GLOBAL FUNCTION FIELDS WITH MANY RATIONAL PLACES

YEO SZE LING

(M. Sc., NUS)

A THESIS SUBMITTED FOR THE DEGREE

OF DOCTOR OF PHILOSOPHY IN MATHEMATICS

DEPARTMENT OF MATHEMATICS

NATIONAL UNIVERSITY OF SINGAPORE

2005

Acknowledgements

It is difficult to put across in a few words my heartfelt gratitude to a great number of people who had, directly or indirectly, assisted and walked me through the challenging and enriching journey in completing this thesis. Though I may not mention everyone here, my appreciation to each of you is well-assured.

First and foremost, I wish to thank my supervisor, Prof. Xing Chaoping for the illuminating discussions (from which I benefited immensely), his invaluable guidance, and most important of all, his unflinching confidence in my ability. I am grateful to Prof. Niederreiter and Prof. Ling San for their constructive opinions and advice on various occasions as well.

To Siman, I like to thank him for the enjoyable and active exchange of ideas.

Indeed, carrying out my research will have been almost impossible without the kind assistance of many of my readers/helpers who readily read to me all the necessary references/books. My most sincere thanks to all of them including Pee Choon, Say Teong, Haomiao, Huixian, Eric, Dini, Wan Ting, Dihua, Mui Kiang, Meng Meng, Jiayi, Peipei and many others. I like to take this opportunity to express my earnest gratitude to Prof Tan Eng Chye, Prof Helmer and Prof Yang Yue for helping me arrange for readers. It has been most helpful.

Further, my appreciation certainly extends to my room mate, Wan Mei, for readily availing herself whenever I require a helping hand. Special thanks to Chong Hui too for his valuable assistance towards the final stages, especially in proof-reading my thesis.

In addition, I am greatly appreciative to the Agency for Science, Technology and Research (A*STAR) for the research scholarship to continue with my Ph.D and the much cherished opportunity to carry on with research.

Finally, I am truly thankful to my family and close friends, particularly my little sister and mum, for their wonderful and unwavering support all these years.

Contents

Summary

In the 1980's, significant and remarkable breakthroughs were achieved in the areas of error-correcting codes and Cryptography with the introduction of Goppa codes and Elliptic Curve Cryptosystems respectively [19, 20, 21, 5]. These two constructions, though specific to two distinct applications of Mathematics, employ a similar Mathematical object, namely algebraic curves over finite fields with sufficient number of rational points, or equivalently in the language of algebraic function fields, global function fields with a large number of rational places relative to their genera. Indeed, the theory of algebraic curves over finite fields and their associated function fields has attracted much devoted research by renown geometers and number theorists alike since the middle of the 20th century. Their research concentrated primarily on abstract and theoretical results, thereby giving rise to numerous advanced ideas in Mathematics. For instance, in 1948, Weil proved the analogue of the famous Riemann hypothesis for function fields and consequently showed that for a given prime power q and positive integer $g > 0$, the number of rational points on an algebraic curve over the field $\mathbf{F}_q$ of genus g cannot exceed $q + 1 + 2gq^{1/2}$. However, proofs of this bound, more commonly known as the Hasse-Weil bound, and other results on algebraic function fields tend to be non-constructive, and it remains to be proven if algebraic curves with large numbers of rational points do exist.

With an increasing number of direct applications for algebraic curves with many rational points as compared to their genera, the search for such curves becomes an important and worthwhile challenge for researchers. The celebrated number theorist, J. P. Serre initiated the work in the 1980's [66, 67], and thereafter, many other mathematicians took up the challenge as well. In particular, using machinery from diverse areas including Kummer and Artin-Schreier theory, elliptic modular curve theory, class field theory and

Drinfeld modules of rank 1, various mathematicians seek to construct algebraic curves containing as many rational points as close to the Hasse-Weil bound as possible, and in a few cases, to give explicit equations of such curves. A comprehensive account of these approaches and research results in these aspects which include applications of algebraic curves with many rational points is well covered by the book of Niederreiter and Xing [55].

This thesis essentially extends the work by Niederreiter and Xing in a series of papers in the late 1990's [41, 42, 43, 44, 46, 48], to continue the search for such curves. More specifically, we will employ results from class field theory together with the theory of Drinfeld modules of rank 1 to construct global function fields with many rational places. In fact, by introducing a new construction of linear codes over finite fields based on global function fields, the genera and splitting behaviour of rational places in subfields of certain classes of cyclotomic function fields can be explicitly expressed. With the aid of some mathematical software packages, these results will help us construct numerous curves having more rational points than the currently-known curves for certain values of q and g.

Further, this thesis delves into a slightly different but related topic, namely, we will explore the lower bounds of $A(q)$ which is the asymptotic bound of the ratio $N_q(g)/g$ as g tends to infinity. Here, $N_q(g)$ denotes the maximum number of rational points that an algebraic curve over $\mathbf{F}_q$ of genus g can have. Some improvements of $A(q)$ for prime values of q including $q = 2, 5, 7, 11$ are established. Such asymptotic bounds are significant since they have a direct impact on coding theory, leading to sequences of codes with increasing lengths exceeding the asymptotic Gilbert-Varshamov bound, the classical benchmark for good families of linear codes. The result of $A(2) \geq 0.257979$ which improves the previously

established bound of $A(2) \geq 0.2555...$ is of particular interest as codes over the binary alphabet have the most practical use.

The first three chapters of this thesis aim to provide an overview of the background materials that are crucial to introduce the main results. More precisely, we will begin with a survey of the theory of algebraic function fields which serve as a starting point of our research. In Chapter 2, we will discuss some well-known examples of algebraic function fields. Using results from general class field theory, we will classify the finite abelian extensions of algebraic function fields in Chapter 3 and describe some of their fundamental properties. In Section 3.5, the general construction of global function fields as subfields of narrow ray class fields that possibly contain many rational points will be presented.

Next, we establish a connection between error-correcting codes and global function fields with many rational places in Chapter 4, which in turn leads to some new function fields. Equipped with all these results, we will then examine the genera and splitting behaviour of places in subfields of cyclotomic function fields, thereby obtaining several more function fields with many rational places. Finally, Chapter 6 will be devoted to the investigation of the asymptotic bounds of $A(q)$ and a couple of new bounds will be given.

Many of the notations used throughout this thesis resemble closely those introduced in [55].

Chapter 1

Algebraic Function Fields

Following the approach pursued in most of the existing literature on algebraic curves and their corresponding number of rational points, this current research will treat this subject via the equivalent language of function field theory. This is possible due to inherent 1-1 correspondence between algebraic function fields and smooth, absolutely irreducible projective curves over finite fields. As such, this first chapter attempts to present a concise summary of the theory of algebraic function fields, the primary Mathematical objects of this thesis.

As the theory of algebraic function fields is rich in its own right, we shall concentrate on results that are applicable to this thesis. Most assertions will be merely stated without proofs. A detailed analysis of the theory of algebraic function fields is covered by books such as those of Stichtenoth [72], and Michael Rosen [61]. Many of the developments in algebraic function fields have their analogs in algebraic number fields. Readers may therefore refer to books on algebraic number theory including Cassels and Fröhlich [8], Koch [31], Neukirch [40] and Weiss [87] for useful background as well.

Throughout this thesis, p will always denote a prime number while $q = p^r$ will refer to an integral power of p.

1.1 Basic definitions

Let K be an arbitrary field. An **algebraic function field** of one variable over K is a finitely generated field extension of K of transcendence degree 1, i.e. there exists an element $x \in F$ such that the degree $[F : K(x)]$ is finite but F is transcendental over K. K is often called the field of constants of the function field and the function field will be simply denoted by F/K. If the algebraic closure of K in F is K itself, we call K the **full constant field** of F/K. Further, if K is the finite field $\mathbf{F}_q$, which will be the case henceforth, F/K is known as a global function field. In other words, we will always assume that K is finite and is the full constant field of the function field F/K. [1]

For a global function field $F/\mathbf{F}_q$, a **valuation ring** O is a proper subring of F containing $\mathbf{F}_q$ with field of fractions F. It is a principal ideal domain with a unique maximal ideal. This unique maximal ideal $P = O - O^*$ is known as a **place** of F, where O^* is the group of units of O.

A **normalized discrete valuation** of an algebraic function field F over $\mathbf{F}_q$ is a surjective map $\nu : F \longrightarrow \mathbf{Z} \cup \{\infty\}$ which satisfies:

(i) $\nu(x) = \infty$ if and only if $x = 0$;

(ii) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F$;

(iii) [Triangle inequality] $\nu(x+y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in F$. Equality holds if

[1] Most of the results in this chapter apply to any arbitrary field K but for practical purposes, concentrating on a finite full field of constants suffices.

$\nu(x) \neq \nu(y)$.

(iv) $\nu(a) = 0$ for any $a \in \mathbf{F}_q^*$.

For a normalized discrete valuation ν of $F/\mathbf{F}_q$, it can be directly checked that $O = \{x \in F : \nu(x) \geq 0\}$ is a discrete valuation ring with the place $P = \{x \in F : \nu(x) > 0\}$. In fact, there is a bijective correspondence between all the places and the normalized discrete valuations of $F/\mathbf{F}_q$.We will denote by ν_P and O_P the normalized discrete valuation and discrete valuation ring, respectively that correspond to a place P. Further, the element $\pi \in P$ for which $\nu_P(\pi) = 1$ is called the **local parameter** or the **uniformizer** at P. Hence, $P = O\pi$.

Given any place P of F, the field $\tilde{F}_p = O_P/P$ is called a **residue class field** of F at P and it can be identified with a finite extension of $\mathbf{F}_q$. The degree of the field extension $[\tilde{F}_P : \mathbf{F}_q]$ is known as the **degree** of P and is denoted by $\deg P$. If $\deg P = 1$, i.e. $\tilde{F}_P = \mathbf{F}_q$, P is said to be $\mathbf{F}_q$**-rational** or simply **rational**.

Similarly, given any place P of a global function field $F/\mathbf{F}_q$, the completion of F at P, commonly known as the P-adic completion of F, will be denoted by F_P. We will again denote the unique extension of ν_P to F_P by ν_P with corresponding discrete valuation ring O_P and place P. It can be verified that the residue class field of F_P at P is isomorphic to $\tilde{F}_P$.

The set of all places of F is denoted by $\mathbf{P}_F$. Given any positive integer $d > 0$, we will use the notation $\mathbf{P}_F^d$ for the set of all places in $\mathbf{P}_F$ of degree d. We have the following lemma.

Lemma 1.1.1 *For a global function field $F/\mathbf{F}_q, \mathbf{P}_F$ is an infinite set but $\mathbf{P}_F^d$ is finite for*

any $d > 0$.

For a place $P \in \mathbf{P}_F$, let π be a local parameter at P. Then, for any nonzero $f \in F_P$ with $\nu_P(f) = v$, there is an infinite sequence $\{a_r\}_{r=v}^{\infty}$ of elements of $\tilde{F}_P$ with $a_v \neq 0$ and

$$f = \sum_{r=v}^{\infty} a_r \pi^r.$$

Such an expansion is called the **local expansion** of f at P. Conversely, every such series converges to an element of F_P. Consequently, $F_P = \tilde{F}_P[[\pi]]$. In particular, the elements of the valuation ring in F_P can be represented as

$$O_P = \{a_0 + a_1\pi + a_2\pi^2 + \cdots : a_i \in \tilde{F}_P \text{ for all } i \geq 0\}.$$

More generally, for any positive integer $n \geq 1$, the ring

$$O_P/P^n = \{a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \bmod P^n : a_0, a_1, \ldots, a_{n-1} \in \tilde{F}_P\}. \tag{1.1}$$

The next theorem, the proof of which is contained in [72], shows that we may approximate an element at several places of F.

Theorem 1.1.2 (i) *[Weak Approximation Theorem:] Let $\mathcal{S} \subseteq \mathbf{P}_F$ be finite. For each $P \in \mathcal{S}$, let $x_P \in F$ and $n_P \in \mathbf{Z}$ be given. Then there exists an element $x \in F$ such that*

$$\nu_P(x - x_P) = n_P$$

for every $P \in \mathcal{S}$. In particular, there exists $x \in F$ with $\nu_P(x) \geq 0$ for all $P \in \mathcal{S}$.

(ii) *[Strong Approximation Theorem:] Let $\mathcal{S}$ be a proper nonempty subset of $\mathbf{P}_F$ and $P_1, \ldots, P_s$ be s distinct places in $\mathcal{S}$. Then for any $x_1, \ldots, x_s \in F$ and integers $n_1, \ldots, n_s$, there exists an element $x \in F$ such that $\nu_{P_i}(x - x_i) = n_i$ for all $i = 1, \ldots, s$ and $\nu_P(x) \geq 0$ for all $P \in \mathcal{S} - \{P_1, \ldots, P_s\}$.*

Let $\mathcal{S}$ be a finite subset of $\mathbf{P}_F$. Then, the formal sum

$$D = \sum_{P \in \mathcal{S}} \nu_P(D) P,$$

where $\nu_P(D)$'s are nonzero integers, is called a **divisor** of F. $\mathcal{S}$ is known as the **support** of D, usually written as $\mathrm{supp}(D)$. If $\mathcal{S} = \emptyset$, then $D = 0$ is the **zero divisor** of F. We will occasionally write D in the form

$$D = \sum_{P \in \mathbf{P}_F} m_P P,$$

where m_P's are integers and $m_P \neq 0$ for finitely many places P. In this case, $\mathcal{S} = \mathrm{supp}(D) = \{P \in \mathbf{P}_F : m_P \neq 0\}$. The set of all divisors of F will be denoted by D_F.

The degree map on $\mathbf{P}_F$ is extended by linearity to D_F, namely, we have

$$\deg\Big(\sum_{P \in \mathrm{supp}(D)} \nu_P(D) P\Big) = \sum_{P \in \mathrm{supp}(D)} \nu_P(D) \deg P.$$

Clearly, $\deg : \mathsf{D}_F \to \mathbf{Z}$ is a surjective homomorphism. We define a partial ordering on D_F as follows: For two divisors D_1 and $D_2 \in \mathsf{D}_F$, $D_1 \leq$ (respectively $\geq$) D_2 if $\nu_P(D_1) \leq$ (respectively $\geq$) $\nu_P(D_2)$ for all $P \in \mathrm{supp}(D_1) \cup \mathrm{supp}(D_2)$. A divisor is called **positive** or **effective** if $D \geq 0$.

Given a place P of F and a nonzero element x of F, the place P is called a **zero** (respectively **pole**) of x if $\nu_P(x) > 0$ (respectively < 0). It is clear that a constant element in $\mathbf{F}_q$ has neither poles nor zeros. However, for $x \in F - \mathbf{F}_q$, x has at least one but finitely many zero places. Since a zero place of x is a pole place of x^{-1}, every $x \in F - \mathbf{F}_q$ has at least one but finitely many pole places as well. Thus, the following is well-defined.

Let $x \in F^*$. The **principal divisor** of x is given by

$$\mathrm{div}(x) = \sum_{P \in \mathbf{P}_F} \nu_P(x) P.$$

For $x \in F - \mathbf{F}_q$, $\mathrm{div}(x)$ can be written as the difference of two positive divisors, i.e.

$$\mathrm{div}(x) = (x)_0 - (x)_\infty,$$

where $\mathrm{supp}((x)_0)$ (respectively $\mathrm{supp}((x)_\infty)$) is the set of all zero (respectively pole) places of x. We have the following proposition.

Proposition 1.1.3 *For any $x \in F - \mathbf{F}_q$,*

$$\deg(x)_0 = \deg(x)_\infty = [F : \mathbf{F}_q(x)].$$

In particular, $\deg \mathrm{div}(x) = 0$.

For a divisor D of F, we form the **Riemann-Roch space** to be the vector space

$$\mathcal{L}(D) = \{x \in F^* : \mathrm{div}(x) + D \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(D)$ can be shown to be finite-dimensional over $\mathbf{F}_q$, and we denote its dimension by $l(D)$. The next result presents the relationship between $\deg D$ and $l(D)$.

Lemma 1.1.4 *For a global function field $F/\mathbf{F}_q$, there exists a constant integer c such that for all divisors $D \in \mathsf{D}_F$,*

$$\deg D - l(D) \leq c.$$

Lemma 1.1.4 allows us to define the genus of F which can be considered as the most important invariant of a function field. More specifically,

Definition 1.1.5 The **genus** of a function field $F/\mathbf{F}_q$ is the integer

$$g = g(F) = \max_D (\deg D - l(D) + 1),$$

where the maximum is extended over all divisors D of F. By putting $D = 0$ in this definition, we see that the genus of F is nonnegative.

As such, for any divisor D of F,

$$l(D) \geq \deg D + 1 - g.$$

In fact, the well-known Riemann-Roch theorem states that equality holds when $\deg D \geq 2g - 1$.

Next, let $K' \supseteq K = \mathbf{F}_q$ and let F'/K' and $F/\mathbf{F}_q$ be two global function fields with F' being an algebraic field extension of F. We say that F'/K' is an **algebraic extension** of $F/\mathbf{F}_q$ and simply write it as F'/F. For a place $P' \in \mathbf{P}_{F'}$, the restriction $P = P' \cap F \subseteq P'$ is a place of F. We describe this instance by saying that P' **lies over** P or P **lies under** P' and we will denote it by $P'|P$. Furthermore, the restriction of $\nu_{P'}$ to F produces a positive integer $e(P'|P)$ such that

$$\nu_{P'}(x) = e(P'|P)\nu_P(x)$$

for every $x \in F$. In particular, $e(P'|P) = \nu_{P'}(\pi)$, where π is the local parameter of F at P. $e(P'|P)$ is called the **ramification index** of P' over P. Further, the residue class field $\tilde{F}_{P'}$ of P' is a finite field extension of $\tilde{F}_P$ and the degree of this extension $f(P'|P)$ is called the **relative degree** of P' over P. From the definition of the degree of places, we obtain

$$\deg P'[K' : \mathbf{F}_q] = \deg P f(P'|P). \tag{1.2}$$

The following proposition is an important equation involving the ramification index and the relative degree of places.

Proposition 1.1.6 *Let F'/K' and $F/\mathbf{F}_q$ be as above and let $P \in F$. Then,*

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

Proposition 1.1.6 shows, in particular, that for every place P of F, there is at least one but at most $[F' : F]$ (and hence finitely many) places of F' lying over it.

Let $\mathcal{S}$ be a nonempty proper subset of $\mathbf{P}_F$ and $\mathcal{T}$ the subset of $\mathbf{P}_{F'}$ that consists of all places of F' lying over places in $\mathcal{S}$. Then $\mathcal{T}$ is called the **over-set** of $\mathcal{S}$ with respect to the extension F'/F. Refer to Section 1.4 for the definition of $O_{\mathcal{S}}$. The integral closure of $O_{\mathcal{S}}$ in F' is given by

$$O_{\mathcal{T}} = \{z \in F' : \nu_{P'}(z) \geq 0 \text{ for all } P' \in \mathcal{T}\}.$$

We now introduce the complementary set of $O_{\mathcal{T}}$ and its properties. We refer the reader to [55, 72] for details and the definition of a $\mathcal{T}$-ideal.

Lemma 1.1.7 *Suppose that $\mathcal{S}$ is a nonempty proper subset of $\mathbf{P}_F$ and $\mathcal{T}$ the over-set of $\mathcal{S}$ with respect to F'/F. Define the complementary set of $O_{\mathcal{T}}$ by*

$$\mathrm{co}(O_{\mathcal{T}}) = \{z \in F' : \mathrm{Tr}_{F'/F}(zO_{\mathcal{T}}) \subseteq O_{\mathcal{S}}\},$$

where $\mathrm{Tr}_{F'/F}$ is the trace function from F' to F. Then:

(i) $\mathrm{co}(O_{\mathcal{T}})$ *is a $\mathcal{T}$-ideal of F' containing $O_{\mathcal{T}}$;*

(ii) $(\mathrm{co}(O_{\mathcal{T}}))^{-1}$ *is an integral ideal of $O_{\mathcal{T}}$.*

(iii) *If $\mathcal{S}$ consists of a single place $P \in \mathbf{P}_F$, then $\mathrm{co}(O_{\mathcal{T}}) = tO_{\mathcal{T}}$ for some $t \in F'$ with $\nu_{P'}(t) \leq 0$ for every $P' \in \mathcal{T}$.*

Definition 1.1.8 The **different** of $O_{\mathcal{T}}$ with respect to $O_{\mathcal{S}}$ is defined by

$$\mathsf{D}_{\mathcal{S}}(F'/F) = (\mathrm{co}(O_{\mathcal{T}}))^{-1}.$$

If $\mathcal{S}$ is a set consisting of one place P of F, we denote $\mathsf{D}_{\mathcal{S}}(F'/F)$ simply by $\mathsf{D}_P(F'/F)$.

We can now define the different exponent of a place P' lying over P.

Definition 1.1.9 Let the place P' of F' lie over the place P of F. Then the **different exponent** of P' over P is defined by

$$d(P'|P) = \nu_{P'}(\mathsf{D}_P(F'/F)),$$

where $\nu_{P'}(\mathsf{D}_P(F'/F)) = \min\{\nu_{P'}(x) : x \in \mathsf{D}_P(F'/F)\}$. In particular, if $\mathrm{co}(O_{\mathcal{T}}) = tO_{\mathcal{T}}$ as in Lemma 1.1.7 (iii), then $d(P'|P) = -\nu_{P'}(t)$.

The next proposition gives some properties of different exponents.

Proposition 1.1.10 *For places $P'|P$ just as before, we have:*

(i) *$d(P'|P)$ is a non-negative integer;*

(ii) *$d(P'|P) \geq e(P'|P) - 1$. Further, $d(P'|P) = e(P'|P) - 1$ if and only if $e(P'|P)$ is relatively prime to p.*

Propositions 1.1.6 and 1.1.10 motivate the following definitions describing the behaviour of the places $P'|P$ in the field extension F'/F. We summarize the definitions in the table below.

