SOME EXPLICIT BASES OF RIEMANN-ROCH SPACES FOR ALGEBRAIC GEOMETRY CODES

TAN YEAN NEE

UNIVERSITI SAINS MALAYSIA

2011

SOME EXPLICIT BASES OF RIEMANN-ROCH SPACES FOR ALGEBRAIC GEOMETRY CODES

by

TAN YEAN NEE

Thesis submitted in fulfillment of the requirement for the Degree of Master of Science

August 2011

ACKNOWLEDGEMENT

First and foremost, I would like to acknowledge the advice and guidance from my supervisor, Dr. Ang Miin Huey. Dr. Ang has supported and supervised me continuously throughout my research and thesis with her patience and knowledge. My research skills and writing skills have been polished and improved during this one and half year under her training. I appreciate the time she spent on guiding me.

I would also like to express my sincerest gratitude to my field supervisor, Professor Ti-Chung Lee, for his kindness and willingness to share his rich fund of knowledge in algebraic geometry codes with me. Without his valuable suggestion and guidance in my research, my thesis would not have been completed.

Besides, a great thankful to Professor How Guan Aun as well for helping me to build up the basic knowledge regarding function fields and encouraging me to pursue for higher degree in my study.

I acknowledge the Universiti Sains Malaysia (USM) for their financial support by awarding me with the USM Fellowship. I would also like to thank all staffs at the School of Mathematical Science, USM, for providing me the support and equipment that I need to produce my thesis.

Last but not least, I would like to thank my beloved friends and family members who have gave me a lot of support and encouragement to pursue this degree.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

BEBERAPA ASAS TAK TERSIRAT BAGI RUANG RIEMANN-ROCH UNTUK KOD GEOMETRI ALJABAR

ABSTRAK

Menurut Teorem Pengkodan Saluran yang dikemukakan oleh Shannan, suatu kod sepatutnya mempunyai panjang yang besar supaya apabila kata kod dihantar melalui saluran, kebarangkalian ralat berlaku adalah menghampiri sifar. Maka, suatu kod linear yang baik sepatutnya mempunyai panyang yang besar, dimensi yang besar and jarak minimum yang besar. Masalah utama teori pengkodan adalah untuk mencari kod-kod linear optimum yang mempunyai dimensi terbesar apabila nilai-nilai bagi panjang dan jarak minimum telah diberikan. Masalah ini adalah setara dengan masalah mencari nilai terbesar yang mungkin bagi kadar maklumat apabila nilai suatu jarak minimum relatif telah diberikan. Satu batasan bawah yang bernama batasan Tsfasman-Vladut-Zink bagi kadar maklumat telah ditemui pada tahun 1982 dengan menggunakan jujukan-jujukan kod geometri aljabar (kod AG). Sejak itu, kod AG telah menjadi salah satu keluarga kod linear yang penting.

Untuk membina suatu kod AG, asas bagi ruang Riemann-Roch yang berkaitan perlu ditentukan terlebih dahulu. Dalam tesis ini, dua kaedah dicadangkan untuk mencari asas tak tersirat bagi ruang-ruang Riemann-Roch untuk kod AG yang dibinakan daripada keluarga-keluarga medan fungsi yang tertentu. Dalam kaedah pertama, asas bagi ruang Riemann-Roch dikenalpastikan dengan menggunakan asas-asas integer tempatan bagi tempat-tempat yang tertentu. Dalam pada itu, kaedah kedua adalah diilhamkan oleh Teorem Luang Weierstrass. Dengan menggunakan kedua-dua kaedah yang dicadangkan, satu asas tak tersirat bagi beberapa ruang

Rieman-Roch diperolehi bagi lima medan fungsi yang popular dalam kajian kod AG. Kelima-lima medan fungsi yang popular ini adalah masing-masing medan fungsi eliptik, medan fungsi hipereliptik, medan fungsi kuartik Klein, medan fungsi Hermitian dan medan fungsi Suzuki.

Akhir sekali, kami membina dua kod AG satu-titik, satu daripada medan fungsi hipereliptik dan satu lagi daripada medan fungsi Suzuki, serta satu kod AG dua-titik daripada medan fungsi eliptik. Sekadar yang kami tahu, kod Suzuki satu-titik yang kami bina adalah salah satu kod linear atas F_8 yang mempunyai jarak minimum yang terbesar dengan panjang 64 dan dimensi 27. Selain itu, kod eliptik dua-titik yang kami bina adalah suatu kod MDS (kod terpisahkan jarak terbesar). Pembinaan kod-kod AG tersebut mengesahkan kedua-dua kaedah yang kami cadangkan adalah praktikal.

