ON APPLICATIONS OF ALGEBRAIC FUNCTION FIELDS TO CODES

by

MEHMET ÖZDEMİR

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Spring 2004

ON APPLICATIONS OF ALGEBRAIC FUNCTION FIELDS TO CODES

APPROVED BY

Assist. Prof. Cem GÜNERİ ....
(Thesis Supervisor)

Prof. Dr. Alev TOPUZOĞLU ....

Assist. Prof. Albert LEVİ ....

Assist. Prof. Ebru BEKYEL ....

Assist. Prof. Erkay SAVAŞ ....

DATE OF APPROVAL: July 22th, 2004

Anneme, babama

ve

yeğenlerim Sena ve Seda'ya...

Acknowledgements

I would like to express my gratitude and deepest regards to my supervisor Assist. Prof. Cem Güneri for his motivation, guidance and encouragement throughout this thesis.

I also would like to thank Mustafa Çoban and Mustafa Parlak for their friendship and endless support.

ON APPLICATIONS OF ALGEBRAIC FUNCTION FIELDS TO CODES

Abstract

The relation between algebraic function fields over finite fields and coding theory started with Goppa's important code construction, which is nowadays called geometric Goppa codes. He used Riemann-Roch spaces of divisors and degree one (rational) places of a function field to write codes with good parameters.

Since Goppa's work, interaction between function fields and codes has been investigated extensively and further applications in coding theory have been found. The aim of this thesis is to describe two of these applications. The first is Goppa's idea and its generalization by Xing-Niederreiter-Lam and Heydtmann using higher degree places of the function field. The second application is the use of number of rational places of a function field to estimate the minimum distance of cyclic codes. We give two examples of cyclic codes; binary Hamming and BCH codes.

Keywords: Algebraic function field, coding theory, geometric Goppa code, cyclic code.

CEBİRSEL FONKSİYON CİSİMLERİNİN KODLAMA TEORİSİNE UYGULAMARI ÜZERİNE

Özet

Sonlu cisimler üzerinde tanımlanmış fonksiyon cisimleri ve kodlama teorisi arasındaki ilişki Goppa'nın geometrik Goppa kodları olarak bilinen önemli gözlemiyle başladı. Goppa, fonksiyon cisimlerinin Riemann-Roch uzayları ve bir dereceli (rasyonel) asal bölenlerini kullanarak iyi parametrelere sahip kodlar oluşturdu.

Goppa'nın çalışmasından bu yana kodlar ve fonksiyon cisimleri arasındaki ilişki yoğun olarak çalışıldı ve kodlama teorisine başka uygulamalar da bulundu. Bu tezin amacı özellikle iki uygulamayı anlamaktır. Birincisi Goppa'nın fikri ve yüksek dereceli asal bölenler kullanarak Xing-Niederreiter-Lam ve Heydtmann tarafından elde edilen genellemedir. Ikinci uygulama fonksiyon cisimlerinin rasyonel asal bölen sayılarını kullanarak cyclic kod adı verilen kodların minimum uzaklıkları hakkında sonuçlara varma metodur. Burda özellike iki kod örneği incelenmiştir; binary Hamming ve BCH kodları.

Anahtar kelimeler: Cebirsel fonksiyon cismi, kodlama teorisi, geometrik Goppa kodu, cyclic kod.

TABLE OF CONTENTS

ON APPLICATIONS OF ALGEBRAIC FUNCTION FIELDS TO CODES

by

MEHMET ÖZDEMİR

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Spring 2004

ON APPLICATIONS OF ALGEBRAIC FUNCTION FIELDS TO CODES

APPROVED BY

Assist. Prof. Cem GÜNERİ ....
(Thesis Supervisor)

Prof. Dr. Alev TOPUZOĞLU ....

Assist. Prof. Albert LEVİ ....

Assist. Prof. Ebru BEKYEL ....

Assist. Prof. Erkay SAVAŞ ....

DATE OF APPROVAL: July 22th, 2004

Anneme, babama

ve

yeğenlerim Sena ve Seda'ya...

Acknowledgements

I would like to express my gratitude and deepest regards to my supervisor Assist. Prof. Cem Güneri for his motivation, guidance and encouragement throughout this thesis.

I also would like to thank Mustafa Çoban and Mustafa Parlak for their friendship and endless support.

ON APPLICATIONS OF ALGEBRAIC FUNCTION FIELDS TO CODES

Abstract

The relation between algebraic function fields over finite fields and coding theory started with Goppa's important code construction, which is nowadays called geometric Goppa codes. He used Riemann-Roch spaces of divisors and degree one (rational) places of a function field to write codes with good parameters.

Since Goppa's work, interaction between function fields and codes has been investigated extensively and further applications in coding theory have been found. The aim of this thesis is to describe two of these applications. The first is Goppa's idea and its generalization by Xing-Niederreiter-Lam and Heydtmann using higher degree places of the function field. The second application is the use of number of rational places of a function field to estimate the minimum distance of cyclic codes. We give two examples of cyclic codes; binary Hamming and BCH codes.

Keywords: Algebraic function field, coding theory, geometric Goppa code, cyclic code.

CEBİRSEL FONKSİYON CİSİMLERİNİN KODLAMA TEORİSİNE UYGULAMARI ÜZERİNE

Özet

Sonlu cisimler üzerinde tanımlanmış fonksiyon cisimleri ve kodlama teorisi arasındaki ilişki Goppa'nın geometrik Goppa kodları olarak bilinen önemli gözlemiyle başladı. Goppa, fonksiyon cisimlerinin Riemann-Roch uzayları ve bir dereceli (rasyonel) asal bölenlerini kullanarak iyi parametrelere sahip kodlar oluşturdu.

Goppa'nın çalışmasından bu yana kodlar ve fonksiyon cisimleri arasındaki ilişki yoğun olarak çalışıldı ve kodlama teorisine başka uygulamalar da bulundu. Bu tezin amacı özellikle iki uygulamayı anlamaktır. Birincisi Goppa'nın fikri ve yüksek dereceli asal bölenler kullanarak Xing-Niederreiter-Lam ve Heydtmann tarafından elde edilen genellemedir. Ikinci uygulama fonksiyon cisimlerinin rasyonel asal bölen sayılarını kullanarak cyclic kod adı verilen kodların minimum uzaklıkları hakkında sonuçlara varma metodur. Burda özellike iki kod örneği incelenmiştir; binary Hamming ve BCH kodları.

Anahtar kelimeler: Cebirsel fonksiyon cismi, kodlama teorisi, geometrik Goppa kodu, cyclic kod.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Goppa found the so-called geometric Goppa codes ([1]) using algebraic function fields over finite fields. Using the Riemann-Roch theorem, one could find or estimate the parameters of these codes. Soon after Tsfasman-Vladut-Zink ([7]) showed that this construction yields an improvement on the Gilbert-Varshamov bound (Theorem 5.1.9 in [4]), a bound which was thought best possible by coding theorists. Since then there has been an extensive research on possible applications of algebraic function fields over finite fields to coding theory.

In this chapter we summarize basic notions and necessary results related to function fields and coding theory. We do not prove any results. The reader is referred to [6] for function fields and to [4] for coding theory.

1.1. Algebraic Function Fields

Let K be a field. *An algebraic function field* F/K of one variable over K is an extension F/K such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K. We will simply call F/K a function field. The set $\widetilde{K} := \{z \in F | \ z \ is \ algebraic \ over \ \mathrm{K}\}$ is a subfield of F, since sums, products and inverses of algebraic elements are also algebraic. We have $K \subseteq \widetilde{K} \subset F$. The field $\widetilde{K}$ is called the *field of constants* of F/K. The extension $\widetilde{K}/K$ is a finite extension and K is called the *full constant field* of F if $\widetilde{K} = K$.

Example 1.1.1 The simplest example of an algebraic function field is the rational function field $F = K(x)$, where x is a transcendental element over K. Any element $0 \neq z \in K(x)$ has a unique representation

$$z = a \prod_i p_i(x)^{n_i}, \tag{1.1}$$

where $0 \neq a \in K$, $p_i(x) \in K[x]$ are monic, pairwise distinct irreducible polynomials and $n_i \in \mathbb{Z}$ for all i.

If K is taken to be a perfect field, i.e. every algebraic extension is separable, then an arbitrary function field F/K can be represented as $F = K(x, y)$, where $K(x)$ is the rational function field and y is separable over $K(x)$. Such a function field F/K is said to be *separably generated.* Note that if K is a finite field or a field of characteristics zero, every function field F/K is separably generated.

Definition 1.1.1 A *valuation ring* of a function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties :
(i) $K \subsetneqq \mathcal{O} \subsetneqq F$,
(ii) for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

A valuation ring $\mathcal{O}$ of F/K is a principal ideal domain. In fact, $\mathcal{O}$ is also a local ring, i.e. a ring which has a unique maximal ideal. This unique maximal ideal is, clearly, the set $\{z \in \mathcal{O} \mid z \notin \mathcal{O}^*\}$ where $\mathcal{O}^*$ denotes the group of units of $\mathcal{O}$.

Definition 1.1.2 A *place* P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Any element $t \in P$ such that $P = t\mathcal{O}$ is called a *prime element* for P.

We denote the set of places of a function field F/K by $\mathbb{P}_F$. This set is known to be an infinite set for any function field. Furthermore, a valuation ring $\mathcal{O}$ and a place P of F/K uniquely determine each other with the following relation:

$$\text{for } 0 \neq x \in F,\, x \in P \iff x^{-1} \notin \mathcal{O}.$$

Therefore, the valuation ring associated with the place $P \in \mathbb{P}_F$ is denoted by $\mathcal{O}_P$. Another notion which is in one to one correspondence with valuation rings, and hence with places, of a function field is the so-called discrete valuation.

Definition 1.1.3 A *discrete valuation* of F/K is a function $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties :
(i) $v(x) = \infty \iff x = 0$.
(ii) $v(xy) = v(x) + v(y)$ for any $x, y \in F$.
(iii) (Triangle inequality) $v(x + y) \geq \min\{v(x), v(y)\}$ for any $x, y \in F$.
(iv) There exists an element $z \in F$ with $v(z) = 1$.
(v) $v(a) = 0$ for any $0 \neq a \in K$.

Triangle inequality becomes an equality in some cases.

Lemma 1.1.1 ***(Strict Triangle Inequality)*** *Let v be a discrete valuation of F/K and $x, y \in F$ with $v(x) \neq v(y)$. Then*

$$v(x + y) = \min\{v(x), v(y)\}. \tag{1.2}$$

Now we will see how to relate discrete valuations and valuation rings (or equivalently places). If t is a prime element for P, then every $0 \neq z \in F$ has a unique representation $z = t^n u$ for some $u \in \mathcal{O}_P^*$ and integer n. The number n is independent of the prime element chosen. Hence, we define $v_P(z) = n$. It is not difficult to see that this function is a discrete valuation . Conversely, let v be a discrete valuation of F/K. The set $\{z \in F|\ v(z) > 0\}$ determines a place P of F/K. Corresponding valuation ring $\mathcal{O}_P$ is $\{z \in F|\ v(z) \geq 0\}$. Therefore, discrete valuations, valuation rings, and places of a function field are in one to one correspondence.

Example 1.1.2 If F/K is a function field, where $\widetilde{K} = K$, then note that any $0 \neq k \in K$ is contained in $\mathcal{O}_P^*$ for any $P \in \mathbb{P}_F$. Therefore, $k = t^0 k$ is the unique representation mentioned above. Hence, $v_P(k) = 0$, for any $P \in \mathbb{P}_F$ and any $k \in K - \{0\}$.

For a valuation ring $\mathcal{O}_P$, the quotient ring $\mathcal{O}_P\ /P$ is a field, since P is maximal in $\mathcal{O}_P$. This field is denoted by F_P and it is called the *residue class field* of P. For an element $z \in \mathcal{O}_P$, we denote the coset $z + P \in \mathcal{O}_P\ /P$ by $z(P)$. For $z \in F - \mathcal{O}_P$, we set $z(P) = \infty$. Hence, we have a map from F to $F_P \cup \{\infty\}$ via the assignment $z \longmapsto z(P)$ for any $z \in F$. Under this map, $K \subset \mathcal{O}_P$ is mapped injectively into F_P, i.e. there exists an isomorphic copy of K in F_P. Therefore, F_P can be viewed as a K-vector space. In fact, F_P is a finite dimensional vector space over K.

Definition 1.1.4 For a place P of F/K, *the degree of* P is defined by

$$\deg P = \dim_K F_P.$$

Definition 1.1.5 Let $0 \neq z \in F$ and $P \in \mathbb{P}_F$. We say that P is a *zero* of z of order m if $v_P(z) = m > 0$ and P is a *pole* of z of order m if $v_P(z) = -m < 0$.

For a nonzero element $x \in F$, there are finitely many zeros and poles. Note that there are, in fact, no zeros or poles for an element $0 \neq k \in K$, by Example 1.1.2. We try to explain the meanings of these fundamental concepts for the simplest function field, that is the rational function field.