Behaviour of	Behaviour	Characteristics
P'	unramified	$e(P'\|P) = 1$
P'	ramified	$e(P'\|P) > 1$
P'	tamely ramified	$e(P'\|P) > 1, \gcd(e(P'\|P), p) = 1$
P'	wildly ramified	$e(P'\|P) > 1, \gcd(e(P'\|P), p) = p$
P'	totally ramified	$e(P'\|P) = [F' : F]$
P	unramified	$e(P'\|P) = 1$ for all $P'\|P$
P	ramified	$e(P'\|P) > 1$ for some $P'\|P$
P	totally ramified	exactly 1 $P'\|P; e(P'\|P) = [F' : F]$
P	splits completely	$e(P'\|P) = f(P'\|P) = 1$ for all $P'\|P$ or exactly $[F' : F]$ places $P'\|P$

It follows from Proposition 1.1.6 that for a place $P \in \mathbf{P}_F$, only a finite number of places $P' \in \mathbf{P}_{F'}$ can be ramified in F'/F. Moreover, by Proposition 1.1.10, if $e(P'|P) = 1$ for some $P'|P$, $d(P'|P) = 1-1 = 0$. We can therefore define the **global different divisor** of F'/F as the positive divisor

$$\mathrm{Diff}(F'/F) = \sum_{P \in \mathbf{P}_F} \sum_{P'|P} d(P'|P)P' \in \mathsf{D}_{F'}.$$

We can now state the **Hurwitz Genus Formula** that relates the genera of two function fields.

Theorem 1.1.11 (Hurwitz Genus Formula) *Suppose that F'/K' is a finite separable extension of $F/\mathbf{F}_q$. Then*

$$2g(F') - 2 = \frac{[F' : F]}{[K' : \mathbf{F}_q]}(2g(F) - 2) + \deg(\mathrm{Diff}(F'/F)),$$

where $g(F')$ and $g(F)$ are the genera of F' and F, respectively.

For a separable field extension F'/F, we can define a **norm map** from $\mathsf{D}_{F'}$ to D_F by

$$N(F'/F) : \sum_{P' \in \mathbf{P}_{F'}} m_{P'} P' = \sum_{P \in \mathbf{P}_F} \sum_{P'|P} f(P'|P) m_{P'} P.$$

Lemma 1.1.12 (i) *For an element $z \in F'$,*

$$N(F'/F)(\mathrm{div}(z)) = \mathrm{div}(N_{F'/F}(z)),$$

where $N_{F'/F}$ on the right hand side denotes the usual norm of elements for field extensions.

(ii) *For a divisor $D \in \mathsf{D}_{F'}$,*

$$[K' : \mathbf{F}_q] \deg D = \deg N(F'/F)(D).$$

Corollary 1.1.13 *Let F'/F be a separable extension of global function fields with full field of constants $\mathbf{F}_q$. Define the* **discriminant** *of F'/F by*

$$D(F'/F) = N(F'/F)(\mathrm{Diff}(F'/F)).$$

Then

$$2g(F') - 2 = [F' : F](2g(F) - 2) + \deg D(F'/F),$$

where $g(F')$ and $g(F)$ are the genera of F' and F, respectively.

Theorem 1.1.11 readily shows that if F' and F have the same full constant field $\mathbf{F}_q$, then the genus of F cannot exceed that of F'. This follows from the fact that $\mathrm{Diff}(F'/F)$ is a positive divisor.

Before we conclude this section, we present a few results that will aid the calculation of the ramification index and different exponent in certain situations. The first proposition is concerned with a tower of function fields.

Proposition 1.1.14 *For a field tower $F \subseteq F' \subseteq F''$ and a corresponding place tower $P''|P'|P$, we have*

(i) $e(P''|P) = e(P''|P')e(P'|P)$.

(ii) $f(P''|P) = f(P''|P')f(P'|P)$.

(iii) $d(P''|P) = e(P''|P')d(P'|P) + d(P''|P')$.

Corollary 1.1.15 *Let F_1/F and F_2/F be finite separable extensions and let $F' = F_1F_2$, the compositum of F_1 and F_2. For $i = 1, 2$, let $S_i = \{P \in \mathbf{P}_F : P$ is ramified in $F_i/F\}$. Given any $P \in \mathbf{P}_F$, let P' be a place of F' lying over P and define $P_i = P' \cap F_i$, where $i = 1, 2$. Suppose that $S_1 \cap S_2 = \emptyset$. Then, the following hold:*

(i) $[F' : F] = [F_1 : F][F_2 : F]$;

(ii) $e(P'|P) = e(P_i|P)$ *for any* $P \in S_i, i = 1, 2$;

(iii) $d(P'|P) = d(P_i|P)$ *for any* $P \in S_i, i = 1, 2$.

Proof: All the assertions follow from Proposition 1.1.14 and the fact that F_1 and F_2 are linearly disjoint. □

We have a generalization of this corollary as stated below.

Lemma 1.1.16 (Abhyankar's Lemma) *Let F_1/F and F_2/F be finite separable extensions of function fields and let $F' = F_1F_2$. Let P' be a place of F' and P a place of F lying under P'. For $i = 1, 2$, define $P_i = P' \cap F_i$. Then, $P_i \in \mathbf{P}_{F_i}$ and $P_i|P$ for $i = 1, 2$. Suppose that at least one of P_i is tamely ramified in F_i/F. Then,*

$$e(P'|P) = \mathrm{lcm}(e(P_1|P), e(P_2|P)).$$

The following theorem gives an example of totally ramified extensions. First of all,

we recall the definition of an **Eisenstein polynomial**. More specifically, a polynomial $f(t) = a_k t^k + a_{k-1} t^{k-1} + \cdots + a_1 t + a_0 \in F[t]$ is called an **Eisenstein polynomial** if there exists a place P such that one of the following conditions is satisfied:

1. $\nu_P(a_k) = 0, \nu_P(a_i) \geq \nu_P(a_0) > 0$ for $1 \leq i \leq k-1$ and $\gcd(k, \nu_P(a_0)) = 1$;

2. $\nu_P(a_k) = 0, \nu_P(a_i) \geq 0$ for $1 \leq i \leq k-1$, $\nu_P(a_0) < 0$ and $\gcd(k, \nu_P(a_0)) = 1$.

In either case, we also say that $f(t)$ is Eisenstein at P.

Lemma 1.1.17 *Let $f(t)$ be an Eisenstein polynomial at a place P as defined above and let y be a root of $f(t)$. Consider the field extension $F' = F(y)$. Then, $f(t)$ is irreducible in $F[t]$ and $[F' : F] = k$. Further, P is totally ramified in F'/F.*

Notice from Proposition 1.1.10 (iii) that the different exponent is easily obtained when a place is tamely ramified. We now provide a method of calculating the different exponent in the case of total ramification.

Proposition 1.1.18 *Let F'/F be a finite separable extension of function fields with corresponding places $P'|P$ as usual. Suppose that P' is totally ramified in F'/F. Let π be a local parameter at P' and let $f(t)$ be the minimal polynomial of π over F. Then,*

$$d(P'|P) = \nu_{P'}(f'(\pi)),$$

where $f'(t)$ denotes the derivative of $f(t)$. Moreover, for any other place Q of F, the different exponent of a place Q' of F' lying over it satisfies $d(Q'|Q) \leq \nu_{Q'}(f'(\pi))$.

1.2 Some Algebraic Extensions

In this section, we explore some general algebraic extensions of global function fields. As before, $F/\mathbf{F}_q$ is a global function field and $K' \supseteq \mathbf{F}_q$.

Let $F' = FK'$. Then, it can be checked that F' is an algebraic extension of F and F'/K' is a function field with full constant field K'. F'/F is called a **constant field extension** of F. It is an unramified extension, that is, all places of F are unramified in F'/F. Suppose further that $K' = \mathbf{F}_{q^n}$ is finite. Then, $[F' : F] = [K' : K] = n$ and $\mathrm{Gal}(F'/F) \cong \mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \cong \mathbf{Z}/n\mathbf{Z}$. Consequently, the Hurwitz genus formula yields $g(F') = g(F)$.

Lemma 1.2.1 *Let F'/F be a constant field extension such that $F' = F\mathbf{F}_{q^n}$. Let P be a place of F with degree* $\deg P = d$. *Then,*

(i) *There are exactly* $\gcd(d, n)$ *places of F' lying over P.*

(ii) *Each place P' of F' lying over P has degree* $\deg P' = d/\gcd(d, n)$ *and relative degree* $f(P'|P) = n/\gcd(d, n)$.

Proof: The proof follows from the fact that $\tilde{F}_{P'} = \tilde{F}_P \cdot \mathbf{F}_{q^n}$ for any place $P'|P$. Since $\tilde{F}_P = \mathbf{F}_q, \tilde{F}_{P'} = \mathbf{F}_{q^l}$, where $l = nd/\gcd(d, n)$. □

Corollary 1.2.2 *Let F'/F be a constant field extension such that $F' = F\mathbf{F}_{q^n}$. Then, every rational place of F remains rational in F' and a place of degree n splits into n rational places in F'.*

For the remaining of this section, we assume that F' is a normal and separable extension over F. We further assume that $[K' : K]$ is finite which in turn implies that $[F' : F]$

is finite. In this case, the extension F'/F is called a **Galois extension**.

Once again, let P be a place of F and P' be a place of F' with $P'|P$. Let G be the Galois group $\mathrm{Gal}(F'/F)$. For every $\sigma \in G$, it can be directly verified that

$$\sigma(O_{P'}) = O_{\sigma(P')} = \{\sigma(x) : x \in O_{P'}\}$$

is a discrete valuation ring of F' containing O_P with place $\sigma(P')$. Hence, $\sigma(P')$ is a place of F' lying over P and we have

$$\nu_{\sigma(P')}(\sigma(x)) = \nu_{P'}(x)$$

for every $x \in F'$. In this way, G acts on the set of places lying over P. In fact, this action is transitive, i.e. for any two places P_1 and P_2 of F' with $P_1|P$ and $P_2|P$, there is a $\sigma \in G$ such that $P_2 = \sigma(P_1)$. The next lemma is a direct consequence of this transitive action.

Lemma 1.2.3 *Let F'/F be a Galois extension and let P_1 and P_2 be any two places of F' lying over P. Then,*

(i)
$$e(P_1|P) = e(P_2|P);$$

(ii)
$$f(P_1|P) = f(P_2|P);$$

(iii)
$$d(P_1|P) = d(P_2|P).$$

Proposition 1.1.6 can now be simplified to:

Corollary 1.2.4 *Let F'/F be a Galois extension and let P be a place of F. Suppose that $P_1, P_2, \ldots, P_k$ are distinct places of F' lying over P. Then,*

$$\sum_{i=1}^{k} e(P_i|P)f(P_i|P) = ke(P'|P)f(P'|P) = [F' : F],$$

where P' is any of the P_i's.

Next, we explore some subgroups of $G = \mathrm{Gal}(F'/F)$. Let P be a place of F and P' a place of F' lying over P. For any integer $i \geq -1$, define the i**th-lower ramification group** of P' over P by

$$G_i(P'|P) = \{\sigma \in G : \nu_{P'}(\sigma(x) - x) \geq i + 1 \text{ for all } x \in O_{P'}\}.$$

If π is a local parameter at P', then we may also define $G_i(P'|P)$ as

$$G_i(P'|P) = \{\sigma \in G : \nu_{P'}(\sigma(\pi) - \pi) \geq i + 1\}.$$

Obviously,

$$G \supseteq G_{-1}(P'|P) \supseteq G_0(P'|P) \supseteq G_1(P'|P) \supseteq \cdots \supseteq \{1\}.$$

By Galois theory, we have corresponding i**th-lower ramification fields**

$$F \subseteq F_{-1}(P'|P) \subseteq F_0(P'|P) \subseteq \cdots \subseteq F',$$

where $F_i(P'|P)$ is the fixed field of $G_i(P'|P)$.

We summarize the main properties of the i th-lower ramification groups in the theorem below.

Theorem 1.2.5 *For any integer $i \geq -1$, let $G_i(P'|P)$ be the i th-lower ramification groups defined above.*

(i) *For any* $\sigma \in G, G_i(\sigma(P')|P)$ *and* $G_i(P'|P)$ *are conjugate groups, i.e.* $G_i(\sigma(P')|P) = \sigma G_i(P'|P)\sigma^{-1}$.

(ii) $G_i(P'|P) = \{1\}$ *for sufficiently large* i.

(iii) $G_{-1}(P'|P)$ *has cardinality* $e(P'|P)f(P'|P)$ *and* $G_0(P'|P)$ *is a normal subgroup of* $G_{-1}(P'|P)$ *with cardinality* $|G_0(P'|P)| = e(P'|P)$.

(iv) $G_1(P'|P)$ *is a normal subgroup of* $G_0(P'|P)$ *and the factor group* $G_0(P'|P)/G_1(P'|P)$ *is cyclic with order relatively prime to* p.

(v) $G_i(P'|P)$ *are* p*-elementary abelian groups for* $i \geq 1$.

Let us take a closer look at the first two ramification groups, namely, $G_{-1}(P'|P)$ and $G_0(P'|P)$ known respectively as the **decomposition group** and the **inertia group** of $P'|P$. The corresponding ramification fields are then called **decomposition field** and **inertia field**. Note that $G_0(P'|P) = \{\sigma \in G : \sigma(P') = P'\}$.

Proposition 1.2.6 *With the notations above, we have*

(i) *For each* $\sigma \in G_{-1}(P'|P)$, *let* $\overline{\sigma} \in \mathrm{Gal}(\tilde{F}_{P'}/\tilde{F}_P)$ *be defined by*

$$\overline{\sigma}(z) = \sigma(z) + P'$$

for all $z \in O_{P'}$. *Then the map that sends* $\sigma \mapsto \overline{\sigma}$ *is a surjective homomorphism from* $G_{-1}(P'|P)$ *to* $\mathrm{Gal}(\tilde{F}_{P'}/\tilde{F}_P)$ *with kernel* $G_0(P'|P)$. *Consequently,* $G_{-1}(P'|P)/G_0(P'|P) \cong \mathrm{Gal}(\tilde{F}_{P'}/\tilde{F}_P)$.

(ii) P *splits completely in* $F_{-1(P'|P)}/F$, *i.e. if* P_{-1} *is a place of* $F_{-1}(P'|P)$ *lying over* P, *then*

$$e(P_{-1}|P) = f(P_{-1}|P) = 1.$$

(iii) *Let P_{-1} be any place of $F_{-1}(P'|P)$ lying over P. Then, P' is the only place of F' lying over P_{-1}. Moreover, if $P_0 = P' \cap F_0(P'|P)$, then $e(P_0|P_{-1}) = 1$ and $e(P'|P_0) = e(P'|P) = [F' : F_0(P'|P)]$.*

Corollary 1.2.7 *Let L be an intermediate field of F'/F. Let P' be a place of F' lying over $P \in \mathbf{P}_F$ and let $Q \in \mathbf{P}_L$ be the place lying under P'. Then we have:*

(i) *P is unramified in L/F if and only if $L \subseteq F_0(P'|P)$;*

(ii) *Q is totally ramified in F'/L if and only if $L \supseteq F_0(P'|P)$;*

(iii) *P splits completely in L/F if and only if $L \subseteq F_{-1}(P'|P)$;*

(iv) *P' is the only place of F' lying over Q if and only if $L \supseteq F_{-1}(P'|P)$.*

Corollary 1.2.8 *Suppose that L_1/F and L_2/F are two finite separable extensions and L is the compositum of L_1 and L_2. Then for a place $P \in \mathbf{P}_F$, we have:*

(i) *P splits completely in L/F if and only if P splits completely in both L_1/F and L_2/F;*

(ii) *P is unramified in L/F if and only if P is unramified in both L_1/F and L_2/F.*

Now, suppose that P is unramified in F'/F, i.e. the inertia field $F_0(P'|P) = F'$. By Proposition 1.2.6 (i), the decomposition group $G_{-1}(P'|P)$ is isomorphic to the cyclic group $\mathrm{Gal}(\tilde{F}_{P'}/\tilde{F}_P)$ which is in turn isomorphic to $\mathbf{Z}/f\mathbf{Z}$, where $f = f(P'|P)$. Consequently, there is a unique $\sigma \in G_{-1}(P'|P)$ such that

$$\sigma(z) \equiv z^{q^{\deg P}} \bmod P'$$

for all $z \in O_{P'}$. Observe that σ depends only on $P'|P$ and it is called the **Frobenius symbol** of P' over P. We denote it by $\left[\frac{F'/F}{P'}\right]$ and it has the following properties:

Theorem 1.2.9 *Suppose that the finite Galois extension F'/F is unramified at $P \in \mathbf{P}_F$ and let P' be a place of F' lying over P. Assume that L is an intermediate field of F'/F and $R \in \mathbf{P}_L$ is the place lying under P'. Then we have:*

(i) *For any $\tau \in \mathrm{Gal}(F'/F)$,*

$$\left[\frac{F'/F}{\tau(P')}\right] = \tau \left[\frac{F'/F}{P'}\right] \tau^{-1}.$$

(ii)

$$\left[\frac{F'/L'}{P}\right] = \left[\frac{F'/F}{P'}\right]^{f(R|P)}.$$

(iii) *If L/F is a Galois extension, then the restriction of $\left[\frac{F'/F}{P'}\right]$ to L is equal to $\left[\frac{L/F}{R}\right]$.*

Proof: (i) This follows from Theorem 1.2.5 and the uniqueness of the Frobenius symbol.

(ii) This can be easily seen from the definitions of the respective Frobenius symbols and that the residue class field $\tilde{F}_R = \mathbf{F}_{q^{df}}$, where $f = f(R|P)$.

(iii) Let $\sigma = \left[\frac{F'/F}{P'}\right]$. By the definition of the Frobenius symbol, we have

$$\sigma(z) \equiv z^{q^d} \bmod P'$$

for all $z \in O_P$, where $d = \deg P$. Clearly $O_R \subseteq O_{P'}$. Thus, the above equation characterizing the Frobenius symbol is again satisfied for all $z \in O_R$. The uniqueness of the Frobenius symbol yields our desired result. □

If in addition, F'/F is an abelian extension, then it follows from Theorem 1.2.9 (i) that the Frobenius symbol $\left[\frac{F'/F}{P'}\right]$ does not depend on P', but rather, it depends only on the place P of F lying under P'. It is thus unambiguous to write the Frobenius symbol as $\left[\frac{F'/F}{P}\right]$, which is called the **Artin symbol** of P in F'/F.

Proposition 1.2.10 *Let F'/F be a Galois abelian extension and let L be a subfield of F'/F. Suppose that F'/F is unramified at $P \in \mathbf{P}_F$. Then P splits completely in L/F if and only if the Artin symbol $\left[\frac{F'/F}{P}\right]$ belongs to* $\mathrm{Gal}(F'/L)$.

Proof: Now, P splits completely in L/F if and only if the decomposition group of P is trivial if and only if the Artin symbol $\left[\frac{L/F}{P}\right]$ is trivial and by (ii) of the preceding theorem, this holds if and only if the restriction of $\left[\frac{F'/F}{P}\right]$ to L is trivial if and only if $\left[\frac{F'/F}{P}\right]$ lies in $\mathrm{Gal}(F'/L)$. □

1.3 Upper Ramification Groups and the Hilbert's Different Formula

We continue to let F'/F be a Galois extension of function fields with $G = \mathrm{Gal}(F'/F)$. Further, suppose throughout this section that F'/F is an abelian extension. Fix a place P of F and a place $P' \in \mathbf{P}_{F'}$ lying over P.

Consider the P-adic completion F_P and the P'-adic completion $F'_{P'}$ of F and F' respectively. Given any $\sigma \in G$, σ induces an isomorphism σ' between $F'_{P'}$ and $F'_{\sigma(P')}$ keeping F_P fixed. Thus, if $\sigma \in G_{-1}(P'|P)$, σ' becomes an automorphism of $F'_{P'}$. In fact, the map θ sending $\sigma \in G_{-1}(P'|P)$ to $\sigma' \in \mathrm{Gal}(F'_{P'}/F_P)$ is an isomorphism. As a consequence, $F'_{P'}/F_P$ is Galois and

$$[F'_{P'} : F_P] = |G_{-1}(P'|P)| = e(P'|P)f(P'|P).$$

For all integers $i \geq -1$, we define the i th-lower ramification groups of $F'_{P'}/F_P$ by

$$G_i(F'_{P'}/F_P) = \{\tau \in \mathrm{Gal}(F'_{P'}/F_P) : \nu_{P'}(\tau(a) - a) \geq i + 1 \text{ for all } a \in O_{P'}\},$$

where $\nu_{P'}$ and $O_{P'}$ refer to the normalized discrete valuation and the valuation ring of $F'_{P'}$, respectively.

One sees easily that the map θ induces an isomorphism between $G_i(P'|P)$ and $G_i(F'_{P'}/F_P)$ for all $i \geq -1$. In view of this, we simply write $G_i = G_i(P'|P)$ for $G_i(F'_{P'}/F_P)$ and let $g_i = |G_i|$.

Define the map $\eta : [-1, \infty) \to [-1, \infty)$ by

$$\eta(u) = \begin{cases} u & \text{if } -1 \leq u \leq 0, \\ \frac{g_1 + g_2 + \cdots + g_{\lfloor u \rfloor} + (u - \lfloor u \rfloor) g_{\lfloor u \rfloor + 1}}{g_0} & \text{otherwise} \end{cases}$$

(Here, $\lfloor x \rfloor$ refers to the greatest integer $<= x$.)

We summarize some facts on the function η in the next lemma. The reader may refer to [65] for their proofs.

Lemma 1.3.1 *Let $\eta : [-1, \infty] \to [-1, \infty]$ be the map defined above. Then,*

(i) *η is piecewise linear, continuous, strictly increasing and concave on the interval $[-1, \infty]$. Hence, the inverse map $\psi = \eta^{-1}$ is well-defined on $[-1, \infty]$.*

(ii) *ψ is piecewise linear, continuous, strictly increasing and convex on $[-1, \infty]$.*

(iii) *If u is an integer, then $\psi(u)$ is an integer too.*

(iv) *[Hasse-Arf Theorem] If u is an integer such that $G_u \neq G_{u+1}$, then $\eta(u)$ is an integer.*

For any integer $i \geq -1$, we define the i **th-upper ramification groups** by

$$G^i = G^i(P'|P) = G_{\psi(i)}$$

and the i**th-upper ramification fields** $F^i = F^i(P'|P)$ as the corresponding fixed fields of G^i. This definition makes sense according to Lemma 1.3.1 (iii). Again, we have

$$G^{-1} \supseteq G^0 \supseteq G^1 \supseteq \dots$$

and $G^u = \{1\}$ for sufficiently large u. Moreover, we see directly from the definition that if L is an intermediate field with $F \subseteq L \subseteq F'$ and P_L is a place of L lying under P', the restriction map that sends $\mathrm{Gal}(F'/F)$ to $\mathrm{Gal}(L'/F)$ sends $G^i(P'|P)$ onto $G^i(P_L|P)$.