SOME EXPLICIT BASES OF RIEMANN-ROCH SPACES FOR ALGEBRAIC GEOMETRY CODES

ABSTRACT

According to Shannon's Channel Coding Theorem, a code should have long length so that the probability of errors occurring, during the transmission of codewords through a channel, approaches zero. Hence, a good linear code should have long length, large dimension and large minimum distance. The main problem in coding theory is to find optimal linear codes having the largest value of dimension for a given value of length and minimum distance. This problem is equivalent to the problem of finding the largest possible value of information rate for a given value of relative minimum distance. A lower bound on information rate named Tsfasman-Vladut-Zink bound has been found in year 1982 using sequences of algebraic geometry codes (AG codes). Since then, AG code has become an important family of linear codes.

To construct an AG code, a basis of its relevant Riemann-Roch spaces needs to be determined first. In this thesis, two methods to find explicit bases of the Riemann-Roch spaces for AG codes from certain families of function fields are proposed. In the first method, a basis of a Riemann-Roch space is identified by using the local integral bases of certain places. On the other hand, the second method is inspired by the Weierstrass Gap Theorem. Using the two proposed methods, an explicit basis of some Riemann-Roch space is found for each of the five popular function fields in the study of AG codes, namely, elliptic function fields,

hyperelliptic function fields, function fields of the Klein Quartic, Hermitian function fields and Suzuki function fields.

Lastly, we construct two one-point AG codes, one from a hyperelliptic function field and another from a Suzuki function field, as well as a two-point AG codes from an elliptic function field. To the best of our knowledge, the constructed one-point Suzuki code happens to be one of the knowing linear codes over F_8 having the greatest minimum distance with length 64 and dimension 27. Moreover, our constructed two-point elliptic code is a maximal distance separable (MDS) code. These constructions of AG codes verify the practicality of our two proposed methods.

CHAPTER 1
INTRODUCTION

1.1 Literature Review

In this era of information technology where fully developed, people rely heavily on digital communication systems to transmit messages, such as a casual email to a friend or some confidential information to a government agency. In order to enable the message to be transmitted digitally through the communication system, we must first digitalize the messages into a string of bits. Let F_q be a finite field with q elements. If a message is represented by a string of k digits over F_q, that is, $a_1 a_2 ... a_k$, where $a_i \in F_q$ for every i, then it is called a *message word of length* k *over* F_q.

In reality, all channels used to transmit the digitalized messages are noisy and errors might easily occur during the transmission of these messages. A scratched CD, an old telephone line and unstable radio frequency are some examples of noisy channels. This might lead to an irreversible tragedy if the receiver failed to notice the corrupted messages. Hence, the idea of reducing the number of undetected errors by the receiver has brought up the theory of error correcting and detecting codes.

To protect the messages from errors that occurred during the transmission, each message word of length k is encoded into a string of n digits with $n > k$. Each encoded string of n digits is called a *codeword*. A set of length n codewords over F_q is called a *code of length* n *over* F_q. The extra $n-k$ digits that are added into each codeword are called *check digits.* The function of these check digits is to increase the minimum distance of the code [17]. It is a well-known result that a code

with minimum distance d is able to detect up to $(d-1)$-errors or correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$- errors [17].

Let $F_q^n = \{a_1 ... a_n \mid a_1, ..., a_n \in F_q\}$. Clearly, F_q^n is a vector space over F_q, if we define the addition of any two elements in F_q^n and the scalar multiplication of any element in F_q^n with a scalar in F_q, coordinate-wise [17]. All codes of length n over F_q, which are subspaces of F_q^n, are called *linear codes*. It is clear that if $\mathfrak{U} = \{v_1, v_2, ..., v_k\}$ is a basis of a linear code C over F_q, then, $M = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}$ is a $k \times n$ matrix with rank k, such that $C = \{vM \mid v \in F_q^k\}$. The matrix M is called a *generator matrix of* C. In general, the encoding of linear codes can be done by using any of its generator matrices [17]. In short, a linear code with length n, dimension k (or size q^k) and minimum distance d is denoted by $[n, k, d]$-*linear code*. One advantage of linear code is that it is easier to get its minimum distance. If C is a linear code, then its minimum distance $d(C) = \min\{wt(v) \mid v \in C \setminus \{0\}\}$ where $wt(v)$ is the number of nonzero digits in v.

For an $[n, k, d]$-linear code C over F_q, denote $R(C) = \frac{k}{n}$ as the *information rate* of C and $\delta(C) = \frac{d}{n}$ as the *relative minimum distance* of C. According to the Shannon's Channel Coding Theorem, every communication channel has its channel capacity $\mathfrak{C}$ [3]. For every r less than $\mathfrak{C}$, there exists a sequence of linear codes with information rate approaching r and the probability of error occurred is approaching zero simultaneously [3]. In other words, to find a good code, we need the length of

the code to be large enough. Hence, it is clear that good linear codes are supposed to have long length, large dimension and large minimum distance.