Example 1.1.3 Let $F = K(x)$ be the rational function field over K. It is clear that K is the full constant field of $K(x)/K$ since every element in $K(x) - K$ is transcendental over K. For any monic, irreducible polynomial $p(x) \in K[x]$, there is an *affine place* $P_{p(x)}$ of $K(x)$ defined by

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \middle|\ f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}. \tag{1.3}$$

Its corresponding valuation ring is given by

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \middle|\ f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \tag{1.4}$$

We can describe the corresponding discrete valuation v_P for $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ as follows: Note that $p(x)$ is a prime element for $P_{p(x)}$. Any $z \in K(x) - \{0\}$ can be uniquely written as $z = p(x)^n(f(x)/g(x))$ with $n \in \mathbb{Z}$ and $f(x), g(x) \in K[x]$ both of which are not divisible by $p(x)$. Then $v_P(z) = n$. The residue class field

$K(x)_P = \mathcal{O}_P/P$ of P is isomorphic to $K[x]/(p(x))$. Therefore, $\deg P = \deg(p(x))$. If $p(x)$ is linear, i.e. $p(x) = x - \alpha$ for some $\alpha \in K$, we denote its affine place by P_α. In this case the degree of $P = P_\alpha$ is one. Another place of the rational function field $K(x)$ is the *infinite place* which is

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \Big| \; f(x), g(x) \in K[x], \deg(f(x)) < \deg(g(x)) \right\}. \tag{1.5}$$

Valuation ring $\mathcal{O}_\infty$ of the infinite place P_∞ can be described by

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \Big| \; f(x), g(x) \in K[x], \deg(f(x)) \leq \deg(g(x)) \right\}. \tag{1.6}$$

The element $1/x$ is a prime element for P_∞, and corresponding discrete valuation v_∞ for the infinite place is given by $v_\infty(f(x)/g(x)) = \deg(g(x)) - \deg(f(x))$. Another fact is that $\deg P_\infty = 1$. All places of the rational function field $K(x)/K$ are only the infinite place P_∞ and the affine places $P_{p(x)}$ for irreducible polynomials $p(x) \in K[x]$. Therefore, the set of degree one places of $K(x)/K$ is in one to one correspondence with $K \bigcup \{\infty\}$.

From here on F/K will always denote an algebraic function field of one variable such that K is the full constant field of F/K, unless otherwise specified. We will further assume that K is a perfect field. For our interests later, K will be a finite field which is perfect.

Theorem 1.1.2 ***(Weak approximation Theorem)*** *Let F/K be a function field, $P_1, P_2, ..., P_n$ be pairwise distinct places of F/K , $x_1, x_2, ..., x_n \in F$ and $r_1, r_2, ...r_n \in \mathbb{Z}$. Then there exists $x \in F$ such that*

$$v_P(x - x_i) = r_i \quad \textit{for} \quad \textit{i=1,2,...,n} \tag{1.7}$$

Definition 1.1.6 The (additively written) free abelian group which is generated by the places of F/K is denoted by $\mathcal{D}_F$ and it is called the *divisor group* of F/K. The elements of $\mathcal{D}_F$ are called *divisors* of F/K. In other words, a divisor is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_p P, \tag{1.8}$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for almost all $P \in \mathbb{P}_F$.

For $Q \in \mathbb{P}_F$ and $D = \sum_{P \in \mathbb{P}_F} n_p P$, we define $v_Q(D) = n_Q$. Note that $v_Q(D) = 0$ for almost all $Q \in \mathbb{P}_F$, by definition of a divisor. This allows us to define a partial order on the divisor group $\mathcal{D}_F$ via the relation $D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2)$ for all $P \in \mathbb{P}_F$. We call $D \in \mathcal{D}_F$ a *positive divisor* if $D \geq 0$. We extend the notion of degree of a place to the divisor group by setting $\deg D = \deg(\sum_{P \in \mathbb{P}_F} n_p P) = \sum_{P \in \mathbb{P}_F} n_p \deg P = \sum_{P \in \mathbb{P}_F} v_P(D) \deg P$. Note that $\deg D$ is an integer.

We know that a nonzero element $x \in F$ has finitely many zeros and poles. Denote by Z (respectively N) the set of zeros (poles) of x in $\mathbb{P}_F$. Then we define the *zero divisor* of x by

$$(x)_0 := \sum_{P \in Z} v_P(x) P, \tag{1.9}$$

and the *pole divisor* of x by

$$(x)_\infty := \sum_{P \in N} -v_P(x) P. \tag{1.10}$$

Note that both $(x)_0$ and $(x)_\infty$ are positive divisors. Finally, we define the *principal divisor* of $x \in F$ by

$$(x) = (x)_0 - (x)_\infty. \tag{1.11}$$

An important fact is that $\deg(x)_0 = \deg(x)_\infty = [F : K(x)] < \infty$, if $x \in F - K$. This means that any nonconstant function has as many poles as zeros, counted with multiplicities. For a nonzero constant function $k \in K$, $(k)_0 = (k)_\infty = (k) = 0$ by Example 1.1.2. We now associate an important space to a divisor of F/K.

Definition 1.1.7 For a divisor $A \in \mathcal{D}_F$ we set

$$L(A) := \{x \in F \mid \ (x) \geq -A\} \cup \{0\}. \tag{1.12}$$

$L(A)$ is a finite dimensional K-vector space for any $A \in \mathcal{D}_F$. It is called the *Riemann-Roch space of* A and we define the *dimension of a divisor* to be $\dim A := \dim_K L(A)$. If $\deg A < 0$, then we have $\dim A = 0$. It is also easy to see that $\dim 0 = 1$. Calculating the dimension of a divisor is a difficult problem in general. The main tool for this is the Riemann-Roch Theorem, which will be stated after more preperation.

Definition 1.1.8 The *genus* of F/K is defined by

$$g(F) = \max\{\deg A - \dim A + 1 | \ A \in \mathcal{D}_F\}. \tag{1.13}$$

The genus of the rational function field is zero. In general, genus is a nonnegative integer (if $A = 0$, then $\deg A = 0$ and $\dim A = 1$). The following genus formula for the so-called Artin-Schreier extensions will be used in Chapter 3.

Proposition 1.1.3 *Let $F = \mathbb{F}_{q^m}(x, y)$ be defined by $y^q - y = f(x)$, where $m > 1$ and $f(x) \in \mathbb{F}_{q^m}[x]$ such that* $\gcd(\deg f, char\mathbb{F}_q) = 1$. *Then the genus of F is*

$$g = \frac{(q-1)(\deg f - 1)}{2}.$$

Here, we also mention a result of great importance which will be used in Chapter 3.

Theorem 1.1.4 ***(Hasse-Weil Bound)*** *Let F be a function field over $\mathbb{F}_q$ of genus g and let N denote the number of rational places of F. Then*

$$| N - (q+1) | \leq 2g\sqrt{q}.$$

For any $A \in \mathcal{D}_F$, the quantity $i(A) = \dim A - \deg A + g - 1$ is called the *index of speciality of A*. Index of speciality of a divisor of a function field is always a non-negative integer.

Definition 1.1.9 An *adele* of F/K is a mapping

$$\alpha : \mathbb{P}_F \to F$$
$$P \mapsto \alpha_P$$

such that $\alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$.

An adele can be regarded as an element of the direct product $\prod_{P \in \mathbb{P}_F} F$. We will use the notation $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ for an adele. The set of all adeles of F/K forms a K-vector space and it is called the *adele space* of F/K, and denoted by $\mathcal{A}_F$. The *principal adele* of an element $x \in F$ is defined to be the adele all of whose components equal to x. This way we can view F as a subspace of $\mathcal{A}_F$.

Embedding of F into $\mathcal{A}_F$ this way is called the *diagonal embedding.* We can extend the valuation v_P to $\mathcal{A}_F$ by setting $v_P(\alpha) := v_P(\alpha_P)$. For any $A \in \mathcal{D}_F$, the set $\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F | \, v_P(\alpha) \geq -v_P(A)$ for all $P \in \mathbb{P}_F\}$ is a K-subspace of $\mathcal{A}_F$.

Definition 1.1.10 A *Weil differential* of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in \mathcal{D}_F$.

The set $\Omega_F := \{\omega \mid \omega$ is a Weil differential of $F/K\}$ is called *the module of Weil differentials* of F/K. Note that Ω_F is a K vector space. For $A \in \mathcal{D}_F$ we let

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \text{ vanishes} \quad \text{on} \quad \mathcal{A}_F(A) + F\}$$

It is easy to see that $\Omega_F(A)$ is a K-subspace of Ω_F.

Lemma 1.1.5 *For $A \in \mathcal{D}_F$ we have*

$$\dim \, \Omega_F(A) = i(A). \tag{1.14}$$

The following definition gives Ω_F the structure of a vector space over F.

Definition 1.1.11 For $x \in F$, $\alpha \in \mathcal{A}_F$ and $\omega \in \Omega_F$ we set

$$(x\omega)(\alpha) = \omega(x\alpha) \tag{1.15}$$

where $(x\alpha)$ denotes the adele obtained by multiplying each component of α by $x \in F$.

For any Weil differential ω of F/K there exists unique divisor (ω) of F/K such that for every divisor $A \in \mathcal{D}_F$ with $A \leq (\omega)$, ω vanishes on $\mathcal{A}_F(A) + F$. This unique divisor called the *canonical* divisor of ω. It follows immediately from this definition that $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega = 0$ or $(\omega) \geq A\}$ for $A \in \mathcal{D}_F$. The degree of a canonical divisor is $2g - 2$, and the dimension is g.

Theorem 1.1.6 *Let A be an arbitrary divisor and $W = (\omega)$ a canonical divisor of F/K. Then the mapping*

$$\begin{aligned} \alpha : L(W - A) &\rightarrow \Omega_F(A) \\ x &\mapsto x\omega \end{aligned}$$

is an isomorphism of K-vector spaces.

Now we can state one of the most important theorems in the theory of algebraic function fields.

Theorem 1.1.7 ***(Riemann-Roch Theorem)*** *Let W be a canonical divisor of F/K. Then for any $A \in \mathcal{D}_F$, we have*

$$\dim A = \deg A + 1 - g + \dim(W - A). \tag{1.16}$$

Note that $\dim A \geq \deg A + 1 - g$ in general. It follows that if $\deg A \geq 2g - 1$ then $\dim A = \deg A + 1 - g$. This is because $\deg(W - A) < 0$ and hence $\dim(W - A) = 0$. In the following definition another embedding of the F into $\mathcal{A}_F$ will be introduced apart from the the diagonal embedding defined before. This leads to the definition of a local component of a Weil differential.

Definition 1.1.12 *(a)* For $x \in F$, let $i_P(x)$ be the adele whose P-component is x, and all other components are 0.
(b) For a Weil differential $\omega \in \Omega_F$ its *local component* at P is defined as

$$\begin{aligned} w_P : F &\rightarrow K \\ x &\mapsto w(i_P(x)) \end{aligned}$$

Lemma 1.1.8 *Let $\omega \in \Omega_F$ and $\alpha = (\alpha_P) \in \mathcal{A}_F$. Then $\omega_P(\alpha_P) \neq 0$ for at most finitely many places P, and*

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P) \tag{1.17}$$

In particular,

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0. \tag{1.18}$$

The following is a useful lemma second part of which says that a Weil differential is uniquely determined by any of its local components.

Lemma 1.1.9 *(a) Let $\omega \neq 0$ be a Weil differential of F/K and $P \in \mathbb{P}_F$. Then*

$$v_P(\omega) = \max\{r \in \mathbb{Z} \mid \omega_P(x) = 0 \ \textit{for all} \ x \in F \ \textit{with} \ v_P(x) \geq -r\}. \qquad (1.19)$$

(b) If $\omega, \omega^{'} \in \Omega_F$ and $\omega_P = \omega^{'}_P$ for some $P \in \mathbb{P}_F$, then $\omega = \omega^{'}$.

Now we define algebraic extensions of function fields. We call a function field F'/K' an *algebraic extension* of F/K if $F' \supseteq F$ is an algebraic field extension with $K' \supseteq K$. If $[F' : F] < \infty$, this algebraic extension is called a *finite extension.* For any finite extension, we have $[K' : K] < \infty$. Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$. If $P \subseteq P'$, then a place $P' \in \mathbb{P}_{F'}$ is said to *lie over* $P \in \mathbb{P}_F$. We also say P' is an *extension* of P or P *lies under* P' and we denote this relation by $P' \mid P$.

