. It is easy to verify that, all $P_{\alpha_i, \beta}$, $(\alpha_i, \beta) \in H^*(k)$ but $P_i = P_{\alpha_i, \beta}$, are zeros of $(y - \beta_i)^{q-1} + 1$. On the other hand, we have

$$(x - \alpha_i) = \sum_{\beta \in H(\alpha_i)} P_{\alpha_i, \beta} - qP_\infty.$$ 

Thus $(\eta_i)_\infty = P_i + P_\infty$. Furthermore

$$\text{res}_{P_i}(\eta_i) = \text{res}_{P_i}(\frac{1}{x - \alpha_i} + \frac{(y - \beta_i)^{q-1}}{x - \alpha})d(x - \alpha_i)) = 1,$$

since $x - \alpha_i$ is a local parameter of $P_i$. □

The following proposition immediately follows from the above proposition and Proposition 4.10.

**Proposition 6.7** \{\{\eta_i + \Omega(-\delta P_\infty) | i = 1, \ldots, n\} is a basis of $\Omega(-\delta P_\infty - D)/\Omega(-\delta P_\infty)$, so that for every $\omega \in \Omega(-\delta P_\infty - D)$, $\omega - \sum_{i=1}^n \text{res}_{P_i}(\omega)\eta_i \in \Omega(-\delta P_\infty)$.\}

The following proposition shows the exact difference between $\sum_{i=1}^n \text{res}_{P_i}(\omega(i))\eta_i$ and $\omega(i)$.

**Proposition 6.8** For every $i = (i_1, i_2) \in \Sigma(q)$, denote

$$\sigma(i) := -\sum_{j=1}^n \text{res}_{P_j}(\omega(i))\eta_j = \sum_{j=1}^n \alpha_j^{i_1} \beta_j^{i_2} \eta_j.$$ 

Moreover, define $(1, q^2 - q) = \{i + (1, q^2 - q) | i \in \Sigma(q)\}$. Then for every $i \in \Sigma(q, m)$, we have

$$\sigma(i) = \begin{cases} -\omega(i) & \text{if } i \notin (1, q^2 - q) \\ -\omega(i) + x^i y^j dx & \text{if } i \in (1, q^2 - q) \text{ and } i_2 \leq q^2 - 2, \end{cases}$$

where $j = i - (1, q^2 - q)$. Moreover for every $i = (i_1, i_2) \in \Sigma(q, m)$ such that $i_2 = k(q^2 - 1) + i'_2$ with $k, i'_2 \in \mathbb{N}$ and $i'_2 \leq q^2 - 2$, we have $\sigma(i) = \sigma(i_1, i'_2)$. Therefore if $(1, q^2 - 1) \in \Sigma(q, m)$ then $(1, q^2 - 1) = -x dx/(x^{q^2} - x)$.

To prove this proposition, we need the following lemmas. First by the properties of the deg on $k[x, y]$ (see Lemma 4.2), we immediately have the following lemma.

**Lemma 6.5** Let $A(x, y) = \sum_{i \in \Sigma(q)} a_{i, q^2 - q} x^i y^{i_2} \in k[x, y]$. If $A(x, y) \neq 0$, then there does not exist any nonzero $B(x, y) = \sum_{i \in \Sigma(q)} b_i x^i y^{i_2} \in k[x, y]$ such that $A(x, y) = (x^{q^2} - x)B(x, y)$.

**Lemma 6.6** For every $i \in \{1, \ldots, n\}$, define

$$c_i(x, y) := \sigma_{\alpha_i}(x) \{(y - \beta_i)^{q-1} + 1\}.$$

Then $c_i(x, y) = \sum_{j \in \Sigma(q) \setminus (1, q^2 - q)} c_j x^i y^{i_2}$, for some constants $c_j \in k$. 


Proof. For every \( k \in \{0, \ldots, q^2 - 1\} \), we have \( k = u_k(q+1) + r_k \), such that \( u_k, r_k \in \mathbb{N}, 0 \leq r_k \leq q \) and \( u_k \leq q - 2 \) if \( r_k \neq 0 \). Thus we can write \( \theta(x) = \sum_{k=0}^{q^2-1} \sigma_k x^{u_k} (y^q + y)^{u_k} \) since \( x^{u_k} = y^q + y \). Hence by the binomial expansions of \( (y^q + y)^{u_k} \) and \( (y - \beta_i)^{q-1} \), we get

\[
c_i(x, y) = \sum_{k=0}^{q^2-1} \sum_{s=0}^{q-1} a_{k,s,t}^{(i)} x^{r_k} y^{(q-1)s + u_k + t},
\]

for some constants \( a_{k,s,t}^{(i)} \in k \). Moreover, it is easy to see that for \( 0 \leq s \leq u_k \) and \( 0 \leq t \leq q - 1 \), \( (r_k, (q-1)s + u_k + t) \notin \{(1, q^2 - q)\} \). This proves the lemma. \( \square \)

Proof of Proposition 6.8. By Proposition 6.7 and Proposition 6.3(b) we have \( \sigma(i) + \omega(i) = B(x, y) dx \), where \( B(x, y) dx = \sum_{j \in \Sigma^2 \lambda - 1 \Sigma}(b_j x^{j_1} y^{j_2} dx + \Omega(-\delta P_\infty) \) with \( b_j \in k \). This means that

\[
\sum_{i=1}^{n} \alpha_i^{j_1} \beta_i^{j_2} c_i(x, y) + x^{i_1} y^{i_2} = (x^q - x) B(x, y),
\]

where \( c_i(x, y) \) is defined in Lemma 6.6. Thus:

1) If \( i \in \Sigma(q) \setminus \{(1, q^2 - q)\} \), then by Lemma 6.5 and Lemma 6.6 we get \( B(x, y) = 0 \). Hence \( \sigma(i) = -\omega(i) \).

2) If \( i \in \{(1, q^2 - q)\} \), then there exists a \( j \in \Sigma(q) \) such that \( i = j + (1, q^2 - q) \) with \( j_2 \leq q - 2 \). Thus we can derive that \( x^{i_1} y^{i_2} = (x^q - x)x^{j_1} y^{j_2} = x^{j_1+1} \sum_{k=j_2} q^2-1 d_k y^k \) for some constant \( d_k \in k \), by \( x^{q+1} = y^q + y \). This implies that

\[
\sum_{i=1}^{n} \alpha_i^{j_1} \beta_i^{j_2} c_i(x, y) - x^{j_1+1} \sum_{k=j_2} q^2-1 d_k y^k = (x^q - x) A(x, y),
\]

where \( A(x, y) = B(x, y) - x^{j_1} y^{j_2} \) and \( j \in \Sigma^2 \lambda - 1 \Sigma(q) \). Hence by Lemma 6.5 and Lemma 6.6, we get \( B(x, y) = x^{j_1} y^{j_2} \). This proves the second case.

The last conclusion of the proposition is an immediate consequence of \( \beta y^{q-1} = 1 \) for \( \beta \in k \). \( \square \)

By the above proposition, we can see that the only thing we have to do in order to attain our goal is to eliminate \( x^{j_1} y^{j_2} \) in the second case. The following two formulas are created just for this purpose.

**Definition 6.7** For every \( i \in \{1, \ldots, n\} \), define

\[
\mu_1(i, k) = \alpha_i^{k+2} x^{i_2-2-k} \sum_{u=0}^{k} \beta_i^{-(u+1)} y^u, \text{ for } 0 \leq k \leq q - 2
\]

and \( \mu_2(i, k) = \alpha_i^{-k} \beta_i^{-k} x^k y^{q-1-k}, \text{ for } 0 \leq k \leq q - 1 \), where \( (\alpha_i, \beta_i) \in H^*(k) \)

**Proposition 6.9** Suppose \( m = l(q + 1) - \delta \geq 2g \). Then

\[
\sum_{k=0}^{q-2} \sum_{j=1}^{n} \alpha_j^{i_1} \beta_j^{i_2} \mu_1(j, k) + \sum_{k=q+1-\delta}^{q-1} \sum_{j=1}^{n} \alpha_j^{i_1} \beta_j^{i_2} \mu_2(j, k) = \begin{cases} 
-x^{i_1} y^{u_2} & \text{if } i \in \Sigma(q, m) \setminus \{(1, q^2 - q)\} \setminus \{(1, q^2 - 1)\}, \\
-1 - x^{i_1} y^{u_2} & \text{if } i = (1, q^2 - 1), \\
0 & \text{if } i \in \Sigma(q, m) \setminus \{(1, q^2 - q)\},
\end{cases}
\]

where \( u = i - (1, q^2 - q) \) and if \( \delta = 1 \) the second part of the left side of the equation is considered as a zero.
To prove this proposition we need the following preparation.

**Definition 6.8** For any \((s, t) \in \Sigma\), define 
\[ \Delta(s, t) = \sum_{i=1}^{n} a_i \beta_i^t. \]

**Proposition 6.10** Let \(0 \leq s \leq q \) and \(t' = k(q^2 - 1) + t\) where \(k, t \in \mathbb{N}\) and \(t \leq q^2 - 2\), then
\[ \Delta(s, t') = \Delta(s, t) = \begin{cases} -1 & \text{if } (s, t) = (0, 0), \\ 0 & \text{otherwise.} \end{cases} \]

**Proof.** See Appendix.

**Corollary 6.1** Let \(i = (i_1, i_2) \in \Sigma(q, m)\). Then

(i) Let \(0 \leq k \leq q - 2\). Define \(j(i_2, v)\) to be \(i_2 - (v + 1)\) in case \(v + 1 \leq i_2\) and \(q^2 - 1 + i_2 - (v + 1)\) otherwise, where \(v \in \{0, 1, \ldots, k\}\). Then
\[ \Delta(i_1 + k + 2, j(i_2, v)) = \begin{cases} -1 & \text{if } k = q - 1 - i_1 \text{ and } v = i_2 - q^2 + q \\ 0 & \text{or } k = q - 2, v = 0 \text{ and } i = (1, q^2 - 1), \\ & \text{otherwise.} \end{cases} \]

(ii) Let \(0 \leq k \leq q - 1\). then
\[ \Delta(i_1 + q - k, i_2 + k - q) = \begin{cases} -1 & \text{if } k = i_1 - 1 = q^2 - i_2 - 1, \\ 0 & \text{otherwise.} \end{cases} \]

**Proof.** See Appendix. \(\Box\)

**Proof of Proposition 6.9.** For \(\mu_1(j, k)\) we have
\[
\sum_{k=0}^{q-2} \sum_{j=1}^{n} \alpha_j^i \beta_j^k \mu_1(j, k) = \sum_{k=0}^{q-2} \sum_{v=0}^{k} \Delta(i_1 + k + 2, j(i_2, v)) x^{q-2-k} y^v
\]
\[
= \begin{cases} -x^{v_2} y^{v_2} & \text{if } 1 \leq i_1 \leq q - 1 \\ & \text{and } q^2 - q \leq i_2 \leq q^2 - i_1 - 1, \\ -1 & \text{if } i = (1, q^2 - 1), \\ 0 & \text{otherwise.} \end{cases} \tag{1}
\]

where the third equality follows from Corollary 6.1 (i), \(j(i_2, v)\) is defined in Corollary 6.1 and \(u = i - (1, q^2 - q)\).

For \(\mu_2(j, k)\) we have
\[
\sum_{k=q+1}^{q-1} \sum_{j=1}^{n} \alpha_j^i \beta_j^k \mu_2(j, k) = \sum_{k=q+1}^{q-1} \Delta(i_1 + q - k, i_2 + k - q) x^{q-1-k} y^{q-1-k}
\]
\[
= \begin{cases} -x^{v_2} y^{v_2} & \text{if } 1 \leq i_1 \leq q \text{ and } i_2 = q^2 - i_1, \\ 0 & \text{otherwise}, \end{cases} \tag{2}
\]

where the last equality follows from Corollary 6.1 (ii) and \(u = i - (1, q^2 - q)\).

Furthermore, since \(i_2 \leq q^2 - i_1\) provided \(i \in \Sigma(q, m)\), we have
\[
\Sigma(q, m) \cap (1, q^2 - q) = \{ i \in \Sigma(q, m) | 1 \leq i_1 \leq q, q^2 - q \leq i_2 \leq q^2 - i_1 \}. \tag{3}
\]

Now the proposition follows immediately from (1), (2) and (3). \(\Box\)
Definition 6.9 For every \( i \in \{1, \ldots, n\} \) and \( 1 \leq \delta \leq q + 1 \), define
\[
\varepsilon_i(\delta) = \begin{cases} 
\eta_i - \sum_{k=0}^{q+1-\delta} \mu_1(i, k)dx - \sum_{k=q+1-\delta}^{q} \mu_2(i, k)dx & \text{if } \delta \neq 1 \\
\eta_i - \sum_{k=0}^{q} \mu_1(i, k)dx & \text{if } \delta = 1.
\end{cases}
\]
Therefore by Proposition 6.3(b) and Proposition 6.6, we have
\[
\varepsilon_i(\delta) \in \Omega(-P_1 - \delta P_\infty) \text{ and } res_P(\varepsilon_i(\delta)) = 1,
\]
for every \( i = 1, \ldots, n \).

Proposition 6.11 Suppose \( m = l(q + 1) - \delta \). Then
\[
\omega(i) = \sum_{i=1}^{n} res_P(\omega(i))\varepsilon_i(\delta) \text{ for every } i \in \Sigma(q, m).
\]
Therefore for every \( \omega \in \Omega(l(q + 1)P_{0,0} - \delta P_\infty - D) \), we have \( \omega = \sum_{i=1}^{n} res_P(\omega)\varepsilon_i(\delta) \) by Proposition 6.4.

Proof. It is easy to prove that for every \( i \in \Sigma(q, m) \) either \( i_2 \leq q^2 - 2 \) or \( i = (t, q^2 - 1) \) with \( t \in \{0, 1\} \). Thus the proposition follows from Proposition 6.8, Proposition 6.9 and the following Lemma 6.7.