The Singleton Bound states that for any $[n, k, d]$-linear code, its parameters must fulfil the inequality $k + d \le n + 1$ [17]. For this reason, for a fixed value of n (where n can be chosen to be as large as we want), it is impossible for us to construct a linear code having the value of k and d to be as large as possible, simultaneously. *The main coding theory problem* is to determine the largest value $B_q(n,d)$ of k for a given value of n and d such that there exist an $[n, B_q(n,d), d]$ -linear code. The $[n, B_q(n,d), d]$-linear code is called an *optimal code*.

Define $V_q = \{(\delta(C), R(C)) \in \mathbb{R} \times \mathbb{R} \mid 0 \le \delta(C), R(C) \le 1, C \text{ is a code over } F_q\}$ and $U_q \subseteq [0,1] \times [0,1]$ as the set of limit points of V_q . Then, note that $(\delta, R) \in [0,1] \times [0,1]$ is in U_q if and only if there exists a sequence of codes over F_q in which the lengths are arbitrary large such that their relative minimum distance and information rate will then converge to δ and R, respectively. Since n needs to be large enough, the problem of finding $B_q(n,d)$ is the same as the problem of finding the largest possible value of R for a given value of δ such that $(\delta, R) \in U_q$ (as large R indicates large k). Unfortunately, elements in U_q are difficult to be determined.

According to Proposition 8.4.2 of [29], there exist a decreasing continuous function $\alpha_q : [0,1] \to [0,1]$ such that

$$U_q = \{(\delta, R) \mid 0 \le \delta \le 1 \text{ and } 0 \le R \le \alpha_q(\delta)\}.$$

In other words, for a given value of δ , $\alpha_q(\delta)$ is the largest possible value of R such that $(\delta, R) \in U_q$. So far, it is known that $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for all

$1-q^{-1} \le \delta \le 1$ [29]. However, the values of $\alpha_q(\delta)$ remains unknown for $0 < \delta < 1-q^{-1}$. In order to estimate $\alpha_q(\delta)$ for $0 < \delta < 1-q^{-1}$, several bounds for $\alpha_q(\delta)$ have been introduced [29]. For instance, the Plotkin Bound (an upper bound) and the Gilbert Varshamov (GV) Bound (a lower bound) [29]. From 1952 to 1982, the GV Bound was known as the best lower bound for the values of $\alpha_q(\delta)$ [9, 34]. In 1982, Tsfasman, Vladut and Zink came out with a better lower bound for $\alpha_q(\delta)$, known as the TVZ Bound, using sequences of algebraic geometry codes (AG codes) [10, 33]. More precisely, for $q \ge 49$ where q is a perfect square, the TVZ Bound performs better than the GV Bound in estimating the smallest possible value of $\alpha_q(\delta)$ [29]. The following graph illustrates the Plotkin Bound, GV Bound and TVZ Bound for $q = 64$ in the plane R versus δ. The possible values of $\alpha_q(\delta)$ lie in the shaded region of this graph. We can see that the TVZ Bound improves on the GV Bound over a certain interval.

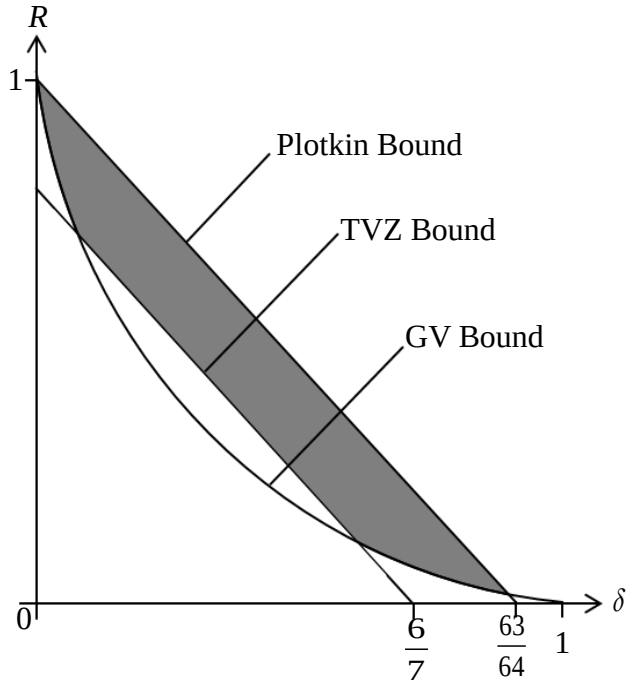

Figure 1.1 Comparison between GV Bound and TVZ Bound for $q = 64$.