Theorem 1.1.10 *Let F'/K' be an algebraic extension of F/K. Let P (respectively P') be a place of F/K (respectively F'/K') and let $\mathcal{O}_P \subseteq F$ (respectively $\mathcal{O}_{P'} \subseteq F'$) be the corresponding valuation ring. Suppose that v_P, $v_{P'}$ are corresponding discrete valuations. Then the following are equivalent:*
(a) $P' \mid P$.
(b) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.
(c) There exists an integer $e \geq 1$ such that $v_{P'}(x) = ev_P(x)$ for all $x \in F$.
If $P' \mid P$, we have $P = P' \cap F$ and $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. An important fact is that any place $P \in \mathbb{P}_F$ has finitely many places in $\mathbb{P}_{F'}$ over it.

The number in part (c) can be defined as follows: If $t \in F$ is a prime for P, then $e = v_{P'}(t)$.

Definition 1.1.13 Let F'/K' be an algebraic extension of F/K, and let $P' \in \mathbb{P}'_F$ be a place of F'/K' lying over $P \in \mathbb{P}_F$.
(i) The integer $e(P'|P) := e$ with $v_{P'}(x) = ev_P(x)$ for any $x \in F$ is called the *ramification index* of P' over P.
(ii) $f(P'|P) := [F'_{P'} : F_P]$ is called the *relative degree* of P' over P.

An important fact related to the numbers e and f is:

$$\sum_{P'|P} e(P^{'} \mid P)f(P^{'} \mid P) = [F^{'} : F].$$

The ramification index $e(P'|P)$ is an integer which is greater than or equal to 1. We say that $P'|P$ is *unramified* if $e(P'|P) = 1$. Otherwise, i.e. $e(P'|P) > 1$, we say $P'|P$ is *ramified*. We say that P is *ramified* (respectively, *unramified*) in F'/F if there is at least one $P' \in \mathbb{P}_F$ over P such that $P'|P$ is ramified (respectively, if $P'|P$ is unramified for all $P'|P$). P is *totally ramified* in F'/F if there is only one extension $P' \in \mathbb{P}_{F'}$ of P and the ramification index is $e(P'|P) = [F' : F]$. The following definition allows us to define homomorphism from divisor group $\mathcal{D}_F$ to $\mathcal{D}_{F'}$

Definition 1.1.14 Let $F^{'}/K^{'}$ be an algebraic extension of F/K. For a place $P \in \mathbb{P}_F$, we define its *conorm* by

$$Con_{F^{'}/F}(P) = \sum_{P'|P} e(P^{'} \mid P)P^{'}. \tag{1.20}$$

The conorm map can be extended to homomorphism from $\mathcal{D}_F$ to $\mathcal{D}_{F'}$ by setting:

$$Con_{F^{'}/F}(\sum n_P P) = \sum n_P Con_{F'/F}(P) \tag{1.21}$$

Now we will associate any Weil differential of F/K with a Weil differential of $F^{'}/K^{'}$, where $F^{'}/F$ is finite separable extension. For this we need to consider the set $\mathcal{A}_{F'/F} = \{\alpha \in \mathcal{A}_{F'} \mid \alpha_{P'} = \alpha_{Q^{'}}$ whenever $P^{'} \cap F = Q^{'} \cap F\}$. This set is a $F^{'}$ subspace of $\mathcal{A}_{F'}$. Note that trace mapping $Tr_{F^{'}/F} : F^{'} \to F$ is nondegenerate since $F^{'}/F$ is separable. This map can be extended to $\mathcal{A}_{F'/F}$ as

$$(Tr_{F^{'}/F}(\alpha))_P := Tr_{F^{'}/F}(\alpha_{P'}) \tag{1.22}$$

for $\alpha \in \mathcal{A}_{F^{'}/F}$, where $P^{'}$ is any place lying over P.

Theorem 1.1.11 *In accordance with the definition above, for every Weil differential ω of F/K, there exists a unique Weil differential $\omega^{'}$ of $F^{'}/K^{'}$ such that*

$$Tr_{K^{'}/K}(\omega^{'}(\alpha)) = \omega(Tr_{F^{'}/F}(\alpha)) \quad \textit{for} \quad \textit{all} \quad \alpha \in \mathcal{A}_{F^{'}/F} \tag{1.23}$$

This unique Weil differential is called the *cotrace* of ω in $F^{'}/F$, and denoted by $Cotr_{F^{'}/F}(\omega)$. The map $Cotr_{F^{'}/F}(\omega)$ can be constructed explicitly . For this, let's consider the dual space $K^* = \{\varphi : K^{'} \to K \mid \varphi \text{ is } K\text{-linear}\}$ of $K^{'}$ over K. If we set $\lambda\varphi(u) = \varphi(\lambda u)$ for $\varphi \in K^*$ and $\lambda, u \in K^{'}$, then K^* is a $K^{'}$-vector space of dimension 1. $Tr_{K'/K}$ is also an element of K^*. So we can regard it as a $K^{'}$-basis for K^*, which implies that there exists a unique $\lambda \in K^{'}$ such that $\varphi = \lambda Tr_{K'/K}$. Keeping this fact in mind, we can state the following lemma which gives explicit construction of Cotrace.

Lemma 1.1.12 *Let $F^{'}/K^{'}$ be a finite separable extension of function field F/K, and consider $\omega \in \Omega_F$. Define $\omega_1 = \omega o Tr_{F'/F} : \mathcal{A}_{F'/F} \to K$ and $\omega_2 : \mathcal{A}_{F'} \to K$ such that $\omega_2(\alpha^{'}) = \omega_1(\alpha)$ where $\alpha^{'} = \alpha + \beta$ such that $\alpha \in \mathcal{A}_{F'/F}$ and $\beta \in \mathcal{A}_{F'}(Con_{F'/F}((\omega)))$. For $\alpha^{'} \in \mathcal{A}_{F'}$ define $\varphi_{\alpha^{'}} \in K^*$ by $\varphi_{\alpha'}(\mu) = \omega_2(\mu\alpha^{'})$ where $\mu \in K^{'}$. Let $\lambda_{\alpha'} \in K^{'}$ such that $\varphi_{\alpha'} = \lambda_{\alpha'} Tr_{K'/K}$. Then*

$$Cotr_{F'/F}(\omega)(\alpha^{'}) = \lambda_{\alpha'} \tag{1.24}$$

Now we define constant field extensions of function fields. For this we consider the function field F/K where K is assumed to be perfect. Let $K^{'}/K$ be an algebraic extension. The compositum $F^{'} := FK^{'}$ is a function field over $K^{'}$, and it is called the *constant field extension* of F/K.

Lemma 1.1.13 *Let $F = FK^{'}$ be an algebraic constant field extension of F/K. Then we have:*
(a) $K^{'}$ is the full constant field of $F^{'}$.
(b) Any subset of F that is linearly independent over K remains so over $K^{'}$.
(c) $[F : K(x)] = [F^{'} : K^{'}(x)]$ for any $x \in F \backslash K$.

Next theorem states some of the most important properties of constant field extensions.

Theorem 1.1.14 *In an algebraic constant field extension $F = FK^{'}$ of F/K, the following holds:*
(a) $F^{'}/F$ is unramified, that is, $e(P^{'} \mid P) = 1$ for all $P \in \mathbb{P}_F$ and all $P^{'} \mid P$.
(b) $F^{'}/K^{'}$ has the same genus as F/K.

(c) For any divisor $A \in \mathcal{D}_F$, we have $deg(Con_{F'/K'}(A)) = degA$.
(d) If W is a canonical divisor of F/K then $Con_{F'/F}(W)$ is also a canonical divisor of F'/K'.
(e) The residue class field $F'_{P'}$ of any place $P' \in \mathbb{P}_{F'}$ is the compositum $F_P K'$, where $P = P' \cap F$.
(f) For any $\omega \in \Omega_F$ we have $Con_{F'/F}((\omega)) = (Cotr_{F'/F}(\omega))$.

When the base field is finite, we have:

Lemma 1.1.15 *Consider a function field $F/\mathbb{F}_q$ and let $F_r = F\mathbb{F}_{q^r}/\mathbb{F}_{q^r}$ be a constant field extension of $F/\mathbb{F}_q$. Then, for any place $P \in \mathbb{P}_F$ of degree m, we have $Con_{F_r/F}(P) = P_1 + ... + P_d$ with $d = \gcd(m, r)$ pairwise distinct places $P_i \in \mathbb{P}_{F_r}$ and $\deg P_i = m/d$.*

An extension F'/K' of F/K is said to be *Galois* if F'/F is a Galois extension of finite degree. The following lemma is about the action of automorphisms in $Gal(F'/F)$ on the places of the function field F'/K'.

Lemma 1.1.16 *Let $F' \supseteq F$ be an algebraic extension of function fields, $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ with $P' \mid P$. Consider an automorphism σ of F'/F. Then $\sigma(P') = \{\sigma(z) \mid z \in P'\}$ is a place of F', and we have*
(a) $v_{\sigma(P')}(f) = v_{P'}(\sigma^{-1}(f))$ for all $f \in F'$
(b) $\sigma(P') \mid P$
(c) The Galois group acts transitively on the set of extensions of P, i.e. if $P_1, P_2 \in \mathbb{P}_{F'}$ such that $P_1 \mid P$ and $P_2 \mid P$, then $P_2 = \sigma(P_1)$ for some $\sigma \in Gal(F'/F)$.

We finish the introduction of algebraic function fields with the notion of differentials and how these are related to the notion of Weil differentials. For this we begin with the following definition.

Definition 1.1.15 Let M be a module over F. A mapping $\delta : F \to M$ is said to be a *derivation* of F/K if δ is K-linear and satisfies the product rule:

$$\delta(uv) = u\delta(v) + v\delta(u), \quad \textit{for any} \quad u, v \in F. \tag{1.25}$$

An element $x \in F$ is called a *separating element* of F/K if $F/K(x)$ is finite separable extension. The following lemma helps us to determine whether an element of a function field is separating or not.

Lemma 1.1.17 *Let F/K be a function field where K is a perfect field of characteristic p. Then any element $z \in F$ satisfying $v_P(z) \neq 0 \; (mod\, p)$ for some place $P \in \mathbb{P}_F$ is a separating element of F/K.*

Suppose x is a separating element of F/K and that $\delta_1, \delta_2 : F \to F$ are derivations of F/K with $\delta_1(x) = \delta_2(x)$. Then $\delta_1 = \delta_2$, i.e. a derivation is uniquely determined by its value on a separating element. For any separating element x of F/K there exist a unique derivation $\delta : F \to F$ such that $\delta(x) = 1$. This unique derivation of F/K is called *the derivation with respect to x* and denoted by δ_x. The set $Der_F := \{\eta : F \to F \mid \eta \text{ is a derivation of } F/K\}$ is called the *module of derivations* of F/K. For $\eta_1, \eta_2 \in Der_F$ we define

$$(\eta_1 + \eta_1)(z) := \eta_1(z) + \eta_2(z) \;\; and \;\; (u\eta_1)(z) := u\eta_1(z) \;\text{ for }\; \eta_1, \eta_2 \in Der_F, \;\; z, u \in F.$$

For any separating element x of F/K and $\eta \in Der_F$, we have $(\eta(x)\delta_x)(x) = \eta(x)\delta_x(x) = \eta(x)$. So Der_F is a *one dimensional* F- module. Furthermore, if x and y are two separating elements of F/K, then $\delta_y = \delta_y(x)\delta_x$. This is called the the *chain rule.* Now the notion of the differential follows.

Definition 1.1.16 (a) On the set $Z := \{(u, x) \in F \times F \mid x \text{ separating } \}$ we define a relation $\sim$ by

$$(u, x) \sim (v, y) \iff v = u\delta_y(x). \tag{1.26}$$

By the chain rule, $\sim$ is a equivalence relation.
(b) The equivalence class of (u, x) with respect to $\sim$ is called a *differential* of F/K and denoted by udx. We denote the equivalence class of $(1, x)$ simply by dx.

Let $\triangle_F := \{udx \mid u \in F \text{ and } x \in F \text{ is separating}\}$ be the set of all differentials. For a separating element $t \in F$ and $udx, vdy \in \triangle_F$, we have $udx = (u\delta_t(x))dt$ and

$vdy = (v\delta_t(y))dt$. So, we define:

$udx+vdy := (u\delta_t(x)+v\delta_t(y))dt$ and $z(udx) := (zu)dx$ for $udx, vdy \in \triangle_F$, $z \in F$.

By these definitions, $\triangle_F$ turns out to be an F-module. In fact, $\triangle_F$ is a 1-dimensional F-module just like Ω_F.