By letting $l_0 = 0$, let the numbers $1 \leq l_1 < l_2 < \cdots < l_s$ be such that $G_{l_i+1} = G_{l_i+2} = \cdots = G_{L_{i+1}}, G_{l_i} \neq G_{l_{i+1}}, i = 0, 1, \dots, s-1$ and $G_{l_s+1} = \{1\}$. Likewise, define the numbers $u_0 = 0, u_1, u_2, \dots, u_t$ for the upper ramification groups.

Observe that by combining Lemma 1.3.1 (iii) and (iv), we must have $\eta(l_j) = u_j$ for all j which further implies that $s = t$.

Lemma 1.3.2 *For* $j = 0, \dots, s-1$,

$$[G^0 : G^{u_{j+1}}] = \frac{l_{j+1} - l_j}{u_{j+1} - u_j}.$$

Proof: From the definition of η and the preceding remark, it follows by induction that for $j = 0, 1, \dots, s-1$,

$$(l_{j+1} - l_j)\frac{g_{l_{j+1}}}{g_0} = u_{j+1} - u_j.$$

Hence,

$$\begin{aligned} [G^0 : G^{u_{j+1}}] &= [G_0 : G_{l_{j+1}}] \\ &= \frac{g_0}{g_{l_{j+1}}} \\ &= \frac{l_{j+1} - l_j}{u_{j+1} - u_j}. \end{aligned}$$

□

We can now present the Hilbert's different formula that calculates the different exponent of P' over P.

Theorem 1.3.3 (Hilbert's Different Formula) *Let F'/F be a finite Galois extension and let P' be a place of F' lying over $P \in \mathbf{P}_F$. Then, the different exponent $d(P'|P)$ is given by:*

(i) *[Lower index]*

$$d(P'|P) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

(ii) *[Upper index]*

$$d(P'|P) = \sum_{i=0}^{\infty}(|G^0| - [G^0 : G^i]).$$

Proof: (i) This is derived from Proposition 1.1.18. Refer to [72, Chapter III] for details.

(ii) From (i),

$$\begin{aligned} d(P'|P) &= \sum_{i=0}^{\infty}(g_i - 1) \\ &= g_0 - 1 + \sum_{j=0}^{s-1}(l_{j+1} - l_j)(g_{l_{j+1}} - 1) \\ &= |G^0| - 1 + \sum_{j=0}^{s-1}(l_{j+1} - l_j)(|G^{u_{j+1}}| - 1) \\ &= |G^0| - 1 + \sum_{j=0}^{s-1}(l_{j+1} - l_j)(|G^0| - [G^0 : G^{u_{j+1}}])/[G^0 : G^{u_{j+1}}] \\ &= |G^0| - 1 + \sum_{j=0}^{s-1}(u_{j+1} - u_j)(|G^0| - [G^0 : G^{u_{j+1}}]) \\ &= \sum_{i=0}^{\infty}(|G^0| - [G^0 : G^i]). \end{aligned}$$

□

The integer $u_s + 1$ defined above is usually denoted by $c(P'|P)$ and is called the **conductor exponent** of $P'|P$. In other words, $c(P'|P)$ is the smallest integer j for which $G^j = \{1\}$. Notice that as F'/F is an abelian extension, the i th-upper ramification groups are independent of the choice of P' lying over P. Thus, the conductor exponent is the same for all $P'|P$ and we will simply write c_P for the conductor exponent $c(P'|P)$. Since G^0 is the inertia group, it follows immediately that $c(P'|P) = 0$ if and only if $P'|P$ is unramified. This makes it meaningful to define the **conductor** of F'/F as the positive divisor

$$\mathrm{Con}(F'/F) = \sum_{P \in \mathbf{P}_F} c_P P.$$

Corollary 1.3.4 *Let F'/F be an abelian Galois extension with the same constant field $\mathbf{F}_q$. Then, the genus of F' is given by*

$$2g(F')-2 = [F':F](2g(F)-2)+|G|\deg \mathrm{Con}(F'/F)-\sum_{P\in \mathrm{supp}(\mathrm{Con}(F'/F))}\sum_{j=0}^{c_P-1}[G:G^j]\deg P.$$

Equivalently,

$$2g(F')-2 = [F':F](2g(F)-2)+[F':F]\deg \mathrm{Con}(F'/F)-\sum_{P\in \mathrm{supp}(\mathrm{Con}(F'/F))}\sum_{j=0}^{c_P-1}[F^j:F]\deg P.$$

Proof: For each $P \in \mathbf{P}_F$, we have

$$\sum_{P'|P} f(P'|P)P = [G:G^0]P$$

since G^0 is the inertia group of $P'|P$. The result now follows from Corollary 1.1.13. □

Corollary 1.3.5 *Let F'/F be an abelian Galois extension of global function fields with full constant field $\mathbf{F}_q$. Let P be a place of F with conductor exponent $c_P = n$. Suppose that $G^{n-1} = G$. Then the genus of F' is given by*

$$2g(F') - 2 = [F':F](2g(F) - 2 + n\deg P) - n\deg P.$$

In particular, if P is totally ramified in F'/F and $c_P \leq 2$, then

$$g(F') = 1 - \deg P + [F':F](g(f) + \deg P - 1).$$

Proof: Since $G^0 = G^1 = \cdots = G^{n-1} = G$, the first result is a direct consequence of Corollary 1.3.4. The second assertion is trivial for $c_P < 2$. So suppose $c_P = 2$. Since P is totally ramified, we conclude from the properties of ramification groups that $G_0 = G_1 = G$. Clearly, $G^1 = G_1 = G$. Hence the assumptions for the first assertion hold and the genus formula follows. □

1.4 Divisor Classes and Divisor Class Groups

Recall that for a global function field $F/\mathbf{F}_q$, we have defined D_F to be the set of all divisors of F. In fact, D_F is a free abelian group on the set of places $\mathbf{P}_F$ under the following operation:

$$\sum_{P\in\mathbf{P}_F} m_P P + \sum_{P\in\mathbf{P}_F} n_P P = \sum_{P\in\mathbf{P}_F} (m_P + n_P)P.$$

Hence, the degree map $\deg : \mathsf{D}_F \to \mathbf{Z}$ is a group homomorphism and its kernel is denoted by D_F^0.

According to Proposition 1.1.3, for every $z \in F^*$, the principal divisor $\mathrm{div}(z)$ has degree 0. Let $\mathrm{Princ}(F)$ be the subgroup of $\mathrm{Div}^0(F)$ consisting of all principal divisors $\mathrm{div}(z)$. Then, the factor group $\mathrm{Cl}(F) = \mathrm{Div}^0(F)/\mathrm{Princ}(F)$ is finite and its cardinality is commonly known as the **divisor class number** of F, denoted by $h(F)$.

More generally, for a subset $\mathcal{T}$ of $\mathbf{P}_F$, let $\mathrm{Div}_{\mathcal{T}}(F)$ be the group of divisors of F with support away from $\mathcal{T}$. Since $\mathbf{Z}$ is a principal ideal domain, there exists a positive integer $d = \deg \mathcal{T}$ such that the degree map restricted to $\mathrm{Div}_{\mathcal{T}}(F)$ has image $d\mathbf{Z}$. In particular, if $\mathcal{T}' = \mathbf{P}_F - \mathcal{T}$ is finite, then d is the gcd of the degrees of all the places in $\mathcal{T}'$. $\mathrm{Div}^0_{\mathcal{T}}(F)$ will again refer to the group of divisors of $\mathrm{Div}_{\mathcal{T}}(F)$ of degree 0. For a positive divisor D of F, we will write $\mathrm{Div}_D(F)$ and $\mathrm{Div}^0_D(F)$ for $\mathrm{Div}_{\mathrm{supp}(D)}(F)$ and $\mathrm{Div}^0_{\mathrm{supp}(D)}(F)$, respectively.

Let $\mathcal{S}$ be a subset of $\mathbf{P}_F$ such that $\mathcal{S}' = \mathbf{P}_F - \mathcal{S}$ is nonempty and finite. Define the integral ring $O_{\mathcal{S}}$ to be the intersection

$$O_{\mathcal{S}} = \bigcap_{P\in\mathcal{S}} O_P,$$

i.e. $O_{\mathcal{S}}$ consists of all the elements of F with poles only in $\mathcal{S}'$. The unit group $O_{\mathcal{S}}^*$ is called the group of $\mathcal{S}$-units of F.

Theorem 1.4.1 (Dirichlet Unit Theorem) *Let $\mathcal{S}$ be a subset of $\mathbf{P}_F$ such that $\mathcal{S}' = \mathbf{P}_F - \mathcal{S}$ is nonempty and finite. Then, $O_{\mathcal{S}}^*/\mathbf{F}_q^*$ is a free abelian group of rank $|\mathcal{S}'| - 1$.*

$O_{\mathcal{S}}$ is in fact a Dedekind domain with prime ideals $P \cap O_{\mathcal{S}}, P \in \mathcal{S}$ and field of fractions F.

Lemma 1.4.2 *Let n be a positive integer and let $P \in \mathcal{S}$. The map $\mu : O_{\mathcal{S}} \to O_P/P^n$ defined by*

$$x \mapsto x + P^n$$

is surjective with kernel $P^n \cap O_S$.

Proof: Clearly, μ is a well-defined map with kernel $O_{\mathcal{S}} \cap P^n$. It remains to show that μ is onto. Let $x + P^n \in O_P/P^n$. Since $\mathcal{S}$ is a proper subset of $\mathbf{P}_F$, we may apply the strong theorem to obtain an $x' \in F$ such that

(i) $\nu_P(x' - x) > \max(n, \nu_P(x))$;

(ii) $\nu_Q(x') \geq 0$ for all $Q \in \mathcal{S} - \{P\}$. Then, $x' \in O_{\mathcal{S}}$ and $x' - x \in P^n$. Hence, $\mu(x') = x' + P^n = x + P^n$. □

We define the $\mathcal{S}$-ideal class group $\mathrm{Cl}(O_{\mathcal{S}})$ to be the quotient of the group of $\mathcal{S}$-fractional ideals of $O_{\mathcal{S}}$ by the group of principal ideals of the form $zO_{\mathcal{S}}, z \in F^*$. One can show that the $\mathcal{S}$-ideal class group has finite order $h(\mathcal{S})$.

Next, let $D = \sum_{P \in \mathbf{P}_F} m_P P$ be an effective divisor of F with $\mathrm{supp}(D) \subseteq \mathcal{S}$. Observe that D can be identified with the ideal $\prod_{P \in \mathrm{supp}(D)} (P \cap O_{\mathcal{S}})^{m_P}$, and thus, D will represent the corresponding ideal under this identification too. We say that an element $z \in F^*$ is equivalent to $1 \bmod D$, written as $z \equiv 1 \bmod D$ if for all $P \in \mathrm{supp}(D), \nu_P(z-1) \geq m_P$.

An ideal J of $O_{\mathcal{S}}$ is prime to D if all prime ideals Q of $O_{\mathcal{S}}$ that divide J (or equivalently, the places in the support of J as a divisor) are not in $\mathrm{supp}(D)$. Clearly, the principal ideal $zO_{\mathcal{S}}$ is prime to D for $z \equiv 1 \bmod D$. Let $I_D(O_{\mathcal{S}})$ be the group of all fractional ideals of $O_{\mathcal{S}}$ that are prime to D and $\mathrm{Princ}_D(\mathcal{S})$ be the group of principal ideals of the form $zO_{\mathcal{S}}$ such that $z \equiv 1 \bmod D$. The quotient group $I_D(O_{\mathcal{S}})/\mathrm{Princ}_D(\mathcal{S})$ is denoted by $\mathrm{Cl}_D(O_{\mathcal{S}})$. This group is called the $\mathcal{S}$-ray class group mod D. Notice that when $D = 0$, we obtain the $\mathcal{S}$-ideal class group defined above.

In addition, let $\mathrm{Princ}_D(F)$ be the group of principal divisors $\mathrm{div}(z)$, where $z \equiv 1 \bmod D$. With all these notations, we have the following proposition.

Proposition 1.4.3 (i) $\mathrm{Cl}_D(O_{\mathcal{S}})$ *is isomorphic to* $\mathrm{Div}_D^0(F)/(\mathrm{Div}_{\mathcal{S}}^0(F) + \mathrm{Princ}_D(F))$.

(ii) *We have the following exact sequence:*

$0 \to \mathrm{Div}_{\mathcal{S}}^0(F)/(\mathrm{Div}_{\mathcal{S}}^0(F) \cap \mathrm{Princ}_D(F)) \to \mathrm{Div}_D^0(F)/\mathrm{Princ}_D(F) \to \mathrm{Div}_D^0(F)/(\mathrm{Div}_{\mathcal{S}}^0(F) + \mathrm{Princ}_D(F)) \stackrel{\deg}{\to} \mathbf{Z}/\deg \mathcal{S}\mathbf{Z}$.

Proof: (i) Define a map θ that sends the divisor $\sum_{P \in \mathbf{P}_F - \mathrm{supp}(D)} m_P P \in \mathrm{Div}_D^0(F)$ to $\prod_{P \notin \mathcal{S}} (P \cap O_{\mathcal{S}})^{m_P} \mathrm{Princ}_D(\mathcal{S})$. It is clear that θ is onto and has kernel $\mathrm{Div}_{\mathcal{S}}^0(F) + \mathrm{Princ}_D(F)$. Thus, θ induces the isomorphism as required.

(ii) All the maps are canonical. □

Corollary 1.4.4 *If* $\mathcal{S}$ *consists of a single rational place, then* $\mathrm{Cl}(F) \simeq \mathrm{Cl}(O_{\mathcal{S}})$. *In particular,* $h(F) = h(O_{\mathcal{S}})$.

Proof: Put $D = 0$ in the above proposition. Then $\mathrm{Div}_{\mathcal{S}}^0(F) = \mathbf{F}_q^*$ and $\deg \mathcal{S} = 1$. The desired isomorphism follows. □

Let D be as above. Suppose that ∞ is a fixed rational place of F with $\infty \notin \text{supp}(D)$. Define $\text{Cl}_D(F)$ to be the factor group

$$\text{Cl}_D(F) = \text{Div}_D^0(F)/\text{Princ}_D(F).$$

We represent the elements of $\text{Cl}_D(F)$ by the equivalence classes $[C]$, where $C \in \text{Div}_D^0(F)$.

Lemma 1.4.5 *Every element of* $\text{Cl}_D(F)$ *can be written in the form* $[H - (\deg H)\infty]$ *for some positive divisor* H *of* $\text{Div}_D^0(F)$. *Moreover, for a finite subset* $\mathcal{T}$ *of* $\mathbf{P}_F$ *such that* $\mathcal{T} \cap \text{supp}(D) = \emptyset$, H *can be chosen such that* $\text{supp}(H) \cap \mathcal{T} = \emptyset$.

Proof: Let $[C]$ be an arbitrary element of $\text{Cl}_D(F)$. Write $C = \sum_{P \in \mathbf{P}_F} c_P P$. Let $\mathcal{S} = \mathbf{P}_F - \{\infty\}$. By the strong approximation theorem (Theorem 1.1.2 (ii)), there exists an element $z \in F^*$ such that

(i)

$$\nu_P(z) = -c_P$$

for all $P \in \text{supp}(C)$;

(ii)

$$\nu_P(z-1) \geq m_P$$

for all $P \in \text{supp}(D)$;

(iii)

$$\nu_P(z) = 0$$

for all $P \in \mathcal{T}, P \notin \text{supp}(C)$; and

(iv)

$$\nu_P(z) \geq 0$$

for all $P \in \mathcal{S} - \mathrm{supp}(C) - \mathrm{supp}(D) - \mathcal{T}$. Let $H = C + \mathrm{div}(z)$. Then, $[C] = [H]$ with H having the desired form. $\square$

As a consequence of Lemma 1.4.5, we can identify an element $\prod_{P \neq \infty, P \notin \mathrm{supp}(D)} (P \cap O_{\mathcal{S}})^{m_P} \mathrm{Princ}_D(\mathcal{S}) \in \mathrm{Cl}_D(O_{\mathcal{S}})$ when $\mathcal{S}' = \{\infty\}$ with the divisor $\sum_{P \neq \infty, P \notin \mathrm{supp}(D)} m_P P - \sum_{P \neq \infty, P \notin \mathrm{supp}(D)} m_P \deg P \infty + \mathrm{Princ}_D(F) \in \mathrm{Cl}_D(F)$. This identification will be made often throughout the thesis, depending on the more convenient form for the particular context.

1.5 Upper Bounds for Number of Rational Places

This thesis is primarily concerned with the search of global function fields with large number of rational places relative to their genera. How large can this number be? In this section, we will present some well-known upper bounds for the number of rational places that a global function field of fixed genus can have. First, we need to introduce the **zeta functions** and the L**-polynomials** of F.

Recall from Lemma 1.1.1 that for any integer d, the set $\mathbf{P}_F^d$ of all places of F of degree d is finite. It is therefore obvious that given any integer k, the number of positive divisors of F of degree k is finite. The following definition is now meaningful.

Definition 1.5.1 For a global function field $F/\mathbf{F}_q$, we define the **zeta function** of F by

$$Z_F(t) = Z(t) = \sum_{k=0}^{\infty} A_k t^k \in \mathbf{C}[t],$$

where A_k is the number of positive divisors of F of degree k.

In fact, $Z_F(t)$ is a rational function according to the following theorem.

Theorem 1.5.2 *For a global function field $F/\mathbf{F}_q$, the zeta function $Z_F(t)$ can be written as*

$$Z_F(t) = L_F(t)/(1-t)(1-qt),$$

where $L_F(t)$ is a polynomial over $\mathbf{Z}$ of degree $2g$, g being the genus of F.

The polynomial $L_F(t)$ in the above theorem is called the **L-polynomial** of F and it satisfies the following properties.

Lemma 1.5.3 *Let $F/\mathbf{F}_q$ be a global function field of genus g with $L_F(t)$ as its L-polynomial. Write $L_F(t)$ as*

$$L_F(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbf{Z}[t].$$

Then,

(i) $L_F(t) = q^g t^{2g} L_F(\frac{1}{qt})$.

(ii) $a_0 = 1$ *and* $a_{2g-i} = q^{g-i} a_i$ *for all* $0 \le i \le g$. *Thus,* $a_{2g} = q^g$.

(iii) $\sum_{i=0}^{2g} a_i = h(F)$, *where $h(F)$ denotes the divisor class number of F.*

For a positive integer n, let F_n be the constant field extension $F_n = F\mathbf{F}_{q^n}$. We can similarly define the zeta function and L-polynomial over F_n, denoted by $Z_{F_n}(t)$ and $L_{F_n}(t)$, respectively.

Lemma 1.5.4 *With notations as above,*

(i)

$$Z_{F_n}(t^n) = \prod_{\zeta^n=1} Z_F(\zeta t),$$

where the product is taken over all nth roots of unity.

(ii) *ω is a root of $L_F(t)$ if and only if ω^n is a root of $L_{F_n}(t)$.*

In 1948, Weil proved the analog of the famous Riemann hypothesis for algebraic function fields, namely,

Theorem 1.5.5 *Let $L_F(t)$ be the L-polynomial of a global function field $F/\mathbf{F}_q$ of genus g. Suppose that the complex numbers $1/\omega_1, 1/\omega_2, \ldots, 1/\omega_{2g}$ are the roots of $L_F(t)$. Then, $|\omega_i| = \sqrt{q}$ for $1 \leq i \leq 2g$.*

Remark 1.5.6 *We can prove the preceding theorem in several ways. For instance, Bombieri's elementary proof is discussed in [72, Chapter V] while the l-adic cohomology approach is presented in [23, Appendix C].*

An immediate consequence of Theorem 1.5.5 yields an upper bound for the number of rational places of F, denoted by $N(F)$.

Theorem 1.5.7 (Hasse-Weil Bound) *Let $F/\mathbf{F}_q$ be a global function field of genus g. Then the number $N(F)$ of rational places of $F/\mathbf{F}_q$ satisfies*

$$|N(F) - (q+1)| \leq 2gq^{1/2}.$$

If $N(F)$ attains the Hasse-Weil bound, F is called a **maximal** function field. Obviously, F can only be maximal when $g = 0$ or q is a square. Moreover, the proposition below holds (refer to [13], [96] and [12] for more details).

Proposition 1.5.8 *Let $F/\mathbf{F}_q$ be a maximal function field. Then the genus g of F satisfies one of the following:*

(i)

$$g = (q - \sqrt{q})/2,$$

or (ii)

$$g \leq (\sqrt{q}-1)^2/4.$$

Proposition 1.5.8 shows, in particular, that the Hasse-Weil bound is not sharp for large genus relative to q. Serre improved the bound for nonsquares q as follows.

Theorem 1.5.9 (Serre bound) *Let $F/\mathbf{F}_q$ be a global function field with genus g. Denote by $N(F)$ the number of rational places of F. We have*

$$|N(F)-(q+1)| \leq g\lfloor 2q^{1/2}\rfloor.$$

Next we fix q and an integer $g \geq 0$. Consider all global function fields $F/\mathbf{F}_q$ of genus g. Let $N_q(g)$ be the maximum number of rational places contained in all such fields, i.e. $N_q(g) = \max\{N(F)\}$, where the maximum is extended over all global function fields of genus g. A function field $F/\mathbf{F}_q$ of genus g is said to be **optimal** if $N(F) = N_q(g)$. According to the Serre bound,

$$N_q(g) \leq q+1+g\lfloor 2q^{1/2}\rfloor.$$

This bound can be improved by the so-called "explicit Weil formulas' introduced by Serre [66] which will now be presented.