This discovery of TVZ Bound had brought the attention of coding theorists to AG codes. In addition to this, the importance of the study of AG codes can also be reflected by the existence of the efficient decoding algorithm for AG codes [29, 14].

There are two approaches we can use to study AG codes. The first approach is to study the AG codes from the viewpoint of algebraic geometry, in which there is a need for a background in geometry, such as the theory of algebraic curves and projective plane [25, 26]. The second approach, in which this thesis is based on, is the study of AG codes by using function fields as the main tool. Hence, a strong background in ring theory and field theory is a necessary.

1.2 Objectives

As AG codes are linear codes, we need to find a basis for the code in order to get its generator matrix. It is known that in order to find a basis of an AG code, we need to find an explicit basis of its relevant Riemann-Roch spaces [29]. Ad-hoc methods have been used to get an explicit basis of Riemann-Roch spaces for AG-codes from Hermitian function fields and elliptic function fields [4, 27, 28]. However, there are still some function fields, in which the bases of their Riemann-Roch spaces are still not found out explicitly. In order to facilitate the construction of AG codes, it is worth the effort for us to find a unifying method or algorithm to get an explicit basis of Riemann-Roch spaces.

In this thesis, our objectives are to

(i) propose two general methods or algorithms to get an explicit basis of the Riemann-Roch spaces;

(ii) find some explicit bases of some Riemann-Roch spaces using the two methods introduced in the first objective;

(iii) construct AG codes from popular function fields in the study of AG codes using the explicit bases of the Riemann-Roch spaces that we have found in the second objective.

1.3 A Brief Outline

The structure of this thesis is as follows:

In Chapter 2, we discuss those theories of function fields that are relevant to our work. The definition and important properties of function fields, valuation rings, places, Riemann-Roch spaces, genus, and the extension of function fields are summarized in this chapter. Also, important results, such as Riemann-Roch Theorem, Fundamental Equality, Hurwitz Genus Formula, Dedekind's Different Theorem, existence of integral bases and Kummer's Theorem are also stated here. Chapter 2 ends with a brief introduction to the AG codes.

In Chapter 3, we focus on five interesting function fields, namely, elliptic function fields, hyperelliptic function fields, function fields of the Klein Quartic, Hermitian function fields and Suzuki function fields, which are popular in study of AG codes. We also summarize some important properties of these function fields that will assist our discussion in Chapters 4 and 5. To make this thesis self-contained, a short proof for some of these results is given.

Chapter 4 discusses our work with respect to our first and second objectives. Firstly, two proposed methods to find an explicit basis of the Riemann-Roch space are presented in the beginning of this chapter. The idea of the first method is based on integral bases and is introduced in algorithm form. On the other hand, the idea of the second method is based on the Weierstrass Gap Theorem and is proved as a proposition. Due to the restriction from the Weierstrass Gap Theorem, the second

method is only applicable on a specific category of Riemann-Roch spaces for one-point AG codes. Secondly, for each of the five interesting function fields introduced in Chapter 3, we work out an explicit basis for a specific Riemann-Roch space for one-point AG codes by using our two proposed methods. Those results regarding elliptic function fields have been published in the proceedings of the 6th IMT-GT Conference on Mathematics, Statistics and Its Applications (ICMSA 2010) [31].

In Chapter 5, with respect to our third objective, we construct two one-point AG codes, one is from hyperelliptic function fields and another is from Suzuki function fields, as well as a two-point AG code from elliptic function fields. To the best of our knowledge, the one-point Suzuki code that we construct happens to be one of the knowing linear code over F_8 having the greatest minimum distance with length 64 and dimension 27 [11]. In addition, the two-point elliptic code that we construct is a maximal distance separable (MDS) code.

Chapter 6 gives a deeper discussion on the results that we have obtained, such as the comparison of our two proposed methods together with their strong points and shortcomings. Besides that, we also discuss about how to extend our proposed methods to two-point AG codes.

Lastly, in the concluding chapter, we give a summary of our results and some future research directions.

CHAPTER 2
PRELIMINARIES

In this chapter, we recall some fundamental definitions and theorems of function fields, AG codes which will be needed in our subsequent discussion. Please take note that if the proof of the theorems in this chapter can be found in our listed references, we omit the proofs. On top of this, we shall refer the reader of this thesis to [5, 15, 16] for any undergraduate algebra stuffs that we used throughout this thesis.