We have defined the notion of discrete valuation of a function field in Definition. 1.1.3. We can define a discrete valuation on any field F. In general, it is a map $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfying properties (i)-(iv) in Definition. 1.1.3. Given a field F and a discrete valuation v on F, we call the pair (F, v) a valued field. We say that a sequence $(x_n)_{n\geq 0} \in F$ is *convergent* if there exists an element $x \in F$ such that for any $c \in \mathbb{R}$ there is an index n_0 such that $v(x-x_n) \geq c$ whenever $n \geq n_0$. A sequence $(x_n)_{n\geq 0}$ is called a *cauchy sequence* if for any $c \in \mathbb{R}$ there is an index n_0 such that $v(x_m - x_n) \geq c$ whenever $n, m \geq n_0$. It can be easily verified that if a sequence is convergent, then its limit is unique. Also, all convergent sequences are cauchy but the converse is not true in general. A valued field is said to be *complete* if all cauchy sequences are convergent. The valued field $(\tilde{F}, \tilde{v})$ is said to be a *completion* of the valued field (F, v) if

(a) $F \subseteq \tilde{F}$ and v is restriction of $\tilde{v}$ to F,

(b) $\tilde{F}$ is complete with respect to $\tilde{v}$,

(c) F is dense in $\tilde{F}$.

It can be shown that a completion can be found for every valued field (F, v). For a place P of a function field F/K, (F, v_p) is a valued field. The completion of F with respect to v_p is called the *P-adic completion* of F. We denote this completion by $\tilde{F}_P$ and the valuation of $\tilde{F}_P$ by v_P.

Theorem 1.1.18 *Let $P \in \mathbb{P}_F$ be a place of degree one and $t \in F$ be a P-prime element. Then any element $z \in \tilde{F}_P$ has a unique representation of the form*

$$z = \sum_{i=n}^{\infty} a_i t^i \quad \textit{with} \quad n \in \mathbb{Z} \quad \textit{and } a_i \in K. \tag{1.27}$$

This is called the P-adic power series expansion of z with respect to t.

Conversely, if $(c_i)_{i\geq n}$ is a sequence in K, then the series $\sum_{i=n}^{\infty} c_i t^i$ converges in $\tilde{F}_P$ and we have

$$v_P\big(\sum_{i=n}^{\infty} c_i t^i\big) = \min\{i \mid c_i \neq 0\}. \tag{1.28}$$

Definition 1.1.17 Assume P is a place of F/K of degree one, and let $t \in F$ be a P-prime element. If $z \in F$ has the P-adic expansion $z = \sum_{i=n}^{\infty} a_i t^i$ with $n \in \mathbb{Z}$ and $a_i \in K$, we define *the residue of z with respect to P and t* by

$$res_{P,t}(z) = a_{-1}. \tag{1.29}$$

Likewise, we can define the residue of a differential $\omega \in \triangle_F$ with respect to a place P of degree one. For this, we choose a P-prime element $t \in F$ and write $\omega = udt$ with $u \in F$. Note that we can write ω in this form since $\triangle_F$ is a one dimensional F-module. Then we define residue of ω at P by

$$res_P(\omega) = res_{P,t}(u). \tag{1.30}$$

It is easy to see that (1.30) is independent of the choice of prime element t for P.

Lemma 1.1.19 *Consider the rational function field $K(x)$. There exists a unique Weil differential $\eta \in \Omega_{K(x)}$ with $(\eta) = -2P_\infty$ and $\eta_{P_\infty}(x^{-1}) = -1$.*

Now we will consider the map $\delta : F \to \Omega_F$ which is defined as

$$\begin{aligned} \delta : F &\to \Omega_F \\ x &\mapsto \delta(x), \end{aligned} \tag{1.31}$$

where $\delta(x) = Cotr_{F/K(x)}(\eta)$ for a separating element x of F/K and $\delta(x) := 0$ if x is not a separating element.

Theorem 1.1.20 *Let F/K be an algebraic function field over the perfect field K and $x \in F$ be separating element. Then*

(a) The map δ defined above is a derivation of F/K.

(b) The map

$$\begin{aligned} \mu : \triangle_F &\to \Omega_F \\ zdx &\to z\delta(x) \end{aligned}$$

is an isomorphism of differential module $\triangle_F$ onto Ω_F.

As a consequence of this theorem, we can identify the differential module $\triangle_F$ with the module Ω_F of Weil differentials of F/K, where K is a perfect field. So any differential $\omega = zdx \in \triangle_F$ is the same as the Weil differential $\omega = z\delta(x) \in \Omega_F$, where x is separating, $z \in F$, and δ is defined as in (1.31).

1.2. Coding Theory

Let $\mathbb{F}_q$ be a finite field with q elements. We consider the n-dimensional vector space $\mathbb{F}_q^n$. For $a = (a_1, a_2, ..., a_n)$ and $b = (b_1, b_2, ..., b_n) \in \mathbb{F}_q^n$, let

$$d(a,b) =\mid \{i \mid a_i \neq b_i\} \mid . \tag{1.32}$$

This is called the *Hamming Distance* on $\mathbb{F}_q^n$. We define the *weight* of $a \in \mathbb{F}_q^n$ as

$$w(a) =\mid \{i \mid a_i \neq 0\} \mid= d(a,0). \tag{1.33}$$

A *q-ary linear code C* is a linear subspace of $\mathbb{F}_q^n$. Elements of C are called *codewords.* We call n *the length* of C and $\dim_{\mathbb{F}_q} C$ *the dimension* of C. The *minimum distance $d(C)$* of a code $C \neq 0$ is defined as

$$d(C) = \min\{d(a,b) \mid a, b \in C,\ a \neq b\} = \min\{w(c) \mid c \neq 0\}. \tag{1.34}$$

So, an $[n, k, d]$ code is a code with length n, dimension k and minimum distance d.

The *dual* code of C, denoted by $C^\perp$, is the orthogonal of C with respect to the usual inner product on $\mathbb{F}_q^n$, i.e.

$$C^\perp = \{(a_1, ..., a_n) \in \mathbb{F}_q^n \mid \sum_i a_i c_i = 0 \text{ for all } (c_1, ..., c_n) \in C\}.$$

Obviously, $\dim C^{\perp} = n - \dim C$.

The *weight distribution* of an $[n,k]$ code is the $(n+1)-$tuple $(A_0, ...A_n)$ given by

$$A_i :=\mid \{c \in C \mid w(c) = i\} \mid .$$

It is often given by a polynomial $W_C(X) \in \mathbb{Z}[X]$ which is called the *weight enumerator* :

$$W_C(X) = \sum_{i=0}^{n} A_i X^i$$

The following theorem gives a relation between the weight distribution of the codes C and its dual $C^{\perp}$.

Theorem 1.2.21 ***(The MacWilliams Identity)*** *Let C be a q-ary code of length n with weight enumerator $W_C(X)$. Then,*

$$W_{C^{\perp}}(X) = q^{-k}(1+(q-1)X)^n W_C\Big(\frac{1-X}{1+(q-1)X}\Big).$$

A q-ary linear code C of length n which is closed under cyclic shift is called a *cyclic* code, i.e.

$$(c_0, ..., c_{n-1}) \in C \Longrightarrow (c_{n-1}, c_0, ..., c_{n-2}) \in C.$$

In general, one assumes that $\gcd(n,q) = 1$. Note the following $\mathbb{F}_q$-linear isomorphism:

$$\begin{array}{rcl} \mathbb{F}_q^n & \rightarrow & R = \mathbb{F}_q^n[t]/(t^n-1) \\ (c_0, ..., c_{n-1}) & \mapsto & \sum_{i=0}^{n-1} c_i t^i \end{array}$$

Under this correspondence, a cyclic code can be viewed a subset of R. In fact, it is an ideal in the quotient ring. Since R is a principal ideal ring, C has a unique generating polynomial $g(x)$, called the *generator polynomial* of C. An important fact is that $\dim C = n - \deg(g(t))$.

CHAPTER 2

GENERALIZED GEOMETRIC GOPPA CODES

In this chapter, we will first present Goppa's construction [1] of the codes using algebraic function fields. In his construction, Goppa used rational places. The codes could be defined both in terms of Riemann-Roch spaces or spaces of Weil differentials. Later, the notion of generalized geometric Goppa codes were introduced by Xing-Niederreiter-Lam [9] using places of arbitrary degree, and Heydtmann [2] investigated the duals of the generalized codes. These works are explained in Sections 2 and 3.

2.1. Geometric Goppa Codes

We refer to Section II.2 in [6] for the proofs of the results in this section. We fix some notation:
$F/\mathbb{F}_q$ is an algebraic function field of genus g,
$P_1, P_2, .., P_n$ are pairwise distinct rational places of $F/\mathbb{F}_q$,
$D = P_1 + P_2 ... + P_n$,
G is a divisor of $F/\mathbb{F}_q$ with $SuppG \cap SuppD = \emptyset$,

Now we consider the map

$$\begin{aligned} \alpha : L(G) &\rightarrow \mathbb{F}_q^n \qquad (2.1) \\ f &\mapsto (f(P_1, f(P_2), ..., f(P_n)). \qquad (2.2) \end{aligned}$$

Since $f \in L(G)$ and $SuppG \cap SuppD = \emptyset$, $v_{P_i}(f) \geq 0$ and this definition makes sense. The image of α is called *Geometric Goppa Code* associated with the divisors D and G. It is denoted by $C_L(D, G)$. One can calculate its parameters k and d by means of Riemann-Roch theorem (Theorem 1.1.7).

Theorem 2.1.1 *$C_L(D, G)$ is a q-ary $[n, k, d]$ code with parameters*

$$k = \dim G - \dim(G - D) \text{ and } d \geq n - \deg G. \qquad (2.3)$$

If $\deg G < n$ then the map α in (2.1) is injective and

$$k = \dim G \geq \deg G + 1 - g. \qquad (2.4)$$

Furthermore, $k = \deg G + 1 - g$ if $\deg G \geq 2g - 1$.

Another code associated with the divisors G and D is introduced now. Let G and $D = P_1 + P_2 + ... + P_n$ be divisors as before. Then the code $C_\Omega(D, G)$ is defined as

$$C_\Omega(D, G) = \{(\omega_{P_1}(1), \omega_{P_2}(1), ..., \omega_{P_n}(1)) \mid \omega \in \ \Omega_F(G - D)\}. \qquad (2.5)$$

The following theorem is analogous to Theorem 2.1.1.

Theorem 2.1.2 *$C_\Omega(D, G)$ is a q-ary $[n^{'}, k^{'}, d^{'}]$ code with parameters*

$$k^{'} = i(G - D) - i(G) \text{ and } d^{'} \geq \deg G - (2g - 2). \qquad (2.6)$$

If $\deg G > 2g - 2$, then we have

$$k^{'} = i(G - D) \geq n + g - 1 - \deg G. \qquad (2.7)$$

Furthermore, $k^{'} = n + g - 1 - \deg G$ if $2g - 2 < \deg G < n$.

There is a close relation between $C_\Omega(D,G)$ and $C_L(D,G)$, which is that they are dual to each other with respect to canonical inner product on $\mathbb{F}_q^n$. That is,

$$C_L(D,G) = C_\Omega(D,G)^\perp. \tag{2.8}$$

Furthermore, $C_\Omega(D,G)$ can be written as $C_L(D,H)$ for a suitable divisor H. The following lemma states how we choose H.

Lemma 2.1.3 *(a) Let F/K be an algebraic function field. Then there exists a Weil differential η such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for $i = 1, 2, ..., n$.*
(b) If η is the Weil differential as above and $H = D - G + (\eta)$, then

$$C_\Omega(D,G) = C_L(D,G)^\perp = C_L(D,H). \tag{2.9}$$

2.2. Generalization

In order to define the generalization of geomtric Goppa codes, we first need to extend the notion of a code, which was defined in Chapter 1, Section 2.

Let $\mathbb{F}_q$ be a finite field with q elements, and $k_1, ..., k_n$ be natural numbers. Let $\prod_{i=1}^n \mathbb{F}_{q^{k_i}}$ denote the cartesian product of extensions of $\mathbb{F}_q$. A *code C (over a mixed alphabet)* is an $\mathbb{F}_q$- subspace of $\prod_{i=1}^n \mathbb{F}_{q^{k_i}}$. The length of C is n and the dimension k of C is $\dim_{\mathbb{F}_q} C$. Note that $k > n$ could happen in this case, unlike the situation in the usual linear codes. For $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \prod_{i=1}^n \mathbb{F}_{q^{k_i}}$, we define the distance of a to b by

$$d(a,b) = \mid \{i \mid \ a_i \neq b_i\} \mid,$$

the weight of a by

$$w(a) = \mid \{i \mid \ a_i \neq 0\} \mid,$$

and the minimum distance of C by

$$d = \min\{w(a) \mid \ a \neq 0\}.$$

Note that when $k_1 = k_2 = ... = k_n = 1$, all these definitions reduce to the case of the usual linear codes over $\mathbb{F}_q$. The context will make it clear whether we are dealing with a code in the sense of Chapter 1 or as above (over a mixed alphabet).

We have seen in the previous section that classical geometric Goppa codes are constructed via rational places of a function field. Unlike these codes, generalized geometric Goppa codes are constructed using places of arbitrary degree of a function field F/K. Before the construction, let's fix some notation which will be valid for the rest of this chapter:
$F/\mathbb{F}_q$ is an algebraic function field of genus g,
$P_1, P_2, .., P_n$ are pairwise distinct places of $F/\mathbb{F}_q$,
$k_i = degP_i$ for $1 \leq i \leq n$,
$D = P_1 + P_2 ... + P_n$,
G is a divisor of $F/\mathbb{F}_q$ with $SuppG \cap SuppD = \emptyset$.
Now we define generalized geometric Goppa code as follows.