Theorem 1.5.10 *For $k \geq 1$, suppose that $c_1, \ldots, c_k$ are k nonnegative real numbers such that at least one of them is not equal to zero and the inequality*

$$1+\lambda_k(t)+\lambda_k(t^{-1}) \geq 0$$

holds for all $t \in \mathbf{C}$ with $|t|=1$, where $\lambda_k(t) = \sum_{n=1}^{k} c_n t^n$. Then we have

$$N_q(g) \leq \frac{g}{\lambda_k(q^{-1/2})} + \frac{\lambda_k(q^{1/2})}{\lambda_k(q^{-1/2})} + 1$$

for any q and g.

Remark 1.5.11 *The optimization of the explicit Weil formulas can be carried out via linear programming as suggested by Oesterlé in an unpublished manuscript to Serre (see [69]). Hence, the upper bound of $N_q(g)$ obtained by this method will be called the Oesterlé bound.*

In fact, the exact values of $N_q(1)$ and $N_q(2)$ are known for all prime powers q (refer to [66]). However, for larger values of g, there have yet been explicit formulas to describe $N_q(g)$. Instead, tables containing upper and lower bounds on $N_q(g)$ obtained through various means have been tabulated by several mathematicians. A comprehensive and updated survey of bounds on $N_q(g)$, where q is a small power of 2 and 3, and $g \leq 50$ is maintained by Van Der Geer and Van Der Vlugt [82]. For bounds on $N_5(g)$, we may refer to [55].

Chapter 2

Examples of Function Fields

After developing some general concepts of global function fields, we are now ready to explore explicit examples of these function fields. As such, this chapter introduces four of the most common global function fields, namely, rational function fields, cyclotomic function fields, as well as Kummer extensions and Artin-Schreier extensions of global function fields. These function fields are of particular interest as their genera, and in some cases, their defining equations can be explicitly obtained. Many of the results in the first three sections will be quoted without proofs, and readers may refer to [72] for further details. As cyclotomic function fields play a critical role in subsequent chapters, we will present its theory with greater depth.

2.1 Rational Function Fields

By merely looking at its definition, an obvious example of a global function field is the rational function field $F = \mathbf{F}_q(x)$, where x is an indeterminate. Indeed, it is one of the

most fundamental global function fields since it has genus $g(F) = 0$. Moreover, one can show that any global function field with genus 0 is a rational function field.

Let us examine the places of F. For a monic irreducible polynomial $p(x)$ of $\mathbf{F}_q[x]$, we may define a surjective function $\nu_{p(x)} : F \to \mathbf{Z} \cup \{\infty\}$ by setting $\nu_{p(x)}(f(x))$ to be the power of $p(x)$ occuring in $f(x)$ for every $f(x) \in F$. It can be directly verified that $\nu_{p(x)}$ is a normalized discrete valuation with corresponding valuation ring

$$O_{p(x)} = \{f(x)/g(x) \in F : g(x) \neq 0, \gcd(p(x), g(x)) = 1\}$$

with place

$$P_{p(x)} = p(x)O_{p(x)} = \{f(x)/g(x) \in F : g(x) \neq 0, p(x)|f(x) \text{ and } \gcd(p(x), g(x)) = 1\}.$$

The residue class field is isomorphic to the finite field $\mathbf{F}_q[x]/(p(x))$ which implies that $\deg P = \deg p(x)$.[1]

Next, by extending the degree function $-\deg$ on $\mathbf{F}_q[x]$ to the whole of $\mathbf{F}_q(x)$, we obtain another normalized discrete valuation ν_∞. More specifically, for all $f(x)/g(x) \in \mathbf{F}_q(x), g(x) \neq 0$,

$$\nu_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x).$$

Since its valuation ring

$$O_\infty = \{f(x)/g(x) \in F : g(x) \neq 0, \deg f(x) \leq \deg g(x)\}$$

has place

$$P_\infty = \{f(x)/g(x) \in F : g(x) \neq 0, \deg f(x) < \deg g(x)\},$$

[1] In this thesis, we often let $p(x)$ denote the place $P_{p(x)}$ corresponding to a monic irreducible polynomial $p(x) \in \mathbf{F}_q[x]$.

it follows that its residue class field is isomorphic to $\mathbf{F}_q$. Consequently, P_∞ is a rational place of F.

Theorem 2.1.1 *The places corresponding to $p(x)$, where $p(x)$ is a monic irreducible polynomial of $\mathbf{F}_q[x]$ together with P_∞ described above constitute all the places of F.*

Proof: Refer to [72, Chapter I]. □

Remark 2.1.2 *The places $p(x)$ are often referred to as the finite places of F while P_∞, which is in fact a pole of x, is called the infinite place of F.*

Corollary 2.1.3 *The rational function field $F = \mathbf{F}_q(x)$ is maximal.*

Proof: By Theorem 2.1.1, all the finite rational places of F correspond to monic linear polynomials of F, that is, they are of the form $x - a, a \in \mathbf{F}_q$. Therefore, there are q finite rational places of F. Together with the infinite place P_∞, F has $q+1$ rational places in all, which is precisely the Hasse-Weil bound for $g = 0$. □

Let $f(x)$ be a nonconstant element in F. Write $f(x) = \alpha \prod_{i=0}^{t} p_i(x)^{e_i} \in F$ where $p_i(x)$'s are monic irreducible polynomials over $\mathbf{F}_q, \alpha \in \mathbf{F}_q$ and e_i are integers. It is clear that the principal divisor of $f(x)$ is given by

$$\operatorname{div}(f(x)) = \sum_{i=1}^{t} e_i p_i(x) - \deg f(x) P_\infty$$

which verifies Proposition 1.1.3 stating that $\deg \operatorname{div}(f(x)) = 0$.

Since the genus of F is 0, the L-polynomial of F is $L_F(t) = 1$ according to Lemma 1.5.3. Consequently, F has class number 1, i.e. every divisor of F of degree 0 is principal.

Finally, we prove that every extension of the rational function field with genus > 0 must be ramified, namely,

Lemma 2.1.4 *Let F'/F be an algebraic separable extension of global function fields with F being the rational function field $\mathbf{F}_q(x)$. Suppose that the genus of F' is positive. Then there must exist a place $P \in \mathbf{P}_F$ such that P is ramified in F'/F.*

Proof: Suppose to the contrary that all places of F are unramified in F'/F. This implies that the different $\mathrm{Diff}(F'/F)$ is 0. By the Hurwitz genus formula, the genus of F' is given by

$$2g(F') - 2 = [F' : F](2g(F) - 2) = -2[F' : F] \leq -2.$$

This clearly gives $g(F') \leq 0$ which contradicts our assumption. □

In the next two sections, we will discuss the properties of two of the most well-known Galois extensions of a global function field, one of which has degree relatively prime to p while the other has degree a power of p. For both of these extensions, F will denote a global function field of genus $g(F)$.

2.2 Kummer Extensions

Throughout this section, let n be a positive integer that divides $q-1$, in which case there exists an element $\zeta \in \mathbf{F}_q$ such that $\zeta^n = 1$. Since $\mathbf{F}_q^*$ is a cyclic group, we may assume that ζ is a primitive n-th root of unity, that is, $\zeta^n = 1$ and $\zeta^i \neq 1$ for $1 < i < n$.

For an element $f \in F$, f is said to be nth **Kummer non-degenerate** if f cannot be written in the form $f = g^m$ for some $g \in F$ and $m|n, m > 1$. The next lemma gives a

sufficient condition for f to be n-th Kummer non-degenerate.

Lemma 2.2.1 *Suppose that there is a place $P \in \mathbf{P}_F$ such that $\gcd(\nu_P(f), n) = 1$. Then, f is nth Kummer nondegenerate.*

Proof: Suppose not. Write $f = g^m$, where $g \in F$ and $m|n, m > 1$. Then,

$$\nu_P(f) = \nu_P(g^m) = m\nu_P(g)$$

which implies that $\gcd(\nu_P(f), n) = m$, a contradiction. □

Theorem 2.2.2 *Let f be an nth Kummer nondegenerate element of F. Suppose that y is a root of the polynomial $h(t) = t^n - f$. Then the extension $F' = F(y)$ is called a Kummer extension and the following hold:*

(i) *$h(t)$ is the minimal polynomial of y over F. Thus, $[F' : F] = n$.*

(ii) *The extension F'/F is Galois and cyclic. Furthermore, $\mathrm{Gal}(F'/F) = \{\sigma : \sigma(y) = \zeta^i y, i = 1, 2, \ldots, n\}$.*

(iii) *Let P be a place of F and P' a place of F' lying over it. Then $e(P'|P) = n/\gcd(\nu_P(f), n)$.*

(iv) *Suppose that there exists a place Q of F such that $\gcd(\nu_Q(f), n) = 1$, i.e. Q is totally ramified in F'/F. Then $\mathbf{F}_q$ is the full constant field of F'.*

Corollary 2.2.3 *Let F'/F be a Kummer extension as in Theorem 2.2.2. Assume further that there exists a place Q of F that is totally ramified in F'/F. Then the genus of F' is given by*

$$g(F') = 1 + n(g(F) - 1) + \frac{1}{2} \sum_{P \in \mathbf{P}_F} (n - \gcd(\nu_P(f), n)) \deg P.$$

Proof: Let P be a place of F and P' a place of F' lying over it. Since $\gcd(n,p)=1$, it follows from Theorem 2.2.2 and Proposition 1.1.10 that $d(P'|P) = n/\gcd(\nu_P(f),n) - 1$. Further,

$$\sum_{P'|P} f(P'|P) = n/e(P'|P) = \gcd(\nu_P(f),n).$$

Thus, the discriminant of F'/F is

$$D(F'/F) = \sum_{P\in\mathbf{P}_F} \gcd(\nu_P(f),n)(n/\gcd(\nu_P(f),n)-1)P = \sum_{P\in\mathbf{P}_F} (n-\gcd(\nu_P(f),n))P$$

and the genus is obtained from Corollary 1.1.13. □

Corollary 2.2.4 *Let q be odd. Let F be the rational function field $\mathbf{F}_q(x)$ and let $f \in \mathbf{F}_q[x]$ be a product of distinct monic irreducible polynomials. Suppose that $F' = F(y) = \mathbf{F}_q(x,y)$ with $y^2 = f(x)$. Then all conditions in Theorem 2.2.2 are satisfied and the genus of F' is given by*

$$g(F') = \begin{cases} (\deg f - 1)/2 & \text{if } \deg f \text{ is odd,} \\ (\deg f - 2)/2 & \text{if } \deg f \text{ is even} \end{cases}$$

Proof: Write $f = \alpha p_1(x)p_2(x)\dots p_t(x)$ as a product of monic irreducible polynomials $p_1(x),\dots,p_t(x)$ and $\alpha \in \mathbf{F}_q^*$. Since $\nu_{p_i(x)}(f) = 1$ for all $i = 1,\dots,t$, f is Kummer nondegenerate. Let P_∞ denote the infinite place of F. Then $\nu_{P_\infty}(f) = -\deg f$. Hence, Corollary 2.2.3 yields

$$g(F') = 1 + 2(0-1) + \frac{1}{2}(\sum_{i=1}^{t} \deg p_i(x) + (2 - \gcd(2,\deg f))$$

which gives the result. □

Remark 2.2.5 *Suppose that* $\deg f = 3$ *in Corollary* 2.2.4. *It follows that the genus of* F' *is* 1. *Such fields are known as* **elliptic function fields**.

In order to investigate the splitting behaviour of unramified places in such extensions, the following theorem may be helpful.

Theorem 2.2.6 *Let* F *be a global function field and* $F' = F(y)$, *with* $h(t)$ *being the minimal polynomial of* y *over* F. *Let* P *be a place of* F *that is unramified in* F'/F. *Suppose that* $h(t) \in O_P[t]$, *where* O_P *is the valuation ring of* P *in* F. *Factor* $h(t)$ *into a product of irreducible factors over* $\tilde{F}_P$, *namely,*

$$h(t) = \prod_{i=1}^{s} \gamma_i(t)^{\epsilon_i} \bmod P.$$

Let $\Gamma_i(t) \in F[t]$ *be such that* $\Gamma_i(t) = \gamma_i(t) \bmod P$ *for* $i = 1, \ldots, s$. *Then* $\epsilon_i = 1$ *for all* $i = 1, \ldots, s$ *and there are exactly* s *places* $P_1, \ldots, P_s$ *lying over* P, *where* P_i *is uniquely defined by the condition* $\Gamma_i(y) \in P_i$. *Further,* $f(P_i|P) = \deg \gamma_i(t)$ *for each* i.

Proof: This is in fact a special case of the Kummer's theorem (refer to [72, Chapter III]). □

Example 2.2.7 Let F be the rational function field $\mathbf{F}_7(x)$. Consider the field $F' = F(y)$, where

$$y^2 = f(x) = x^3 + 4x^2 + 3x + 2.$$

According to Theorem 2.2.2, F'/F is a Kummer extension with $[F' : F] = 2$. Applying Corollary 2.2.3, it is easy to see that $g(F') = 1$, i.e. F' is an elliptic function field. Next, we explore the splitting behaviour of the places of F in the extension. Since f has odd

degree, ∞ is ramified in F'/F. Clearly, we have the following congruences:

$$\begin{aligned} f(1) &\equiv 3 \bmod 7, \\ f(2) &\equiv f(3) \equiv f(5) \equiv 2^2 \bmod 7, \\ f(4) &\equiv f(6) \equiv 1^2 \bmod 7. \end{aligned}$$

By Theorem 2.2.6, $x+6$ is unramified and has a unique place Q lying over it with $f(Q|(x+6)) = 2$. All other finite rational places split completely in the extension. Consequently, F' has 13 rational places. F' is optimal since according to the Serre bound,

$$N_7(1) \leq 8 + \lfloor 2\sqrt{(7)} \rfloor = 13.$$

Similarly, we can check that the following places of degree 2 split completely in F'/F : $P_1 = x^2+1, P_2 = x^2+4, P_3 = x^2+2x+3, P_4 = x^2+2x+5, P_5 = x^2+6x+3, P_6 = x^2+6x+4$. Together with the place lying over $x+6$, F' has 13 places of degree 2.

Kummer extensions over different base fields have been used to construct global function fields with many rational places. See [55], [81] and [14] for some of these constructions.

2.3 Artin-Schreier Extensions

Apart from the Kummer extension, another field extension widely used in the construction of global function fields with many rational places is the Artin-Schreier extension ([77], [80] and [55]). We will now proceed to introduce this extension.

Define the Artin-Schreier operator on F by

$$\wp(z) = z - z^p, z \in F.$$

An element $f \in F$ is called **Artin-schreier non-degenerate** if f is not in the image of $\wp$.

For a place P of F, we define the Artin-Schreier reduced valuation of an element $f \in F$ by

$$\nu_P^*(f) = \max\{\nu_P(f - \wp(z)) : z \in F\}.$$

Lemma 2.3.1 *Let $f \in F$ and let P be a place of F. Then either $\nu_P^*(f) \geq 0$ or $\gcd(\nu_P^*(f), p) = 1$. Hence, we may define the integers m_P associated to P by*

$$m_P = \begin{cases} -1 & \text{if } \nu_P^*(f) \geq 0, \\ -\nu_P^*(f) & \text{otherwise} \end{cases}$$

As in Lemma 2.2.1, one checks easily that a sufficient condition for $f \in F$ to be Artin-Schreier nondegenerate is that there exists a place P of F such that $m_P > 0$.

Theorem 2.3.2 *Let f be an Artin-Schreier nondegenerate element of F. Consider the polynomial $h(t) = t^p - t - f \in F[t]$. Let y be a root of $h(t)$. Then the extension $F' = F(y)$ is called an* **Artin-Schreier extension** *and the following properties hold:*

(i) *$h(t)$ is the minimal polynomial of y and $[F' : F] = p$.*

(ii) *The extension F'/F is Galois and cyclic. Further,*

$$\mathrm{Gal}(F'/F) = \{\sigma : \sigma(y) = y + i, i = 0, 1, \ldots, p-1\}.$$

(iii) *For a place P of F, P is unramified in F'/F if and only if $m_P < 0$.*

(iv) *For a place P of F, P is totally ramified in F'/F if and only if $m_P > 0$. Let P' be a place of F' lying over P. Then, for $0 \leq j \leq m_P$, the ramification groups $G_j(P'|P)$ and $G^j(P'|P)$ are all equal to G. In particular, the conductor exponent $c_P = m_P + 1$ and the*

different exponent

$$d(P'|P) = (p-1)(m_P+1).$$

(v) *Suppose that there is a place P of F that is totally ramified in F'/F. Then $\mathbf{F}_q$ is the full constant field of F' and the genus of F' is given by*

$$g(F') = pg(F) + \frac{p-1}{2}\left(-2 + \sum_{P\in\mathbf{P}_F}(m_P+1)\deg P\right).$$

According to Theorem 2.3.2, a place P is unramified in the Artin-Schreier extension exactly when $\nu_P^*(f) \geq 0$. The next proposition gives the condition for P to split completely in F'/F.

Proposition 2.3.3 *Let F'/F be the Artin-Schreier extension with $F' = F(y)$ described in Theorem 2.3.2. Then a place P splits completely in F'/F if and only if $\nu_P^*(f) > 0$.*

Proof: First, suppose that $\nu_P^*(f) > 0$. By definition, there is an element $z \in F$ with $\nu_P(f - \wp(z)) > 0$. Let $f' = \wp(y-z)$. We have

$$\nu_P(f') = \nu_P((y-z)^p - (y-z)) = \nu_P(f-\wp(z)) > 0,$$

i.e. $f' \equiv 0 \bmod P$. Since $z \in F, F' = F(y) = F(y-z)$ and the minimal polynomial of $y-z$ over F is

$$h(t) = t^p - t - f'.$$

We can now apply Theorem 2.2.6 to conclude that P splits completely in F'/F. Conversely, assume that P splits completely in F'/F. Then $\nu_P^*(f) \geq 0$ since P is unramified in F'/F. Therefore, there exists $z \in F$ with $F' = F(y-z)$ and $\nu_P(f-\wp(z)) \geq 0$. Let $f' = f - \wp(z)$. Clearly, $\nu_P^*(f) = \nu_P^*(f')$ and the minimal polynomial of $y-z$ over F is $h'(t)$, where $h'(t)$ is

defined as before. Since $\nu_P(f') \geq 0$, using Theorem 2.2.6, $h'(t) \bmod P$ has a root $z' \in \tilde{F}_P$. Thus,

$$\nu_P^*(f') \geq \nu_P(f' - \wp(z')) > 0$$

and the proof is complete. □

Remark 2.3.4 *Similarly, we can define Artin-Schreier extensions of order p^k for some integer k. In this case, we define the Artin-Schreier operator by letting $\wp(z) = A(z)$, where $A(z)$ is a linearized polynomial in z. (See [72] for details.)*

2.4 Cyclotomic Function Fields

We pointed out in the introduction that algebraic function fields are analogs of algebraic number fields. In this section, we discuss the cyclotomic function fields which, in many aspects, have properties that mirror those of cyclotomic number fields. In fact, the theory of cyclotomic function fields owes its origin to a paper by Carlitz in 1938 that introduced the Carlitz module [6]. Motivated by this idea, Hayes constructed the cyclotomic function fields and showed that these fields describe all the maximal abelian extensions of rational function fields [24].

In what follows, let F be the rational function field $F = \mathbf{F}_q(x)$ and R the ring of polynomials $\mathbf{F}_q[x]$. Let $\bar{F}$ denote a fixed algebraic closure of F.

Our first aim is to endow the additive group of $\bar{F}$ with an R-module structure. To do this, let ρ be an endomorphism on $\bar{F}$ defined by

$$\rho(z) = z^q + xz = \rho_1(z) + \rho_2(z)$$

for all $z \in \bar{F}$. Observe that ρ_1 and ρ_2 are themselves endomorphisms on $\bar{F}$ which satisfy the relationship

$$\rho_1 \circ \rho_2 = \rho_2^q \circ \rho_1.$$

Now define a map $R \to \mathrm{End}(\bar{F})$ by setting $x \mapsto \rho$, and then extending it to the whole of R, namely,

$$f \mapsto \rho(f)$$

for all $f \in R$. Further, we define the following R-action: Given any $z \in \bar{F}, f \in R$, let $z^f = f(\rho(z))$ and for any $\alpha \in \mathbf{F}_q$, let $z^\alpha = \alpha z$.

Lemma 2.4.1 *The R-action defined above turns the additive group of $\bar{F}$ into an R-module.*

Next, we wish to express z^f as a polynomial in z explicitly. In the remainder of this section, M will always denote a monic polynomial in R. Moreover, let M have the factorization

$$M = \prod_{i=1}^{t} P_i^{e_i},$$

where the P_i's are distinct monic irreducible polynomials in R.

Lemma 2.4.2 *z^M can be expressed in the form*

$$z^M = \sum_{i=0}^{d} [M, i] z^{q^i},$$

where $d = \deg M$ and each $[M, i]$ is a polynomial in x satisfying the following properties:

(i) *$[M, i] = 0$ if $i < 0$ or $i > d$;*

(ii) *$[M, 0] = M$ and $[M, d] = 1$;*

(iii) *$[M, i]$ has degree $q^i(d - i)$ for $1 \leq i \leq d - 1$.*

Proof: In view of Lemma 2.4.1, we will only show this lemma for the case $M = x^l$ for some integer l. We prove it by induction on l. The cases $l = 0$ and $l = 1$ are trivial. Assume that the result holds for $l - 1$. Write

$$z^{x^{l-1}} = \sum_{i=0}^{l-1} [x^{l-1}, i] z^{q^i}.$$

Then,

$$\begin{aligned} z^{x^l} &= (z^{x^{l-1}})^x \\ &= \sum_{i=0}^{l-1} ([x^{l-1}, i] z^{q^i})^x \\ &= (\sum_{i=0}^{l-1} ([x^{l-1}, i] z^{q^i})^q + x \sum_{i=0}^{l-1} ([x^{l-1}, i] z^{q^i}) \\ &= \sum_{i=0}^{l} ([x^{l-1}, i-1]^q + x[x^{l-1}, i]) z^{q^i}. \end{aligned}$$

Thus, $[x^l, i] = 0$ for $i < 0$ and $i > l$. For $0 \leq i \leq l$,

$$[x^l, i] = [x^{l-1}, i-1]^q + x[x^{l-1}, i].$$

Using our induction hypothesis, it is straightforward to check that (ii) and (iii) hold for l. □

Consider the set Λ_M to be the subset of $\bar{F}$ consisting of all the M-torsion points, i.e.

$$\Lambda_M = \{z \in \bar{F} : z^M = 0\}.$$

As R is commutative, Λ_M is an R-module as well. Our task in the next proposition is to give a more precise structure of Λ_M.