Lemma 6.7 In \( \mathbb{F} = k(x, y) \), we have
\[
\frac{x}{xq - x} + 1 + y^{q-1} = \frac{xy^{q^2-1}}{xq - x}.
\]
Proof. The proof immediately follows from \((y^{q-1} + 1)^q = y^{q^2 - q + 1} \) and \( x^{q+1} = y^q + y \).
We leave it to the reader.

Definition 6.10 (See Definition 4.10) For the code \( C_0(D, mP_\infty) \), define the syndrome \( S(\omega) \) of \( \omega = (w_1, \ldots, w_n) \in k^n \) by
\[
S(\omega)dx = \sum_{i=1}^{n} w_i \frac{y^i - \beta_i^l}{\beta_i^l} \varepsilon_i(\delta),
\]
where \( m = l(q + 1) - \delta \).

Theorem 6.1 Suppose \( m = l(q + 1) - \delta \), where \( l \) and \( \delta \) are defined as before. Then \( S(\omega) \in k[x, y] \) and
\[
c \in C_0(D, mP_\infty) \text{ if and only if } S(c) \equiv 0 \pmod{y^l}.
\]
Furthermore
\[
S(\omega) = \sum_{i=1}^{n} \omega_i \left( \sum_{k=0}^{q} \sum_{k=0}^{q-1} \alpha_i^k \beta_i^{l-k} y^{l-1-k} + \sum_{k=0}^{q} \sum_{k=0}^{q} \alpha_i^{l+2} \beta_i^{l-(\nu+1)} x^{q-2-k} y^\nu
+ T_\delta(x, y) \right) \pmod{y^l},
\]
where
\[
T_\delta(x, y) = \begin{cases} 
\sum_{k=q+1-\delta}^{q} \alpha_i^{l+k-q} \beta_i^{l-k-q} x^k y^{q-1-k} & \text{if } \delta \neq 1 \\
0 & \text{if } \delta = 1.
\end{cases}
\]
Proof. The first part of the theorem is a special case of Theorem 4.5.
Suppose \( \delta \neq 1 \) (for \( \delta = 1 \) the proof is the same). Since we can derive \((y - \beta) \cdot \{(y - \beta)^{q-1} + 1 \} = (x - \alpha) \cdot \sum_{k=0}^{q} \alpha^k x^{q-k} \) for every \((\alpha, \beta) \in H^*(k) \), we have
\[
S(\omega) = \sum_{i=1}^{n} \omega_i \beta_i^{-l} \left( (\sum_{j=0}^{l} \beta_i^j y^{l-1-j}) \sum_{k=0}^{q} \alpha_i^k x^{q-k} - \sum_{k=0}^{q} \mu_1(i, k) + \sum_{k=q+1-\delta}^{q} \mu_2(i, k) \right) (y^l - \beta_i^l).
\]
Now the proof of the second part is just a straightforward verification from the above equality.
6.3 Encoding the codes

In this section we give an encoding method for the code $C_\Omega^\sim(D, mP_\infty)$.

**Definition 6.11** Let $m$ be a positive integer and suppose $m = l(q + 1) - \delta$, where $l, \delta$ are nonnegative integers and $1 \leq \delta \leq q + 1$. A polynomial subspace $P(m, q)$ is defined by:

$$P(m, q) = \langle X^iY^{j+1} | 0 \leq i \leq q, 0 \leq j, (i, j) \neq (0, 0) \text{ and } iq + j(q + 1) \leq q^3 - 1 + 2g - m - 1 \rangle.$$

**Remark 6.3** Let $\mathcal{H}^*(k)$ be defined by

$$\mathcal{H}^*(k) := \{(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)\}, \text{ where } n = q^3 - 1.$$

Then by Proposition 6.4, the code $C_\Omega^\sim(D, mP_\infty)$ can be denoted as follows

$$C_\Omega^\sim(D, mP_\infty) = \{(f(\alpha_1, \beta_1), \ldots, f(\alpha_n, \beta_n)) | f \in P(m, q)\}.$$

**Proposition 6.12 (Encoding message symbols)** Let $K$ be the dimension of the code $C_\Omega^\sim(D, mP_\infty)$, and $\Sigma(q, m)$ be denoted by $\{(i_1, j_1), \ldots, (i_K, j_K)\}$ such that $Q(i_k, j_k) < Q(i_{k+1}, j_{k+1})$ for $1 \leq k \leq K - 1$. Let $\alpha = (a_1, \ldots, a_K) (a_k \in k)$ be the message symbols to be encoded, and let

$$a(X, Y) = \sum_{k=1}^{K} a_k X^{i_k} Y^{j_k}.$$

Then

$$c := (a(\alpha_1, \beta_1), \ldots, a(\alpha_n, \beta_n)) \in C_\Omega^\sim(D, mP_\infty).$$

**Proof.** Since for every $(i_k, j_k) \in \Sigma(q, m)$ we have

$$(i_k, j_k) = (i, j + 1) \text{ for some } (i, j) \in \Sigma^{(m)}(q).$$

Furthermore, for every $i \in \Sigma^{(m)}(q)$ $Q(i) \leq q^3 - 1 + 2g - m - 1$. Thus $a(X, Y) \in P(m, q)$. This means that $c \in C_\Omega^\sim(D, mP_\infty)$. □

Now we show how to recover the message symbols. Let $c = (c_1, \ldots, c_n), c_i \in k$ be the codeword encoded by the above encoding method, and let

$$c(i, j) := \sum_{\nu=1}^{n} c_\nu \alpha_{\nu}^{q^3-i} \beta_{\nu}^{2-j}.$$

And we still denote $\Sigma(q, m)$ by $\{(i_1, j_1), \ldots, (i_K, j_K)\}$ as above.

**Proposition 6.13 (Recovering message symbols)** Let the assumptions be as in Proposition 6.12. Suppose a codeword $c$ of $C_\Omega^\sim(D, mP_\infty)$ is encoded by the above encoding method. Then its message symbols are

$$a_1 = -c(i_1, j_1), a_2 = -c(i_2, j_2), \ldots, a_K = -c(i_K, j_K).$$
Chapter 6: Codes from Hermitian Curves

Proof. If \( c = (c_1, \ldots, c_n) \), then by the encoding method we have

\[
c_\nu = \sum_{k=1}^{K} a_k \alpha_{\nu}^k \beta_{\nu}^k,
\]

for every \( \nu = 1, \ldots, n \). Now consider any \((i_k, j_k) \in \Sigma(q,m)\) we have

\[
c(i_k, j_k) = \sum_{\nu=1}^{n} \sum_{\mu=1}^{K} a_\mu \alpha_{\nu}^{\mu} \beta_{\nu}^{\mu} \alpha_{\nu}^{q+1-i_k} \beta_{\nu}^{q^2-2-j_k}
\]

\[
= \sum_{\mu=1}^{K} a_\mu \sum_{\nu=1}^{n} \alpha_{\nu}^{q+1+i_\mu-1-i_k} \beta_{\nu}^{q^2-2+j_\mu-j_k} = -a_k,
\]

by the following lemma and since \( 0 \leq i_k \leq q \) and \( 0 \leq j_k \leq q^2 - 2 \) for \( 1 \leq k \leq K \).

This proves the proposition. \( \square \)

Lemma 6.8 Let \( 0 \leq s \leq 2q \) and \( 0 \leq t \leq q^2 - 2 \), then

\[
\Delta(s,t) = \begin{cases} 
-1 & \text{if } (s,t) = (0,0) \text{ or } (q+1,q^2-q-1) \text{ and } (q+1,q^2-2), \\
0 & \text{otherwise}.
\end{cases}
\]

Proof. Recall that \( \alpha^{q+1} = \beta^q + \beta \) for every \((\alpha, \beta) \in \mathcal{H}^*(k)\), one can prove the lemma immediately by Proposition 6.10.

6.4 Decoding the codes by finding a minimal recurrence relation

In this section, we first define for every received word a non-gap subscript sequence and its recurrence relation. After that we show that finding an error vector of a received word can be reduced to finding a minimal recurrence relation for the non-gap subscript sequence.

By Theorem 6.1, the syndrome of \( w \) can be written as

\[
S(w) = \sum_{u_1=0}^{q} \sum_{u_2=0}^{l-1} S_{u_1} u_1^{u_1} y^{u_2} + y' S(x,y)
\]

where \( S_{u} \in k \) for \( 0 \leq u_1 \leq q \) and \( 0 \leq u_2 \leq l-1 \), and \( S(x,y) \in k[x,y] \).

Definition 6.12 (1) Define a sequence \( \{U^0_{i}\}_{i \in \Sigma(q)} \) of \( w \) as follows

\[
U^0_{i_1,i_2} = \begin{cases} 
S_{q-i_1,l-1-i_2} & \text{if } i_2 \leq l-1 \\
0 & \text{otherwise}.
\end{cases}
\]

We call this sequence a non-gap subscript sequence of \( w \).

(2) Define a 2-dimensional array \( \{U_i\}_{i \in \Sigma} \) induced by the non-gap subscript sequence \( \{U^0_{i}\}_{i \in \Sigma(q)} \), as follows:

(i) \( U_i = U^0_i \) if \( i \in \Sigma(q) \);

(ii) For every \( i \in \Sigma \setminus \Sigma(q) \), suppose \( i_1 = k(q+1) + i'_1 \) with \( i'_1 \leq q \), then define

\[
U_i = \sum_{\nu=0}^{k} \binom{k}{\nu} U^0_{i'_1 \nu(q+1)+k+i_2}.
\]

In the following, we also call \( \{U_i\}_{i \in \Sigma} \) a non-gap subscript sequence of \( w \), and denote it by \( U \).
Definition 6.13 Let $k[X,Y]$ be the polynomial ring of two variables over $k$. Then a polynomial $f \in k[X,Y]$ can be written as $f(X,Y) = \sum_{i \in \mathcal{C}_f} f_i X^i Y^j$, where $\mathcal{C}_f = \{ i \in \Sigma | f_i \neq 0 \}$. Define $k[X,Y](q)$ by $k[X,Y](q) = \{ f \in k[X,Y] | \mathcal{C}_f \subseteq \Sigma(q) \}$. For $0 \neq f \in k[X,Y](q)$, define the degree of $f$ to be an element $s$ in $\mathcal{C}_f$ such that $Q(s) = \max\{Q(i) | i \in \mathcal{C}_f\}$, and denote it by $\text{Deg}(f)$. Furthermore we call $Q(\text{Deg}(f))$ the $Q$-degree of $f$.

Definition 6.14 Let $U$ be a non-gap subscript sequence. Let $f = \sum_{i \in \mathcal{I}(q)} f_i X^i Y^j \in k[X,Y]$ and $i \in \Sigma(q)$. If $\sum_{i \in \mathcal{I}(q)} f_i U^i = 0$, then $f$ is called a recurrence polynomial for $U$ at $i$. We denote $\sum_{i \in \mathcal{I}(q)} f_i U^i$ by $f(U)(i)$.

Theorem 6.2 (Decoding Theorem) Suppose $m = l(q + 1) - \delta$, where $l$ and $\delta$ are defined as before. Let $\omega \in k^n$, suppose $\omega = c + e$, where $c$ is a codeword of $C_0(d, mP_\infty)$ and $e$ is an error vector. Let $U$ be the non-gap subscript sequence of $\omega$.

Existence: There exist $f(X,Y) \in k[X,Y](q)$ and $r \in k[x,y]$ such that $(r/f(x,y))dx \in \Omega(-D - \delta P_\infty)$, where $f(x,y) \in k[x,y]$, $(\text{res}_p(rdx/f(x,y))), ..., \text{res}_n(rdx/f(x,y))) = e$, and the following holds

i) $f[U,n_m] = 0$, where $n_m \in \Sigma(q)$ and $Q(n_m) = m + 1$.

ii) $r \equiv f(x,y)S(\omega) \mod y'$.

Uniqueness: Let $t = [(d^* - 1)/2 - ((q - 1)/2)^2 + 1]/2$, where $d^*$ is the designed minimum distance of the code. Suppose the weight of $e$ is less than or equal to $t$. Let $f(X,Y) \in k[X,Y](q)$ such that condition (i) holds and the $Q$-degree of $f(X,Y)$ is minimal among all the $Q$-degrees of recurrence polynomials for $(U,n_m)$. Then after taking $r \equiv f(x,y)S(\omega) \mod y'$, we have

$(\text{res}_p(rdx/f(x,y))), ..., \text{res}_n(rdx/f(x,y))) = e$, and $(r/f(x,y))dx \in \Omega(-\delta P_\infty - D)$. We call this $f(x,y)$ a minimal recurrence relation of $(U,n_m)$.

Proof. By the existence part of Theorem 4.7, there exist $f_0,p,r \in k[x,y]$, such that $(r/f_0)dx \in \Omega(-D - \delta P_\infty)$, $(\text{res}_p(rdx/f_0), ..., \text{res}_n(rdx/f_0)) = e$, and (i) $f_0 S(\omega) = r + py'$ and (ii) $\deg(r) - \deg(f_0) \leq 2g - 2 + \delta$ hold. Thus we can write $f_0$ as follows, $f_0 = \sum_{i \in \mathcal{I}(q)} f_i x^i y^j$ with $\mathcal{C}_f \subseteq \Sigma(q)$. Now take $f(X,Y) = \sum_{i \in \mathcal{I}(q)} f_i X^i Y^j$. Then $f(X,Y) \in k[X,Y](q)$. Suppose $\text{Deg}(f) = s$, we have $Q(s) = \deg(f)$ and $f(x,y) = f_0$. Furthermore, by the definition of non-gap subscript sequence $U$ of $\omega$, we can expand $f_0 S(\omega)$ to

$f_0 S(\omega) = \sum_{u_1 = 0}^{q} \sum_{u_2 = 0}^{l-1} A_u x^{u_1} y^{u_2} + y'A(x,y)$,

where $A_u = f[U](q - u_1, l - 1 - u_2)$ and $A(x,y) \in k[x,y]$. Therefore

$\deg(r) - \deg(f_0) \leq 2g - 2 + \delta \Rightarrow f[U](q - u_1, l - 1 - u_2) = 0$ (4)

for every $(q - u_1, l - 1 - u_2) \in \Sigma^{m + 1 - \delta}(q)$. 


which follows from Lemma 6.9, where $S = Q(s)$. It is equivalent to $f[U, n_m] = 0$. This proves the existence.