Definition 2.2.1 The image of the following map is called *a generalized geometric Goppa code* associated with the divisor D and G.

$$\alpha : L(G) \rightarrow \prod_{i=1}^{n} \mathbb{F}_{q^{k_i}} \tag{2.10}$$

$$f \mapsto (f(P_1), ..., f(P_n)) \tag{2.11}$$

Note that this definition makes sense: for $f \in L(G)$, we have $v_{P_i}(f) \geq 0$ because $suppG \cap suppD = \emptyset$, and for a place P of F of degree k_i and a function $f \in F$ with $v_p(f) \geq 0$, the residue class $f(P)$ of f in the residue class field of P can be associated with an element of $\mathbb{F}_{q^{k_i}}$. The image of α is obviously a $\mathbb{F}_q$ vector space. The following lemma states the parameters of this code. Note the similarity of the results to those of Theorem 2.1.1.

Lemma 2.2.4 *$C_L(D, G)$ is an $[n, k_L, d_L]$ code with the parameters*

$$k_L = \dim G - \dim(G - D) \text{ and } d_L \geq n - \deg G. \tag{2.12}$$

In addition, if $\deg G < N$ where $N = \sum_{i=1}^{n} k_i$, then $k_L = \dim G \geq \deg G - g + 1$, and consequently we have $k_L = \deg G - g + 1$ if $2g - 2 < \deg G < N$.

Proof: For the proof we consider the kernel of the associated mapping.

$$\begin{aligned} Ker(\alpha) &= \{f \in L(G) \mid f(P_i) = 0 \;\; for \;\; i = 1, ..., n\} \\ &= \{f \in L(G) \mid f \in P_i \;\; for \;\; i = 1, ..., n\} \\ &= \{f \in L(G) \mid v_{P_i}(f) > 0 \;\; for \;\; i = 1, ..., n\} \\ &= L(G - D). \end{aligned}$$

So, we have $\dim C_L(D, G) = \dim G - \dim(G - D)$. If $\deg G < \deg D$ then $\deg(G - D) < 0$ and $\dim(G - D) = 0$. Therefore, $k_L = \dim G \geq \deg G - 1 + g$ with equality holding if $2g - 2 < \deg G < N$ by the Riemann-Roch Theorem (Theorem 1.1.7).

For the minimum distance, let us take $0 \neq f \in L(G)$ with $w(\alpha(f)) = d_L$. Then there exists $n - d_L$ places $P_{i_1}, ..., P_{i_{n-d_L}}$ such that $f(P_{i_j}) = 0$ for $1 \leq j \leq n - d_L$. Therefore,

$$0 \neq f \in L(G - (P_{i_1} + P_{i_2} ... + P_{i_{n-d_L}})).$$

Since it is a non-zero element, we have

$$\begin{aligned} 0 \leq \deg(G - (P_{i_1} + P_{i_2} ... + P_{i_{n-d_L}})) &= \deg G - \sum_{j=1}^{n-d_L} k_{i_j} \\ &= \deg G - \sum_{j=1}^{n-d_L} (k_{i_j} - 1) - n + d_L \end{aligned}$$

which yields,

$$d_L \geq n - \deg G + \sum_{J=1}^{n-d_L} (k_{i_j} - 1) \geq n - \deg G.$$

□

Xing, Nedereiter and Lam were the first to introduce generalization of classical geometric Goppa codes using higher degree places (see [9]). Their generalization via a q-ary code in the sense of Chapter 1 and can be recovered from our general code (over mixed alphabet) definition. For this, let $C_1, ..., C_n$ be q-ary linear code with parameters $[n_i, k_i, d_i]$ for $i = 1, ..., n$. Since $\dim C_i = k_i$, $\mathbb{F}_{q^{k_i}}$ and C_i are $\mathbb{F}_q-$isomorphic for all i. Let $\pi_1, ..., \pi_n$ be fixed isomorphisms from $\mathbb{F}_{q^{k_i}}$ to $C_i \subseteq \mathbb{F}_q^{n_i}$.

This way, an element of $\mathbb{F}_{q^{k_i}}$ can be viewed as an element of C_i, i.e. n_i-tuple over $\mathbb{F}_q$ for each i. This idea is called *concetenation* in coding theory. Now the Xing -Nedereiter-Lam construction can be given.

Definition 2.2.2 The image of the following map is called *the concatenated generalized geometric Goppa code:*

$$\begin{aligned}\alpha : L(G) &\rightarrow \mathbb{F}_q^m \\ f &\rightarrow (\pi_1(f(P_1)), ..., \pi_n(f(P_n)))\end{aligned}$$

where $m = \sum_{i=1}^{n} n_i$.

We denote this concatenated code by $C(P_1, ..., P_n; G; C_1, ..., C_n)$.

Theorem 2.2.5 *If* $\deg G < \sum_{i=1}^{n} k_i$ *then* $C(P_1, ..., P_n; G; C1, ..., C_n)$ *is a* q*-ary* $[m, k, d]$ *code with*

$$\begin{aligned} k &\geq \deg G - g + 1, \ \textit{equality holding if} \ \deg G \geq 2g - 1 \\ \textit{and} & \\ d &\geq \sum_{i=1}^{s} d_i - \deg G - \max\big\{ \sum_{i \in R} (d_i - k_i) \mid R \subseteq \{1, ...n\} \big\}, \end{aligned}$$

where the empty sum is defined to be 0 *as usual.*

Proof: We consider the kernel of α again.

$$\begin{aligned} Ker(\alpha) &= \{f \in L(G) \mid \pi_i(f(P_i)) = 0 \ \text{for} \ 1 \leq i \leq n\} \\ &= \{f \in L(G) \mid f(P_i)) = 0 \quad \text{for} \ 1 \leq i \leq n\} \ (\pi_i\text{'s} \quad \text{are} \quad \text{isomorphisms}) \\ &= L(G - D). \end{aligned}$$

Since $\deg G < \deg D$ we have $\dim(G - D) = 0$, which implies $k = \dim G$. So, it is again an immediate consequence of Riemann-Roch Theorem that the dimension k satisfies $k = \dim G \geq \deg G - g + 1$ with equality if $\deg G \geq 2g - 1$. For the minimum distance, let's take an arbitrary nonzero function $f \in L(G)$. We define the following subset of $\{1, ..., n\}$:

$$R = \{i \mid f(P_i) = 0\} \tag{2.13}$$

Let T be complement of R in $\{1, ..., n\}$. Then,

$$w(\alpha(f)) = \sum_{i \in T} w(\pi_i(f(P_i))) \geq \sum_{i \in T} d_i. \tag{2.14}$$

(2.13) implies that $f \in L(G - \sum_{i \in R} P_i)$. So we have

$$\deg G \geq \sum_{i \in R} \deg P_i = \sum_{i \in R} k_i = \sum_{i \in R} d_i - \sum_{i \in R} (d_i - k_i). \tag{2.15}$$

Adding the equations (2.14) and (2.15) we get

$$w(\alpha(f)) + \deg G \geq \sum_{i=1}^{n} d_i - \sum_{i \in R} (d_i - k_i).$$

Taking the maximum of both sides over all the subsets of $\{1, ..., n\}$, we obtain the desired result. □

An immediate corollary of this theorem is that if we have $k_i \geq d_i$ for $1 \leq i \leq n$ with the inequality $\deg G < \sum_{i=1}^{n} k_i$, then the minimum distance d of the $C(P_1, ..., P_n; G; C_1, ..., C_n)$ satisfies

$$d \geq \sum_{i=1}^{n} d_i - \deg G.$$

2.3. Dual of the Generalized Geometric Goppa Code

We know that the dual of the classical geometric Goppa code $C_L(D, G)$, which is constructed via rational places, is $C_\Omega(D, G)$ (2.8). The code $C_\Omega(D, G)$ was defined as an evaluation of local components of Weil differentials of $\Omega_F(G - D)$ at rational places. Now we will define a new code which is again denoted by $C_\Omega(D,G)$ without restrictions on the degrees of the places $P_1,...,P_n$.

As before, let $P_1,...,P_n$ be arbitrary places of $F/\mathbb{F}_q$ with degrees k_i, for $1 \leq i \leq n$, and let $\mathbb{F}_{q^\ell}$ be smallest field containing all $\mathbb{F}_{q^{k_i}}$ for $i = 1,..,n$. We will consider the constant field extension $F^{'} = F\mathbb{F}_{q^\ell}/\mathbb{F}_{q^\ell}$. We will also consider the conorms $D^{'} = Con_{F^{'}/F}(D)$ and $G^{'} = Con_{F^{'}/F}(G)$. Since $suppG \cap suppD = \emptyset$ the code $C_L(D^{'},G^{'}) \subseteq \mathbb{F}_{q^\ell}^N$ is a q^ℓ-ary classical geometric Goppa code, where $N = \sum_{i=1}^n k_i$. We will also need the constant field extensions $F_{k_i} = F\mathbb{F}_{q^{k_i}}/\mathbb{F}_{q^{k_i}}$ and the corresponding conorms $D_{k_i} = Con_{F_{k_i}/F}(D)$ and $G_{k_i} = Con_{F_{k_i}/F}(G)$ for $i = 1,...n$.

Throughout the section, we let P_i^* be a fixed place of $F_{k_i}/\mathbb{F}_{q^{k_i}}$ above P_i for $i \leq 1 \leq n$. Since $\deg P_i^* = 1$, the residue class fields of these places F_{P_i} and $F_{k_i P_i^*}$ satisfy $F_{P_i} \cong F_{k_i P_i^*} \cong \mathbb{F}_{q^{k_i}}$. If $Q_i^* \in \mathbb{P}_{F_{k_i}}$ is an arbitrary place above P_i then there exists only one place of degree 1 in $F^{'}$ above Q_i^*, which will be denoted by $Q_i^{'}$. Then the residue class fields F_{P_i}, $F_{k_i P_i^*}$ can be considered as subfields of the residue class field of $P_i^{'}$, which implies we can identify $f(P_i) = f(P_i^*) = f(P_i^{'}) \in \mathbb{F}_{q^{k_i}}$ for any $f \in L(G) \subseteq L(G_{k_i}) \subseteq L(G^{'})$. Keeping these facts in mind we have the following construction.

Definition 2.3.3 We define the code $C_\Omega(D,G)$ as follows:

$$C_\Omega(D,G) = \{(Cotr_{F_{k_1}/F}(\omega)_{P_1^*},...,Cotr_{F_{k_n}/F}(\omega)_{P_n^*}) \mid \omega \in \Omega_F(G-D)\}.$$

$C_\Omega(D,G)$ is an $\mathbb{F}_q$ subspace of $\prod_{i=1}^n \mathbb{F}_{q^{k_i}}$, i.e. a code over mixed alphabet. The following lemma gives us information about the parameters of this code.

Lemma 2.3.6 *$C_\Omega(D,G)$ is an $[n,k_\Omega,d_\Omega]$ code with parameters,*

$$k_\Omega = i(G-D) - i(G) \text{ and } d_\Omega \geq \deg G - (N-n) - (2g-2),$$

where $N = \deg D = \sum_{i=1}^n k_i$.
In addition, if $degG > 2g-2$ then

$$k_\Omega = i(G-D) \geq N - \deg G + g - 1$$

and as a result, we have

$$k_\Omega = N + g - 1 - degG \ \ if \quad 2g-2 < degG < N.$$

Proof: Let $P \in \mathbb{P}_\mathbb{F}$ be a place of degree one and ω be a Weil differential with $v_P(\omega) \geq -1$. Then we claim

$$\omega_P(1) = 0 \Longleftrightarrow v_P(\omega) \geq 0.$$

The implication $\Leftarrow$ is an immediate result of Lemma 1.1.9 by choosing $r = 0$. Conversely, let's assume that $\omega_P(1) = 0$. Let $x \in F$ with $v_P(x) \geq 0$. Since $\deg P = 1$, we can write $x = a + y$ with $a \in \mathbb{F}_q$ and $v_P(y) \geq 1$. Then we have,

$$\omega_P(x) = \omega_P(a+y) = \omega_P(a) + \omega_P(y) = a\omega_P(1) + 0 = 0. \tag{2.16}$$

So, again by Lemma 1.1.9 we have $v_P(\omega) \geq 0$.