Proposition 2.4.3 (i) Λ_M *is finite and is a vector space over* $\mathbf{F}_q$ *of dimension* $\deg M$.

(ii) $\Lambda_M \cong \bigoplus_{i=1}^{t} \Lambda_{P_i^{e_i}}$.

(iii) Λ_M *is a cyclic* R*-module isomorphic to* $R/(M)$.

Proof:

(i) Writing z^M as a polynomial in z as in Lemma 2.4.2, we see that its derivative is M which is nonzero. Hence, z^M is separable and has exactly $q^{\deg M}$ roots in $\bar{F}$. Since Λ_M is a module over $\mathbf{F}_q$, it is a vector space over $\mathbf{F}_q$ of dimension $\deg M$.

(ii) Since each $\Lambda_{P_i^{e_i}}$ is a P_i-primary component of Λ_M, the result follows directly from the general theory of modules over principal ideal domains.

(iii) We will show that each $\Lambda_{P_i^{e_i}}$ is cyclic and is isomorphic to $R/(P_i^{e_i})$ as an R-module. The general result can be deduced from (ii) above. For simplicity, we show that Λ_{P^e} is cyclic and isomorphic to $R/(P^e)$, where P is a monic irreducible polynomial in R of degree d. We prove by induction on e. From (i), Λ_P is the finite field $\mathbf{F}_{q^d}$ which is certainly cyclic and isomorphic to $R/(P)$. So we assume that the result is true for $e-1$. Define a map $\psi : \Lambda_{P^e} \to \Lambda_{P^{e-1}}$ such that $\alpha \mapsto \alpha^P$. ψ is clearly surjective with kernel Λ_P. By our induction hypothesis, $\Lambda_{P^{e-1}}$ is cyclic. Let $\lambda \in \Lambda_{P^e}$ be such that $\psi(\lambda)$ is the generator of $\Lambda_{P^{e-1}}$. Now, pick any $\alpha \in \Lambda_{P^e}$. Then there exists $f \in R$ with $\alpha^P = (\lambda^P)^f = \lambda^{Pf}$. Thus, $(\alpha - \lambda^f)^p = 0$ which implies that $\alpha - \lambda^f$ lies in the kernel of ψ. We have already shown that Λ_P is cyclic and it is easy to see that $\lambda^{P^{e-1}}$ generates Λ_P. Consequently, $\alpha - \lambda^f = \lambda^{P^{e-1}g} = \lambda^{f+P^{e-1}g}$ for some $g \in R$.

This shows that Λ_{P^e} is cyclic and we are done. Finally, the map that takes $f \bmod P^e$ in $R/(P^e)$ to $\lambda^f \in \Lambda_{P^e}$ is an isomorphism between the R-modules. □

Lemma 2.4.4 (i) *The set of generators of* Λ_M *is in 1 to 1 correspondence with* $(R/(M))^*$.

More specifically, Suppose that λ is any generator of Λ_M. $f \in (R/(M))^*$ if and only if λ^f is also a generator of Λ_M.

(ii)

$$\Phi(M) = |(R/(M))^*| = \prod_{i=1}^{t}(q^{\deg P_i} - 1)q^{\deg P_i(e_i-1)}.$$

Proof: (i) Let $f \in (R/(M))^*$. Since $\gcd(f, M) = 1$, there exist polynomials u and v such that $fu + vM = 1$. Hence,

$$\lambda = \lambda^{uf+vM} = \lambda^{uf} + \lambda^{vM} = \lambda^{uf}.$$

Therefore, λ^f is a generator of $(R/(M))^*$. Conversely, suppose that λ^f is a generator of Λ_M for some $f \in R$. We need to show that $\gcd(f, M) = 1$. Suppose not. Let $\gcd(f, M) = u$. We then have

$$\lambda^{fM/u} = (\lambda^f)^{M/u} = (\lambda^M)^{f/u} = 0,$$

contrary to our assumption that λ^f is a generator of λ_M. Consequently, $f \in (R/(M))^*$ and the bijection is established.

(ii) This is trivial. □

Let $F' = F(\Lambda_M)$ be the splitting field of z^M over F. Then, F'/F is an abelian, finite and separable extension by Proposition 2.4.3. In fact, F'/F is a simple extension, namely, we can write $F' = F(\lambda)$ for some generator $\lambda \in \Lambda_M$.

Definition 2.4.5 The splitting field of z^M over F is called the **cyclotomic function field** with modulus M.

Lemma 2.4.6 *$F(\Lambda_M)$ is a compositum of the fields $F(\Lambda_{P_1^{e_1}}), \ldots, F(\Lambda_{P_t^{e_t}})$.*

Proof: Since for each $i, 1 \leq i \leq t, \Lambda_{P_i^{e_i}} \subseteq \Lambda_M$, the field $F(\Lambda_{P_i^{e_i}})$ is a subfield of $F(\Lambda_M)$. This implies that $F(\Lambda_{P_1^{e_1}})F(\Lambda_{P_2^{e_2}}) \ldots F(\Lambda_{P_t^{e_t}})$ is a subfield of $F(\Lambda_M)$. Conversely, by Proposition 2.4.3 (ii), if λ is a generator of Λ_M, we can find $\lambda_1, \ldots, \lambda_t, \lambda_i \in \Lambda_{P_i^{e_i}}$ such that $\lambda = \lambda_1 + \cdots + \lambda_t$. Thus, $F(\Lambda_M)$ is a subfield of the compositum of the fields and the lemma is proved. □

In view of Lemma 2.4.6, we will next investigate $F(\Lambda_{P^n})$ for a monic irreducible polynomial P of degree d and positive integer n. Note that for a monic irreducible polynomial Q of R, we will also denote by Q its zero place.

Lemma 2.4.7 *Let $F' = F(\Lambda_{P^n})$. Let λ be any generator of Λ_{P^n}. Then $\nu_{P'}(\lambda) \geq 0$ for any place P' of F' lying over P and $\nu_{P'}(\lambda)$ is identical for any λ. Further, if Q is a place of F different from P, then, $\nu_{Q'}(\lambda) = 0$ for any place Q' of F' lying over Q.*

Proof: According to Lemma 2.4.2, we can express λ^{P^n} as

$$\lambda^{P^n} = P^n\lambda + [P^n, 1]\lambda^q + \cdots + \lambda^{q^{dn}} = 0.$$

Since each $[P^n, i]$ is a polynomial in x, $\nu_{P'}([P^n, i]) \geq 0$. Suppose that $\nu_{P'}(\lambda) < 0$. Then it is clear that $\nu_{P'}(\lambda^{q^{dn}}) < \nu_{P'}([P^n, i]\lambda^{q^i})$ for all $0 \leq i \leq dn - 1$. By the strict triangle inequality, this yields $\nu_{P'}(\lambda^{P^n}) < 0 \neq \infty$. Thus, $\nu_{P'}(\lambda) \geq 0$. Now, let λ^f be another generator of Λ_M. By Lemma 2.4.4, $\gcd(f, P) = 1$. As before, we write

$$\lambda^f = f\lambda + \cdots + \lambda^{q^{\deg f}}.$$

Assume first that $\nu_{P'}(\lambda) > 0$. Since $\nu_{P'}(f) = 0, \nu_{P'}(f\lambda) < \nu_{P'}([f, i]\lambda^{q^i})$ for all $0 < i \leq \deg f$ and so $\nu_{P'}(\lambda^f) = \nu_{P'}(\lambda)$ by the strict triangle inequality. On the other hand, if

$\nu_{P'}(\lambda) = 0$, $\nu_{P'}(\lambda^f)$ must be 0 for otherwise, replacing λ by λ^f and from what we have just established, $\nu_{P'}(\lambda) > 0$.

Similarly, we can show that for a place Q of F different from P, $\nu_{Q'}(\lambda) \geq 0$. Suppose that $\nu_{Q'}(\lambda) > 0$. Since $\nu_{Q'}(P^n) = 0, \nu_{Q'}(P^n\lambda) < \nu_{Q'}([P^n, i]\lambda^{q^i})$ for $1 \leq i \leq dn$. Once again by the strict triangle inequality, we have $\nu_{Q'}(\lambda^{P^n}) = \nu_{Q'}(\lambda) < \infty$. Consequently, $\nu_{Q'}(\lambda) = 0$. □

The above lemma helps us to study the ramification behaviour of places in the extension F'/F.

Theorem 2.4.8 *Let λ be a fixed generator of Λ_{P^n}.*

(i) $\gamma(z) = \frac{z^{P^n}}{z^{P^{n-1}}}$ *is Eisenstein at P. In particular, P is totally ramified in $F(\Lambda_{P^n})/F$ and $[F(\Lambda_{P^n}) : F] = (q^d - 1)q^{d(n-1)}$. λ is a local parameter at P' for the unique place $P'|P$ with $\gamma(z)$ as its minimal polynomial.*

(ii) $\mathrm{Gal}(F(\Lambda_{P^n})/F)$ *is isomorphic to $(R/(M))^*$.*

(iii) *Any other place Q of F different from P is unramified in $F(\Lambda_{P^n})/F$.*

(iv) *Let Q be any place of F different from P. Then the Artin symbol (c.f. page 19) of Q sends λ to λ^Q.*

Proof: (i) For any $f \in (R/(P^n))^*$, since λ^f is a generator of Λ_{P^n} by Lemma 2.4.4, $\gamma(\lambda^f) = 0$. As $|(R/(P^n))^*| = \Phi(P^n) = (q^d - 1)q^{d(n-1)}$, after a comparison of degrees, we deduce that $\gamma(z)$ can be expressed as

$$\gamma(z) = \prod_{f \in (R/(P^n))^*} (z - \lambda^f).$$

Note that $\lambda^{P^n} = (\lambda^{P^{n-1}})^P = P\lambda^{P^{nn-1}} + \ldots$, and it is therefore easy to see that the

constant term in $\gamma(z)$ is P. By comparing the constant terms of the expressions of $\gamma(z)$ yields

$$P = \pm \prod_{f \in (R/(P^n))^*} \lambda^f. \tag{2.1}$$

Since $\nu_{P'}(P) > 0$, it follows that at least one, and hence all of the $\lambda^f \in P'$. Consequently, all the coefficients in $\gamma(z)$, except for the leading coefficient, lie in P'. But $\gamma(z) \in R[z]$ which implies that these coefficients actually lie in P. As a consequence, $\gamma(z)$ is Eisenstein at P. From equation (2.1), we obtain $\nu_{P'}(P) = \Phi(P^n) = \Phi(P^n)\nu_{P'}(\lambda)$. Thus, $\nu_{P'}(\lambda) = 1$, i.e. λ is a local parameter at P. The remaining assertions follow from

Lemma 1.1.17.

(ii) Let $\sigma \in \mathrm{Gal}(F(\Lambda_{P^n})/F)$. Then $\sigma(\lambda)$ is a root of $\gamma(z)$ and so $\sigma(\lambda) = \lambda^f$ for some $f \in (R/(P^n))^*$. It can then be directly verified that the map sending σ to f provides an isomorphism between $\mathrm{Gal}(F(\Lambda_{P^n})/F)$ and $(R/(P^n))^*$.

(iii) Replacing λ by α for any $\alpha \in \Lambda_{P^n}$ in the proof of Lemma 2.4.7, we can likewise show that $\nu_{Q'}(\alpha) = 0$. Since $\gamma'(\lambda) = \prod_{f \in (R/(P^n))^*, f \neq 1}(\lambda - \lambda^f)$, $\nu_{Q'}(\gamma'(\lambda)) = 0$. Applying Proposition 1.1.18 gives us our result.

(iv) Let σ denote the Artin symbol of Q. Suppose that $\sigma(\lambda) = \lambda^f$ for some $f \in R$. By the definition of Artin symbols, $\lambda^f \equiv \lambda^{q^{d'}} \bmod Q'$, where Q' is a place of F' lying over Q and $d' = \deg Q$. From the proof of (i), we can conclude that for any monic irreducible polynomial $P_0 \in R$, $P_0 | [P_0^l, i]$ for all $0 \leq i < l \deg P_0 - 1$ and any positive integer l. Hence, $\lambda^Q \equiv \lambda^{q^{d'}} \bmod Q'$. Since $\nu_{Q'}(\lambda^Q - \lambda^f) = \nu_{Q'}(\lambda^{Q-f}) = 0$ for $Q \neq f$, i.e. $\lambda^f \bmod Q \neq \lambda^Q \bmod Q$, we conclude that $Q = f$. □

Remark 2.4.9 *As in the cyclotomic number field case, we can show that the integral*

closure of O_P in $\mathbf{F}'$ is $O_{P'} = O_P[\lambda]$ for any generator λ of Λ_{P^n}.

By employing the technique of Newton polygons, we can determine the ramification behaviour of the infinite place ∞ of F. For a proof of the next theorem, we refer the reader to [24] or [55].

Theorem 2.4.10 *The decomposition group and inertia group of ∞ are both isomorphic to $\mathbf{F}_q^*$. More precisely, there are exactly $\frac{\Phi(P^n)}{q-1}$ places of $F(\Lambda_{P^n})$ lying over ∞, each of which has ramification index $q-1$.*

We have developed the necessary results to calculate the genus of $F(\Lambda_{P^n})$ which we shall proceed to do.

Theorem 2.4.11 (i) *Let P' be the unique place of $F(\Lambda_{P^n})$ lying over P. Then,*

$$d(P'|P) = q^{d(n-1)}(nq^d - n - 1).$$

(ii) *The genus of $F(\Lambda_{P^n})$ is given by*

$$2g(F(\Lambda_{P^n})) - 2 = q^{d(n-1)}\left((qdn - dn - q)\frac{q^d - 1}{q-1} - d\right).$$

Proof: (i) From Proposition 1.1.18 and Theorem 2.4.8, $d(P'|P) = \nu_{P'}(\gamma'(\lambda))$. Now, differentiating the equation

$$z^{P^n} = Z^{P^{n-1}}\gamma(z)$$

yields

$$\gamma'(\lambda) = P^n - \lambda^{P^{n-1}}.$$

Therefore,

$$\nu_{P'}(\gamma'(\lambda)) = n\Phi(P^n) - q^{d(n-1)} = q^{d(n-1)}(nq^d - n - 1).$$

(ii) The only other ramified place in the extension is ∞, which by Theorem 2.4.10 has ramification index $e(P_\infty|\infty) = q-1$ for any place P_∞ lying over ∞. Since $q-1$ is coprime to p, $d(P_\infty|\infty) = q-2$ and the genus of F' can now be obtained via the Hurwitz genus formula. □

Finally, we return to the general case where M is any arbitrary monic polynomial. Lemma 2.4.6 tells us that $F(\Lambda_M)$ is the compositum of the subfields $F(\Lambda_{P_i^{e_i}}), i = 1, \ldots, t$. Since P_i is ramified only in the component $F(\Lambda_{P_i^{e_i}})$, each $F(\Lambda_{P_i^{e_i}})$ is disjoint from the compositum of the remaining fields. Armed with this fact and the results we have attained so far, the following assertions can be directly established.

Theorem 2.4.12 *Consider the cyclotomic function field $F' = F(\Lambda_M)$.*

(i) $[F' : F] = \Phi(M)$ *and* $\mathrm{Gal}(F'/F) \cong (R/(M))^*$.

(ii) *Only the places $P_1, \ldots, P_t$ are ramified in F'/F. If P_i' is a place of F' lying over $P_i, i = 1, \ldots, t$, $e(P_i'|P_i) = \Phi(P_i^{e_i})$.*

(iii) *The decomposition group and the inertia group of ∞ are both isomorphic to $\mathbf{F}_q^*$.*

(iv) *The genus of F' is given by*

$$2g(F') - 2 = \Phi(M)[-2 + \frac{q-2}{q-1} + \sum_{i=1}^{t} (\deg P_i) q^{\deg P_i (e_i - 1)} (e_i q^{\deg P_i} - e_i - 1)/\Phi(P_i^{e_i})].$$

We will conclude this section by providing an example of a cyclotomic function field in which the number of rational places it contains is relatively large.

Example 2.4.13 $g(F'/\mathbf{F}_2) = 78, N(F'/\mathbf{F}_2) = 49$. Let F be the rational function field $F = \mathbf{F}_2(x)$. Let $M = (x^3 + x + 1)(x^3 + x^2 + 1) \in \mathbf{F}_2[x]$. Then, $\Phi(M) = 49$. Let F' be the

cyclotomic function field with modulus M, i.e. $F' = F(\Lambda_M)$. By Theorem2.4.12 (iv),

$$g(F') = 49(-2 + 3(6)/7 + 3(6)/7) = 78.$$

Since $q - 1 = 1, \infty$ splits completely in F'/F. Consequently, $N(F') \geq [F' : F] = 49$. The Osterl'e bound for $N_2(78)$ is 57. Therefore, x and $x + 1$ cannot split in F' and we have $N(F') = 49$. This example improves the lower bound of 48 given in [55, Table 4.5.2].

Chapter 3

Examples of Explicit Class Fields

The task of finding global function fields with many rational places was initiated by Serre who used methods from general class field theory to exhibit such fields [66], [67]. Later, several researchers including Schoof [63], Auer [2], [3], [4], Lauter [32, 33, 34, 35], Niederreiter and Xing [41, 42, 43, 44, 46, 48, 55], as well as many others employ some class fields, namely ray class fields and narrow ray class fields to seek for more constructions.

The aim of this present chapter is to summarize some of the main properties of ray class fields and narrow ray class fields. Most of the details have been left out since they can be readily found in the literature. As in the preceding chapters, we follow many of the notations used in [55].

3.1 General results of Class Field Theory

Before we can delve into the various class fields, we need some general results from class field theory. For background and further results on class field theory, we refer to the books

of Cassels and Fröhlich [8], Neukirch [40], Serre [65], and Weil [86].

We will continue to work with a global function field $F/\mathbf{F}_q$. For any place P of F, recall that F_P is the P-adic completion of F at P. For the valuation ring O_P of F_P, let $U_P = O_P^*$ be the unit group of F_P. Then for any positive integer n, we define the nth **unit group of** P to be the subgroup of U_P such that

$$U_P^{(n)} = \{x \in O_P : \nu_P(x-1) \geq n\}.$$

We also write $U_P^{(0)}$ for U_P. Clearly, $U_P = \mathbf{F}_q^* \times U_P^{(1)}$.

Definition 3.1.1 An **idèle** α of F is an element of $\prod_{P \in \mathbf{P}_F} F_P^*$ such that if $\alpha = (\alpha_P)_{P \in \mathbf{P}_F}$, then $\alpha_P \in U_P$ for all but finitely many $P \in \mathbf{P}_F$. The group of all idèles of F is known as the idèle group of F and is denoted by J_F.

Since each element $f \in F^*$ has finitely many zero and pole places, we can embed F^* into J_F diagonally and identify F^* with the image of this embedding. The factor group J_F/F^* is called the **idèle class group** of F and will be denoted by C_F.

For a finite abelian extension F' of F, the idèle group J_F can be considered as a subgroup of $J_{F'}$ by identifying each element $\alpha = (\alpha_P) \in J_F$ with $\beta = (\beta_Q) \in J_{F'}$, where $\beta_Q = \alpha_P$ for all $Q|P$. Since $J_F \cap F'^* = F^*, C_F$ can be viewed as a subgroup of $C_{F'}$ as well.

The norm map $N_{F'/F}$ from F' to F can be extended to $J_{F'}$ to J_F, (also denoted by $N_{F'/F}$) by defining

$$N_{F'/F}((\beta_Q)) = (\prod_{Q|P} N_{F'/F}(\beta_Q)) \in J_F$$

for all $(\beta_Q) \in J_{F'}$. Clearly, $N_{F'/F}$ induces a norm map $N_{F'/F} : C_{F'} \to C_F$.

Theorem 3.1.2 *Let F'/F be a finite abelian extension with $P'|P$ as before. There exists a* **local Artin reciprocity map** $\theta_{F'_{P'}/F_P} : F_P^* \longrightarrow \mathrm{Gal}(F'_{P'}/F_P) = G_{-1}(P'|P)$ *such that:*

(i) $\mathrm{Ker}(\theta_{F'_{P'}/F_P}) = \mathrm{N}_{F'/F}((F'_{P'})^*), \quad \mathrm{im}(\theta_{F'_{P'}/F_P}) = \mathrm{Gal}(F'_{P'}/F_P)$.

(ii) If $F'_{P'}/F_P$ *is unramified, i.e.* $G_0(F'_{P'}/F_P) = \{1\}$, *then* $\theta_{F'_{P'}/F_P}(x) = \pi^{\nu_P(x)}$ *for all* $x \in F_P$, *where* π *is the Frobenius automorphism.*

(iii) $\theta_{F'_{P'}/F_P}$ *maps the i th unit group* $U_P^{(i)}$ *of* F_P *onto the i th upper ramification group* $G^i(F'_{P'}/F_P) = G^i(P'|P)$ *for all integers* $i \geq 0$.

Notice that since F'/F is abelian, the choice of P' is immaterial and we can write θ_P to mean $\theta_{F'_{P'}/F_P}$. From (iii) of the above theorem, we see immediately that a place P of F is unramified in F'/F if the local Artin reciprocity map sends the unit group U_P to $\{1\}$.

Next we define the **global Artin reciprocity map** to be the product of the local Artin reciprocity maps, namely $\theta_{F'/F} : J_F \to \mathrm{Gal}(F'/F)$ such that

$$\theta_{F'/F} = \prod_{P \in \mathbf{P}_F} \theta_P.$$

With this definition, for $\alpha = (\alpha_P) \in J_F$,

$$\theta_{F'/F}(\alpha) = \prod_{P \in \mathbf{P}_F} \theta_P(\alpha_P).$$

This definition is well-defined since $\theta_P(\alpha_P) = \pi_P^{\nu_P(\alpha_P)}$ when P is unramified, and $\nu_P(\alpha_P) = 0$ if $\alpha_P \in U_P$. So $\theta_P(\alpha_P) = 1$ for all but finitely many $P \in \mathbf{P}_F$.