The uniqueness immediately follows from the uniqueness part of Theorem 4.7. and the above equivalent condition (4).  

Lemma 6.9 Let $s, n_m \in \Sigma(q)$ such that $Q(n_m) = m + 1$ (it is always possible by Lemma 6.1 and Remark 6.2). If we denote $Q(s) = S$ and suppose $m + 1 \geq S$, then

$$
\Sigma^{m+1-S}(q) = \{(q, l-1) - i| 0 \leq i_1 \leq q, 0 \leq i_2 \leq l-1 \text{ and } Q(i) \geq q(q-1) + S + \delta - 1\}.
$$

Proof. Since $Q((q, l-1) - i) = q^2 + (l-1)(q + 1) - Q(i)$, we have

$$
Q(i) \geq q(q-1) + S + \delta - 1 \iff Q((q, l-1) - i) < m + 1 - S.
$$

This proves the lemma.  

Remark 6.4 In Chapter 7, we will give an algorithm to find a minimal recurrence relation for a non-gap subscript sequence $(U, n_m)$ by finding a set of minimal degree recurrence polynomials, where the degree set of those minimal degree polynomials is also nondegenerate. So the complexity of decoding algorithm is less than $3qm^2 + 2n^2 + 7q^3m$ provided $q \geq 4$.

### 6.5 Computing the residues

Let $(\alpha, \beta) \in \mathcal{H}^*(k)$, and $f, r \in k[x, y]$ such that $\deg(f) < q^3$, $\deg(r) < q^3$ and $r dxf=f \in \Omega(-\delta P_\infty - D)$. In this section we will show how to compute the residue $rdx/f$ at $P_{\alpha, \beta}$ explicitly.

Remark 6.5 (i) From Section 6.1.1, we know that $x^{q+1} = y^q + y$ in $k[x, y]$ and $\alpha^{q+1} = \beta^q + \beta$. Therefore if $\alpha \neq 0$, we have $y - \beta = \alpha^q(x - \alpha) + \alpha(x - \alpha)^q + (x - \alpha)^{q+1} - (y - \beta)^q$. By this equality we can derive, that for every $j \in \mathbb{N}$,

$$
y^j = \{\beta + \alpha^q(x - \alpha) + (x - \alpha)^{q+1} - (x - \alpha)^{q+j}\}^j + R_j(x, y),
$$

where $R_j(x, y) \in k[x, y]$ and has at least valuation $q^3$ at $P_{\alpha, \beta}$.

(ii) For every $f \in k[x, y]$, we can write it as $f = \sum_{j=0}^{\mu_f} (\sum_{i=0}^{\nu_i} a_{ij} x^i) y^j$.

In the following we will construct several sets of data. In fact one can use these sets as a database to construct an algorithm of computing residues, see Proposition 6.15.

Definition 6.15 Let $i, j \in \mathbb{N}$. If $\alpha \neq 0$,

(1) for every $k \in \{0, \ldots, i\}$, define $A_k(\alpha, i)$ to be the coefficient of $(x - \alpha)^k$ in the binomial expansion of $x^i = \{(x - \alpha) + \alpha\}^i$;

(2) for every $l \in \{0, \ldots, j(q^2 + q)\}$, define $B_l(\alpha, \beta; j)$ to be the coefficient of $(x - \alpha)^l$ in the expansion of $\{(\beta + \alpha^q(x - \alpha) + (x - \alpha)^{q+1} - (x - \alpha)^{q+j})\}^j$. 

If $\alpha = 0$, for every $l \in \{0, \ldots, j(q^2 + q)\}$, define $B_l(0, \beta; j)$ to be the coefficient of $x^l$ in the expansion of $(x^{q+1} - x^{q+j} - \beta^j)$.
Definition 6.16 Suppose \( f = \sum_{j=0}^{\mu_f}(\sum_{i=0}^q a_{ij}x^i)y^j \in k[x,y] \). For every \( s \in \mathbb{N} \), define
\[
f[\alpha, \beta; s] := \begin{cases} \sum_{j=0}^{\mu_f} \sum_{i=0}^q a_{ij} B_{s-1}(0, \beta; j) & \text{if } \alpha = 0, \\ \sum_{j=0}^{\mu_f} \sum_{i=0}^q a_{ij} \sum_{t=0}^s \lambda_t(\alpha, i) B_{s-1}(\alpha, \beta; j) & \text{otherwise}. \end{cases}
\]

Proposition 6.14 Let \( f \) be as in the above definition. Then
\[
f = \sum_{s=0}^{\mu_f(\beta + q) + q} f[\alpha, \beta; s](x - \alpha)^s + f^*,
\]
where \( f^* \in k[x,y] \) and \( v_{p_{\alpha, \beta}}(f^*) \geq q^3 \).

Proof. For every \( \alpha \in k \) the ring \( k[x,y] \) has \( \{(x - \alpha)^iy^j| i, j \in \mathbb{N}\} \) as a basis. Every \( y^j \) can be written as a linear combination of \( 1, (x - \alpha), \ldots, (x - \alpha)^{\beta(\beta + q)} \) with a remainder term \( R_j(x,y) \) which has at least valuation \( q^3 \) at \( p_{\alpha, \beta} \), by Remark 6.5 and Definition 6.15. Thus we can write
\[
f = \sum_{s=0}^{\mu_f(\beta + q) + q} a_s(x - \alpha)^s + f^*,
\]
for some constants \( a_s \in k, \) \( f^* \in k[x,y] \) and \( v_{p_{\alpha, \beta}}(f^*) \geq q^3 \). It is a straightforward verification that \( a_s = f[\alpha, \beta; s] \), see Definition 6.15. \( \square \)

Corollary 6.2 \( v_{p_{\alpha, \beta}}(f) = k \) if and only if
\[
f[\alpha, \beta; k] \neq 0 \text{ and } f[\alpha, \beta; s] = 0 \text{ for } 0 \leq s \leq k - 1.
\]

Proof. By the facts of Section 6.1.1 and the assumption on \( \deg(f) \), we have \( v_{p_{\alpha, \beta}}(f) \leq -v_{p_{\infty}}(f) < q^3 \). Thus by Proposition 6.14, we have
\[
\sum_{s=0}^{\mu_f(\beta + q) + q} f[\alpha, \beta; s](x - \alpha)^s = k.
\]
Therefore \( v_{p_{\alpha, \beta}}(f) = k \) is equivalent to \( f[\alpha, \beta; k] \neq 0 \) and \( f[\alpha, \beta; s] = 0 \) for \( 0 \leq s \leq k - 1. \) \( \square \)

Proposition 6.15
\[
\text{res}_{p_{\alpha, \beta}}(\frac{r}{f}dx) = \frac{r[\alpha, \beta; v_f - 1]}{f[\alpha, \beta; v_f]},
\]
where \( v_f := v_{p_{\alpha, \beta}}(f) \).

Proof. By Proposition 6.14 and the assumption of \( \deg(f) < q^3 \) and \( \deg(r) < q^3 \), we have
\[
f = \sum_{s=0}^{\mu_f(\beta + q) + q} a_s(x - \alpha)^s + f^* \text{ and } r = \sum_{s=0}^{\mu_r(\beta + q) + q} b_s(x - \alpha)^s + r^*,
\]
respectively, where \( a_s = f[\alpha, \beta; s] \) and \( a_{v_f} \neq 0, \) \( b_s = r[\alpha, \beta; s] \) and \( v_r = v_{p_{\alpha, \beta}}(r). \) Since \( f[\alpha, \beta; (x - \alpha)^{v_f}]^{-1}|_{x = \alpha, y = \beta} = 1, \) we can write
\[
\frac{1}{f} = \frac{1}{a_{v_f}(x - \alpha)^{v_f}}(1 + \sum_{k=1}^{\infty} c_k(x - \alpha)^k),
\]
where
for some constants $c_k \in k$, since $(x - \alpha)$ is a local parameter of $P_{\alpha, \beta}$. Furthermore we have $v_r \geq v_f - 1$ since $r dx / f \in \Omega(-\delta \pi_\infty - D)$. Thus it is a straightforward verification that

$$\frac{r}{f} dx = \left\{ \frac{b_{v_f - 1}}{a_{v_f}(x - \alpha)} + \sum_{k=0}^{\infty} d_k (x - \alpha)^k \right\} d(x - \alpha),$$

where $d_k \in k$ for $k = 0, 1, \ldots$. This implies that

$$\text{res}_{P_{\alpha, \beta}}(\frac{r}{f} dx) = \frac{r[\alpha, \beta; v_f - 1]}{f[\alpha, \beta; v_f]},$$

since $x - \alpha$ is a local parameter of $P_{\alpha, \beta}$. □
A Appendix: The proofs of Proposition 6.10 and Corollary 6.1

To prove the proposition, we need the following lemma.

**Lemma 6.10** Let $i = (i_1, i_2) \in \Sigma(q) \setminus \{0\}$ and $Q(i) \leq q^3 + 2q^2 - 2$. If $Q(i) \leq q^3$, then $v_{P_{\omega}}(x^{i_1}y^{i_2}/(x^{q^2} - x)) \geq 0$, otherwise

$$\frac{x^{i_1}y^{i_2}}{x^{q^2} - x} = \left(\frac{y}{x}\right)^k + (j + 1)(\frac{y}{x})^{k-q^2+1} + f,$$

where $k = Q(i) - q^3$, $j = i_1 + i_2 - q^2 + q - 1$ and $f \in F$ with $v_{P_{\omega}}(f) \geq 0$.

Therefore if $i = (0, q^2 - q + 1)$ then $\text{res}_{P_{\omega}}(\frac{x^{i_1}y^{i_2}}{x^{q^2} - x}d(\frac{y}{x})) = 1$, otherwise it is equal to zero.

**Proof.** Since $v_{P_{\omega}}(x^{i_1}y^{i_2}/(x^{q^2} - x)) = -Q(i) + q^3$, we have $v_{P_{\omega}}(x^{i_1}y^{i_2}/(x^{q^2} - x)) \geq 0$ if $Q(i) \leq q^3$. Now suppose $Q(i) > q^3$, then $j(q + 1) \geq 0$, thus $j \geq 0$. Because of $x^{q+1} = y^q + y$, we have the following expansions:

$$x^{j(q+1)} = y^j + jy^{q-1} + \sum_{i=2}^{q} \left(\begin{array}{c} j \\ i \end{array}\right) y^{j-1-i} + 1;$$

$$x^{q^2-1} = y^{q^2-1} - y^{q^2-1} + \sum_{i=2}^{q-1} \left(\begin{array}{c} q-1 \\ i \end{array}\right) y^{q-1-i};$$

$$x^{q^2-1}(x^{q^2-1} - 1) = y^{2q^2-1} + \sum_{i=2}^{q-1} b_i y^{2q^2-1-i}.$$  

for some constants $b_j \in k$. Moreover

$$\frac{y^{q-1)^2}}{x^{q^2-1} - 1} = \left(\frac{y}{x}\right)^{-(q^2 - 1)} - \sum_{i=2}^{q-1} \frac{b_i}{x^{q^2-1} - 1},$$

by the previous equality and $-(q^2 - 1) + 2(q^2 - q) - i(q - 1) = q^2 - q - (i + 1)(q - 1)$. Now by the above equalities and $j(q + 1) = k + i_1 - 1$ and $i_2 - k = q^2 - q - jq$, we can derive

$$x^{i_1}y^{i_2}/x^{q^2} = \left(\frac{y}{x}\right)^k + (j + 1)(\frac{y}{x})^{k-q^2+1} + f,$$

where $f \in F$ and $v_{P_{\omega}}(f) \geq 0$. Finally, it is easy to see that $k = 1$ if and only if $i = (0, q^2 - q + 1)$, and $k - q^2 + 1 = 1$ if and only if $i = (0, q^2)$ and $j = q - 1$. Thus

$$\text{res}_{P_{\omega}}(\frac{x^{i_1}y^{i_2}}{x^{q^2} - x}d(\frac{y}{x})) = 1,$$

if $i = (0, q^2 - q + 1)$ and otherwise it is equal to zero, since $x/y$ is a local parameter of $P_{\omega}$. □

**Proof of Proposition 6.10.** Since $\beta^{q^2-1} = 1$ for every $\beta \in k$, we have $\Delta(s, t') = \Delta(s, t)$. Hence it is sufficient to consider $\Delta(s, t)$ with $0 \leq t \leq q^2 - 2$.  

If \((s,t) = (0,0)\) then \(\Delta(0,0) = q^3 - 1 = -1\). Now suppose \((s,t) \neq (0,0)\). It is easy to see that the poles of \(x^s y^t/(x^q - x)\) are in the set \(\mathcal{H}^*(k) \cup \{(0,0), P_\infty\}\). Now consider the residue of \((x^s y^t dx)/(x^q - x)\) at \(P_\infty\). By [6, Theorem 9 and Corollary to Theorem 9, Ch.VI], we have \(dy = x^q dx\) since \(x^{q+1} - y^q - y = 0\) and

\[
\left(\frac{x}{y}\right)^q d\left(\frac{1}{y}\right) = \frac{dy}{y^2},
\]

since \((x/y)^{q+1} - (1/y)^q - 1/y = 0\) if \(y \neq 0\). Thus \(d(x/y) = -(y/x)^q(1/y^2)x^q dx = -y^{q-2} dx\). Therefore

\[
\frac{x^s y^t}{x^q - x} dx = \frac{x^s y^{i_2}}{x^q - x} dx,
\]

where \(i_2 = t - q + 2\) and \(Q((s,i_2)) \leq q^3 + 2q^2 - 2\). Therefore by Lemma 6.10, we have

\[
\text{res}_{P_\infty}\left(\frac{x^s y^t}{x^q - x} dx\right) = \begin{cases} -1 & \text{if } s = 0, t = q^2 - 1; \\ 0 & \text{otherwise}, \end{cases}
\]

but by the assumption we have \(t \leq q^2 - 2\), hence \(\text{res}_{P_\infty}\left(\frac{x^s y^t}{x^q - x} dx\right) = 0\) if \((s,t) \neq (0,0)\).