Now we will consider the following mapping

$$\begin{array}{rcl} \alpha : \Omega_F(G-D) & \rightarrow & C_\Omega(D,G) \\ \omega & \mapsto & (Cotr_{F_{k_1}/F}(\omega)_{P_1^*}(1), ..., Cotr_{F_{k_n}/F}(\omega)_{P_n^*}(1)) \end{array}$$

We know that $(Cotr_{F_{k_i}/F}(\omega)) = Con_{F_{k_i}/F}(\omega)$ in constant field extensions by Theorem 1.1.14. Since $\omega \in \Omega_F(G-D)$ and constant field extensions are unramified, we have $v_{P_i}(\omega) = v_{P_i^*}(Cotr_{F_{k_i}/F}(\omega)) \geq -1$. Now we can consider the kernel of the mapping α:

$$\begin{array}{rcl} Ker(\alpha) & = & \{\omega \in \Omega_F(G-D) \mid Cotr_{F_{k_i}/F}(\omega)_{P_1^*}(1) = 0 \quad \text{for } 1 \leq i \leq n\} \\ & = & \{\omega \in \Omega_F(G-D) \mid v_{P_i^*}(Cotr_{F_{k_i}/F}(\omega)) = v_{P_i}(\omega) \geq 0 \quad \text{for } 1 \leq i \leq n\} \\ & = & \Omega_F(G) \end{array}$$

Thus, $k_\Omega = \dim \Omega_F(G-D) - \dim \Omega_F(G) = i(G-D) - i(G)$. If $\deg G > 2g-2$ then $i(G) = \dim G - \deg G + g - 1 = 0$ by the Riemann-Roch theorem. Therefore, $k_\Omega = i(G-D) = \dim(G-D) - \deg(G-D) + g - 1 = \dim(G-D) - \ degG + \deg D + g - 1 \geq N - \deg G + g - 1$. In addition, if $2g-2 < \deg G < N$ then $\dim(G-D) = 0$ which implies $k_\Omega = N - \deg G + g - 1$.

For the minimum distance, let's choose $\omega \in \Omega_F(G-D)$ such that $w(\alpha(\omega)) = d_\Omega$. Then there exists $n - d_\Omega$ places $P_1, ..., P_{n-d_\Omega}$ such that $Cotr_{F_{k_{i_j}}/F}(\omega)_{P^*_{i_j}}(1) = 0$ for $j = 1, ..., n - d_\Omega$. Then we have

$$0 \neq \omega \in \Omega_F(G - D + \sum_{k=1}^{n-d_\Omega} P_{i_k}),$$

which implies that

$$\begin{aligned} 2g - 2 \geq \deg(G - D + \sum_{n=1}^{n-d_\Omega} P_{i_k}) &= \deg G - N + \sum_{j=1}^{n-d_\Omega} k_{i_j} \\ &= \deg G - N + \sum_{j=1}^{n-d_\Omega} (k_{i_j} - 1) + n - d_\Omega \end{aligned}$$

Hence

$$d_\Omega \geq degG - (N - n) - (2g - 2).$$

□

Remark 2.3.1 We can obviously concatenate these codes as we did with the generalized geometric Goppa codes $C_L(D, G)$. Let's take again n distinct codes $C_1, ..., C_n$ with parameters $[n_i, k_i, d_i]$ for $1 \leq i \leq n$, and let $\pi_1, ...\pi_n$ be $\mathbb{F}_q$-linear isomorphisms mapping $\mathbb{F}_{q^{k_i}}$ onto $C_{_i}$. Then define

$$C_\Omega(D; G; C_1, ..., C_n) = \{(\pi_1(c_1), ..., \pi_n(c_n)) \mid (c_1, ..., c_n) \in C_\Omega(D, G)\}.$$

The length m of this code is obviously $\sum_{i=1}^{i=n} n_i$. By an argument similar to that of Theorem 2.2.5, it can be easily shown that $C_\Omega(D; G; C_1, ..., C_n)$ is an $[m, k, d]$ code with

$$k \geq N - \deg G + g - 1 \quad \text{equality} \quad \text{holding} \quad \text{if} \quad \deg G < \deg D = N,$$

and we also have

$$d \geq \deg G - (2g - 2) - \sum_{i=1}^{n} (k_i - d_i) - \max\Big\{\sum_{i \in R} (d_i - k_i) \mid R \subseteq 1, ..., n\Big\}.$$

In analogy with the classical geometric Goppa code $C_L(D, G)$ and its dual $C_\Omega(D, G)$, we want to show that the generalized geometric Goppa code $C_L(D, G)$ (Definition 2.2.1) and the code $C_\Omega(D, G)$ (Definition 2.3.3) are "dual" to each other. For this, we introduce an inner product on $\prod_{i=1}^{n} \mathbb{F}_{q^{k_i}}$.

Definition 2.3.4 (a) For $a = (a_1, ..., a_n)$ and $b = (b_1, ..., b_n) \in \prod_{i=1}^{n} \mathbb{F}_{q^{k_i}}$, we define

$$< a, b >= \sum_{i=1}^{n} Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(a_i b_i). \tag{2.17}$$

(b) The dual of a code $C \subseteq \prod_{i=1}^{n} \mathbb{F}_{q^{k_i}}$ with respect to above inner product is defined in the usual manner, i.e.

$$C^{\perp} = \{a \in \prod_{i=1}^{n} \mathbb{F}_{q^{k_i}} \mid < a, c >= 0, \ \forall c \in C\}.$$

It is clear that $\dim C^{\perp} = N - \dim C$.

Before we state and prove the main theorem, i.e. $C_L(D, G)^{\perp} = C_{\Omega}(D, G)$, we will need some lemmas. Note that for each $i = 1, ..., n$, the extension F_{k_i}/F is galois, and hence the galois group acts transitively on the set of the extensions of P_i by Lemma 1.1.16.

Lemma 2.3.7 *Let $\omega \in \Omega_F$ and $f \in F$. Then for any $\sigma \in Gal(F_{k_i}/F)$, we have*

$$\sigma(Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(f)) = Cotr_{F_{k_i}/F}(\omega)_{\sigma(P_i^*)}(f).$$

Proof: We prove this lemma using the construction of $Cotr(\omega)$ in Lemma 1.1.12. So the notation will be consistent with that lemma. For $\mu \in \mathbb{F}_{q^{k_i}}$, we define $\alpha_{\mu}^* = (\alpha_{\mu Q^*}^*) = i_{P_i^*}(\mu f) \in \mathcal{A}_{F_{k_i}}$. Then by the weak approximation theorem, there exists $x_{P_i} \in F_{k_i}$ such that

$$v_{Q_i^*}(\alpha_{\mu Q^*}^* - x_{P_i}) \geq -v_{Q_i^*}(Con_{F_{k_i}/F}((\omega))) \quad \text{for} \quad \text{all} \quad Q_i^* \mid P_i \tag{2.18}$$

Now we let $\beta_{\mu}^* = (\beta_{\mu Q^*}^*) = \sum_{Q_i^* | P_i} i_{Q_i^*}(x_{P_i})$. Since $Q_i^* \cap F = P_i$ for all $Q_i^* \mid P_i$ we have $\beta_{\mu}^* \in \mathcal{A}_{F_{k_i}}$, and $\alpha_{\mu}^* - \beta_{\mu}^* \in \mathcal{A}_{F_{k_i}}(Con_{F_{k_i}/F}((\omega))$. Thus, in accordance with the Lemma 2.3.6, we get $\varphi_{\alpha_1^*} = \omega_2(\mu\alpha_1^*) = \omega_1(\beta_{\mu}^*)$. For a fixed $\sigma \in Gal(F_{k_i}/F)$, the following hold

$$\begin{aligned} v_{\sigma(Q_i^*)}(\sigma(\alpha_{\mu Q_i^*}^*) - \sigma(x_{P_i})) &= v_{Q_i^*}(\sigma^{-1}(\sigma(\alpha_{\mu Q_i^*}^*) - \sigma(x_{P_i}))) \quad (\text{by} \quad \text{Lemma 1.1.16}) \\ &= v_{Q_i^*}(\alpha_{\mu Q^*}^* - x_{P_i}) \geq -v_{Q_i^*}(Con_{F_{k_i}/F}((\omega))) \ (\text{by} \ (2.18)) \\ &= -v_{\sigma(Q_i^*)}(Con_{F_{k_i}/F}((\omega))), \ \text{for all} \ Q_i^* \mid P_i. \end{aligned}$$

The last equation is due to the fact that a constant field extension is unramified. Likewise, we let $v = \sigma(\mu)$ and define $\alpha_v^\circ = (\alpha_{vQ^*}^\circ) = i_{\sigma(P_i^*)}(vf) = i_{\sigma(P_i^*)}(\sigma(\mu f)$. By the same argument above we have

$$v_{Q_i^*}(\alpha_{vQ^*}^\circ - \sigma(x_{P_i})) = v_{Q_i^*}(\sigma(\alpha_{\mu\sigma^{-1}(Q_i^*)}^*) - \sigma(x_{P_i})) \geq -v_{Q_i^*}(Con_{F_{k_i}/F}((\omega))),$$

for all $Q_i^* \mid P_i$. Now, let $\beta_v^\circ = (\beta_{vQ^*}^\circ) = \sum_{Q_i^*|P_i} i_{Q_i^*}(\sigma(x_{P_i}))$. Then we have $\beta_v^\circ \in \mathcal{A}_{F_{k_i}/F}$ and $\alpha_v^\circ - \beta_v^\circ \in \mathcal{A}_{F_{k_i}}(Con_{F_{k_i}/F}((\omega))$, so

$$\begin{aligned}
\varphi_{\alpha_1^\circ} = \omega_2(v\alpha_1^\circ) &= \omega_1(\beta_v^\circ) = \omega(Tr_{F_{k_i}/F}(\beta_v^\circ) = \omega_{P_i}(Tr_{F_{k_i}/F}(\sigma(x_{P_i}))) \\
&= \omega_{P_i}\big(\sum_{\sigma' \in Gal(F_{k_i}/F)} \sigma' o\sigma(x_{P_i})\big) \\
&= \omega_{P_i}\big(\sum_{\sigma' \in Gal(F_{k_i}/F)} \sigma'(x_{P_i})\big) \\
&= \omega_{P_i}(Tr_{F_{k_i}/F}(x_{P_i})) = \omega_1(\beta_\mu^*) = \omega_2(\mu\alpha_1^*) = \varphi_{\alpha_1^*}(\mu)
\end{aligned}$$

In the above equations, we use again Lemma 1.1.12 and the extended definition of trace. We continue as follows,

$$\begin{aligned}
\varphi_{\alpha_1^\circ}(\mu) &= \varphi_{\alpha_1^*}(\sigma^{-1}(\mu)) = \lambda_{\alpha_1^*}.Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(\sigma^{-1}(\mu)) = Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(\lambda_{\alpha_1^*}.\sigma^{-1}(\mu)) \\
&= \sum_{\sigma' \in Gal(F_{k_i}/F)} \sigma'(\lambda_{\alpha_1^*}.\sigma^{-1}(\mu)) \\
&= \sum_{\sigma' \in Gal(F_{k_i}/F)} \sigma' o\sigma^{-1}(\sigma(\lambda_{\alpha_1^*}).(\mu)) \\
&= \sum_{\sigma' \in Gal(F_{k_i}/F)} \sigma'(\sigma(\lambda_{\alpha_1^*}).(\mu)) \\
&= Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(\sigma(\lambda_{\alpha_1^*}).\mu) \\
&= \sigma(\lambda_{\alpha_1^*}).Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(\mu)
\end{aligned}$$

In the end we have $Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(f) = \lambda_{\alpha_1^*}$ and $Cotr_{F_{k_i}/F}(\omega)_{\sigma(P_i^*)}(f) = \sigma(\lambda_{\alpha_1^*})$ so the proof is completed. □

Lemma 2.3.8 *Let F/K be an algebraic function field, and F'/K' be a finite separable extension of F/K. For any $\omega \in \Omega_F$ and $P \in \mathbb{P}_F$, we have*

$$\sum_{P'|P} Cotr_{F'/F}(\omega)_{P'}(f) = \omega_P(f), \textit{ for all } f \in F.$$

Proof: Note that by Lemma 1.1.8, we have

$$\sum_{P'|P} Cotr_{F'/F}(\omega)_{P'}(f) = Cotr_{F'/F}(\omega)\big(\sum_{P'|P} i_{P'}(f)\big).$$

We also have $\sum_{P'|P} i_{P'}(f) \in \mathcal{A}_{F'/F}$, so we can use Lemma 1.1.12 for calculating the value of this adele at $Cotr_{F'/F}(\omega)$. With the same notation as in this lemma, we have

$$\begin{aligned}
\varphi_{\sum_{P'|P} i_{P'}}(\mu) &= \omega_2(\mu \sum_{P'|P} i_{P'}(f)) = \omega_1(\sum_{P'|P} \mu i_{P'}(f)) \\
&= \omega o Tr_{F'/F}(\sum_{P'|P} i_{P'}(\mu f)) \\
&= \omega(i_P(Tr_{F'/F}(\mu f))) \text{ (Definition of Trace function)} \\
&= \omega(i_P(f Tr_{K'/K}(\mu))) \text{ (since } f \in F \text{ and } \mu \in K^{'}) \\
&= \omega(i_P(f) Tr_{K'/K}(\mu)) \\
&= \omega(i_P(f)) Tr_{K'/K}(\mu) \text{ (since } \omega \text{ is K-linear)} \\
&= \omega_P(f) Tr_{K'/K}(\mu)
\end{aligned}$$

So, we have

$$Cotr_{F'/F}(\omega)\big(\sum_{P'|P} i_{P'}(f)\big) = \omega_P(f) = \sum_{P'|P} Cotr_{F'/F}(\omega)_{P'}(f).$$

□

Now the main theorem follows.