2.1 Function Fields

As we have mentioned in Chapter 1, we use the approach of function fields to construct AG codes in this thesis. Throughout this thesis, we always denote F_q as a finite field with q elements where q is a power of a prime.

2.1.1 Function fields and valuation rings

We start with the definition of function fields.

Definition 2.1.1.1 Let F be an extension field of F_q, we denote F/F_q as a *function field* if there is a transcendental element $x \in F$ over F_q such that F is a finite algebraic extension field of $F_q(x)$.

One of the simplest examples of function fields is $F_q(x)/F_q$, in which x is transcendental over F_q. More precisely, each element in $F_q(x)$ is of the form $\frac{f(x)}{g(x)}$

where $f(x)$ and $g(x)$ are polynomials over F_q with indeterminate x. In function field theory, these $F_q(x)/F_q$ play the role as the 'ground fields' of other function fields. For a function field F/F_q, if we choose $x \in F$ such that x is a separating element for F/F_q (the definition of separation element will be introduced in Section 2.3.4), then $F/F_q(x)$ is a finite separable extension. It follows that F can be represented as a simple algebraic field extension of $F_q(x)$. In other words, x and y will exist in F such that $F = F_q(x, y) = F_q(x)(y)$ where $\phi(y) = 0$ for some irreducible polynomial $\phi(T)$ over $F_q(x)$ with indeterminate T. Owing to its importance, $F_q(x)/F_q$ have been given a special name, as described in the Definition 2.1.1.2.

Definition 2.1.1.2 A function field $F_q(x)/F_q$ where $x \in F$ is transcendental over F_q, is called a *rational function field*.

Definition 2.1.1.3 Let F/F_q be a function field.

(i) A set $\tilde{F}_q$ that consists all algebraic elements of F over F_q is called the *field of constants* of F/F_q.

(ii) F_q is said to be *algebraically closed* in F if $\tilde{F}_q = F_q$. In this case, F_q is called the *full constant field* of F.

We use an algebraic structure, called valuation ring, to study the function field.

Definition 2.1.1.4 A *valuation ring* Λ of a function field F / F_q is a subring of F such that $F_q \subsetneq \Lambda \subsetneq F$ and for every $z \in F$, either $z \in \Lambda$ or $z^{-1} \in \Lambda$.

The following proposition shows some properties of a valuation ring. The proof of this proposition can be found on page 2 of [29].

Proposition 2.1.1.5 Let Λ be a valuation ring of a function field F / F_q. Then Λ has exactly one maximal ideal P. More precisely, $P = \Lambda \setminus \Lambda^*$ where $\Lambda^* := \left\{ a \in \Lambda \mid a^{-1} \in \Lambda \right\}$. In addition, a nonzero element $z \in F$ is in the maximal ideal P if and only if $z^{-1} \notin \Lambda$. Furthermore, we have $\tilde{F}_q \subseteq \Lambda$ and $\tilde{F}_q \cap P = \{0\}$.

For a valuation ring Λ, one can see that for each element $z \in \Lambda$, if $z^{-1} \in \Lambda$, then $z^{-1} \notin P$ where P is the unique maximal ideal of Λ. Conversely, if $z^{-1} \notin \Lambda$, then z must be in $\Lambda \setminus \Lambda^* = P$. Hence, Λ is uniquely determined by its maximal ideal P, namely $\Lambda = \left\{ z \in F \mid z^{-1} \notin P \right\}$. Therefore, we denote a valuation ring Λ as Λ_p, where P is its maximal ideal. We give a name to this P as follows:

Definition 2.1.1.6 A *place* P of the function field F / F_q is the maximal ideal of some valuation ring Λ of F / F_q.

Throughout this thesis, we denote the set consisting of all places of a function field F / F_q as P_F. Please take note that there is a one-to-one correspondence

between the elements in the set consisting of all valuation rings of a function field F / F_q and P_F, given by

$$\Lambda_P \mapsto P .$$

The surjective property of this relation is very clear from the definition of P_F. Suppose that P is a place corresponding to the valuation rings Λ and Λ'. From the previous discussion, we knew that each Λ and Λ' is determined by its maximal ideal P; i.e., $\Lambda = \left\{ z \in F \mid z^{-1} \notin P \right\} = \Lambda'$. Hence, the injective property of this relation is verified too. Therefore, a valuation ring will be considered the same as its corresponding place, throughout our subsequent discussion.

2.1.2 Properties of places

In this section, we further investigate some important properties of places of a function field in order to study the properties of that function field. As a place P of F / F_q is the maximal ideal of Λ_P, we know that $k_P := \Lambda_P / P$ will be a field [5].