Finally, by the residue theorem [6, Theorem 3, Ch.III] and Proposition 6.2, we have

\[
\Delta(s,t) = -\sum_{(\alpha,\beta) \in \mathcal{H}^*(k)} \text{res}_{P_\alpha,\beta}\left(\frac{x^s y^t}{x^q - x} dx\right)
\]

\[
= \text{res}_{P_\infty}\left(\frac{x^s y^t}{x^q - x} dx\right) = \begin{cases} -1 & \text{if } (s,t) = (0,0); \\ 0 & \text{otherwise}. \end{cases}
\]

\(\square\)

**Proof of Corollary 6.1.** By the assumption, we can write \(i_1 + k + 2 = \mu(q + 1) + \nu\), where \(\mu \in \{0,1\}\) and \(0 \leq \nu \leq q\). Then by Proposition 6.10, we have \(\Delta(i_1 + k + 2, j(i_2, v)) = 0\) if \(\mu = 0\) and \(\nu \neq 0\), and \(\Delta(i_1 + k + 2, j(i_2, v)) = \Delta(0, j(i_2, v) + 1) + \Delta(0, j(i_2, v) + q)\) if \(\mu = 1\) and \(i_1 + k + 2 = q + 1\) since \(\alpha^{q+1} = \beta^q + \beta\). Furthermore, by \(i \in \Sigma(m,q)\), we have \(j(i_2, v) \leq q^2 - 1\) and \(j(i_2, v) + q \leq q^2 - 1\), and the equalities hold, respectively, if and only if \(v = 0, k = q - 2\) with \(i = (1, q^2 - 1)\) and \(v = i_2 - q^2 + q\), respectively. This proves the (i). The proof of (ii) is similar to the above, we leave it to the reader. \(\square\)
Chapter 7
A Realization of the Decoding Algorithm

In this chapter, for the codes $C_0^n(D, mP_\infty)$ from Hermitian curves (discussed in Chapter 6), we give a realization of their decoding algorithm. The main procedure is to give an algorithm for finding minimal recurrence polynomials of non-gap subscript sequences, which is inspired by Sakata's idea [61]. Due to the difference between the problems we have and the one solved by Sakata's algorithm, we cannot use Sakata's algorithm directly. The main differences between them are the orders of sequences those two problem have. Although we may modify Sakata's algorithm to our problem, the complexity will be less if we construct an algorithm directly for our problem.

In Section 7.1, we define a minimal recurrence pair and auxiliary pair, respectively. In Section 7.2, we present the main theorem of this chapter, which tells us how to find a minimal recurrence pair for a non-gap subscript sequence. Section 7.3 consists of three algorithms, they are: an algorithm for finding minimal recurrence polynomials, an algorithm for computing residues and a decoding algorithm, respectively. The decoding algorithm given in that section actually is a realization of Decoding Theorem 6.3. In Section 7.4, the complexity of those decoding algorithms is given. Finally, a simple example is given in Section 7.5.

Many notations defined in Chapter 6 will be used in this chapter. They are: The finite field $k = GF(q^2)$, the set of all nonnegative integer pairs $\Sigma$, the map $Q : \Sigma \to \mathbb{N}$ (Definition 6.3), two sets $\Sigma(q)$ and $\Sigma^4(q)$ (Definition 6.4), a non-gap subscript sequence $U$ (Definition 6.12), a subset of polynomials $k[X,Y](q)$ (Definition 6.13), the degree map $\text{Deg} : k[X,Y](q) \to \Sigma(q)$ (Definition 6.13) and a recurrence polynomial $f$ for $(U, n)$ (Definition 6.14), which can be also denoted by $f[U, n] = 0$.

7.1 Minimal recurrence pair and other notations

In this section we present some notations which will be used in the rest of this chapter. The main notations will be minimal recurrence pair and auxiliary pair.

Definition 7.1 (Next non-gap) Let $n \in \Sigma(q)$. Define $n^+ \in \Sigma(q)$ satisfying: (i) $Q(n^+) > Q(n)$; (ii) there does not exist any element $i \in \Sigma(q)$ such that $Q(n) < Q(i) < Q(n^+)$. It means that $Q(n^+)$ is the next non-gap after $Q(n)$. 

Proposition 7.1 Let \( n,t \in \Sigma(q) \), denote \( Q(n) = N \) and \( Q(n^+) = N^+ \) and \( Q(t) = T \). Then \( \Sigma^{N^+ - T}(q) = \Sigma^{N - T + 1}(q) \).

Proof. This can be easily proved by the above definition and Remark 6.2. We leave it to the reader. \( \square \)

Definition 7.2 (Maximal set and minimal set) Let \( S \subseteq \Sigma(q) \). The maximal set of \( S \) is defined by

\[
\{ s \in S \mid \text{there is no } t \in S \text{ such that } t > s \},
\]

where \( t = (t_1, t_2) > s = (s_1, s_2) \) means that both \( t_i \geq s_i \) for \( i = 1, 2 \) and \( t \neq s \). We denote it \( \text{MAX}(S) \). The minimal set of \( S \) is defined by

\[
\{ s \in S \mid \text{there is no } t \in S \text{ such that } t < s \}.
\]

We denote it \( \text{MIN}(S) \).

Definition 7.3 (Minimal recurrence pair) Let \( U \) be a non-gap subscript sequence and \( n \in \Sigma(q) \). Let \( D(n) \) be defined by \( D(n) := \text{MIN}\{ \text{Deg}(f) \mid f \in k[X,Y](q), f[U,n] = 0 \} \). For every \( s \in D(n) \), choose an \( f_s \) such that \( f_s[U,n] = 0 \) and \( \text{Deg}(f_s) = s \). Define \( F(n) = \{ f_s \mid s \in D(n) \} \). We call it a minimal recurrence set for \( (U,n) \), and call \( <D(n), F(n)> \) a minimal recurrence pair for \( (U,n) \). Furthermore, we denote

\[
\mathcal{D}(n,V) := \{ s \in D(n) \mid f_s[U,n^+] = 0 \} \quad \text{and} \quad \mathcal{D}(n,N) := \{ s \in D(n) \mid f_s[U,n^+] \neq 0 \}.
\]

Remark 7.1 (a) It is easy to see that,

\[
\Sigma_D(n)(q) \supseteq \{ \text{Deg}(f) \mid f \in k[X,Y](q) \text{ and } f[U,n] = 0 \}.
\]

(b) It can be proved by Corollary 7.2 in Appendix B, that \( \mathcal{D}(n,V) \) and \( \mathcal{D}(n,N) \) do not depend on the choice of the elements of \( F(n) \).

Now the question is how to find a minimal recurrence set \( F(n^+) \) provided that a minimal recurrence set \( F(n) \) is given. In the next section we will give a theorem to solve this problem, which is called the main theorem of this chapter. The main idea is to use a so-called auxiliary pair which is constructed from some known minimal recurrence pairs \( F(m) \), where \( Q(m) < Q(n^+) \). Before doing this, we need more notations. The rest of this section are the definitions of those notations and their properties.

In the following we always assume \( n, s \in \Sigma(q) \), \( S \) be a subset of \( \Sigma(q) \).

(1) Denote \( \Sigma_s(q) := \{ i \in \Sigma(q) \mid s \leq i \} \) and \( \Sigma_S(q) = \bigcup_{s \in S} \Sigma_s(q) \). Conversely, we denote \( \Gamma_s(q) := \{ i \in \Sigma(q) \mid s \geq i \} \) and \( \Gamma_S(q) = \bigcup_{s \in S} \Gamma_s(q) \).

(2) Let

\[
\chi(k) = \begin{cases} 
-1 & \text{if } k < 0 \\
0 & \text{if } 0 \leq k.
\end{cases}
\quad \text{and} \quad
\xi(\varepsilon) := \begin{cases} 
(q + 1, -q) & \text{if } \varepsilon = -1 \\
(0, 0) & \text{if } \varepsilon = 0.
\end{cases}
\]

Define \( c(n,s) := n - s + \xi(\chi(n_1 - s_1)) \).
Remark 7.2 It is easy to see that,
(1) \( Q(e) = 0 \) for \( e \in \{-1, 0\} \);
(2) \( Q(n) - Q(s) \in \mathcal{N}(q) \) if and only if \( c(n, s) \in \Sigma(q) \).
(3) Let \( f \in k[X, Y](q) \) with \( \text{Deg}(f) = s \). The necessary and sufficient condition for \( f[U, n] = 0 \) but \( f[U, n^+] \neq 0 \) is \( c(n, s) \in \Sigma(q) \) and \( f[u|c(n, s)] \neq 0 \).

(3) Denote \( \Lambda(n, s) := \{ i \in \Sigma(q) | c(n, i) \geq s \} \). Furthermore, for a set \( S \) we denote \( \Lambda(n, S) := \bigcup_{n \in S} \Lambda(n, s) \).
(4) The maximal complementary set of \( S \) is defined by \( \text{MAX} \{ \Sigma(q) \setminus \Sigma_S(q) \} \). We denote it \( \text{Cmax}(S) \).
(5) A finite subset \( S \) of \( \Sigma(q) \) is called a nondegenerate set if and only if for any \( s, t \in S \), \( s \neq t \).

Remark 7.3 It is easy to prove the following statements,
(ii) For a nondegenerate set \( S \subseteq \Sigma(q) \), \( S = \text{MIN}(\Sigma_S(q)) \) and \( S = \text{MAX}(\Gamma_S) \).
(ii) For any set \( S \subseteq \Sigma(q) \), \( \text{MAX}(S), \text{Cmax}(S) \) and \( \text{MIN}(S) \), respectively, are nondegenerate sets.

Proposition 7.2 Let \( S \) be a nondegenerate set of \( \Sigma(q) \), then \#(S) \leq q.

Proof. Let \( s, t \in S \) such that \( s \neq t \). We claim that \( s_1 \neq t_1 \). Otherwise, \( s \leq t \) if \( s_2 \leq t_2 \) and \( s \geq t \) if \( s_2 \geq t_2 \), a contradiction. Therefore \#(S) = \#(s_1 \in S) \leq q \) since \( S \subseteq \Sigma(q) \). □

Proposition 7.3 Let \( S \) be a nondegenerate set of \( \Sigma(q) \). Then \( \text{Cmax}(S) \) is a unique nondegenerate set such that \( \Gamma_{\text{Cmax}(S)} = \Sigma(q) \setminus \Sigma_S(q) \).

Proof. By the definition of \( \text{Cmax}(S) \), it is obvious that \( \Gamma_{\text{Cmax}(S)} \supseteq \Sigma(q) \setminus \Sigma_S(q) \). Now for every \( i \in \Gamma_{\text{Cmax}(S)} \), there exists a \( c \in \text{Cmax}(S) \) such that \( i \leq c \). Hence \( i \notin \Sigma_S(q) \), otherwise \( c \in \Sigma_S(q) \) which is a contradiction. Thus \( i \in \Sigma(q) \setminus \Sigma_S(q) \). Therefore \( \Gamma_{\text{Cmax}(S)} \subseteq \Sigma(q) \setminus \Sigma_S(q) \). The uniqueness of \( \text{Cmax}(S) \) is obvious. □

(6) Let \( N := Q(n) \). If for every \( m \in \Sigma^N(q) \), \( f[U, m] = 0 \) but \( f[U, n] \neq 0 \), then \( n \) is called the order of \( f \) with respect to \( U \) and denoted by \( \text{Ord}(f) \).

Definition 7.4 (Reducing \( f \)) Let \( f \in k[X, Y] \). For every \( i \in \mathcal{C}_f \), suppose \( i_1 = i_{12}(q + 1) + i_{11} \), where \( i_{12}, i_{11} \in \mathbb{N} \) and \( 0 \leq i_{11} \leq q \). Define \( \bar{f} = \sum_{i \in \mathcal{C}_f} f_i X^{s_2}(Y^q + Y)^{i_2} Y^{i_2} \).

Proposition 7.4 Let \( f \in k[X, Y] \), then \( \bar{f} \in k[X, Y](q) \), and \( f[U](i) = \bar{f}[U](i) \) for every \( i \in \Sigma(q) \). Furthermore, if there exists an \( s \in \mathcal{C}_f \cap \Sigma(q) \) (for \( \mathcal{C}_f \) we refer to Definition 6.13) such that \( Q(i) < Q(s) \) for every \( i \in \mathcal{C}_f \setminus \{s\} \). Then \( \text{Deg}(\bar{f}) = s \). Moreover, if \( f[U](i) = 0 \) for every \( i \in \Sigma^Q(n) - Q(s)(q) \), where \( n \in \Sigma(q) \), then \( \bar{f}[U, n] = 0 \).

Proof. See Appendix A. □

(7) Define \( \text{max}(n, s) := (\max(n_1, s_1), \max(n_2, s_2)) \). Furthermore, we define,
(i) \( \mathcal{U}(n, s; 0) := \{ \max(s, n - c) | c \in \text{Cmax}(\mathcal{D}(n)) \} \).
(ii) $\mathcal{U}(n,s; -1) := \{\max(s, n - c + \xi(-1)) | c \in \text{Cmax}(\mathcal{D}(n)) \text{ and } n_1 - c_1 < 0\}.$

(iii) $\mathcal{V}(n,s) = \begin{cases} \{(s_1, n_2 - q + 1) \} \cap \Sigma(q) & \text{if } s_1 > n_1 \\ \{(s_1, n_2 + 1), (n_1 + 1, s_2), (n_1 + 1, n_2 - q + 1) \} \cap \Sigma(q) & \text{otherwise} \end{cases}.$

(iv) $\mathcal{W}(n,s) = \begin{cases} \{c(n,s), (q, n_2 - s_2 - q) \} \cap \Sigma(q) & \text{if } n_1 \neq q, n_1 \geq s_1 \text{ and } n_2 - s_2 \geq q \\ \{c(n,s)\} & \text{otherwise} \end{cases}.$

Definition 7.5 (Auxiliary pair) Let $U$ be a non-gap subscript sequence, let $S \subseteq \Sigma(q)$ and $n \in \Sigma(q).$ If for every $i \in S,$ there exists a $g_i \in k[X,Y](q)$ with $\text{Deg}(g_i) = t$ and $Q(\text{Ord}(g_i)) < Q(n),$ such that $i \in \mathcal{W}(\text{Ord}(g_i), t),$ then we call $< S, \mathcal{G} >$ an auxiliary pair for $(U, n^+),$ where $\mathcal{G} := \{g_i | i \in S\}.$

7.2 Main Theorem

Before we give the main theorem we need the following two propositions which are called Procedure I and II. Actually these two procedures give a method to construct minimal recurrence polynomials for $(U, n^+)$ provided that a minimal recurrence pair for $(U, n)$ and an auxiliary pair for $(U, n^+),$ respectively are given.