Theorem 2.3.9 *The codes $C_L(D,G)$ and $C_\Omega(D,G)$ are dual to each other with respect to inner product defined in Definition 2.3.4.*

Proof: First we will prove the inclusion $C_L(D,G)^\perp \supseteq C_\Omega(D,G)$. For this, let $a = (Cotr_{F_{k_1}/F}(\omega)_{P_1^*}(1), ..., Cotr_{F_{k_n}/F}(\omega)_{P_n^*}(1)) \in C_\Omega(D,G)$ and let's take $b = (f(P_1), ..., f(P_n)) = (f(P_1^*), ..., f(P_n^*)) \in C_L(D,G)$. Then, by definition of inner product, given in Definition 2.3.4, we have

$$\begin{aligned}
< a,b > &= \sum_{i=1}^{n} Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1).f(P_i)) \\
&= \sum_{i=1}^{n} Tr_{\mathbb{F}_{q^{k_i}}/\mathbb{F}_q}(Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1).f(P_i^*)) \\
&= \sum_{i=1}^{n} \sum_{\sigma\in Gal(F_{k_1}/F)} \sigma(Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1).f(P_i^*)) \\
&= \sum_{i=1}^{n} \sum_{\sigma\in Gal(F_{k_1}/F)} \sigma(Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1)).\sigma(f(P_i^*)) \\
&= \sum_{i=1}^{n} \sum_{\sigma\in Gal(F_{k_1}/F)} Cotr_{F_{k_i}/F}(\omega)_{\sigma(P_i^*)}(1).(f+\sigma(P_i^*)) \quad \text{(by lemma 2.3.7)} \\
&= \sum_{i=1}^{n} \sum_{Q_i^*|P_i} Cotr_{F_{k_i}/F}(\omega)_{Q_i^*}(1).f(Q_i^*) \\
&= \sum_{i=1}^{n} \sum_{Q_i^*|P_i} Cotr_{F'/F_{k_1}}(Cotr_{F_{k_i}/F}(\omega)_{Q_i^{'}}(1).f(Q_i^{'}) \quad \text{(by lemma 2.3.8)} \\
&= \sum_{i=1}^{n} \sum_{Q_i^*|P_i} Cotr_{F'/F}(\omega)_{Q_i^{'}}(1).f(Q_i^{'}) \\
&= 0.
\end{aligned}$$

To prove the converse, it is enough to show that the dimension of two spaces are equal.

$$\begin{aligned}
\dim C_\Omega(D,G) &= i(G-D)-i(G) \quad \text{(by lemma 2.3.6)} \\
&= \dim(G-D)-\deg(G-D)+g-1-(\dim G-\deg G+g-1) \\
&= \deg D+\dim(G-D)-\dim G \\
&= N-\dim C_L(D,G)=\dim C_L(D,G)^{\perp}.
\end{aligned}$$

□

After establishing the duality, our next aim is to show that $C_\Omega(D,G)$ can be represented as $C_L(D,H)$ with an appropriate divisor H as it is the case for the dual of a classical geometric Goppa code (Lemma 2.1.3). For this we begin with the following lemma.

Lemma 2.3.10 *Let $P_1, ..., P_n$ be distinct places of $F/\mathbb{F}_q$ as before. Then there exists $z, t \in F$ such that*

$$v_{P_i}(z) = 0,\ z(P_i) = 1 \ and\ v_{P_i}(t) = 1 \ for\ i = 1, ..., n.$$

Proof: We know that there exists $z \in F$ such that $v_{P_i}(z-1) > 0$ for $i = 1, ...n$, by the Weak Approximation Theorem (Theorem 1.1.2). If $v_{P_i}(z) < 0$, then by the Strict Triangle Inequality (Lemma 1.1.5), we would have $v_{P_i}(z-1) = \min\{v_{P_i}(z), v_{P_i}(-1)\} < 0$, which is a contradiction. If $v_{P_i}(z) > 0$ then we would have, again by Strict Triangle Inequality, $v_{P_i}(z-1) = 0$ which is also a contradiction. So we have $v_{P_i}(z) = 0$ for $i = 1, ..., n$. Since $z - 1 \in P_i$ for $i = 1, ..., n$ we have $z(P_i) = 1(P_i) = 1$. Existence of the t with $v_{P_i}(t) = 1$ for $i = 1, ..., n$ is again an immediate result of the Weak Approximation Theorem. □

Lemma 2.3.11 *Let $P_1, ..., P_n$ be rational places of a function field F/K and z and t be elements of F with the properties in previous lemma. Then the differential $\omega = z.dt/t$ satisfies*

$$v_{P_i}(\omega) = -1 \ and\ res_{P_i}(\omega) = 1 \ for\ i = 1, ..., n. \tag{2.19}$$

Proof: Since $v_{P_i}(t) = 1$, t is a P-prime element. Then, we have $res_{P_i}(\omega) = res_{P,t}(z/t)$. So we look at the P-adic expansion of z/t with respect to t. As $v_{P_i}(z) = 0$ this expansion has the form

$$(1 + a_1 t + ...)\frac{1}{t} = (\frac{1}{t} + a_1 + ...) \text{ by Theorem } 1.1.18.$$

So we get $v_{P_i}(\omega) = -1$ and $res_{P_i}(\omega) = 1$ by Theorem 1.1.18. □

Lemma 2.3.12 *Let $z, t \in F$ with the properties in the previous lemmas. Then the Weil differentials $\omega = z/t.dt \in \Omega_F$ and $\omega^{'} = z/t.dt \in \Omega_{F'}$ satisfy*

$$\omega^{'} = Cotr_{F'/F}(\omega).$$

Proof: As $v_{P_i}(t) = 1$, dt is a non-trivial element of both function fields $F/\mathbb{F}_q$ and $F^{'}/\mathbb{F}_{q^\ell}$, by Lemma 1.1.17. Let η and $\eta^{'}$ be the the unique Weil differentials of the rational function fields $\mathbb{F}_q(t)/\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}(t)/\mathbb{F}_{q^\ell}$ with the properties

$$(\eta) = -2P_\infty \quad \text{and} \quad (\eta^{'}) = -2P_\infty^{'}$$
$$\eta_{P_\infty}(t^{-1}) = -1 \quad \text{and} \quad \eta^{'}_{P^{'}_\infty}(t^{-1}) = -1$$

where P_∞ and $P_\infty^{'}$ are the infinite places of the rational function fields $\mathbb{F}_q(t)/\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}(t)/\mathbb{F}_{q^\ell}$, respectively. The existence of these Weil differentials is assured by Lemma 1.1.19.

The function field $\mathbb{F}_{q^\ell}(t)/F_{q^\ell}$ is a constant field extension of $\mathbb{F}_q(t)/\mathbb{F}_q$. So $(\eta^{'}) = (Cotr_{F_{q^\ell}(t))/F_q(t)}(\eta)$ for $\deg P_\infty = 1$, and we have $Cotr_{F_{q^\ell}(t)/F_q(t)}(\eta)_{P_\infty}(t^{-1}) = -1$ by Lemma 2.3.8. This shows that $Contr_{F_{q^\ell}/t)/F_q(t)}(\eta)$ has the same two properties as $\eta^{'}$. As $\eta^{'}$ is the unique Weil differential of $\Omega_{F'}$ satisfying these properties we have

$$\eta^{'} = Cotr_{\mathbb{F}_{q^\ell}(t)/\mathbb{F}_q(t)}(\eta) \tag{2.20}$$

Keeping this fact in mind, we have

$$\begin{aligned}
\omega^{'} = z/t.dt &= z/t.Cotr_{F'/\mathbb{F}_{q^\ell}(t)}(\eta^{'}) && (\text{by} \quad \text{Theorem 2.3.6}) \\
&= z/t.Contr_{F'/\mathbb{F}_{q^\ell}(t)}(Contr_{\mathbb{F}_{q^\ell}(t)/\mathbb{F}_q(t)}(\eta^{'}) && (\text{by} \quad \text{Equation (2.20)}) \\
&= z/t.Cotr_{F'/\mathbb{F}_q(t)}(\eta) && (\text{by} \quad \text{Definition 1.1.11}) \\
&= Cotr_{F'/F}(z/t.Contr_{F/\mathbb{F}_q(t)}(\eta))
\end{aligned}$$

□

The following lemma gives us the existence of a Weil differential which we will need for writing $C_\Omega(D,G)$ as a generalized geometric Goppa code $C_L(D,H)$ for some divisor H.

Lemma 2.3.13 *Let $z, t \in F$ with $v_{P_i}(z) = 1$, $z(P_i) = 1$ and $v_{P_i}(t) = 1$ for $i = 1, ..., n$. Then the Weil differential $\omega = z/t.dt \in \Omega_F$ has the following properties*

$$v_{P_i}(\omega) = -1 \ \textit{and} \ Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1) = 1, \ \textit{for} \quad \textit{all} \quad i = 1, ..., n.$$

Proof: Let $z, t \in F$ with properties as stated. Since $F^{'}/\mathbb{F}_{q^{\ell}}$ is a constant field extension of $F/\mathbb{F}_q$, these elements also satisfy $v_{P_i^{'}}(z) = 0$, $z(P_i^{'}) = 1$ and $v_{P_i^{'}}(t) = 1$ for $i = 1, ..., n$. Since all $P_i^{'}$'s are rational, the Weil differential $\omega^{'} = z/t.dt \in \Omega_{F^{'}}$ satisfies

$$v_{P_i^{'}}(\omega^{'}) = -1 \text{ and } res_{P_i^{'}}(\omega^{'}) = 1.$$

by Lemma 2.3.11 hence,

$$-1 = v_{P_i^{'}}(\omega^{'}) = v_{P_i^{'}}(Cotr_{F^{'}/F}(\omega)) = v_{P_i}(\omega).$$

by Lemma 2.3.12. We also have

$$1 = res_{P_i^{'}}(\omega^{'}) = \omega^{'}_{P_i^{'}}(1) = Cotr_{F^{'}/F}(\omega)_{P_i^{'}}(1) = Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1).$$

These equalities complete the proof. □

After we assure the existence of the Weil differential in Lemma 1.1.19, we can state the following lemma.

Lemma 2.3.14 *Suppose $\omega \in \Omega_F$ is a Weil differential with the properties in previous lemma. Namely,*

$$v_{P_i}(\omega) = -1 \text{ and } Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1) = 1, \text{ for } i = 1, ..., n. \tag{2.21}$$

Then we have

$$C_L(D, G)^{\perp} = C_{\Omega}(D, G) = C_L(D, D - G + (\omega)).$$

Proof: Note that $D = \sum_{i=1}^{n} P_i$ and $v_{P_i}(\omega) = -1$, for all $i = 1, ..., n$. This implies $supp(D - G + (\omega)) \cap SuppD = \emptyset$. Hence the code $C_L(D, D - G + (\omega))$ is well-defined. By Theorem 1.1.6 we know that there exists an isomorphism

$$\begin{aligned} \alpha : L_G(D - G + (\omega)) &\rightarrow \Omega_F(G - D) \\ x &\mapsto x\omega. \end{aligned}$$

So,

$$\begin{aligned}
Cotr_{F_{k_i}/F}(x\omega)_{P_i^*}(1) &= xCotr_{F_{k_i}/F}(\omega)_{P_i^*}(1)\\
&= Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(x)\\
&= x(P_i^*)Cotr_{F_{k_i}/F}(\omega)_{P_i^*}(1)\\
&= x(P_i).
\end{aligned}$$

□

CHAPTER 3

ON THE WEIGHTS OF SOME CYCLIC CODES

In this chapter we exhibit an application of algebraic function fields over finite fields to codes, which is different than the idea in Chapter 2. The method is to relate the weights of codewords to the number of rational places of function fields. Then, using the Hasse-Weil Bound one can write a lower bound on the minimum distance of the codes studied. Our main reference is Schoof's nice paper [5].

Throughout this chapter we will assume the following fact: If $f(x, y) \in \mathbb{F}_q(x, y)$ is an irreducible polynomial, then the number of the $\mathbb{F}_q$-rational points of $f(x, y) = 0$ is the same as the number of degree one (rational) places of the function field $F = \mathbb{F}_q(x, y)$ defined by $f(x, y) = 0$. The reader is referred to Appendix B in [6].