Definition 2.1.2.1 For a function field F / F_q, we call the field $k_P = \Lambda_P / P$ as the *residue class field* of *P*, where *P* is a place of F / F_q. In addition, the map $\xi : F \to k_P \cup \{\infty\}$ such that

$$\xi(z) = \begin{cases} z + P & , z \in \Lambda_P \\ \infty & , z \notin \Lambda_P \end{cases}$$

is called the *residue class map* with respect to *P*.

Observe that the residue class map induces a canonical embedding of F_q into k_P. Thus, we can consider F_q as a subfield of k_P.

Definition 2.1.2.2 Let F / F_q be a function field and $P \in P_F$. Then

(i) the *degree* of *P* is defined as $\deg P := \left[k_P : F_q\right]$, where $\left[k_P : F_q\right]$ is the degree of the field extension of k_P over F_q, and

(ii) we call a place *P* a *rational place* of F / F_q if it is of degree one.

As we can see from the next theorem, every place is a principal ideal. The proof of this theorem can be found on page 3 of [29].

Theorem 2.1.2.3 Let Λ_P be a valuation ring of the function field F / F_q and let P be its corresponding place. Then P is a principle ideal, that is $P = t\Lambda_P$ for some $t \in P$. If $P = t\Lambda_P$, then any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \Lambda_P^*$.

The next definition gives a name to generators of a place.

Definition 2.1.2.4 For a place $P \in P_F$ of a function field F / F_q, any element $t \in P$ satisfying $P = t\Lambda_P$ is called a *prime element* for *P*.

From Theorem 2.1.2.3, we observed that if we choose another prime element t' of P such that $P = t\Lambda_P = t'\Lambda_P$, then t can be written as $t = t'v$ for some $v \in \Lambda_P^*$.

For each nonzero element $z \in F$, we can write $z = t^n u = (t'v)^n u = (t')^n w$ for some $u, w \in \Lambda^*$. Hence, regardless of the choice of t and t', the integer n in the representation of $z \in F \setminus \{0\}$ will remain unchanged. By this observation, for a place P in F / F_q, we can define a function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ as in the following definition.

Definition 2.1.2.5 For a place $P \in P_F$ of a function field F / F_q with its corresponding valuation ring Λ_P, choose a prime element t for P; that is, $P = t\Lambda_P$. The function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ is defined by

$$v_P(z) = \begin{cases} n, & z = t^n u, n \in \mathbb{Z}, u \in \Lambda_P^* \\ \infty, & z = 0. \end{cases}$$

Note that for a place $P \in P_F$, any element $z \in F$ with $v_P(z) = 1$ is a prime element of P. This function v_p is an example of discrete valuation, where the definition of discrete valuation is given in the following.

Definition 2.1.2.6 A *discrete valuation* of F / F_q is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following conditions:

(i) $v(z) = \infty$ if and only if $z = 0$.

(ii) $v(zy) = v(z) + v(y)$, for every $z, y \in F$.

(iii) $v(z + y) \geq \min\{v(z), v(y)\}$, for every $z, y \in F$.

(iv) there exists $t \in F$ such that $v(t) = 1$.

(v) $v(a) = 0$, for every $0 \neq a \in F_q$.

Condition (iii) in Definition 2.1.2.6 is called the *Triangle Inequality*. A stronger version, which is the *Strict Triangle Inequality*, can be derived easily from the five conditions of the discrete valuation (page 5 of [29]).

Proposition 2.1.2.7 (Strict Triangle Inequality)

Let F / F_q be a function field and v be a discrete valuation of F / F_q. For any element $z, y \in F$, if $v(z) \neq v(y)$, then $v(z+y) = \min\{v(z), v(y)\}$.

2.1.3 Zeros and poles

By using the discrete valuation v_p of a place P, we can partition a function field F / F_q into three mutually disjoint sets $F \setminus \Lambda_P$, Λ^*_P and P, as shown in the next theorem.

Theorem 2.1.3.1 Let F / F_q be a function field. For a place $P \in P_F$, we have

$$\begin{aligned} F \setminus \Lambda_P &= \{ z \in F \mid v_P(z) < 0 \}; \\ \Lambda_P &= \{ z \in F \mid v_P(z) \geq 0 \}; \\ \Lambda_P^* &= \{ z \in F \mid v_P(z) = 0 \}; \\ P &= \{ z \in F \mid v_P(z) > 0 \}. \end{aligned}$$

The proof of Theorem 2.1.3.1 is given on page 6 of [29]. Note that each different place gives a different discrete valuation. In order to investigate a function field, we further investigate the relation between the places and the elements of the function field.