Proposition 7.5 (PROCEDURE I) Let $f \in k[X,Y](q)$ with $\text{Deg}(f) = s,$ such that $f[U,n] = 0$ but $f[U,n^+] \neq 0.$ Let $t \in \Sigma(q)$ such that $t > s$ and $c(n,t) \notin \Sigma(q).$ Denote $r = t - s$ and $h := h(f) = X^r Y^r f.$ Then $\text{Deg}(h) = t$ and $h[U,n^+] = 0.$

Proof. See Appendix B. □

Proposition 7.6 (PROCEDURE II) Let $f,g \in k[X,Y](q)$ with $\text{Deg}(f) = s$ and $\text{Deg}(g) = t.$ Suppose for a non-gap subscript sequence $U,$

$\text{Ord}(f) = n$ so that $f[U](c(n,s)) = d_j \neq 0,$

$\text{Ord}(g) = m$ so that $g[U](c(m,t)) = d_g \neq 0,$

where $m,n \in \Sigma(q)$ with $Q(m) < Q(n),$ and $c(n,s)$ and $c(m,t) \in \Sigma(q).$

Suppose $w \in \mathbb{Z} \times \mathbb{Z}$ with $Q(w) = Q(n) - Q(m) + Q(t)$ and $r \in \Sigma(q)$ such that $r \geq s$ and $r - w \geq 0.$ Let

$h := h(f,g) = X^w Y^w f - (d_j/d_g)X^n Y^n g,$

where $u = r - s$ and $v = r - w.$ Then we have $\text{Deg}(h) = r$ and $h[U,n^+] = 0.$

Proof. See Appendix B. □

Theorem 7.1 (Main Theorem) Let $n \in \Sigma(q).$ Suppose $< \mathcal{D}(n), \mathcal{F}(n) >$ is a minimal recurrence pair for $(U, n)$ and $< \text{Cmax}(\mathcal{D}(n)), \mathcal{G}(n) >$ is an auxiliary pair for $(U, n^+).$ Define

$T := \text{MIN}\{\Sigma_p(n) \setminus \Lambda(n, \mathcal{D}(n), N)\}.$
Chapter 7: A Realization of the Decoding Algorithm

Then \( T = D(n^+) \), so that \( \Gamma_{C_{\text{max}}(D(n^+))} = \Gamma_{C_{\text{max}}(D(n))} \cup \Lambda(n, D(n, N)) \). Furthermore,

\[
D(n^+) = \text{MIN}\{D(n, V) \cup \bigcup_{t \in D(n,N)} \{U(n, t, 0) \cup U(n, t, -1) \cup V(n, t)\}\}
\]

Therefore by using the Procedures I and II, we can construct a minimal recurrence pair \( < D(n^+), F(n^+) > \) for \( (U, n^+) \) by \( < D(n), F(n) > \) and \( < \text{Cmax}(D(n)), G(n) > \).

**Proof.** See Appendix C. \( \Box \)

The following theorem tells us how to find an auxiliary pair.

**Theorem 7.2** Let the assumption be as in Theorem 7.1. Then

\[
\text{Cmax}(D(n^+)) = \text{MAX}\{\text{Cmax}(D(n)) \cup \bigcup_{t \in D(n,N)} W(n, t)\}.
\]

Furthermore, for every \( c \in \text{Cmax}(D(n^+)) \), define \( g_c = g_c \in G(n) \) if \( c \) is in \( \text{Cmax}(D(n)) \), and \( g_c = f_t \in F(n) \) if \( c \in W(n, t) \). And denote

\[
G(n^+) := \{g_c|c \in \text{Cmax}(D(n^+))\}.
\]

Then we get an auxiliary pair \( < \text{Cmax}(D(n^+)), G(n^+) > \) for \( (U, (n^+)^+) \).

**Proof.** See Appendix D. \( \Box \)

### 7.3 Algorithms

The first algorithm of this section is an algorithm for finding a minimal recurrence pair \( < D(n), F(n) > \) for a given non-gap subscript sequence \( (U, n) \). For convenience we add the following notations,

\[
[D(k), F(k)] := \{(s, f)|s \in D(k), f \in F(k) \text{ with } \text{Deg}(f) = s\},
\]

\[
[C_{\text{max}}(D(k)), G(k)] := \{(c, g_c, t, m)|c \in C_{\text{max}}(D(k)) \text{ and } g_c \in G(k)\},
\]

where \( < C_{\text{max}}(D(k)), G(k) > \) is an auxiliary pair for \( (U, k^+) \), \( t := \text{Deg}(g) \) and \( m := \text{Ord}(g) \).

**Algorithm 7.1 (MinPol(U, n)) :**

**Step 0:** \( (0.0) \) Input a non-gap subscript sequence \( U \);

\( (0.1) \) Check \( U_0 = 0 \)?

\( (0.1.1) \) if ‘Yes’, then define \( [D(0), F(0)] := \{(0, 1)\} \) and \( [C_{\text{max}}(D(0)), G(0)] := \emptyset \);

\( (0.1.2) \) if ‘No’, then define \( [D(0), F(0)] := \{((1, 0), X), ((0, 1), Y)\} \) and

\( [C_{\text{max}}(D(0)), G(0)] := \{(0, 1, 0, 0)\}, \text{where } 0 = (0, 0)\);

**Step 1:** \( k := 0 \);
Step 2: For every \((s, f) \in [D(k), F(k)]\), check \(c(k, s) \in \Sigma(q)\)?

1. If 'No', put \(s\) into \(D(k, V)\);
2. If 'Yes', compute \(d_f = f_U(c(k, s))\). Then check \(d_f = 0\)? If 'Yes', put \(s\) into \(D(k, V)\); if 'No', put \(s\) into \(D(k, N)\);

Step 3: Compute \(MIN\{D(k, V) \cup \cup_{s \in D(k, N)} \{U(k, s, 0) \cup U(k, s, -1) \cup V(k, s)\}\}\) and define it to be \(D(k^+)\).

Step 4: For every \(s^* \in D(k^+)\),

1. if \(s^* = s \in D(k, V)\), take the \((s, f)\) from \([D(k), F(k)]\) and put it into \([D(k^+), F(k^+)]\);
2. if \(s^* \in V(k, s)\), then take the \((s, f)\) from \([D(k), F(k)]\) and do PROCEDURE I to get an \(h = h(f)\). Put \((s^*, h)\) into \([D(k^+), F(k^+)]\);
3. if \(s^* = \max(s, k - c - \zeta(e)) \in U(k, s, \zeta(e))\), then take the \((s, f)\) from \([D(k), F(k)]\) and \((e, g, \text{Deg}(g), \text{Ord}(g))\) from \([Cmax(D(k^+)), G(k^+)]\) and do PROCEDURE II to get \(h = h(f, g)\). Put \((s^*, h)\) into \([D(k^+), F(k^+)]\);

Step 5: Compute \(\text{MAX}\{\text{Cmax}(D(k)) \cup \cup_{t \in D(k, N)} W(k, t)\}\) and define it to be \(\text{Cmax}(D(k^+))\);

Step 6: For every \(c \in \text{Cmax}(D(k^+))\),

1. if \(c \in \text{Cmax}(D(k))\) then take the \((c, g, \text{Deg}(g), \text{Ord}(g))\) from \([\text{Cmax}(D(k)), G(k)]\) and put it into \([\text{Cmax}(D(k^+)), G(k^+)]\);
2. if \(c \in W(k, t)\), then take the \((t, f)\) from \([D(k), F(k)]\) and put \((c, f, t, k)\) into \([\text{Cmax}(D(k^+)), G(k^+)]\);

Step 7: If \(k^+ = n\), then output \([D(n), F(n)]\), otherwise define \(k := k^+\) go to Step 2.

Theorem 7.3 MinPol\((U, n) = [D(n), F(n)]\).

Proof. For \(k = 0\), (i) if \(U_0 = 0\), it is easy to see that \(\{(0, 1)\} = [D(0), F(0)]\) since \(\text{MIN}(\Sigma(q)) = \{0\}\), and \([\text{Cmax}(D(0)), F(0)] = \emptyset\), therefore \(< \text{Cmax}(D(0)), F(0) >\) is an auxiliary pair for \((U, 0^+)\), where \(0^+ = (1, 0)\).

(ii) if \(U_0 \neq 0\), then \(1[U, 0] \neq 0\) but \(X[U, 0] = 0\) and \(Y[U, 0] = 0\) since \((1, 0) > 0\) and \((0, 1) > 0\). Thus \(\{((1, 0), X), ((0, 1), Y)\} = [D(0), F(0)]\). On the other hand, by the definition of maximal complementary set, we have \(\text{Cmax}(D(0)) = 0\). Thus \(< D(0), \{1\} >\) is an auxiliary pair for \((U, 0^+)\).

Suppose for \(k = n\), the conclusion is true, then the conclusion is also true for \(k = n^+\) by Theorem 7.1, Theorem 7.2 and the Procedure I and II. This proves the theorem. □

Now we will give another algorithm, namely an algorithm for computing residues of \(r dx/f\) at point \(P_{a, \beta}\), which can be proved by Theorem 6.15. Recall Definition 6.15, we denote \(A[k^+] = \{A_k(\alpha; i) | \alpha \in k^*, 0 \leq k \leq i \leq q\}\) and \(B[\mathcal{H}^*(k)] = \{B_l(\alpha, \beta; j) | (\alpha, \beta) \in \mathcal{H}^*(k), 0 \leq j \leq q^2\) and \(0 \leq l \leq j(q^2 + q)\}\).

Algorithm 7.2 (Residue\((f, r, \alpha, \beta)) : (*)\) Set the database \(A[k^+]\) and \(B[\mathcal{H}^*(k)]\) before running the algorithm.
Chapter 7: A Realization of the Decoding Algorithm

Step 0: Input $(\alpha, \beta) \in H^*(k), f$ and $r$;

Step 1: Compute $f[\alpha, \beta; 0]$ (by means of Definition 6.16), check $f[\alpha, \beta; 0] = 0$? If "No", then output $\text{res}_{P, \sigma}(rdx/f) = 0$ and goto END, else goto next step;

Step 2: $k := 1$;

Step 3: Compute $f[\alpha, \beta; k]$;

Step 4: Check $f[\alpha, \beta; k] = 0$? If 'Yes', then $k := k + 1$ and goto Step 3, else $v_{P, \sigma}(f) = k$;

Step 5: Compute $r[\alpha, \beta; k - 1]$ (by means of Definition 6.16), output

$$\text{res}_{P, \sigma}(\frac{rdx}{f}) = \frac{r[\alpha, \beta; k - 1]}{f[\alpha, \beta; k]}$$

END.

Finally we give an algorithm for decoding the code $C_{G,T}(D, mP_\infty)$, where $m = l(q + 1) - \delta \geq 2g$ and $n_m \in \Sigma(q)$ such that $Q(n_m) = m + 1$.

Algorithm 7.3 (Decoder($\mathbf{z}$)):

Step 0: Input $\mathbf{z} \in k^n$;

Step 1: Compute $S(\mathbf{z})$ to get $(S_u,v)_{u \leq q_v}^{l-1}$ (by means of Theorem 6.2);

Step 2: Transfer the sequence $(S_u,v)_{u \leq q_v}^{l-1}$ to a non-gap subscript sequence $U$ (by means of Definition 6.12);

Step 3: Do MinPol($U, n_m$), if for some $k$ such that $Q(k) < Q(n_m)$, 

$$\min\{Q(D(k))\} > t + g$$

then output "The number of errors is great than $t$." and goto END; otherwise get $[D(n_m), F(n_m)]$;

Step 4: Compute $s = \min\{Q(i)|i \in D(n_m)\}$, take the $(s, f)$ from $[D(n_m), F(n_m)]$;

Step 5: Compute $r \equiv fS(\mathbf{z}) \pmod{y^l}$;

Step 6: For $i = 1, \ldots, n$, do Residue($f, r, \alpha_i, \beta_i$) = $\text{res}_{P, \sigma}(rdx/f)$;

Step 7: Output $e = (\text{res}_{P, \sigma}(rdx/f), \ldots, \text{res}_{P, \sigma}(rdx/f))$;

END.

Theorem 7.4 Let $d^*$ be the designed minimum distance of code $C_{G,T}(D, mP_\infty)$ with $2g \leq m \leq q^3 - 1 + 2g - 2$. Let $t = \lfloor (d^* - 1)/2 - \lfloor (q - 1)/2 \rfloor^2 + 1/2 \rfloor$. Let $\mathbf{z} \in k^n$ such that $\mathbf{z} = \mathbf{e} + \mathbf{e}$, where $\mathbf{e}$ is a codeword and the wight of $\mathbf{e}$ is less than $t$. Then Decoder($\mathbf{z}$) = $\mathbf{e}$.