3.1. Subfield Subcodes and Trace Codes

In this short section we introduce two ways of constructing linear codes over $\mathbb{F}_q$ from a given linear code C over $\mathbb{F}_{q^m}$, $m > 1$. Let C be a q^m-ary linear $[n, k, d]$ code and for simplicity let Tr denote the trace map $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : .F_{q^m} \to \mathbb{F}_q$, for.

Definition 3.1.1 Let $C \subset (\mathbb{F}_{q^m})^n$ be a code over $\mathbb{F}_{q^m}$.
(a) $C \mid_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$ is called *the subfield subcode* (*or restriction* of C to $\mathbb{F}_q$).
(b) $Tr(C) = \{Tr(c) \mid c \in C\}$ is called *the trace code* of C

Note that both $C \mid_{\mathbb{F}_q}$ and $Tr(C)$ are q-ary linear codes of length n. An important theorem which relates these codes is due to Delsarte (see Theorem VIII.1.2 in [6]).

Theorem 3.1.1 ***(Delsarte)*** *For any code C over $\mathbb{F}_{q^m}$, we have*

$$(C \mid_{\mathbb{F}_q})^{\perp} = Tr(C^{\perp}).$$

3.2. On the Weights of Binary Hamming and Dual BCH Codes

Let $q = 2^m$, where $m > 1$. Let α be a primitive element, i.e. $< \alpha >= \mathbb{F}_q^*$. Let $f_\alpha(t) \in \mathbb{F}_2[t]$ be the minimal polynomial of α over $\mathbb{F}_2$. We define the binary *Hamming Code* as the cyclic code of length $q-1 = 2^m - 1$, where the generator polynomial is $f_\alpha(t)$, i.e.

$$H_m =< f_\alpha(t) >\subset \mathbb{F}_2[t]/(t^{q-1} - 1).$$

We know that $\dim H_m = q - 1 - m$ since $\deg f_\alpha(t) = m$. Let C be the cyclic code over $\mathbb{F}_q$ of length $q-1$ with the generator polynomial $(t - \alpha) \in \mathbb{F}_q[t]$, i.e.

$$C =< t - \alpha >\subset \mathbb{F}_q[t]/(t^{q-1} - 1).$$

Note that C consists of the polynomials $a(t) = \sum_{i=0}^{q-2} a_i t^i \in \mathbb{F}_q[t]$ which vanish at α. Hence, $C \mid_{\mathbb{F}_2}= H_m$ as the restriction consists exactly of the polynomials with binary coefficients that vanish at α, i.e. they are multiples of $f_\alpha(t)$. Therefore, by Delsarte's theorem, we have

$$H_m^{\perp} = Tr(C^{\perp}).$$

Note that if $a(t) = a_0 + a_1 t + ... + a_{q-2}t^{q-2} \in C$ then by the above discussion we have

$$\begin{aligned} 0 = a(\alpha) &= a_0 + a\alpha + ... + a_{q-2}\alpha^{q-2} \\ &= (a_0, ..., a_{q-2}).(1, \alpha, ..., \alpha^{q-2}), \end{aligned}$$

where . denotes the usual dot product in $\mathbb{F}_q^{q-1}$. Hence $(1, \alpha, ..., \alpha^{q-2}) \in C^{\perp}$. Note that $\dim C^{\perp} = \deg(t-\alpha) = 1$. Hence,$(1, \alpha, ..., \alpha^{q-2})$ is a basis for $C^{\perp}$ and we have

$$\begin{aligned} C^{\perp} &= \{\lambda(1, \alpha, ..., \alpha^{q-2}) \mid \lambda \in \mathbb{F}_q\} \\ &= \{(\lambda x)_{x \in \mathbb{F}_q^*} \mid \ \lambda \in \mathbb{F}_q\}, \end{aligned}$$

where $(\lambda x)_{x \in \mathbb{F}_q^*}$ denotes a vector of length $q-1$ whose coordinates are obtained by evaluating x at the elements of $\mathbb{F}_q^*$. Then, Delsarte's theorem implies that

$$H_m^{\perp} = \{(Tr(\lambda x))_{x \in \mathbb{F}_q^*} \mid \ \lambda \in \mathbb{F}_q\}.$$

At this point, we need to recall a well known fact.

Theorem 3.2.2 ***(Hilbert's Theorem 90)*** *Given $\mathbb{F}_q$ and an extension $\mathbb{F}_{q^s}$, we have*

$$Tr_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\beta) = 0 \Longleftrightarrow thereexists \mu \in \mathbb{F}_{q^s} such that \mu^q - \mu = \beta.$$

Proof: See Theorem 2.5 in [3].□

Lemma 3.2.3 *Let $c_\lambda = (Tr(\lambda x))_{x \in \mathbb{F}_q^*} \in H_m^{\perp}$ be a codeword, where $\lambda \in \mathbb{F}_q^*$. Then the weight of c_λ is*

$$w(c_\lambda) = q - 1 - N/2$$

where N is defined by

$$N = \{(x, y) \in \mathbb{F}_q^2 \mid \ y^2 - y = \lambda x \, and \, x \in \mathbb{F}_q^*\}.$$

Proof: By Hilbert's Theorem 90, for $x \in \mathbb{F}_q^*$, $Tr(\lambda x) = 0$ if and only if there exists $y \in \mathbb{F}_q^*$ such that $y^2 - y = \lambda x$. In this case, note that

$$(y+1)^2 - (y+1) = y^2 + 1 - y - 1 = y^2 - y = \lambda x$$

is also true, i.e. each $x \in \mathbb{F}_q^*$ with $Tr(\lambda x) = 0$ brings two solutions to the equation $y^2 - y = \lambda x$. Hence

$$\begin{aligned} w(Tr(\lambda x)) &= q - 1 - \mid \{x \in \mathbb{F}_q^* \mid \ Tr(\lambda x) = 0\} \mid \\ &= q - 1 - N/2. \end{aligned}$$

□

If $\lambda \neq 0$, then studying $\mathbb{F}_q$-solutions of $y^2 - y = \lambda x$ is the same as studying $\mathbb{F}_q$-rational places of the function field $F = \mathbb{F}_q(x, y)$ defined by $y^2 - y = \lambda x$, by our discussion at the beginning of the chapter. The genus of F is $(2-1)(1-1)/2 = 0$ by Proposition 1.1.3, i.e. F is a rational function field. Hence, it has $q+1$ rational places. Disregarding the unique place at infinity and the two rational places corresponding to $x = 0$, we have $N = q - 2$ in Lemma 3.2.3. Hence, we obtained

Corollary 3.2.4 *The code $H_m^\perp$ has $q-1$ codewords of weight $q/2$.*

Proof: Put $N = q - 2$ in Lemma 3.2.3. This implies that

$$w(c_\lambda) = q - 1 - \frac{q-2}{2} = \frac{q}{2}$$

for any $\lambda \in \mathbb{F}_q^*$. □

Corollary 3.2.4 gives us the weight enumerator of the dual of H_m. Hence, one can find the weight enumerator of H_m via the McWilliams Identity. Namely:

$$W_{H_m}(x) = \frac{1}{q}\big((1+x)^{q-1} + (q-1)(1-x)^{q-2}(1+x)^{\frac{q}{2}-1}\big).$$

The numbers $A_1, ..., A_{q-1}$ can be found by expanding the polynomial above.

The method mentioned above can also be used for other cyclic codes. As an example, we briefly discuss the *double error correcting BCH codes.* Again, $q = 2^m$, with $m > 1$, $\alpha \in \mathbb{F}_q^*$ is a primitive element and $f_\alpha(t), f_{\alpha^3}(t) \in \mathbb{F}_2[t]$ are the minimal polynomials of α and α^3 over $\mathbb{F}_2$, respectively. We define the code B_m as a binary code of length $q - 1 = 2^m - 1$ whose generator polynomial is $f_\alpha(t)f_{\alpha^3}(t)$, i.e.

$$B_m =< f_\alpha(t)f_{\alpha^3}(t) >\subset \mathbb{F}_2[t]/(t^{q-1} - 1).$$

Since $\deg(f_\alpha(t)) = \deg(f_{\alpha^3}(t)) = m$, we have $\dim B_m = q-1-2m$ and $\dim B_m^\perp = 2m$. Arguing as in the case of Hamming code, one can show that

$$B_m^\perp = \{(Tr(\lambda_1 x + \lambda_2 x^3))_{x\in\mathbb{F}_q^*} \mid \lambda_1, \lambda_2 \in \mathbb{F}_q\}.$$

Note that $B_m^\perp$ has $q^2 = 2^{2m}$ codewords, which is consistent with the fact that $\dim B_m = 2m$. If $c_{\lambda_1,\lambda_2} \in B_m^\perp$ such that $\lambda_2 = 0$, then the weight of c_{λ_1,λ_2} is $q/2$, since it is just a codeword associated with the rational field as in H_m. If $\lambda_2 \neq 0$, then the related equation via Hilbert's Theorem 90 is

$$y^2 - y = \lambda_1 x + \lambda_2 x^3. \tag{3.1}$$

If F denotes the function field $F = \mathbb{F}_q(x, y)$ defined by (3.1), then the genus is $g = (2-1)(3-1)/2 = 1$. This time we do not know the exact number of rational places, the Hasse -Weil bound gives us the upper bound of $q + 1 + 2\sqrt{q}$. The weight of c_{λ_1,λ_2} is as before,

$$w(c_{\lambda_1,\lambda_2}) = q - 1 - \frac{N}{2}$$

where N is the number of rational places except the place at infinity and the two places corresponding to $x = 0$. Hence, $N \leq q - 2 + 2\sqrt{q}$. Therefore, we have

$$\begin{aligned} w(c_{\lambda_1,\lambda_2}) &= q - 1 - \frac{N}{2} \\ &\geq q - 1 - \frac{q - 2 + 2\sqrt{q}}{2} \\ &= \frac{2q - 2 - q + 2 - 2\sqrt{q}}{2} = \frac{q - 2\sqrt{q}}{2}. \end{aligned}$$

So, for some of the codes in $B_m^\perp$ (those with $\lambda_2 = 0$) we know that the exact weight is $q/2$. For other codewords ($\lambda_2 \neq 0$), we just know the weight is at least $\frac{q-2\sqrt{q}}{2}$, which is a number less than $q/2$. In this case, what we can conclude is that the minimum distance of $B_m^\perp$ satisfies

$$d(B_m^\perp) \geq \frac{q - 2\sqrt{q}}{2}.$$

Remark 3.2.1 Using properties of genus 1 (elliptic) function fields, Schoof [5] obtains the complete weight enumerator of $B_m^\perp$ (and hence of B_m).

Remark 3.2.2 Using the method described here, Wolfmann [8] gives a lower bound on the minimum distance of a large class of cyclic codes.

Bibliography

[1] Goppa, V. G., *Codes on algebraic curves*, Soviet Mathematics. Doklady, **24**, (1981), 170–172.

[2] Heydtmann, A. E., *Generalized geometric Goppa codes*, Communications in Algebra, **30**, (2002), 2763–2789.

[3] Lidl, R. and Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 2000.

[4] van Lint, J. H., *Introduction to Coding Theory*, Springer-Verlag, 1999.

[5] Schoof, R., *Families of curves and weight distributions of codes*, Bulletin of the American Mathematical Society **32** (1995), 171–183.

[6] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

[7] Tsfasman, M.A.,Vladut, S. G., Zink , T., *Moduler curves, Shimura curves, and Goppa codes better than Varshanov-Gilbert bound*, Mathematische Nachrichten, **109**, (1982), 21–28.

[8] Wolfmann, J., *New bounds on cyclic codes from algebraic curves* , Lecture Notes in Computer Science **388** (1989), 47–62.

[9] Xing, C.,Neiederreiter, H., and Lam, K.Y., *A generalization of Algebraic-Geometry Codes*, IEEE Transactions on Information Theory, **45**, 1999, 2498–2501.

Bibliography

[1] Goppa, V. G., *Codes on algebraic curves*, Soviet Mathematics. Doklady, **24**, (1981), 170–172.

[2] Heydtmann, A. E., *Generalized geometric Goppa codes*, Communications in Algebra, **30**, (2002), 2763–2789.

[3] Lidl, R. and Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 2000.

[4] van Lint, J. H., *Introduction to Coding Theory*, Springer-Verlag, 1999.

[5] Schoof, R., *Families of curves and weight distributions of codes*, Bulletin of the American Mathematical Society **32** (1995), 171–183.

[6] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.

[7] Tsfasman, M.A.,Vladut, S. G., Zink , T., *Moduler curves, Shimura curves, and Goppa codes better than Varshanov-Gilbert bound*, Mathematische Nachrichten, **109**, (1982), 21–28.

[8] Wolfmann, J., *New bounds on cyclic codes from algebraic curves* , Lecture Notes in Computer Science **388** (1989), 47–62.

[9] Xing, C.,Neiederreiter, H., and Lam, K.Y., *A generalization of Algebraic-Geometry Codes*, IEEE Transactions on Information Theory, **45**, 1999, 2498–2501.