Theorem 3.1.3 *The global Artin reciprocity map* $\theta_{F'/F}$ *is a surjective homomorphism from* J_F *to* $\mathrm{Gal}(F'/F)$. *It has kernel* $F^* N_{F'/F}(J_{F'})$. *Hence, it induces a surjective map*

$$(\cdot, F'/F) : C_F \to \mathrm{Gal}(F'/F)$$

with kernel $N_{F'/F} = F^* N_{F'/F}(J_{F'})/F^* = F^* \mathcal{N}_{F'/F}(C_{F'})$.

Definition 3.1.4 $(\cdot, F'/F)$ defined in Theorem 3.1.3 is known as the **norm residue symbol** of F'/F.

The following is an important theorem relating finite abelian extensions of F and subgroups of C_F.

Theorem 3.1.5 (i) (*Artin Reciprocity*) *For any finite abelian extension F'/F of global function fields, there is a canonical isomorphism*

$$C_F/\mathcal{N}_{F'/F} \simeq \mathrm{Gal}(F'/F)$$

induced by the norm residue symbol $(\cdot, F'/F)$.

(ii) (*Existence Theorem*) *For every (open) subgroup X of C_F of finite index, there exists a unique finite abelian extension F' of F such that F' is contained in the abelian closure F^{ab} of F and $\mathcal{N}_{F'/F} = X$.*

(iii) *Given two finite abelian extensions E_1/F and E_2/F in F^{ab}, we have $E_1 \subseteq E_2$ if and only if $\mathcal{N}_{E_1/F} \supseteq \mathcal{N}_{E_2/F}$, i.e. if and only if $F^* \cdot \mathrm{N}_{E_1/F}(J_{E_1}) \supseteq F^* \cdot \mathrm{N}_{E_2/F}(J_{E_2})$.*

Proposition 3.1.6 *Let X be an open subgroup of C_F of finite index and let F' be the finite abelian extension of F so that $\mathcal{N}_{F'/F} = X$. Suppose that H is a subgroup of J_F such that $X = H/F^*$. For a place $P \in \mathbf{P}_F$, the following hold:*

(i) *P is unramified in F'/F if and only if $U_P \subseteq H$;*

(ii) *P splits completely in F'/F if and only if $F_P^* \subseteq H$.*

3.2 Ray Class Fields

We have seen in Section 3.1 that open subgroups of the idèle class group give rise to finite abelian extensions of F. Our goal in this section, as well as the next, will be to define suitable subgroups of C_F and study the properties of the corresponding class fields. Note that all subgroups of C_F considered here will be open.

Let $\mathcal{S}$ be a subset of $\mathbf{P}_F$ so that $\mathcal{S}' = \mathbf{P}_F - \mathcal{S}$ is nonempty and finite. For an effective divisor D of F with $\mathrm{supp}(D) \cap \mathcal{S}' = \emptyset$, we define $J_{\mathcal{S}}^D$ to be the group

$$J_{\mathcal{S}}^D = \prod_{P \in \mathcal{S}'} F_P^* \times \prod_{P \in \mathcal{S}} U_P^{(\nu_P(D))}$$

and

$$C_{\mathcal{S}}^D = F^* J_{\mathcal{S}}^D / F^*.$$

Clearly, $C_{\mathcal{S}}^D$ is a subgroup of C_F and we call it the idèle $\mathcal{S}$-ray class group with modulus D.

From these definitions of $J_{\mathcal{S}}^D$ and $C_{\mathcal{S}}^D$, we easily obtain the following lemma.

Lemma 3.2.1 *Let $\mathcal{T} \subseteq \mathbf{P}_F$ with $\mathcal{T}' = \mathbf{P}_F - \mathcal{T}$ nonempty and finite. Suppose that D' is another positive divisor of F such that* $\mathrm{supp}(D') \subseteq \mathcal{T}$.

(i) *If $\mathcal{S} \subseteq \mathcal{T}$ and $D \leq D'$, then $C_{\mathcal{T}}^{D'} \subseteq C_{\mathcal{S}}^D$.*

(ii) $C_{\mathcal{S}}^D C_{\mathcal{T}}^{D'} = C_{\mathcal{S}\cap\mathcal{T}}^{\min(D,D')}$, *where the minimum is taken coefficientwise.*

(iii) $J_{\mathcal{S}}^0 / J_{\mathcal{S}}^D \cong \prod_{P \in \mathrm{supp}(D)} U_P / U_P^{(\nu_P(D))}$ *and has order $\Phi(D)$, where $\Phi(D)$ is as defined in Lemma* 2.4.4.

Recall that $O_{\mathcal{S}}^*$ is the group of $\mathcal{S}$-units of F.

Proposition 3.2.2 (i) *The sequence*

$$O_{\mathcal{S}}^* \to J_{\mathcal{S}}/J_{\mathcal{S}}^D \to C_F/C_{\mathcal{S}}^D \cong J_F/\left(F^* \cdot J_{\mathcal{S}}^D\right) \to C_F/C_{\mathcal{S}}^0 \cong J_F/(F^* \cdot J_{\mathcal{S}^0}) \to 1$$

is exact.

(ii) $C_F/C_{\mathcal{S}}^D$ *is isomorphic to* $\mathrm{Cl}_D(O_{\mathcal{S}})$.

This proposition immediately implies that the group $C_{\mathcal{S}}^D$ is of finite index in C_F. Thus, by Theorem 3.1.5, there exists a field $F_{\mathcal{S}}^D$ of F with Galois group

$$\mathrm{Gal}(F_{\mathcal{S}}^D/F) \cong C_F/C_{\mathcal{S}}^D \cong \mathrm{Cl}_D(O_{\mathcal{S}}).$$

We call such a field the **ray class field** with modulus D. By Proposition 3.1.6 and the definition of $C_{\mathcal{S}}^D$, every place in $\mathcal{S}'$ splits completely in $F_{\mathcal{S}}^D/F$ and all places outside the support of D are unramified in this extension. In fact, we can determine the conductor of the extension too.

Lemma 3.2.3 *Let F'/F be a finite abelian extension of global function fields. Suppose that $\mathcal{S} \subseteq \mathbf{P}_F$ is such that $\mathcal{S}' = \mathbf{P}_F - \mathcal{S}$ is nonempty and finite and that all places in $\mathcal{S}'$ split completely in F'/F. Then the conductor of F'/F is the smallest positive divisor D with support in $\mathcal{S}$ such that $F' \subseteq F_{\mathcal{S}}^D$. In particular, the conductor of $F_{\mathcal{S}}^D$ is D.*

We record all the main properties of $F_{\mathcal{S}}^D$ in the next theorem.

Theorem 3.2.4 ***[Properties of ray class fields]***

(i) $F_{\mathcal{S}}^D$ *is the largest finite abelian extension F' of F in which all places in $\mathcal{S}'$ split completely in F'/F and the conductor of $F'/F \leq D$.*

(ii) *The Galois group* $\mathrm{Gal}(F_{\mathcal{S}}^D/F) \cong \mathrm{Cl}_D(O_{\mathcal{S}})$.

(iii) *All places of F outside the support of D are unramified in $F_{\mathcal{S}}^{D}/F$ and for each such place P, its Artin symbol corresponds to the residue class of P in $\mathrm{Cl}_D(O_{\mathcal{S}})$ under the correspondence in* (ii).

(iv) *The full constant field of $F_{\mathcal{S}}^{D}$ is $\mathbf{F}_{q^d}$, where $d = \deg \mathcal{S}$.*

(v) *Let $\mathcal{T}$ and D' be as in Lemma* 3.2.1. *If $\mathcal{S} \subset \mathcal{T}$ and $D \leq D'$, then $F_{\mathcal{S}}^{D} \subseteq F_{\mathcal{T}}^{D'}$. Moreover, $F_{\mathcal{S}}^{D} \cap F_{\mathcal{T}}^{D'} = F_{\mathcal{S}\cap\mathcal{T}}^{\min(D,D')}$.*

In the case when $D = 0$, $F_{\mathcal{S}}^{0}$ is, by the preceding theorem, characterized by the property that it is the largest finite abelian unramified extension of F in which all places in $\mathcal{S}'$ split completely. This is the **$\mathcal{S}$-Hilbert class field** discussed in [60]. The $\mathcal{S}$-Hilbert class field will usually be denoted by $H_{O_{\mathcal{S}}}$. Suppose that $\mathcal{S}'$ consists of a single rational place ∞. From Theorem 3.2.4 (ii) and Corollary 1.4.4, the Galois group of $H_{O_{\mathcal{S}}}/F$ is

$$\mathrm{Gal}(H_{O_{\mathcal{S}}}/F) \cong \mathrm{Cl}(O_{\mathcal{S}}) \cong \mathrm{Cl}(F)$$

and consequently, $[H_{O_{\mathcal{S}}} : F] = h(F)$, the class number of F.

Example 3.2.5 We have seen from Lemma 2.1.4 that all extensions of the rational function fields are ramified. Consequently, the $\mathcal{S}$-Hilbert class field of $\mathbf{F}_q(x)$ is $\mathbf{F}_{q^d}(x)$, where $d = \deg \mathcal{S}$.

Next, we wish to provide a formula to help us calculate the genus of the $\mathcal{S}$-ray class field $F_{\mathcal{S}}^{D}$. Looking at Corollary 1.3.4 suggests that it suffices to know the degrees $[F^n : F]$, where F^n is the nth upper ramification field of P with respect to the extension $F_{\mathcal{S}}^{D}/F$ and P is a place in the support of D.

Write D as $D = \sum_{P\in\mathbf{P}_F} m_P P$. We use the notation $D\backslash P$ to refer to the positive divisor $D - m_P P$.

Lemma 3.2.6 *For a place P in the support of D and a positive integer $n \geq 0$, the nth upper ramification field F^n is given by*

$$F^n = F_{\mathcal{S}}^{D\backslash P+nP}.$$

Proof: Let $P \in \mathrm{supp}(D)$ be any place. Observe that a field F' is a subfield of F^n if and only if its Galois group $\mathrm{Gal}(F'/F) \supseteq G^n$, the nth upper ramification group of P with respect to the field $F_{\mathcal{S}}^D/F$, which is in turn true if and only if the nth upper ramification group of P with respect to the field F'/F is trivial. Equivalently, it follows that the conductor exponent of P in F'/F is at most n and by Theorem 3.2.4 (i), this is precisely the case when $F' \subseteq F_{\mathcal{S}}^{D\backslash P+nP}$. The desired claim then follows. □

With this lemma and the aid of Corollary 1.3.4, we can easily write down the genus formula for $F_{\mathcal{S}}^D$ in terms of the genus of F.

Theorem 3.2.7 *The genus of $F_{\mathcal{S}}^D$ satisfies:*

$$2g(F_{\mathcal{S}}^D) - 2 = [F_{\mathcal{S}}^D : F](2g(F) - 2 + \deg D) - \sum_{P \in \mathrm{supp}(D)} \sum_{i=0}^{m_P - 1} [F_{\mathcal{S}}^{D\backslash P+iP} : F] \deg P.$$

3.3 Narrow Ray Class Fields

We will assume in the remainder of this chapter that F has more than one rational place and we distinguish a rational place ∞. Since ∞ has degree 1, the residue class field of ∞ in the ∞-adic completion F_∞ is the field $\mathbf{F}_q$.

We define a **sign function** sgn: $F_\infty^* \longrightarrow \mathbf{F}_q^*$ as a multiplicative group homomorphism on F_∞^* such that:

(i) $\mathrm{sgn}(\alpha) = \alpha$ for any $\alpha \in \mathbf{F}_q^*$;

(ii) $\mathrm{sgn}(U_\infty^{(1)}) = \{1\}$.

Indeed, we can show that there are exactly $q-1$ distinct sign functions on F_∞^*. From now on, we will fix one such sign function and denote it by sgn.

Define a subgroup of F_∞^* by

$$F_\infty^{\mathrm{sgn}} = \{x \in F_\infty^* : \mathrm{sgn}(x) = 1\}$$

which is the kernel of the sign function. Since the sign function is onto, $[F_\infty^* : F_\infty^{\mathrm{sgn}}] = q-1$.

Let D be an effective divisor of F with support being a subset of $\mathcal{S}$, where $\mathcal{S} = \mathbf{P}_F - \{\infty\}$. We define a subgroup of J_F by

$$J^D(\infty) = F_\infty^{\mathrm{sgn}} \times \prod_{P \in \mathcal{S}} U_P^{(\nu_P(D))}$$

and a subgroup of C_F by

$$C^D(\infty) = F^* J^D(\infty)/F^*.$$

As in the study of ray class groups, we wish to give $C_F/C^D(\infty)$ a group interpretation.

Refer to the definitions of $I_D(O_\mathcal{S})$ and $\mathrm{Princ}_D(\mathcal{S})$ in Section 1.4. Here, we further define $\mathrm{Princ}_D^+(\mathcal{S})$ to be the group of principal ideals $zO_\mathcal{S}$, where $z \equiv 1 \bmod D$ and $\mathrm{sgn}(z) = 1$. The factor group $I_D(O_\mathcal{S})/\mathrm{Princ}_D^+(\mathcal{S})$ which we denote by $C\ell_D^+(O_\mathcal{S})$ is called the **narrow ray class group** with modulus D with respect to the sign function sgn.

Proposition 3.3.1 *With the notations above,*

(i) $\mathrm{Princ}_D^+(O_\mathcal{S})$ *is a subgroup of* $\mathrm{Princ}_D(O_\mathcal{S})$ *and* $\mathrm{Princ}_D(O_\mathcal{S})/\mathrm{Princ}_D^+(O_\mathcal{S}) \simeq \mathbf{F}_q^*$.

(ii) *We have the isomorphisms*

$$C\ell_D^+(O_\mathcal{S})/\mathbf{F}_q^* \simeq C\ell_D^+(O_\mathcal{S})/(\mathrm{Princ}_D(O_\mathcal{S})/\mathrm{Princ}_D^+(O_\mathcal{S})) \simeq \mathrm{Cl}_D(O_\mathcal{S}).$$

By verifying the isomorphism

$$C_F/C^D(\infty) \cong C\ell_D^+(O_\mathcal{S}),$$

we can once again identify the factor group $C_F/C^D(\infty)$ with the ideal group $C\ell_D^+(O_\mathcal{S})$. From (ii) above, we conclude that $C_F/C^D(\infty)$ is finite. Invoking the existence theorem from global class field theory tells us that there exists a finite abelian extension $F^D(\infty)$ of F such that the induced norm residue symbol has kernel $C_F/C^D(\infty)$.

$F^D(\infty)$ is called the **narrow ray class field** with modulus D. It is easy to verify that $F_\mathcal{S}^D$ is a subfield of $F^D(\infty)$ and $[F^D(\infty) : F_\mathcal{S}^D] = q-1$. We summarize the main properties of the extension $F^D(\infty)/F$ in the theorem below.

Theorem 3.3.2 ***[Main properties of narrow ray class fields]***

(i)

$$\mathrm{Gal}(F^D(\infty)/F) \cong C\ell_D^+(O_\mathcal{S}).$$

(ii) *$F_\mathcal{S}^D$ is both the decomposition field and the fixed field of ∞ in $F^D(\infty)$. In particular,*

$$\mathrm{Gal}(F^D(\infty)/F_\mathcal{S}^D) \cong \mathbf{F}_q^*.$$

(iii) *All places not in* $\mathrm{supp}(D)$ *and different from ∞ are unramified in $F^D(\infty)/F$. For such a place P, its Artin symbol is given by the residue class in $C\ell_D^+(O_\mathcal{S})$ under the correspondence in* (i).

(iv) *The conductor of $F^D(\infty)/F$ is $D + \min(q-2, 1)\infty$.*

(v) *$\mathbf{F}_q$ is the full constant field of $F^D(\infty)/F$.*

From property (ii), we conclude that there are exactly $[F_\mathcal{S}^D : F]$ places lying over ∞, each with ramification index $q-1$. Indeed, $F^D(\infty)$ is completely characterized by the

property that it is the largest finite abelian extension of F containing $F_{\mathcal{S}}^{D}$ as a subfield and with the ramification index $e(P_\infty|\infty) = q-1$ for any place P_∞ of $F^D(\infty)$ lying over ∞. Mimicking the proof of Lemma 3.2.6, the nth upper ramification field of any place P in the support of D with respect to the extension $F^D(\infty)/F$ can be shown to be the narrow ray class field $F^{D\backslash P+nP}(\infty)$. As such, we obtain the genus of $F^D(\infty)$ as follows.

Lemma 3.3.3 *The genus of $F^D(\infty)$ satisfies:*

$$\begin{aligned} 2g(F^D(\infty)) - 2 = \; & [F^D(\infty) : F](2g(F) - 2 + \deg D + \frac{q-2}{q-1}) \\ & + \sum_{P \in \mathrm{supp}(D)} \sum_{i=0}^{m_P - 1} [F^{D\backslash P+iP}(\infty) : F] \deg P, \end{aligned}$$

where $D = \sum_{P \in \mathbf{P}_F} m_P P$.

3.4 Drinfeld Modules of rank 1

The narrow ray class field with modulus D just described can be constructed in a different way, namely, by the so-called Drinfeld module of rank 1. This construction was introduced by Hayes (see [25, 26]) as a generalization of the cyclotomic function fields (Section 2.4) with the base field F being any arbitrary global function field having more than one rational place.

Let ∞ be a fixed rational place of F and sgn a fixed normalized sign function of F. With $\mathcal{S}$ as the set of places of F other than ∞, let A denote the integral ring $O_{\mathcal{S}}$ and let H_A be the $\mathcal{S}$-Hilbert class field of F. Denote by $\pi : c \mapsto c^p$ the Frobenius endomorphism of H_A. Consider the left twisted polynomial ring $H_A[\pi]$ whose elements are polynomials in π with coefficients from H_A written on the left; but multiplication in $H_A[\pi]$ is twisted

by the rule

$$\pi z = z^p \pi \qquad \text{for all } z \in H_A.$$

Let Drin : $H_A[\pi] \longrightarrow H_A$ be the map which assigns to each polynomial in $H_A[\pi]$ its constant term.

A **Drinfeld** A**-module** of rank 1 over H_A is a ring homomorphism $\phi : A \longrightarrow H_A[\pi]$, $a \mapsto \phi_a$, such that:

(i) The image of ϕ contains some nonconstant polynomials in $H_A[\pi]$;

(ii) Drin $\circ\, \phi$ is the identity on A;

(iii) $\deg(\phi_a) = -m\nu_\infty(a)$ for all nonzero $a \in A$, where ϕ_a denotes the twisted polynomial associated with a by ϕ. $\deg(\phi_a)$ is the degree of ϕ_a as a polynomial in π. Further, ϕ is sgn-**normalized** if $\mathrm{sgn}(a)$ is equal to the leading coefficient of ϕ_a for all $a \in A$.

Let $M = \prod_{P \neq \infty} (P \cap A)^{m_P}$ be an ideal of A, or equivalently, a positive divisor $D = \sum_{P \neq \infty} m_P P - (\sum_{P \neq \infty} m_P \deg P)\infty$ of F under our usual identification. Roughly speaking, the field extension $F_M = H_A(\Lambda_\phi(M))$ (or equivalently, $H_A(\Lambda_\phi(D))$), determined by a sgn-normalized Drinfeld A module ϕ of rank 1 over H_A is constructed by adjoining the M-torsion points of ϕ to H_A in a fixed algebraic closure of H_A. For the detailed construction and the definition of the M-torsion points, we refer the reader to [27]. Indeed, to avoid introducing more concepts and definitions, we will not delve further into the theory of Drinfeld modules. A comprehensive treatment of this subject is contained in [27] and [22]. Instead, we will quote, in the following theorem, some of the main properties that will be useful in the subsequent chapters.

Theorem 3.4.1 *Let $F_M = H_A(\Lambda_\phi(M)) = H_A(\Lambda_\phi(D))$ be as defined previously. Then:*

(i) *F_M is F-isomorphic to the narrow ray class field $F^D(\infty)$.*

(ii) F_M is independent of the specific choice of the sgn-normalized Drinfeld A-module ϕ of rank 1 over H_A.

(iii) F_M/F is unramified away from ∞ and the places $P \in \mathrm{supp}(D)$.

(iv) The extension F_M/F is abelian and there is an isomorphism

$$\sigma : \mathrm{Cl}_D^+(A) \longrightarrow \mathrm{Gal}(F_M/F),$$

determined by $\sigma_{\mathfrak{J}}\phi = \mathfrak{J} * \phi$ (see [27, Section 4] for the notation) for any nonzero ideal $\mathfrak{J}$ of A coprime to M, and $\lambda^{\sigma_{\mathfrak{J}}} = \phi_{\mathfrak{J}}(\lambda)$ for any generator λ of the cyclic A-module $\Lambda_\phi(M)$. Moreover, for any prime ideal P of A that is coprime to M, the corresponding Artin symbol in F_M/F is exactly $\sigma_{\mathfrak{P}}$. Furthermore, if $M = P^n$ for some prime ideal P of A and $n \geq 1$, then both the decomposition group and the inertia group of ∞ in F_M/F are isomorphic to $\mathbf{F}_q^*$.

(v) The multiplicative group $(A/M)^*$ is isomorphic to $\mathrm{Gal}(F_M/H_A)$ by means of

$$b \mapsto \sigma_{bA},$$

where $b \in A$ satisfies $\mathrm{sgn}(b) = 1$ and is coprime to M.

(vi) Suppose that $M = P^n$ for some prime ideal P of A and $n \geq 1$. Let λ be a generator of the cyclic A-module $\Lambda_\phi(M)$. Then $F_M = H_A(\lambda)$ and the minimal polynomial of λ over H_A is

$$\gamma(z) = \frac{\phi_{P^n}(z)}{\phi_{P^{n-1}}(z)}.$$

Moreover, $\gamma(z)$ is an Eisenstein polynomial at any place Q of H_A lying over P. Thus, Q is totally ramified in F_M/H_A and $\nu_R(\lambda) = 1$ for the place R of F_M lying over Q.