Definition 2.1.3.2 Consider a function field F / F_q, let $z \in F$ and $P \in P_F$. We say that P is a *zero* of z *of order* m if $v_P(z) = m > 0$, that is $z \in P$, whereas P is called a *pole* of z *of order* m if $v_P(z) = -m < 0$, that is $z \notin \Lambda_P$.

The next theorem gives us the information about the number of zeros and poles of the elements in a function field. As a result of this theorem, the existence of places of a function field is guaranteed.

Theorem 2.1.3.3 In a function field F / F_q, every algebraic element has neither zero nor pole, whereas any element which is transcendental over F_q has at least one but finitely many zeros and at least one but finitely many poles. In particular, $P_F \neq \phi$. Moreover, there are infinitely many places of a function field.

2.1.4 Rational function fields

Recall from Definition 2.1.1.2 that F / F_q is a rational function field if $F = F_q(x)$ for some transcendental elements $x \in F$ over F_q. On the other hand, we denote $F_q[x]$ as the polynomial ring over F_q with indeterminate x. Note that each element $z \in F_q(x)$ has a unique representation of the form

$$z = a \prod p_i(x)^{n_i}$$

where $0 \neq a \in F_q$, $n_i \in \mathbb{Z}$ and each $p_i(x) \in F_q[x]$ is monic, pairwise distinct and irreducible over F_q [16]. With this observation, we have the following definition.

Definition 2.1.4.1 Consider a rational function field $F_q(x)/F_q$. For each monic irreducible polynomial $p(x) \in F_q[x]$, we define the sets $\Lambda_{p(x)}$ and $P_{p(x)}$ as follows:

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

One can easily verify that $\Lambda_{p(x)}$ is a valuation ring of the rational function field $F_q(x)/F_q$ and $P_{p(x)}$ is the corresponding place of $\Lambda_{p(x)}$. For convenience, if $p(x) = x - \alpha$ with $\alpha \in F_q$, we denote the place $P_{x-\alpha}$ as P_α. Other than $\Lambda_{p(x)}$, the set Λ_∞ defined in the next definition is also a valuation ring of $F_q(x)/F_q$. The corresponding place of Λ_∞ is given in the following definition and is denoted by P_∞.

Definition 2.1.4.2 Let $F_q(x)/F_q$ be a rational function field. The sets Λ_∞ and P_∞ are defined as

$$\Lambda_\infty := \left\{ \frac{f(x)}{g(x)} \in F_q(x) \,\middle|\, f(x), g(x) \in F_q[x], \deg f(x) \le \deg g(x) \right\}$$
$$P_\infty := \left\{ \frac{f(x)}{g(x)} \in F_q(x) \,\middle|\, f(x), g(x) \in F_q[x], \deg f(x) < \deg g(x) \right\}.$$

The place P_∞ is called the *infinite place* of $F_q(x)$.

As $F_q(x)/F_q$ plays the role as the 'ground field' of other function fields F/F_q, it is very important for us to look further into the important properties of $\Lambda_{p(x)}$ and Λ_∞. One may refer to pages 10 and 11 of [29] for the complete proof of the following propositions.

Proposition 2.1.4.3 Let $F_q(x)/F_q$ be a rational function field and $p(x) \in F_q[x]$ is a monic irreducible polynomial over F_q. Consider the valuation ring $\Lambda_{p(x)}$ and its corresponding place $P_{p(x)} \in P_{F_q(x)}$. Then we have the following.

(i) $p(x)$ is a prime element of $P_{p(x)}$ whereas $P_{p(x)}$ is the unique zero of $p(x)$.

(ii) $\deg P_{p(x)} = \deg p(x)$.

(iii) If $0 \neq z \in F_q(x)$ is written in the form of $z = p(x)^n \frac{f(x)}{g(x)}$ with $n \in \mathbb{Z}$, $f(x), g(x) \in F_q[x]$, $p(x) \nmid f(x)$ and $p(x) \nmid g(x)$, then the corresponding discrete valuation is defined as $v_{P_{p(x)}} : F_q(x) \to \mathbb{Z} \cup \{\infty\}$ where

$$v_{P_{p(x)}}(z) = \begin{cases} n, & z = p(x)^n \frac{f(x)}{g(x)}; \\ \infty, & z = 0. \end{cases}$$

(iv) If $p(x) = x - \alpha$ with $\alpha \in F_q$, that is $\deg P_\alpha = 1$, then the residue class map is defined by $\xi : F_q(x) \to F_q \cup \{\infty\}$ with

$$\xi(z) = z + P_\alpha = z(\alpha) = \begin{cases} \frac{f(\alpha)}{g(\alpha)} & \text{if } z = \frac{f(x)}{g(x)}, g(\alpha) \neq 0; \\ \infty & \text{if } z = \frac{f(x)}{g(x)}, g(\alpha) = 0. \end{cases}$$