Proof. Since $f \in \bigcup_{k \geq 2} I(kP_\infty - \sum_{i \in I} P_i)$, where $I = \{i | e_i \neq 0\}$ and $\mathbf{e} = (e_1, \ldots, e_n)$, we have $\deg(f) \leq t + g \leq (m + 1)/2 < q^3$ and $\deg(r) \leq (m + 1)/2 + q^2 - 1 < q^3$ by Theorem 6.3. Hence the theorem follows from the above algorithm, Theorem 6.3, Theorem 7.3 and Proposition 6.16. □

Remark 7.4. The decoding algorithm given in [36] only decodes the codes

$C_{G,T}(D', l(q + 1)P_\infty)$ where $D' = D + P_{0,0}$. Hence it can only decode the codes

$C_{G,T}^*(D, mP_\infty)$ with $m = l(q + 1)$.
7.4 The complexities of the algorithms

In this section, we will calculate upper bounds for the numbers of elementary calculations needed in algorithms $\text{MinPol}(U,n)$, $\text{Residue}(r,f,\alpha,\beta)$ and $\text{Decoder}(x)$, respectively. We call an elementary comparison between two numbers, a multiplication of two elements of $k$ and an addition of two elements of $k$, respectively, an elementary calculation.

Lemma 7.1 Let $U$ be a non-gap subscript sequence. Then to find a minimal recurrence pair for $(U,n)$, one needs at most $3q(N-1)N + (N - q^2 + q)(3q^3 + 6q^2 - q)$ elementary calculations by using Algorithm 7.1, where $N = Q(n) \geq 2g$.

Proof. We first consider the number of elementary calculations needed for a fixed $k$. Because Step (2.2) will not be executed if $Q(\deg(f)) > Q(k)$, and $\#(D(k)) \leq q$ by Proposition 7.2, one needs at most $2qQ(k)$ elementary calculations in Step 2. By Proposition 7.3 and Proposition 7.2, we have that the numbers of elements in $D(k,V)$, $D(k,N)$, $\mathcal{U}(k,s,e)$ and $V(k,s)$, respectively are at most $q$. Hence

$$\# \{D(k,V) \cup \bigcup_{s \in D(k,N)} (\mathcal{U}(k,s,0) \cup \mathcal{U}(k,s,-1) \cup V(k,s))\} \leq 2q^2 + q.$$  

Moreover, the first coordinate of the elements involved in Step 3 is always less than $q$. Therefore the number of elementary comparisons used in Step 3 is at most $q\{2q^2 + q)/2 - 2\}$ by [32, p.111]. To get $h(f)$ and $h(f,g)$ in Step 4.2 and 4.3, respectively, one needs at most $2Q(k)$ elementary calculations, since $Q(Deg(f)) < Q(k)$ (otherwise it is not necessary to do Step 4.2 and 4.3). To reduce those functions to $\tilde{h}$, one needs at most $2Q(k)$ elementary calculations since the exponent of $x$ appearing in $\tilde{h}$ is at most $2q$ and $x^{q+1+t} = x^t(y^q + y)$ for $0 \leq t < q$. Hence, the total number of elementary calculations needed in Step 4 is at most $4qQ(k)$. Because of $\# \{W(k,t)\} \leq 2$ and $\# \{C_{\text{max}}(D(k))\} \leq q$, we have

$$\# \{C_{\text{max}}(D(k)) \cup \bigcup_{t \in D(k,N)} W(k,t)\} \leq 3q.$$  

Hence the number of elementary calculations needed in Step 5 is $q(9q/2 - 2)$ by [32, p.111]. Finally, it is easy to see that the number of elementary calculations needed in Step 6 is at most $3q$. Therefore, for a fixed $k$, the number of elementary calculations needed in Algorithm 7.1 is at most

$$6qQ(k) + q\{2q^2 + q)/2 - 2\} + q(9q/2 - 2) + 3q = 6qQ(k) + 3q^3 + 6q^2 - q.$$  

Now we can conclude that the total number of elementary calculations needed in Algorithm 7.1 for $(U,n)$ is at most

$$\sum_{k \in \Sigma^n(q)} \{6qQ(k) + 3q^3 + 6q^2 - q\} \leq 3q(N-1)N + (N - q^2 + q)(3q^3 + 6q^2 - q),$$  

since $Q(\Sigma^n(q)) = \{0, \ldots, N-1\} \setminus \{\text{the gaps between 0 and } N-1\}$.

Lemma 7.2 Let $f, r \in K_\infty$ such that $\deg(f) < q^2$, $\deg(r) < q^3$ and $r dx/f \in \Omega(-6F_\infty - D)$. Then the number of elementary calculations needed in Algorithm 7.2 is at most

$$2\deg(f)(v_{F,q}(f) + 1) + 2\deg(r).$$
Chapter 7: A Realization of the Decoding Algorithm

Proof. It follows immediately from Algorithm 7.2. □

**Proposition 7.7** For the code $C^*_n(D, mP_00)$ with $q \geq 4$ and $2g - 1 \leq m \leq q^3 - 1 + 2q - 2$, the number of elementary calculations needed in Algorithm 7.3 is at most $3qm^2 + 2n^2 + 7q^3m$ where the word length of the code is $n = \deg(D) = q^3 - 1$.

**Proof.** It is easy to see that the number of elementary calculations needed in Step 1 is at most $2n^2$. Now suppose $m = l(q + 1) - \delta$, where $l, \delta \in \mathbb{N}^*$ such that $1 \leq \delta \leq q + 1$. Then the number of elementary calculations needed in Step 2 is at most $2l(q + 1)$, which is less than $2(m + q + 1)$. The number of elementary calculations needed in Step 3 is most $3qm(m + 1) + (m + 1 - q^2 + q)(3q^2 + 6q^2 - q)$ by Lemma 7.1 and $Q(m) = m + 1$. The number of elementary calculations needed in Step 4 is $3q/2 - 2$ by [32, p. 111]. In Step 5, computing $fS(x) \mod y'$ requires at most $(m + 1)(m + \delta)$ elementary calculations. Reducing this product to the one in $k[X,Y](q)$, one needs at most $2(m + \delta)$ since $S(x), f \in k[X,Y](q)$. Now consider the Step 6. By Theorem 7.4 we have $\deg(f) \leq (m + 1)/2$ and

$$\deg(r) \leq \deg(f) + 2g - 2 + \delta \leq (m + 1)/2 + q^2 - 1.$$  

Moreover $\sum_{(\alpha, \beta) \in \mathcal{H}^*(k)} v_{\alpha, \beta}(f) \leq \deg(f)$. Hence by Lemma 7.2 the number of elementary calculations needed in Step 6 is at most

$$2(q^3 - 1)(\deg(r) + \deg(f)) + 2(\deg(f))^2 \leq 2q^3m + m^2/2 - m + 2q^5 - 2q^2 + 1/2.$$  

Finally adding all the numbers of elementary calculations needed in all the steps, we get the conclusion of the proposition provided that $q \geq 4$ and $m \geq 2g$. □

### 7.5 A simple example

Consider a Hermitian curve $\mathcal{H}(4)$: $x^5 - y^4 - y = 0$ over $k = GF(16)$. Let $\xi$ be a primitive element of $GF(16)$, we have $k = \langle \xi \rangle$ and

$$\mathcal{H}^*(k) = \{(\alpha, \beta) \in k \times k| \alpha \in k, \beta^4 + \beta = \alpha^5 \text{ and } (\alpha, \beta) \neq (0, 0)\},$$

with genus $g = 6$. Now we order the set $\{P_{\alpha, \beta}|(\alpha, \beta) \in \mathcal{H}^*(k)\}$ as follows:

for every every two pairs $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in \mathcal{H}^*(k)$, and suppose that $\alpha_1 = \xi^{i_1}$ and $\alpha_2 = \xi^{i_2}$, $\beta_1 = \xi^{j_1}$ and $\beta_2 = \xi^{j_2}$, then $P_{\alpha_1, \beta_1} < P_{\alpha_2, \beta_2}$ if $i_1 < i_2$ and $P_{\alpha_1, \beta_1} \leq P_{\alpha_2, \beta_2}$ if $i_1 = i_2$ and $j_1 < j_2$. Hence we can rewrite the point set to be $\{P_i|i = 1, \ldots, 63\}$. Consider the code $C^*_n(D, 39P_00) = C_0(D, 40P_00 - P_0)$, where $D = \sum_{i=1}^{63} P_i, h = y^8$ and $G = (h)_0 = 40P_0$. The length of the code is 63 and the dimension is 28. Then by Definition 6.9, we have

$$\varepsilon_i = \frac{(y + \beta_i)^3 + 1}{x + \alpha_i} + \mu_i(x, y)dx$$

for every $i \in \{1, 2, \ldots, 63\}$, where

$$\mu_i(x, y) = \alpha_i^2\beta_i^{-1}x^{2} + \alpha_i^3(\beta_i^{-1}x + \beta_i^{-2}xy) + \alpha_i^4(\beta_i^{-1} + \beta_i^{-2}y + \beta_i^{-3}y^2).$$

Suppose we received the word $((1111111111110\cdots0)$ with 11 errors Then by Theorem 6.2 and Definition 6.12, we get its correspondent non-gap subscript sequence $U$ as follows:
Now do $\text{MinPol}(U, (0,8))$, after 29 steps, there is only one polynomial $f = X^3 + \xi^4X^2 + \xi X$ with $Q(\text{Deg}(f)) \leq 11 + g = 17$ in the minimal recurrence set of $\mathcal{F}(1, 5)$, see Table 1. Using this polynomial to check the remaining part of the non-gap subscript sequence, we get that $f$ is a minimal recurrence polynomial for $(U, (0,8))$. Next we compute $r = fS(x) \pmod{y^8}$, that is $x^2y^3 + \xi x^3y^2 + \xi^2x^4y + \xi^4y^4 + \xi^5x^3y^2 + \xi^7x^4 + \xi^8xy + \xi^9y + \xi^{10}x^3y + \xi^{11}x^4 + \xi^2xy^2 + \xi^5x^2y + \xi^8xy + \xi^{11}y$. Therefore

$$\text{res}_{\mathcal{P}_i}\left(\frac{r}{f}dx\right) = \begin{cases} 1 & \text{if } 1 \leq i \leq 11 \\ 0 & \text{if } 12 \leq i \leq 63. \end{cases}$$
TABLE 1 (Application of Algorithm 7.1 to the Example)

<table>
<thead>
<tr>
<th>Q(k)</th>
<th>k</th>
<th>U(k)</th>
<th>F(k)</th>
<th>D(k)</th>
<th>G(k)</th>
<th>Cmax(D(k))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0,0</td>
<td>X,Y</td>
<td>1,0,1</td>
<td>1</td>
<td>0,0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0,0</td>
<td>X + ³³</td>
<td>1,0,1</td>
<td>1</td>
<td>0,0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>0,0</td>
<td>X² + ³³X + ³³, Y</td>
<td>2,0,0,1</td>
<td>X + ³³</td>
<td>1,0</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>1</td>
<td>X² + ³³X + ³³, XY</td>
<td>2,0,1,1</td>
<td>X + ³³</td>
<td>1,0</td>
</tr>
<tr>
<td>11</td>
<td>3</td>
<td>0,0</td>
<td>Y² + ³³X² + X</td>
<td>0,2</td>
<td>Y</td>
<td>0,1</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>4</td>
<td>1,0</td>
<td>X³ + ³³X³ + X³</td>
<td>2,0,1,1</td>
<td>X³ + ³³X³</td>
<td>2,0</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>4</td>
<td>0,0</td>
<td>X³ + ³³X³ + X³</td>
<td>2,0,1,1</td>
<td>X³ + ³³X³</td>
<td>2,0</td>
</tr>
<tr>
<td>21</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A Appendix: The proof of Proposition 7.4

To prove Proposition 7.4, we need the following lemmas.

Lemma 7.3 Let U be a non-gap subscript sequence defined by Definition 6.12(2). Suppose i ∈ Σ such that i₁ = k(q + 1) + i'₁ with k ≥ 0 and 0 ≤ i'₁ ≤ q. Then for any j ∈ Σ,

\[ U_{j+1} = \sum_{\nu=0}^{k} \binom{k}{\nu} U_{j+(i'₁, \nu(q-1)+k+i'₂)}. \]
Proof. For \( j \in \Sigma \), we have that \( i_1' + j_1 = l(q + 1) + j_1' \) such that \( l, j_1' \in \mathbb{N} \) and \( 0 \leq j_1' \leq q \). Hence \( i_1 + j_1 = (k + l)(q + 1) + j_1' \). So

\[
U_{j+i} = \sum_{\nu=0}^{k+l} \binom{k+l}{\nu} U_{(j_1' + \nu(q-1) + (k+l) + i_2 + j_2)}
\]

by the definition. Now we have

\[
\begin{align*}
\sum_{\nu=0}^{k} \binom{k}{\nu} U_{j_1' + \nu(q-1) + k + i_2} &= \sum_{\nu=0}^{k} \binom{k}{\nu} \sum_{\mu=0}^{i} \binom{l}{\mu} U_{(j_1' + \nu(q-1) + k + l + i_2 + j_2)} \\
&= \sum_{\nu=0}^{k} \binom{k}{\nu} \sum_{t=\nu}^{l} \binom{l}{t} U_{(j_1' + t(q-1) + k + l + i_2 + j_2)} = \sum_{t=0}^{k+l} \binom{k+l}{t} U_{(j_1' + t(q-1) + k + l + i_2 + j_2)} \\
&= U_{j+i}
\end{align*}
\]

where the third equality follows from \( \sum_{\nu=0}^{l} \binom{l}{\nu} \binom{l}{t-\nu} = \binom{l+i}{i} \). \( \square \)

**Lemma 7.4** Let \( F(X, Y) = (X^{q+1})^k - (Y^q - Y)^k \in k[X, Y] \), where \( k \in \mathbb{N} \). Then \((gF)[U](i) = 0 \) for any \( g \in k[Z] \) and any \( i \in \Sigma \).

**Proof.** It is a consequence of Lemma 7.3. We leave it to the reader. \( \square \)

**Proof of Proposition 7.5:** It is obvious that \( \bar{f} \in k[X, Y](q) \) by its definition. For every \( i \in \mathcal{C}_f \), suppose \( i_1 = i_{12}(q + 1) + i_{11} \) with \( i_{12}, i_{11} \in \mathbb{N} \) and \( 0 \leq i_{11} \leq q \), then

\[
f - \bar{f} = \sum_{i \in \mathcal{C}_f} f_{i} X^{i_{12}} Y^{i_{12}} (X^{(q+1)i_{12}} - (Y^q + Y)^{i_{12}}).
\]

Thus \((f - \bar{f})[U](i) = 0 \) for any \( i \in \Sigma \) by Lemma 7.4. That is \( f[U](i) = \bar{f}[U](i) \).