(vii) *Let $M = M_1M_2$ be a product of two coprime ideals. Then, F_M is the compositum of F_{M_1} and F_{M_2} and $F_{M_1} \cap F_{M_2} = H_A$.*

Remark 3.4.2 *In view of* (ii) *of Theorem* 3.4.1*, we can omit the symbol* ϕ *in the notation* $H_A(\Lambda_\phi(M))$ *and simply write* $F_M = H_A(\Lambda(M))$.

Since $[H_A : F] = h(F)$, it follows from (v) of Theorem 3.4.1 that

$$[F_M : F] = h(F)|(A/(M))^*| = h(F)\Phi(M).$$

This, together with Lemma 3.3.3 allows us to write down explicitly the genus of the narrow ray class field $F_M = F^D(\infty)$, which we will now proceed to do. We will give the formula only for $D = nP$, where P is a place of F of degree d. The general formula can be established likewise.

Theorem 3.4.3 *With* $D = nP$*, the genus of* $F^D(\infty)$ *is*

$$2g(F^D(\infty)) - 2 = h(F)q^{d(n-1)}\left[(q^d-1)(2g(F)-2+\frac{q-2}{q-1}+nd)-d\right].$$

Proof:

$$\begin{aligned}
& 2g(F^D(\infty)) - 2 \\
= \;& h(F)\Phi(P^n)(2g(F)-2+\frac{q-2}{q-1}+nd) - \sum_{i=0}^{n-1} h(F)\Phi(P^i) \\
= \;& h(F)(q^d-1)q^{d(n-1)}(2g(F)-2+\frac{q-2}{q-1}+nd) - h(F)d - dh(F)\sum_{i=1}^{n-1}(q^d-1)q^{d(i-1)} \\
= \;& h(F)(q^d-1)q^{d(n-1)}(2g(F)-2+\frac{q-2}{q-1}+nd) - d - d(q^{d(n-1)}-1) \\
= \;& h(F)q^{d(n-1)}\left[(q^d-1)(2g(F)-2+\frac{q-2}{q-1}+nd)-d\right].
\end{aligned}$$

□

Example 3.4.4 Consider the rational function field $F = \mathbf{F}_q(x)$ with ∞ being the infinite place of F. Then we have seen in Example 3.2.5 that $A = \mathbf{F}_q[x]$ and $H_A = F = \mathbf{F}_q(x)$. A Drinfeld A-module ϕ of rank 1 over F is uniquely determined by the image ϕ_x of x. By the definition we must have

$$\mathrm{Drin}(\phi_x) = (\mathrm{Drin} \circ \phi)(x) = x.$$

Hence, ϕ_x is a nonconstant polynomial in π with the constant term x. Since $\deg(\phi_x) = -r\nu_\infty(x) = r$, it follows that ϕ_x is of the form $x + f(\pi)\pi + z\pi^r$ for an element $z \in F^*$ and $f(\pi) \in F[\pi]$ with $\deg(f(\pi)) \leq r - 2$. By letting $z = 1$ and $f(\pi) = 0$ produces the Carlitz module that we have discussed in Section 2.4. As such, the cyclotomic function fields are in fact narrow ray class fields over the rational function fields.

3.5 Subfields of Narrow Ray Class Fields

The primary goal of this thesis is to search for function fields having as many rational places as close to the best known upper bounds as possible. From 1.2, it is obvious that for an extension F'/F, a rational place of F remains rational in F' if it splits completely in the extension. Moreover, a review of Proposition 1.2.10 suggests that a possible approach to find fields with many rational places is to construct subfields L of suitable field extensions F'/F in which the Artin symbols of sufficient rational places of F are contained in the Galois group $\mathrm{Gal}(F'/L)$.

As such, ray class fields and narrow ray class fields provide good candidates to carry out our search since their Galois groups and Artin symbols of places are explicitly known (Theorems 3.2.4 and 3.3.2).

Let $\mathcal{S}'$ be the set $\{\infty, P_1, \ldots, P_k\}$ for distinct places $P_1, \ldots, P_k$ and $\mathcal{S}^* = \mathcal{S}' - \{\infty\}$. According to Theorem 3.2.4 (v), $F_{\mathcal{S}}^D \subseteq F_{\mathbf{P}_F - \{\infty\}}^D$, where $\mathcal{S} = \mathbf{P}_F - \mathcal{S}'$ and D, is as usual, a positive divisor of F. By Proposition 1.4.3, since $\deg \mathcal{S} = 1$,

$$\mathrm{Gal}(F_{\mathcal{S}}^D/F) \cong \mathrm{Cl}_D(O_{\mathcal{S}}) \cong \mathrm{Cl}_D(F)/(\mathrm{Div}_{\mathcal{S}}^0(F)/(\mathrm{Div}_{\mathcal{S}}^0(F) \cap \mathrm{Princ}_D(F))).$$

Let $A = O_{\mathbf{P}_F - \{\infty\}}$. Denoting $\langle \mathcal{S}^* \rangle_D$ as the subgroup of $\mathrm{Cl}_D(A)$ generated by the places in $\mathcal{S}^*$, and since ∞ has degree 1, this can be written as $\mathrm{Gal}(F_{\mathcal{S}}^D/F) \cong \mathrm{Cl}_D(A)/\langle \mathcal{S}^* \rangle_D$. Further, by Proposition 3.3.1, $C\ell_D^+(A)/\mathbf{F}_q^* \cong \mathrm{Cl}_D(A)$. Putting all these together, we can establish the following construction.

Theorem 3.5.1 *Let $D = \sum_{P \in \mathbf{P}_F} m_P P$ be a positive divisor of F. Let $F' = F^D(\infty) = H_A(\Lambda(D))$ be the narrow ray class field determined by a* sgn*-normalized Drinfeld A-module of rank 1 over the Hilbert class field H_A. Suppose that $\mathcal{S}^* = \{P_1, P_2, \ldots, P_k\}$ is a set of k distinct rational places of F different from ∞ and let G_D be the subgroup of $C\ell_D^+(A)$ generated by $\mathbf{F}_q^*$ and the places in $\mathcal{S}^*$. Let L be the subfield of F' fixed by G_D. Then, L has at least $\frac{h(F)\Phi(D)(k+1)}{|G_D|}$ rational places. The genus of L is given by*

$$2g(L) - 2 = h(F) \left[\frac{\Phi(D)}{|G_D|}(2g(F) - 2 + \deg D) - \sum_{P \in \mathrm{supp}(D)} \sum_{i=0}^{m_P - 1} \frac{\Phi(D \backslash P + iP)}{|G_{D \backslash P + iP}|} \right].$$

Proof: By the fact that $\mathbf{F}_q^*$ is the decomposition group of ∞ in F' and by consideration of the Artin symbols of $P_1, \ldots, P_k$, it is clear that $\infty, P_1, \ldots, P_k$ split completely in L/F. Hence, we conclude from the characterization of $F_{\mathcal{S}}^D$ that L is a subfield of the ray class field $F_{\mathcal{S}}^D$, where $\mathcal{S} = \mathbf{P}_F - \{\infty\} - \mathcal{S}^*$. Further since $C\ell_D^+(A)/G_D \cong \mathrm{Cl}_D(A)/\langle \mathcal{S}^* \rangle_D$, it follows from our earlier discussion that L is indeed the ray class field $F_{\mathcal{S}}^D$. The genus is now obtained via Theorem 3.2.7. $\square$

We observe from this theorem that it is crucial to determine the orders of the subgroups of $C\ell_D^+(A)$ generated by a set of rational places of F. Our next result shows that this problem is connected to having knowledge of the relationship between the places. Here, we will only consider the case when $D = nP$.

For any positive integer n, denote by n_p^* the smallest integer l such that $n \leq p^l$ and $n_p = p^{n_p^*}$. Let $\mathcal{S}^* = \{P_1, P_2, \ldots, P_k\}$ be a set of any k places of F as before. We write $\langle \mathcal{S}^* \rangle_n = \langle P_1, \ldots, P_k \rangle_n$ to be the subgroup of $(A/P^n)^*$ generated by $\mathbf{F}_q^*$ and the places $P_1, P_2, \ldots, P_k$.

Proposition 3.5.2 *Suppose that there is an integer i such that $P_k \in \langle P_1, \ldots, P_{k-1} \rangle_i$ but $P_k \notin \langle P_1, \ldots, P_{k-1} \rangle_{i+1}$. Then*

$$|\langle P_1, \ldots, P_k \rangle_n| = |\langle P_1, \ldots, P_{k-1} \rangle_n | (n/i)_p.$$

Proof: If $n \leq i$, then the result is obvious. So we will assume that $n > i$. For an integer j, let $G_j = \langle P_1, P_2, \ldots, P_{k-1} \rangle_j$. It is clear that $|\langle P_k \rangle_n| = an_p$, where $a = |\langle P_k \rangle_1|$. Since $P_k \in G_1$, it follows that $|G_n \cap \langle P_k \rangle_n| = ap^l$ for some integer l. We claim that $l = n_p^* - (n/i)_p^*$. Indeed, by our assumption, $P_k \in G_i$ and thus, $P_k^{n_p} \in G_n$ as $in_p > n$. So $l \geq n_p^* - (n/i)_p^*$. If $P_k^{p^j} \in G_n$ for $j < (n/i)_p^*$, we will have $P_k \in G_{\lfloor n/p^j \rfloor} > i$. Thus, $l \leq n_p^* - (n/i)_p^*$ and equality holds. Consequently,

$$|\langle P_1, P_2, \ldots, P_k \rangle_n| = |H_n| |\langle P_k \rangle_n| / p^l = |H_n| (n/i)_p.$$

□

Chapter 4

Error-correcting Codes and Algebraic Function Fields

One of the most important applications of global function fields is in the construction of Goppa codes [19, 20, 21]. Shortly after, algebraic curves with many rational points are used to construct algebraic-geometric codes and their generalizations [9, 10, 57, 75, 90, 94, 95]. In this chapter, we introduce a different construction of error-correcting codes via global function fields, which will in turn assist us in finding function fields with many rational places.

4.1 A brief Introduction to Error-Correcting Codes

We will first briefly recall some of the fundamental notions in the theory of error-correcting codes. [39, 83, 91] are excellent references for materials in this section.

Let A be a finite set with q symbols. A **block code** C of length N over A is a nonempty

set of N tuples with coordinates in A. Any element of C is known as a **codeword** of C. The number of codewords in C is the **size** of the code and is denoted by $|C|$.

Definition 4.1.1 Let $\mathbf{c}$ and $\mathbf{d}$ be any two codewords of a code C. The **Hamming distance** of C, denoted by $d(\mathbf{c}, \mathbf{d})$, is defined as the number of positions in which $\mathbf{c}$ and $\mathbf{d}$ differ. Then the **minimum distance** of C is $d(C) = \min\{d(\mathbf{c}, \mathbf{d}) : \mathbf{c}, \mathbf{d} \in C, \mathbf{c} \neq \mathbf{d}\}$.

As in all practical applications, A will be the finite field $\mathbf{F}_q$ in this thesis, that is, C will be a subset of $\mathbf{F}_q^N$. If C is a subspace of $\mathbf{F}_q^N$, we call C a **linear code**. In this case, the dimension κ of C is the dimension of C over $\mathbf{F}_q$ as a vector space. We usually say that a code C is a $[N, \kappa, \delta]$-code over $\mathbf{F}_q$ to mean that C is a linear code of length N, dimension κ and minimum distance δ.

Definition 4.1.2 Let $\mathbf{c}$ be a codeword of a code C. The **support** of $\mathbf{c}$, denoted by $\mathrm{supp}(\mathbf{c})$ is the set of coordinates in which $\mathbf{c}$ is nonzero. $|\mathrm{supp}(\mathbf{c})|$ is called the **Hamming weight** of $\mathbf{c}$ and is denoted by $w(\mathbf{c})$.

Lemma 4.1.3 *For a linear code C, the following are true.*

(i) *For any two codewords $\mathbf{c}$ and $\mathbf{d}$ in C, $d(\mathbf{c}, \mathbf{d}) = w(\mathbf{c} - \mathbf{d})$.*

(ii) *The minimum distance of C is given by*

$$d(C) = \min\{w(\mathbf{c}) : \mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}\}.$$

For an $[N, \kappa, \delta]$-code C, we define the dual code $C^\perp$ to be the dual space of C in $\mathbf{F}_{q^N}$, i.e.

$$C^\perp = \{\mathbf{c} \in \mathbf{F}_q^N : \mathbf{c} \cdot \mathbf{d} = \mathbf{0} \text{ for all } \mathbf{d} \in C\},$$

where the dot represents the usual inner product.

Thus, $C^{\perp}$ is an $[N, N-\kappa]$-linear code over $\mathbf{F}_q$.

Definition 4.1.4 For an $[N, \kappa, \delta]$-code C, any $N \times \kappa$ matrix over $\mathbf{F}_q$ whose rows form a basis of C is called a **generator matrix** of C. A generator matrix of $C^{\perp}$ is called a **parity-check matrix** of C.

Let $\mathcal{G}$ and $\mathcal{H}$ be the generator matrix and the parity-check matrix of C, respectively. Then, the codewords of C can be represented in one of the following ways:

1.
$$C = \{\mathbf{c} \cdot \mathcal{G} : \mathbf{c} \in \mathbf{F_q^{\kappa}}\};$$

2.
$$C = \{\mathbf{c} \in \mathbf{F_q^N} : \mathbf{c} \cdot \mathcal{H}^{\mathbf{T}} = \mathbf{0}\},$$

where $\mathcal{H}^T$ is the transpose of $\mathcal{H}$.

Our next result shows how we can determine the minimum distance of C from its parity-check matrix.

Theorem 4.1.5 *Let $\mathcal{H}$ be the parity-check matrix of a linear code C of length N. Then C has minimum distance δ if and only if every $\delta - 1$ columns of $\mathcal{H}$ are linearly independent and there exist δ columns of $\mathcal{H}$ that are linearly dependent.*

Proof: Let $\mathbf{c}$ be a codeword of C with $w(\mathbf{c}) = \mathbf{w}$. Without loss of generality, we may assume that the first w coordinates of $\mathbf{c}$ are nonzero. Write $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2}, \ldots, \mathbf{c_w}, \mathbf{0}, \ldots, \mathbf{0})$. Let the columns of $\mathcal{H}$ be $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_N}$. Since $\mathbf{c} \in \mathbf{C}$, by (ii) above, $\mathbf{c} \cdot \mathcal{H}^{\mathbf{T}} = \mathbf{0}$, i.e.

$$\sum_{i=1}^{w} c_i \mathbf{u_i} = \mathbf{0}.$$

Consequently, the w columns are linearly dependent. On the other hand, if there exist w columns of $\mathcal{H}$ that are linearly dependent, there must exist w columns of $\mathcal{H}$ and w nonzero constants in $\mathbf{F}_q$ such that

$$\sum_{j=1}^{w} c_{i_j} \mathbf{u}_{i_j} = 0.$$

Thus the vector $\mathbf{c}$ with c_{i_j} in its i_jth position and 0 everywhere else is a codeword of C with weight w. Our desired result follows. □

Similarly, we may determine the minimum distance of C from its generator matrix as we show below.

Definition 4.1.6 Two codes C and C' are said to be equivalent if there exist nonzero constants $a_1, a_2, \ldots, a_N \in \mathbf{F}_q^*$ such that $C' = \{(a_1 c_1, a_2 c_2, \ldots, a_N c_N) : (c_1, \ldots, c_N) \in C\}$.

Clearly, equivalent codes have the same parameters.

Definition 4.1.7 Let $\mathbf{c}$ be a nonzero codeword of a linear code C. The **residual code** with respect to $\mathbf{c}$, denoted by $C_{\mathbf{c}}$ is the code obtained from C by deleting the coordinates in $\mathrm{supp}(\mathbf{c})$ from all the codewords of C.

Lemma 4.1.8 *If C is an $[N, \kappa, \delta]$-code over $\mathbf{F}_q$ and $\mathbf{c} \in C$ is a codeword of weight δ, then $C_{\mathbf{c}}$ is an $[N - \delta, \kappa - 1, \delta']$-code, where $\delta' \geq \lceil \delta/q \rceil$. (*Here, $\lceil x \rceil$ refers to the smallest integer $\geq x$.*)*

Proof: By replacing C with an equivalent code if necessary, assume that the first δ coordinates of $\mathbf{c}$ are all equal to 1. The length of $C_{\mathbf{c}}$ is trivially $N - \delta$. Let τ be the map that deletes the first δ coordinates from each codeword in C. Clearly, τ is a linear

transformation from C onto $C_{\mathbf{c}}$. Since the kernel of τ contains the nonzero codeword $\mathbf{c}$, the rank of τ must be at most $\kappa - 1$. If the rank is strictly less than $\kappa - 1$, then there exists a nonzero codeword $\mathbf{c}' \in \mathbf{C}$ such that $\mathbf{c}'$ is not a multiple of $\mathbf{c}$ and $\tau(\mathbf{c}') = \mathbf{0}$. Let $\mathbf{c}' = (c_1, c_2, \ldots, c_\delta, 0, \ldots, 0)$. Then the codeword $\mathbf{c}' - c_1\mathbf{c} \in \mathbf{C}$ and has weight less than δ, contradicting to δ being the minimum distance of C. Hence, $C_{\mathbf{c}}$ has dimension $\kappa - 1$. Next, we wish to show that $\delta' \geq \lceil \delta/q \rceil$. Let $\mathbf{c}' \in \mathbf{C}$ such that $\mathbf{c}'$ is not in the kernel of τ. Observe that by the pigeonhole principle, there must be an $\alpha \in \mathbf{F}_q$ such that at least δ/q coordinates of $\mathbf{c}'$ are equal to α. Let $\mathbf{u} = \mathbf{c}' - \alpha\mathbf{c} \in \mathbf{C}$. Then we have

$$\mathrm{d} \leq w(\mathrm{u}) \leq w(\tau(\mathrm{u})) + \mathrm{d} - \mathrm{d}/q$$

which yields

$$\delta' \geq w(\tau(\mathrm{u})) \geq \lceil \mathrm{d}/q \rceil.$$

□

Corollary 4.1.9 *Let $\mathcal{G}$ be the generator matrix of an $[N, \kappa]$-linear code C. If C has minimum distance δ, there must exist $N - \delta$ columns of $\mathcal{G}$ with rank $\kappa - 1$. Conversely, suppose that there are $N - \delta$ columns of $\mathcal{G}$ with rank $\kappa - 1$. Then, C must have minimum distance at most δ. In particular, C has minimum distance δ if and only if every $N - \delta + 1$ columns of $\mathcal{G}$ have rank κ and there exists $N - \delta$ columns of $\mathcal{G}$ of rank $\kappa - 1$.*

Proof: First, suppose that $d(C) = \delta$. Let $\mathbf{c}$ be a codeword of C of weight δ. By Lemma 4.1.8, the residual code $C_{\mathbf{c}}$ has dimension $\kappa - 1$. Since the submatrix obtained from $\mathcal{G}$ by deleting the columns of $\mathcal{G}$ corresponding to the coordinates in $\mathrm{supp}(\mathbf{c})$ is a generator matrix of $C_{\mathbf{c}}$, the $N - \delta$ columns in this submatrix must have rank $\kappa - 1$.

Conversely, suppose that there exist $N-\delta$ columns of $\mathcal{G}$ of rank $\kappa-1$. Without loss of generality, we assume that these columns are from the first $N-\delta$ columns of $\mathcal{G}$. Write $\mathcal{G} = [\mathcal{G}'\mathbf{u_{N-\delta+1}} \ldots \mathbf{u_N}]$, where $\mathcal{G}'$ consists of the first $N-\delta$ columns of $\mathcal{G}$. Since $\mathcal{G}'$ has rank $\kappa-1$ and $\mathcal{G}'$ has κ rows, there exists a nonzero $\mathbf{v} = (v_1, \ldots, v_\kappa)$ such that

$$\mathbf{v}\mathcal{G}' = 0.$$

It follows that $\nu\mathcal{G}$ is a codeword of C of weight at most δ. Hence, $d(C) \leq \delta$ as required. The last assertion is an immediate consequence. □

One of the primary goals of coding theory is to construct codes with large minimum distances relative to their lengths and sizes. This is essentially because large minimum distances positively influence the error-correction and error-detection capabilities of the codes. Unfortunately, for a fixed N and κ, the minimum distance δ cannot grow too large according to several well-known bounds that relate these parameters. We will present one such bound in this thesis.

Theorem 4.1.10 (Griesmer bound) *For an $[N, \kappa, \delta]$-code over $\mathbf{F}_q$,*

$$N \geq \sum_{i=0}^{\kappa-1} \lceil \delta/q^i \rceil.$$

Proof: The proof follows by induction on κ. The claim is trivial for $\kappa = 1$. So suppose that it is true for $\kappa-1$, where $\kappa > 1$. Let $\mathbf{c}$ be a codeword of C such that $w(\mathbf{c}) = \delta$. By Lemma 4.1.8, $C_{\mathbf{c}}$ is an $[N-\delta, \kappa-1, \delta']$-code with $\delta' \geq \lceil \delta/q \rceil$. By our induction hypothesis, this implies that

$$N - \delta \geq \sum_{i=0}^{\kappa-2} \lceil \delta'/q^i \rceil \geq \sum_{i=1}^{\kappa-1} \lceil \delta/q^i \rceil.$$

Hence, $N \geq \sum_{i=0}^{\kappa-1} \lceil \delta/q^i \rceil$ and the induction is complete. □

Next, we turn our attention to some important families of linear codes.

Definition 4.1.11 A code C is called a **cyclic code** if a cyclic shift of every codeword lies in C as well. More specifically, $(c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in C$ if and only if $(c_0, c_1, \ldots, c_{N-2}, c_{N-1}) \in C$.

It is easy to verify that the dual code of a cyclic code is itself a cyclic code. For the remaining of this section, we will concentrate on cyclic codes that are linear codes.