Proposition 2.1.4.4 Let $F_q(x)/F_q$ be a rational function field and $P_\infty \in F_q(x)$ be the infinite place. Then we have $\deg P_\infty = 1$. A prime element of P_∞ can be given by $\frac{1}{x}$ and thus P_∞ is a pole of *x*. More precisely, P_∞ is the unique pole of *x*. Moreover, the corresponding discrete valuation v_{P_∞} is given by $v_{P_\infty} : F_q(x) \to \mathbb{Z} \cup \{\infty\}$ where

$$v_{P_\infty}(z) = \begin{cases} \deg g(x) - \deg f(x) & \text{if } z = \dfrac{f}{g}; \\ \infty & \text{if } z = 0. \end{cases}$$

The following theorem indicates that P_∞ and P_α with $\alpha \in F_q$ are all the rational places of a rational function field.

Theorem 2.1.4.5 There are no other places of the rational function field $F_q(x)/F_q$ besides $P_{p(x)}$ and P_∞.

2.2 Riemann-Roch Theorem

From now on, we shall refer to F/F_q as a function field with full constant field F_q unless specifically stated otherwise.

2.2.1 Divisors

Definition 2.2.1.1 Consider a function field F/F_q.

(i) A *divisor* $\sum_{P \in P_F} a_P P$ of F/F_q is a formal sum of places of F/F_q with $a_P \in \mathbb{Z}$ in which finitely many a_P are nonzeros.

(ii) The *support* of a divisor $A = \sum_{P \in P_F} a_P P$ is defined to be the set $\operatorname{supp} A := \{P \in P_F \mid a_P \neq 0\}$.

Let's denote the coefficient of a place P in a divisor A by $v_P(A)$, so that A can be written as $\sum_{P\in P_F} v_P(A)P$. Then if we have two divisors $A=\sum_{P\in P_F} v_P(A)P$ and $A'=\sum_{P\in P_F} v_P(A')P$, the summation and subtraction of these divisors are defined by $A\pm A'=\sum_{P\in P_F}(v_P(A)\pm v_P(A')P$. It can be proven easily that all divisors of F/F_q will form an abelian group.

Definition 2.2.1.2 For a function field F/F_q,

(i) the group consisting of all divisors of F/F_q is called the *divisor group* of F/F_q and is denoted by D_F;

(ii) the divisor $0:=\sum_{P\in P_F}(0)P$ is called the *zero divisor*;

(iii) the *degree* of a divisor A is defined by $\deg A:=\sum_{P\in P_F} v_P(A)\deg P$;

(iv) a partial ordering on D_F is defined by

$A_1\le A_2$ if and only if $v_P(A_1)\le v_P(A_2)$ for all $P\in P_F$.

In particular, $A\ge 0$ if and only if $v_P(A)\ge 0$ for all $P\in P_F$.

According to Theorem 2.1.3.3, any element z of F/F_q has only finitely many zeros and poles. It other words, there are only finitely many places $P\in P_F$ such that $v_P(z)\neq 0$. Hence, the formal sum $\sum_{P\in P_F} v_P(z)P$ is a divisor of F/F_q. Next, for any element $z\in F$, we define an important divisor that has direct link with it using its discrete valuation $v_P(z)$.

Definition 2.2.1.3 For a nonzero element z of a function field F/F_q, the divisor $(z) = \sum_{P \in P_F} v_P(z)P$ is called the *principal divisor* of z.

Note that if $z \in F_q$, then $v_P(z) = 0$ for all $P \in P_F$ and thus $(z) = 0$.

2.2.2 Riemann-Roch spaces and genus

In this section, we introduce the Riemann-Roch spaces. In Chapter 4, we shall propose two methods to find an explicit basis of some Riemann-Roch spaces of elliptic function fields, hyperelliptic function fields, function fields of the Klein Quartic, Hermitian function fields and Suzuki function fields.

Definition 2.2.2.1 For a divisor $A \in D_F$ of the function field F/F_q, the *Riemann-Roch space associated to* A is $L(A) := \{z \in F \mid (z) \geq -A\} \cup \{0\}$.

One can easily prove that $L(A)$ is a vector space over F_q [29]. We denote the dimension of $L(A)$ over F_q by $l(A)$. Since the Riemann-Roch spaces play a very important role in our thesis, we give some of their properties which will be used frequently in our subsequent discussion here. The proof of Proposition 2.2.2.2 is given on page 18 of [29].

Proposition 2.2.2.2 Let F/F_q be a function field and let $A, B \in D_F$.

(i) $L(0) = F_q$.

(ii) If $A < 0$, then $L(A) = \{0\}$.