Furthermore, if there exists an \( s \in \mathcal{C}_f \cap \Sigma(q) \) such that \( Q(i) < Q(s) \) for every \( i \in \mathcal{C}_f \setminus \{s\} \), then it is easy to see that \( Q(i_{11}, t(q-1) + i_{12} + i_2) < Q(s) \) for \( 0 \leq t \leq i_{12} \). Moreover, by the definition of \( \bar{f} \), we have

\[
\bar{f} = \sum_{i \in \mathcal{C}_f} f_{i} X^{i_{12}} \sum_{t=0}^{i_{12}} \binom{i_{12}}{t} Y^{t(q-1) + i_{12} + i_2}.
\]

Hence \( s \in \mathcal{C}_f \) and \( Q(j) < Q(s) \) for every \( j \in \mathcal{C}_f \setminus \{s\} \). That is \( \text{Deg}(\bar{f}) = s \). \( \square \)

**B** **Appendix:** The proof of Proposition 7.5 and 7.6

To prove these propositions we need the following lemma which can be easily proved by Lemma 7.3. We leave the proof to the reader.

**Lemma 7.5** Let \( f \in k[X, Y](q) \) with \( s = \text{Deg}(f) \), such that \( f[U, n] = 0 \). Denote \( Q(n) \) and \( Q(s) \) by \( N \) and \( S \), respectively. Then for every \( i \in \Sigma^{N-S} \), we also have \( \sum_{j \in \mathcal{C}_f} f_j U_{j+i} = 0 \). We still denote this situation by \( f[U](i) = 0 \). Furthermore, if \( Q(i) = Q(n) - Q(s) \), then \( f[U](i) = f[U](c(n, s)) \).
Chapter 7: A Realization of the Decoding Algorithm

Proof of Proposition 7.5. By the definition of $h$, there exists a $j \in C_f$ such that $i = t - s + j$, for every $i \in C_h$. Hence $Q(i) \leq Q(t)$ and the equality holds if and only if $j = s$. Thus $\text{Deg}(h) = t$ by Proposition 7.4. Now let $i \in \Sigma(n)-Q(t)(q)$. Then we have $h[U](i) = \sum_{j \in C_f} f_j U_{j+r-s+i} = 0$ by Lemma 7.5. Therefore $h[U](i) = 0$ by Proposition 7.4. Finally we have $h[U, n^+] = 0$ by Remark 7.2. □

Proof of Proposition 7.6. By the assumption on $r$, we have $h \in k[X, Y]$ and $Q(r - s + i) \leq Q(r)$ for every $i \in C_f$ and the equality holds if and only if $i = s$, and $Q(r - w + j) < Q(r)$ for every $j \in C_g$ since $Q(m) < Q(n)$. Hence $\text{Deg}(h) = r$ by Proposition 7.4. Now for every $i \in \Sigma^{N-R+1}(q)$, where $N = Q(n), R = Q(r)$, we have $Q(r - s + i) \leq Q(n) - Q(s)$ and $Q(r - w + i) \leq Q(m) - Q(t)$, where the equalities hold if and only if $i = c(n, r) \in \Sigma(q)$. Hence

$$h[U](i) = \sum_{j \in C_f} f_j U_{j+r-s+i} - d_f/d_g \sum_{j \in C_g} g_j U_{j+r-w+i} = 0$$

by Lemma 7.5. Now by Proposition 7.4 we can conclude that $h[U, n^+] = 0$. □

Corollary 7.1 Let the assumptions be as in Proposition 7.6, except for $r$ and $w$. For every $c \in W(m, t)$ define

$$w(c, \varepsilon) = \begin{cases} (n_1 - m_1 + l_1 - q - 1, n_2 - c_2) + \xi(\varepsilon) & \text{if } q \neq m_1 \geq l_1 \\
_1 - c + \xi(\varepsilon) & \text{otherwise.} \end{cases}$$

Let $r = \max(s, n - c + \xi(\varepsilon))$, and $u = r - s$ and $v = r - w(c, \varepsilon)$. Then the conclusion of Proposition 7.6 still holds.

Proof. It is easy to see that $Q'(w(c, \varepsilon)) = Q(n) - Q(m) + Q(t)$. Furthermore, if $q \neq m_1 \geq l_1$ and $c = (q, m_2 - l_2 - q)$, we have $n - c + \xi(\varepsilon) \geq w(c, \varepsilon)$. Thus $r \geq w(c, \varepsilon)$. This means that $r$ and $w(c, \varepsilon)$ satisfy the conditions for $r$ and $w$ Proposition 7.6. Hence the conclusion is true. □

C Appendix: The proof of Theorem 7.1

To prove the theorem, we still need some lemmas.

Lemma 7.6 Suppose $s^* \in D(n^+)$ such that $c(n, s^*) \notin \Sigma(q)$, and there exists an $s \in D(n, N)$ such that $s^* > s$.

1) If $s^*_1 = s_1$, then

$$s^* = \begin{cases} (s_1, n_2 + 1) & \text{if } n_1 \geq s_1 \\
_1, n_2 - q + 1 & \text{if } s_1 > n_1 \end{cases}.$$ 

2) If $s^*_1 > s_1$, then $n_1 \geq s_1$ and

$$s^* = \begin{cases} (n_1 + 1, s_2) & \text{if } n_2 - q < s_2 \\
_1 + 1, n_2 - q + 1 & \text{if } n_2 - q \geq s_2 \end{cases}.$$
Proof. We can separate the lemma to the following four cases: Case (1) \( s_1^* = s_1 \) and \( n_1 \geq s_1 \). Case (2) \( s_1^* = s_1 \) and \( s_1 > n_1 \). Case (3) \( s_1^* > s_1 \) and \( n_2 - q < s_2 \). Case (4) \( s_1^* > s_1 \) and \( n_2 - q \geq s_2 \). We will only prove Case (1), the proofs of the other cases are similar to this case. We leave them to the reader.

Proof of Case (1): By the assumption we have \( c(n, t) \in \Sigma(q) \) for every \( t = (s_1, t_2) \) with \( 0 \leq t_2 \leq n_2 \). Thus \( s^* \geq (s_1, n_2 + 1) \). Moreover \( c(n, (s_1, n_2 + 1)) \notin \Sigma(q) \), and \( (s_1, n_2 + 1) \geq s \) since \( s \in \mathcal{D}(n, N) \). Hence \( (s_1, n_2 + 1) \in \Sigma_{s^*}(q) \) by Procedure 1. Thus \( s^* = (s_1, n_2 + 1) \). □

**Lemma 7.7** Let \( U \) be a non-gap sequence, let \( f \in k[X, Y](q) \) with \( \text{Deg}(f) = s \), such that \( f[U, n] = 0 \) but \( f[U, n^+] \neq 0 \). If there exists a \( g \in k[X, Y](q) \) with \( \text{Deg}(g) = t \), such that \( g[U, n^+] = 0 \) then \( Q(n) - Q(s) - Q(t) \notin N(q) \).

Proof. (i) If \( Q(n) - Q(s) \notin N(q) \), it is trivial.

(ii) Now suppose \( Q(n) - Q(s) \in N(q) \) and assume \( Q(n) - Q(s) - Q(t) \in N(q) \). Then there exists an \( r \in \Sigma(q) \) such that \( Q(r) = Q(n) - Q(s) - Q(t) \).

Consider the summation \( A = \sum_{j \in C} g_j \sum_{i \in C} f_i U_j U_r i r \). Since \( Q(j) + Q(r) \leq Q(n) - Q(s) \) for every \( j \in C \) and equality holds if and only if \( j = t \). So \( A = g_t f[U](c(n, s)) \) does not equal to 0 by Proposition 7.5 and Remark 7.1. On the other hand, since \( Q(i) + Q(r) \leq Q(n) - Q(t) \) for every \( i \in C_f \), by Proposition 7.1 we have \( A = \sum_{i \in C_f} h_i (g[U](i + r)) = 0 \), which is a contradiction. This proves the lemma. □

**Corollary 7.2** Let \( f, g \in k[X, Y](q) \) with \( s = \text{Deg}(f) \) and \( t = \text{Deg}(g) \), such that \( f[U, n] = 0 \) and \( g[U, n^+] = 0 \). Then either both of \( f[U, n^+] \) and \( g[U, n^+] \) are equal to zero or both of them are not equal to zero, provided one of the following conditions holds: i) \( c(n, s) \geq t \); ii) \( c(n, t) \geq s \).

Proof. This is a direct consequence of Lemma 7.7. □

**Lemma 7.8** Let \( s^* \in \Lambda(n, \mathcal{D}(n, V)) \), then \( \{ s \in \mathcal{D}(n) \mid s \leq s^* \} \subseteq \mathcal{D}(n, V) \).

Proof. Let \( s \in \mathcal{D}(n) \) such that \( s \leq s^* \). Then there exists an \( f_s \in \mathcal{F}(n) \) such that \( \text{Deg}(f_s) = s \). Now let \( f^* = X^{r_1} Y^{r_2} f_s \), where \( (r_1, r_2) = s^* - s \). Then \( f^*[U, n] = 0 \) and \( \text{Deg}(f^*) = s^* \). On the other hand, by the assumption on \( s^* \), there exists a \( t \in \mathcal{D}(n, V) \) such that \( c(n, s^*) \geq t \). Hence \( (f^*)[U, n^+] = 0 \) by Corollary 7.2. This implies \( f_s[U, n^+] = 0 \). Therefore \( s \in \mathcal{D}(n, V) \). This proves the lemma. □

**Lemma 7.9** Let \( s, s^*, c, n \in \Sigma(q) \). Suppose \( s^* \geq s \), \( s \geq n - s^* + \xi(\chi(n_1 - s_1^*)) \) and \( c(n, \max(s, n - c + \xi(\chi(n_1 - s_1^*)))) \geq t \), where \( \varepsilon \in \{-1, 0\} \). Then \( c \geq t \).

Proof. If \( \chi(n_1 - s_1^*) = 0 \), the proof is trivial. Now consider \( \chi(n_1 - s_1^*) = -1 \). Then \( n_1 - s_1^* < 0 \). On the other hand, we have \( n_1 - (n_1 - c_1 + q + 1) < 0 \). Assume \( n_1 - s_1 \geq 0 \) and \( s_1 \geq n_1 - c_1 + q + 1 \) then \( c_1 \geq q + 1 \), which is a contradiction. Thus \( s_1 \leq n_1 - c_1 + q + 1 \) if \( n_1 \geq s_1 \). Hence

\[
c(n, \max(s, n - c + \xi(-1))) = n - \max(s, n - c + \xi(-1)) + \xi(-1).
\]

Therefore \( c \geq t \). □

**Proof of Theorem 7.1**: Recall that \( \Sigma_T(q) = \Sigma_{\mathcal{D}(n)}(q) \setminus \Lambda(n, \mathcal{D}(n, N)) \).
Chapter 7: A Realization of the Decoding Algorithm

(a) First we shall prove that $\Sigma_{D(n+)}(q) \subseteq \Sigma_T(q)$.

For every $i \in \Sigma_{D(n+)}(q)$, we have $i \geq s'$ for some $s' \in D(n+)$. Hence $i \in \Sigma_{D(n)}(q)$ since $D(n+) \subseteq \Sigma_{D(n)}(q)$. Now suppose $i \in \Lambda(n, D(n, N))$. That is to say there exists a $t \in D(n, N)$ such that $c(n, i) \geq t$. This implies that $Q(n) - Q(s') - Q(t) \in N(q)$, which is a contradiction to $s' \in D(n+)$ and $t \in D(n, N)$ by Lemma 7.7. Therefore $i \in \Sigma_T(q)$.

(b) Now we prove $\Sigma_T(q) \subseteq \Sigma_{D(n+)}(q)$.

By the definition of $T$, for every $s^* \in T$ we have $s^* \geq s$ for some $s \in D(n)$ and $s^* \notin \Lambda(n, D(n, N))$. Let us consider the following two cases (i) $s \in D(n, V)$ and (ii) $s \in D(n, N)$, respectively.

In case (i), we have $s \in \Sigma_{D(n+)}(q)$. That means that $s \notin \Lambda(n, D(n, N))$, otherwise it will contradict to Corollary 7.2. Thus $s \in \Sigma_{D(n)}(q) \setminus \Lambda(n, D(n, N))$. This implies that $s^* = s$ by the definition of $T$.

In case (ii), we have $s^* > s$ since $s \in D(n, N)$. Thus by PROCEDURE I (see Proposition 7.5), there exists an $f = h \in k[X, Y](q)$ such that $f[U, n+] = 0$ and $\text{Deg}(f) = s^*$. Therefore $s^* \in \Sigma_{D(n+)}(q)$.

In case (ii.2), we have $c(n, s^*) \in \Gamma_{C_{\text{max}}(D(n))}$ by Proposition 7.3 and $s^* \notin \Lambda(n, D(n))$. Hence there exists a $c \in C_{\text{max}}(D(n))$ such that $c \geq n - s^* + \xi(n_1 - s^*_1)$. Therefore $s^* \geq \max(s, n - c + \xi(n_1 - s^*_1)) \in \Sigma_{D(n)}(q)$. Furthermore we claim that $\max(s, n - c + \xi(n_1 - s^*_1)) \notin \Lambda(n, D(n, N))$. Otherwise, there exists a $t \in D(n, N)$ such that $c(n, \max(s, n - c + \xi(n_1 - s^*_1))) \geq t$. This implies $c \geq t$ by Lemma 7.9, which is a contradiction with $c \in C_{\text{max}}(D(n))$. Therefore

$$\max(s, n - c + \xi(n_1 - s^*_1)) \in \Sigma_{D(n)}(q) \setminus \Lambda(n, D(n, N)).$$

This implies that $s^* = \max(s, n - c + \xi(n_1 - s^*_1))$. Because $\langle C_{\text{max}}(D(n)), G(n) \rangle$ is an auxiliary pair, there exists a $g \in G(n)$ for $c$. Now take $f_5 \in F(n)$ which satisfies $\text{Ord}(f_5) = n^+$ since $s \in D(n, N)$. Thus we can use PROCEDURE II (see Corollary 7.1) for $f_5$ and $g$ to get $f = h(f_5, g) \in k[X, Y](q)$ with $\text{Deg}(f) = s^*$ and $f[U, n^+] = 0$. Therefore $s^* \in \Sigma_{D(n+)}(q)$.

Now we can conclude that $T \subseteq \Sigma_{D(n+)}(q)$. Therefore $\Sigma_T \subseteq \Sigma_{D(n+)}(q)$.

Combining (a) and (b), we have $\Sigma_T = \Sigma_{D(n+)}(q)$. Therefore $T = D(n+)$ and

$$\Gamma_{C_{\text{max}}(D(n+))} = \Gamma_{C_{\text{max}}(D(n))} \cup \Lambda(n, D(n, N))$$

by Proposition 7.3. Moreover by the above proof and Lemma 7.6 we have

$$D(n+) \subseteq D(n, V) \cup \bigcup_{t \in D(n, N)} \{U_{c \in \{-1,0\}} D(n, t, c) \cup V(n, t) \} \subseteq \Sigma_{D(n)}(q) \setminus \Lambda(n, D(n, N)).$$

This implies the second conclusion of the theorem. The last conclusion has been proved in (ii.1) and (ii.2) already. $\square$

D Appendix: The proof of Theorem 7.2

Proof. By Theorem 7.1, we know that $D(n+) = T = \text{MIN}(\Sigma_{D(n)}(q) \setminus \Lambda(n, D(n, N)))$. Thus for every $c^* \in C_{\text{max}}(D(n+))$, we have either $c^* \in \Gamma_{C_{\text{max}}(D(n))}$ or
\( c^* \in \Lambda(n, D(n, N)) \), since \( \Sigma(q) = \Sigma_T(q) = \Gamma_{C_{\text{max}}(D(n))} \cup \Lambda(n, D(n, N)) \) by Proposition 7.3.

If \( c^* \in \Gamma_{C_{\text{max}}(D(n))} \), then \( c^* \in C_{\text{max}}(D(n)) \) since \( \Gamma_{C_{\text{max}}(T)} \supseteq \Gamma_{C_{\text{max}}(D(n))} \) proved by Theorem 7.1. Hence there exists a \( g_{c^*} \in G(n) \) which is also an element of \( G(n^+) \) corresponding to \( c^* \).

If \( c^* \in \Lambda(n, D(n, N)) \setminus \Gamma_{C_{\text{max}}(D(n))} \): Then there exists a \( t \in D(n, N) \) such that \( c(n, c^*) \geq t \). Then we have \( n - c^* + \xi(\chi(n_1 - c_1^*)) \geq t \), hence \( c^* \leq n - t + \xi(\chi(n_1 - c_1^*)) \), and \( n_1 \geq c_1^* \) implies \( n_1 \geq t_1 \). Let us consider the following two cases (i) \( c(n, t) = n - t + \xi(\chi(n_1 - c_1^*)) \) and (ii) \( c(n, t) \neq n - t + \xi(\chi(n_1 - c_1^*)) \), respectively.

In case (i), we have \( c^* \leq c(n, t) \), and \( c(n, c(n, t)) = t \), this means that \( c(n, t) \in \Lambda(n, D(n, N)) \). Thus \( c^* = c(n, t) \). Now define \( g_{c^*} = f_t \in \mathcal{F}(n) \), then \( g_{c^*} \in G(n^+) \).

In case (ii), we have \( n_1 - c_1^* < 0 \) but \( n_1 - t_1 \geq 0 \), thus \( n_1 < q \). Then \( c^* \leq (q + 1 + n_1 - t_1, n_2 - t_2 - q) \) with \( t_2 \leq n_2 - q \). Suppose either (1) \( c_1^* < q \) or (2) \( c_2^* < n_2 - t_2 - q \). Then take

\[
c' = (c_1^* + 1, c_2^*) \quad \text{and} \quad c'' = (c_1^*, c_2^* + 1),
\]

then \( c', c'' \in \Sigma(q) \), and in the first case we have

\[
c(n, c') = (n_1 - c_1^* + q, n_2 - c_2^* - q) \geq t
\]

and in the second case we have

\[
c(n, c'') = (n_1 - c_1^* + q + 1, n_2 - c_2^* - q - 1) \geq t.
\]

this means that \( c', c'' \in \Lambda(n, D(n, N)) \) but \( c', c'' > c^* \) which is a contradiction to \( c^* \in C_{\text{max}}(T) \). Therefore \( c^* = (q, n_2 - t_2 - q) \). Now define \( g_{c^*} = f_t \), so that \( g_{c^*} \in G(n^+) \).

Therefore, we get the \( G(n^+) \) for \( C_{\text{max}}(D(n^+)) \). This means that \( C_{\text{max}}(D(n^+), G(n^+)) > \) is an auxiliary pair for \( (U, (n^+)^{+}) \).

The last conclusion of this theorem can be proved similarly to the proof of the second conclusion of Theorem 7.1. \( \Box \)
References


References


NEDERLANDSE SAMENVATTING VAN HET PROEFSCHRIFT:

ALGEBRAISCH-MEETKUNDIGE CODES EN
HUN DECODEER ALGORITMEN

Dit proefschrift bestaat uit 7 hoofdstukken en behandelt 3 verschillende problemen op het gebied van algebraïsch-meetkundige codes, ook wel meetkundige Goppa codes genoemd. Het eerste hoofdstuk is een algemene inleiding en geeft een samenvatting van de bereikte resultaten.

Hoofdstuk 2 onderzoekt de vraag welke lineaire codes algebraïsch-meetkundig zijn. Het blijkt dat alle lineaire codes verkregen kunnen worden uit krommen door middel van Goppa's constructie. Door eisen op de graad van de gebruikte divisor op te leggen, krijgen we wel restricties op het bestaan van zulke codes.

Hoofdstuk 3 behandelt het probleem van de expliciete algebraïsche constructie van asymptotisch goede binaire codes met behulp van krommen. We definiëren gegeneraliseerde Hermitese krommen in een projectieve ruimte door middel van homogene vergelijkingen in meerdere variabelen. Door codes op deze krommen als uitwendige codes te gebruiken in een Justesen concatenatie, kunnen we geconcateneerde binaire codes construeren die de Zyablov grens halen voor informatie snelheden kleiner dan 0.30. Zodoende werd onderzoeksprobleem (10.3) in het boek "The theory of error-correcting codes" van MacWilliams en Sloane, op expliciete wijze opgelost en met een complexiteit van de orde $O(n^2)$, waarbij $n$ de woordlengte van de code is.

In de hoofdstukken 4 en 5 wordt een decodeeralgoritme voor meetkundige Goppa codes gegeven door een syndroom van een ontvangen woord te definiëren in een affine ring. Dit algoritme werd door Porter voorgesteld, maar bevatte verschillende fouten en gaten. In dit proefschrift wordt een correcte behandeling van de resultaten van Porter gegeven in grotere algemeenheid en met een fouten corrigerende capaciteit, die beter is. Het decodeeralgoritme kan herleid worden tot het oplossen van de zogenaamde "sleutelcongruentie" in een affine ring. Voor een klasse van meetkundige Goppa codes wordt een algoritme voor het oplossen van de sleutelcongruentie gegeven door middel van een rij van gegeneraliseerde subresultanten in een gegradeerde algebra. Een gevolg hiervan is dat de complexiteit van de orde $O(n^3)$ is.

In de laatste twee hoofdstukken worden vele existentiebewijzen uit de voorafgaande theorie in detail uitgewerkt voor Hermitese krommen over $GF(q^2)$ en hun codes. Er wordt ook een expliciet codeeralgoritme gegeven voor deze codes. Om deze codes te decoderen, herleiden we het decodeeralgoritme, zoals gevonden in hoofdstuk 4, tot een minimale recurrentierelatie voor een rij van een ontvangen woord. Hierdoor wordt de complexiteit van het decoderen kleiner dan $3qm^2 + 2n^2 + 7q^3m$, indien $q \geq 4$ en waarbij $m$ de graad van de gebruikte divisor is.
STATEMENTS

accompanying the dissertation

Algebraic-geometric codes and their decoding algorithm

B.-Z. Shen

I. Let \( f \) be a real-valued function on \( \mathbb{F}_2^n \). Then the Walsh transform (or Walsh spectrum) of \( f \) is defined as \( S_f \):

\[
S_f(v) = \sum_{x \in \mathbb{F}_2^n} f(x)W_v(x), \quad v \in \mathbb{F}_2^n,
\]

where \( W_v(x) = (-1)^{vx}. \) Let \( A \) be an \( m \times n \) matrix over \( \mathbb{F}_2 \). Let \( \text{Im}(A) = \{Ax : x \in \mathbb{F}_2^n\} \). For any subset \( T \) of \( \mathbb{F}_2^n \), let \( \chi_T \) denote the characteristic function of \( T \). Then the Walsh spectrum of the composite \( f \circ A \) is

\[
S_{f \circ A}(w) = 2^{-\text{rank}(A)}\chi_{\text{Im}(A)}(w)S_{x_{\text{Im}(A)}f}((A^-)^t w), \quad w \in \mathbb{F}_2^n,
\]

where \( A^- \) is a generalized inverse of \( A \), that is \( AA^-A = A \).


II. Let \( f \) be a real-valued function on \( \mathbb{F}_2^m \) and let \( E \) be the linear span of \( \{w \in \mathbb{F}_2^m : S_f(w) \neq 0\} \). Let \( \{h_i\}_{i=1}^r \) be a basis of \( E \) and \( H = [h_1, h_2, \ldots, h_r] \). Then there exists a real-valued function \( g \) on \( \mathbb{F}_2^r \) such that \( f = g \circ H^t \), that is

\[
f(x) = g(H^tx), \quad x \in \mathbb{F}_2^m.
\]

We call \( g \) the degenerated function of \( f \). The Walsh spectrum of \( g \) is

\[
S_g(v) = 2^{-(m-r)}S_f(Hv), \quad v \in \mathbb{F}_2^r.
\]


III. Let \( L \) and \( M \) be two subspaces of \( \mathbb{F}_2^m \) such that \( L \oplus M = \mathbb{F}_2^m \), i.e for every \( x \in \mathbb{F}_2^m \) there exist uniquely two elements \( y \in L \) and \( z \in M \) such that \( x = y + z \). A transformation \( P \) of \( \mathbb{F}_2^m \) is called a projection from \( \mathbb{F}_2^m \) to \( L \) along \( M \) if \( P(x) = y \) for every \( x = y + z \) such that \( y \in L \) and \( z \in M \). We denote this \( P \) by \( P_{L,M} \). The distance from \( x \) to \( L \) is defined by

\[
d(x, L) = \min\{d(x, y) : y \in L\}.
\]
Let $A$ be an $m \times n$ matrix over $\mathbb{F}_2$. Let $s$ be an integer such that $s \geq n - \text{rank}(A)$ and $B$ be an $m \times s$ matrix over $\mathbb{F}_2$ such that $\mathbb{F}^m_s = \text{Im}(A) \oplus \text{Im}(B)$ (see Statement I for definition of $\text{Im}(A)$). There exists a projection $P_{\text{Im}(A),\text{Im}(B)}$ such that

$$d(\mathbf{x}, \text{Im}(A)) = d(\mathbf{x}, P_{\text{Im}(A),\text{Im}(B)}(\mathbf{x}))$$

if and only if there exists a basis of $\text{Im}(A)$ such that the weight of each element of this basis is less than 2.


IV. Let $A$ be an $n \times k$ matrix over $\mathbb{F}_2$ and $\mathbf{y} \in \mathbb{F}^n_2$. $\mathbf{x}_0 \in \mathbb{F}^k_2$ is called a minimum distance solution of $A\mathbf{x} = \mathbf{y}$ if $d(\mathbf{y}, A\mathbf{x}_0) = d(\mathbf{y}, \text{Im}(A))$. Furthermore, if there exists an $n \times m$ matrix over $\mathbb{F}_2$ such that $B\mathbf{y}$ is a minimum distance solution of $A\mathbf{x} = \mathbf{y}$ for every $\mathbf{y} \in \mathbb{F}^m_2$, then we say that $A$ has a minimum distance projective solution.

Let $G$ be an $k \times n$ matrix over $\mathbb{F}_2$. If $G'$ has a minimum distance projective solution, then the linear code generated by $G$ cannot correct any error.


V. Let $S$ be the set of all binary sequences and let $A$ be a deterministic algorithm such that for every finite binary sequence it gives a 0 or 1 as an output. Let $\mathbf{a} = (a_0, a_1, \ldots, a_n, \ldots)$ be a sequence of $S$. We denote $p_k^A$ to be the probability that the output of $A$ on input $a_0, a_1, \ldots, a_{k-1}$ of $\mathbf{a}$ is equal to $a_k$. A sequence $\mathbf{a}$ is called non-next-bit predictable at $a_{k-1}$, if for every $\varepsilon > 0$

$$p_k^A < \frac{1}{2} + \varepsilon,$$

for all probabilistic polynomial time algorithms $A$.

Let $K_n$ be the set of all binary sequences with linear complexity $n$. Let $\mathbf{a} \in K_n$, and let $l_k$ be the linear complexity of $a_0, \ldots, a_{k-1}$. Then for all $0 < k \leq 2n - 1$, except $k = l_k - 1 + n$, the sequence $\mathbf{a}$ is non-next-bit predictable at $a_{k-1}$.


VI. They (the cryptography problem and the problems of information and communications) are very similar things, in one case trying to conceal information, and in the other case trying to transmit it.


VII. If one wants to understand an abstract painting, one should study it by copying it carefully, like what mathematicians do when they try to understand a mathematical article.

VIII. Among all visional art, the depiction of human bodies is the most beautiful.