For an integer N, consider the ring $R_N = \mathbf{F}_q[x]/(x^N - 1)$. Define a map $\Gamma : \mathbf{F}_q^N \to R_N$ by

$$(c_0, c_1, \ldots, c_{N-1}) \mapsto \sum_{i=0}^{N-1} c_i x^i.$$

Clearly, Γ is a bijection satisfying $\Gamma(\mathbf{c} + \mathbf{c}')= \Gamma(\mathbf{c})+ \Gamma(\mathbf{c}')$ for all $\mathbf{c}, \mathbf{c}' \in \mathbf{C}$ and $\Gamma(\alpha\mathbf{c})$ $= \alpha\Gamma(\mathbf{c})$ for $\alpha \in \mathbf{F}_q$ and $\mathbf{c} \in \mathbf{C}$.

Moreover, by observing that a cyclic shift of $\mathbf{c}$ corresponds to multiplication by x to $\Gamma(\mathbf{c})$, we can show that a cyclic code C corresponds to an ideal $\Gamma(C)$ of R_N and vice versa. Since R_N is a principal ideal domain, there exists a unique monic polynomial $g(x) \in \mathbf{F}_q[x]$ of smallest degree such that $\Gamma(C) = R_N g(x)$. This polynomial $g(x)$ is called the **generator polynomial** of C. We state the following results on cyclic codes and their generator polynomials without proof.

Proposition 4.1.12 *With the notations above, we have*

(i) *C has dimension κ if and only if $g(x)$ has degree $N - \kappa$.*

(ii) *$\mathbf{c} \in \mathbf{C}$ if and only if $c(x) = \Gamma(\mathbf{c})$ is a multiple of $g(x)$.*

(iii) *The generator polynomial of* $C^{\perp}$ *is given by*

$$h(x) = x^N g(1/x).$$

$h(x)$ *is also known as the* **parity-check polynomial** *of* C.

(iv) *A generator matrix of* C *is given by*

$$\mathcal{G} = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{\kappa-1}g(x) \end{pmatrix}.$$

In particular, let $N = q^m - 1$ for some positive integer m. Recall that a monic irreducible polynomial $m(x)$ divides $x^{q^m-1} - 1$ if $m(x)$ is the minimal polynomial of some $\beta \in \mathbf{F}_{q^m}^*$. Since $\mathbf{F}_q(\beta)$ is a subfield of $\mathbf{F}_{q^m}$, $m(x)$ has degree v where $v|m$. If we write $m(x) = \sum_{i=0}^{v-1} a_i x^i, a_i \in \mathbf{F}_q$, it is easy to see that $m(\beta^{q^j}) = 0$ for all $j = 1, \ldots, v$. In otherwords, $\beta^{q^j}, 1 \leq j \leq v$ are all the roots of $m(x)$.

Now, let α be a primitive element of $\mathbf{F}_{q^m}^*$, i.e. $\alpha^{q^m-1} = 1$ but $\alpha^j \neq 1$ for $1 \leq i \leq q^m - 2$. For $1 \leq i \leq q^m - 2$, let $m_i(x)$ denote the minimal polynomial of α^i. From what we have just said, $m_i(x)$ is also the minimal polynomial of α^{iq^j} for any integer j.

Definition 4.1.13 A **narrow-sense BCH code** over $\mathbf{F}_q$ of **designed distance** δ_0 is a cyclic code of length $q^m - 1$ with generator polynomial

$$g(x) = \mathrm{lcm}(m_1(x), m_2(x), \ldots, m_{\delta_0-1}(x)).$$

Theorem 4.1.14 *A narrow-sense BCH code of designed distance* δ_0 *has minimum distance at least* δ_0.

Proof: Refer to [39]. □

Remark 4.1.15 (a) *The letters B, C and H refer to the names of the founders of the BCH code, namely, Bose, Chaudhuri, and Hocquenghem respectively.*

(b) *Narrow-sense BCH codes are a special case of primitive BCH codes in which the generator polynomial is*

$$g(x) = \text{lcm}(m_a(x), \ldots, m_{a+\delta_0-1}(x))$$

for some integer a, where δ_0 is the designed distance of the code.

In order to determine the dimension of a BCH code, we need to know the degree of the generator polynomial according to Proposition 4.1.12. To simplify our discussion, we will let $q = p$ in the following.

Given any integer i, we define the **cyclotomic set of p modulo $p^m - 1$** containing i as the set

$$C_i = \{ip^j \bmod p^m - 1 : j \in \mathbf{Z}\}.$$

Lemma 4.1.16 *For any integer i, let C_i be the cyclotomic set of p modulo $p^m - 1$ containing i.*

(i) *C_i is finite and $|C_i|$ divides m.*

(ii) *Let $\gamma = p^m - p^{m-1}$. Then,*

$$\bigcup_{i=1}^{\gamma} C_i = \{1, 2, \ldots, p^m - 2\}.$$

(iii) *Suppose that m is even, say $m = 2m_0$. Then, all the C_i's are distinct for $1 \leq i \leq 2p^{m_0}, \gcd(i,p) = 1, i \neq p^{m_0}+1$ and $|C_i| = m$ for each such i. Furthermore, $|C_{p^{m_0}+1}| = m_0$ and $2p^{m_0}+1 \in C_i$ for some $1 \leq i \leq 2p^{m_0}$.*

(iv) *Suppose that m is odd, say $m = 2m_0+1$. Then, all the C_i's are distinct for $1 \leq i \leq p^{m_0+1}, \gcd(i,p) = 1$ and $|C_i| = m$ for each such i. Furthermore, for $p^{m_0+1} \leq j \leq p^{m_0+1}+p, j \in C_i$ for some $1 \leq i < p^{m_0+1}$.*

Proof: (i) Let $m_i(x)$ be the minimal polynomial of α^i. Since for each $j \in C_i, \alpha^j$ is a root of $m_i(x)$ and all roots of $m_i(x)$ are obtained this way, we have

$$|C_i| = \deg m_i(x) \text{ which divides } m.$$

(ii), (iii) and (iv) are easily deduced by representing an integer j as an m-digit number in the p-adic completion of $\mathbf{Z}$ and observing the fact that multiplying j by p modulo $p^m - 1$ is a cyclic shift of this representation. For example, we show (ii). Here, it suffices to show that for any integer j with $p^m - p^{m-1} \leq j < p^m - 1$, there exists an $i < p^m - p^{m-1}$ with $j \in C_i$. Write $j = \sum_{l=0}^{m-1} a_l p^l = (a_0, a_1, \ldots, a_{m-1})$, where $0 \leq a_l \leq p-1$ and $a_{m-1} = p-1$. Since $j \neq p^m - 1$, there exists an index k for which $a_k < p-1$. Then, $i = jp^{m-1-k} \bmod p^m - 1 = (a_{k+1}, \ldots, a_{m-1}, a_0, \ldots, a_k) < j$ and $j \in C_i$. □

Example 4.1.17 1. Let $p = 2$ and $m = 5$. Then, the cyclotomic cosets of 2 modulo

31 are:

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 2, 4, 8, 16\}, \\ C_3 &= \{3, 6, 12, 17, 24\}, \\ C_5 &= \{5, 9, 10, 18, 20\}, \\ C_7 &= \{7, 14, 19, 25, 28\}, \\ C_{11} &= \{11, 13, 21, 22, 26\}. \end{aligned}$$

2. Let $p = 3$ and $m = 2$. Then the cyclotomic cosets of 3 modulo 8 are:

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 3\}, \\ C_2 &= \{2, 6\}, \\ C_4 &= \{4\}, \\ C_5 &= \{5, 7\}. \end{aligned}$$

Corollary 4.1.18 *Let C be a $[p^m - 1, \kappa]$-*BCH *code over $\mathbf{F}_p$ with designed distance δ_0.*

(i) *Suppose that $m = 2m_0$ is even. Then, $\kappa = p^m - 1 - \kappa'$, where κ' satisfies*

$$\kappa' = \begin{cases} m(\delta_0 - 1 - \lfloor (\delta_0 - 1)/p \rfloor) & \text{if } \delta_0 \leq p^{m_0}, \\ m(\delta_0 - 2 - \lfloor (\delta_0 - 1)/p \rfloor) + m_0 & \text{if } p^{m_0} < \delta_0 \leq 2p^{m_0}, \\ m(\delta_0 - 3 - \lfloor (\delta_0 - 1)/p \rfloor) + m_0 & \text{if } \delta_0 = 2p^{m_0} + 1 \end{cases}$$

(ii) *Suppose that $m = 2m_0 + 1$ is odd. Then $\kappa = p^m - 1 - \kappa'$, where κ' satisfies*

$$\kappa' = \begin{cases} m(\delta_0 - 1 - \lfloor (\delta_0 - 1)/p \rfloor & \text{if } \delta_0 \leq p^{m_0+1}, \\ m(\delta_0 - 1 - i - \lfloor (\delta_0 - 1)/p \rfloor) & \text{if } \delta_0 = p^{m_0+1} + i, 1 \leq i \leq p \end{cases}$$

□

4.2 Linear Codes Constructed from Function Fields

In this section, we describe the construction of linear codes using places of global function fields to form the columns of the generator matrix of the code.

As in Chapter 3, let ∞ be a fixed rational place of a global function field $F/\mathbf{F}_q$. Let $A = O_{\mathcal{S}}$, where $\mathcal{S} = \mathbf{P}_F - \{\infty\}$ be the integral ring consisting of all elements of F with poles only at ∞. For every place $P \neq \infty$, we will, for simplicity, also denote by P the prime ideal $P \cap A$ of A. In this way, a divisor of F with support not containing ∞ may be identified with a fractional ideal of A as explained at the end of Section 1.4.

We first establish a useful result pertaining to the p-rank of an abelian group.

Definition 4.2.1 Let l be a prime number. For an abelian group G, the l-rank of G is defined as the dimension of the $\mathbf{F}_l$-vector space G/G^l and is denoted by $d_l(G)$.

Lemma 4.2.2 *Let $Q \neq \infty$ be a place of F with $\deg Q = d$. Then for any positive integer n, the p-rank of the abelian group $(A/Q^n)^*$ is $rd(n - 1 - \lfloor (n-1)/p \rfloor)$, where $q = p^r$.*

Proof: By Lemma 1.4.2, $A/Q^n \cong O_Q/Q^n = \{\sum_{i=0}^{n-1} a_i \pi^i \bmod Q^n : a_i \in \tilde{F}_Q, 0 \leq i \leq n-1\}$, where π is a local parameter at Q. Hence,

$$(A/Q^n)^* = \{\sum_{i=0}^{n-1} a_i \pi^i \bmod Q^n : a_i \in \tilde{F}_Q, 0 \leq i \leq n-1, a_0 \neq 0\}$$

and has cardinality $(q^d-1)q^{d(n-1)}$. Further,

$$\begin{aligned}((A/Q^n)^*)^p &= \{\sum_{i=0}^{n-1} a_i\pi^{ip} \bmod Q^n : a_i \in \tilde{F}_Q, 0 \le i \le n-1, a_0 \neq 0\} \\ &= \{\sum_{i=0}^{n'} a_i\pi^{ip} \bmod Q^n : a_i \in \tilde{F}_Q, 0 \le i \le n'-1, a_0 \neq 0\},\end{aligned}$$

where $n' = \lfloor (n-1)/p \rfloor$. This gives $|((A/Q^n)^*)^p| = (q^d-1)q^{dn'}$ which implies that

$$|(A/Q^n)^*/((A/Q^n)^*)^p| = q^{d(n-1-n')}.$$

Consequently, the dimension of the vector space $(A/Q^n)^*/((A/Q^n)^*)^p)$ is $rd(n-1-n')$ as desired. □

Corollary 4.2.3 *Let $D = \prod_{i=1}^t P_i^{e_i}$ be a fractional ideal of A, where P_i's are distinct places of F with degree $\deg P_i = d_i$ and e_i's are positive integers. Then, the p-rank of $(A/D)^*$ is given by*

$$d_p((A/D)^*) = r\sum_{i=1}^{t} d_i(e_i - 1 - \lfloor (e_i-1)/p \rfloor).$$

Proof: By the Chinese Remainder Theorem of rings, we have the isomorphism

$$(A/D)^* \cong \prod_{i=1}^{t} (A/P_i^{e_i})^*.$$

Our result follows from Lemma 4.2.2. □

Now, consider a fixed positive divisor D of F with support not containing ∞ as in the preceding corollary. Let F' be the narrow ray class field $H_A(\Lambda(D))$ determined by a sgn-normalized Drinfeld module of rank 1 with modulus D defined over the Hilbert class

field H_A. Recall that $\mathrm{Gal}(F'/F) \cong C\ell_D^+(A)$ and $\mathrm{Gal}(F'/H_A) \cong (A/D)^*$. Hence, $(A/D)^*$ can be identified with a subgroup of $C\ell_D^+(A)$. Let V_D be the $\mathbf{F}_p$-vector space obtained by taking the quotient of $C\ell_D^+(A)$ by its maximal abelian subgroup, i.e.

$$V_D = C\ell_D^+(A)/C\ell_D^+(A)^p.$$

Since the p-rank of an abelian group is also equal to the number of summands in the direct product of its p-Sylow subgroup into cyclic components, the dimension κ of V_D is at least as large as that of $(A/D)^*/((A/D)^*)^p$ which, by Corollary 4.2.3 is $r\sum_{i=1}^{t} d_i(e_i - 1 - \lfloor (e_i-1)/p \rfloor)$.

Let S be a finite subset of $\mathbf{P}_F - \{\infty\}$, say $S = \{P_1, P_2, \ldots, P_N\}$. Clearly, each element of S can be viewed as a κ-vector in V_D. Write each element of S as a κ-tuple over $\mathbf{F}_p$. We again denote the vectors by $P_1, \ldots, P_N$. Let $\mathcal{G}(S, D)$ be the matrix whose columns are the vectors $P_1, P_2, \ldots, P_N$. Then, $\mathcal{G}(S, D)$ is a $\kappa \times N$ matrix over $\mathbf{F}_p$ of rank at most κ. Define $C(S, D)$ to be the linear code generated by the rows of $\mathcal{G}(S, D)$. Further, let $C(S, D)^\perp$ be the dual code of $C(S, D)$. Then, $C(S, D)^\perp$ is an $[N, \kappa^*]$-linear code over $\mathbf{F}_p$ with $\kappa^* \geq N - \kappa$ and

$$C(S, D)^\perp = \{(c_1, c_2, \ldots, c_N) \in \mathbf{F}_p^N : \sum_{i=1}^{N} c_i P_i = 0\}.$$

Lemma 4.2.4 *Suppose that there are l columns of $\mathcal{G}(S, D)$, say $P_{i_1}, \ldots, P_{i_l}$ of rank $\kappa' < \kappa$. Then there is a subfield L of F' such that $[L : F] = p^{\kappa - \kappa'}$ and $\infty, P_{i_1}, \ldots, P_{i_l}$ split completely in L/F.*

Proof: By assumption, there is a subgroup G of $C\ell_D^+(A)$ containing $P_{i_1}, \ldots, P_{i_l}$ and $C\ell_D^+(A)^p$ such that $[C\ell_D^+(A) : G] = p^{\kappa - \kappa'}$. Let L be the fixed field of G in F'/F. Then, $[L : F] = p^{\kappa - \kappa'}$ and by a consideration of the Artin symbols, it follows that $P_{i_1}, \ldots, P_{i_l}$

split completely in L/F. Moreover, since the ramification index of ∞ in F'/F is $q-1$ which is coprime to p, ∞ splits completely in L/F. $\square$

With this lemma, we can estimate the minimum distance of $C(S,D)$ as the following theorems and examples show. For the moment, D will be the divisor $2P$ (or equivalently, the prime ideal P^2 of A), where P is a place of F different from ∞ and $\deg P = d$.

Theorem 4.2.5 *Let F be a global function field with genus g and $N(F)$ rational places. Let*

$$\epsilon = \begin{cases} 1 & \text{if } d = 1, \\ 0 & \text{if } d > 1 \end{cases}$$

For $N \leq N(F) - 1 - \epsilon$, let $S \subseteq \mathbf{P}_F - \{P, \infty\}$ consist of N distinct rational places. Assume that S generates $C\ell_D^+(A)$ and that $N_q(pg - p + 1) \leq N_q(pg + (d-1)(p-1))$. Then, the code $C(S, P^2)$ constructed as described above is an $[N, \kappa, \delta]$-code over $\mathbf{F}_p$, where $\kappa \geq rd$ and δ satisfies

$$\delta \geq N + 1 - \lfloor \frac{N_q(pg + (d-1)(p-1)) - \epsilon}{p} \rfloor.$$

Proof: The length N is trivial. So let δ be the minimum distance of $C(S, P^2)$. By Corollary 4.1.9, there must exist $N - \delta$ columns of $\mathcal{G}(S, P^n)$ of rank $\kappa - 1$. Let S' be the set of places represented by these $N - \delta$ columns. By Lemma 4.2.4, we can construct a subfield L of F' such that $[L : F] = p$ and all the places in S' as well as ∞ split completely in L/F. As such, L has at least $p(N - \delta + 1)$ rational places. It remains to calculate the genus of L. Observe that P can be either unramified or totally ramified in L/F. In the former case, the Hurwitz genus formula gives

$$g(L) = 1 + p(g-1) = pg - p + 1.$$

In case P is totally ramified in L/F, since the conductor of P in $L/F \leq 2$, the genus of L is, according to Corollary 1.3.5, given by

$$g(L) = 1 - d + p(g - 1 + d) = pg + (d - 1)(p - 1).$$

Since

$$N_q(pg - p + 1) \leq N_q(pg + (d - 1)(p - 1))$$

by our assumption, the maximum number of rational places in L/F is $N_q(pg+(d-1)(p-1))$. Consequently,

$$p(N - \delta + 1) \leq N_q(pg + (d - 1)(p - 1)) - \epsilon$$

and our desired bound on δ follows. Finally as S generates $C\ell_D^+(A)$, $\kappa \geq rd$. □

The next corollary looks at a special case of Theorem 4.2.5.

Corollary 4.2.6 *Let F be the rational function field $F = \mathbf{F}_q(x)$. Suppose that all other notations are as in Theorem* 4.2.5. *Then, the code $C(S, P^2)$ is an $[N, \kappa, \delta]$-linear code over $\mathbf{F}_p$, where*

$$\begin{aligned} N &\leq q - \epsilon, \\ \kappa &= rd, \\ \delta &\geq N + 1 - \lfloor \frac{N_q((p-1)(d-1)) - \epsilon}{p} \rfloor. \end{aligned}$$

In particular, for $d = 1$ and $N = q - i, 1 \leq i \leq p$, the code $C(S, P^2)$ is optimal.

Proof: Since F is the rational function field, $g = 0$ and $N(F) = q + 1$. Further, $C\ell_{P^2}^+(A) = (A/P^2)^*$ which gives $\kappa = rd$. Since any intermediate field of F'/F must

be ramified, the first assertion follows from Theorem 4.2.5. Now, let $d = 1$ and $N = q - i, 1 \leq i \leq p$. Since $g(L) = 0$, L is also a rational function field. Therefore, $C(S, P^2)$ is a $[q - i, r, q - i + 1 - q/p] = [p^r - i, r, p^{r-1}(p-1) - i + 1]$-linear code over $\mathbf{F}_p$. Since

$$\begin{aligned} \sum_{j=0}^{r-1} \lceil \frac{p^{r-1}(p-1) - i + 1}{p^j} \rceil &= \sum_{j=0}^{r-1} p^j(p-1) - i + 1 \\ &= p^r - i \\ &= N, \end{aligned}$$

the Griesmer bound implies that $C(S, P^2)$ is optimal. □

Example 4.2.7 1. Let $d = 2$ and $q = 64$ in Corollary 4.2.6. Since $N_{64}(1) = 81$, we obtain binary $[64, 12, 25]$ and $[63, 12, 24]$ linear codes which are best known.

2. Let $d = 2$ and $q = 256$ in Corollary 4.2.6. Since $N_{256}(1) = 289$, we obtain binary $[256, 16, 113]$ and $[255, 16, 112]$ linear codes which are best known.

Theorem 4.2.8 *Let $F = \mathbf{F}_q(x)$ be the rational function field. Suppose that $N = \frac{q^p - q}{p}$. Let $S \subseteq \mathbf{P}_F$ consist of N distinct places of F of degree p and let P be a place of S with degree $\deg P = d \neq p$. Then, the code $C(S, P^2)$ is a $[N, rd, \delta]$-linear code over $\mathbf{F}_p$, where*

$$\delta \geq \begin{cases} N + \lceil \frac{pq + p - N_{q^p}((d-1)(p-1))}{p^2} \rceil & \text{if } d > 1, \\ \frac{(p-1)q^p}{p^2} & \text{if } d = 1 \end{cases}$$

Proof: Let δ be the minimum distance of $C(S, P^2)$. Then, Corollary 4.1.9 implies that there are $N - \delta$ columns of the generator matrix $\mathcal{G}(S, P^2)$ of rank $\kappa - 1$, κ being the dimension of $C(S, P^2)$. Denote by S' the set of all places represented by these columns. By Lemma 4.2.4, there exists a subfield L of F'/F such that $[L : F] = p$ and all places in

S' as well as ∞ split completely in L/F. Further, assume that δ' rational places split in L/F. Then L has $p(N-\delta)+q+1-\delta'+\epsilon$ places of degree p and $p\delta'+\epsilon$ rational places, where

$$\epsilon = \begin{cases} 1 & \text{if } d = 1, \\ 0 & \text{if } d > 1 \end{cases}$$

Let L' be the constant field extension $L' = L\mathbf{F}_{q^p}$. Since every place of L of degree p splits into p rational places in L' and every rational place of L remains rational in L', L' has at least

$$N(L') = p^2(N-\delta) + p(q+1-\delta'-\epsilon) + p\delta' + \epsilon = p^2(N-\delta) + p(q+1) + \epsilon(p-1)$$

rational places. Since P is the only ramified place in L with conductor ≤ 2, the Hurwitz genus formula yields

$$g(L') = g(L) = (d-1)(p-1).$$

Thus we have $N(L') \leq N_{q^p}((d-1)(p-1))$ which yields our desired assersions. □

Example 4.2.9 Let $p = 2$ and $d = 1$ in the preceding theorem. We obtain binary linear codes with parameters $[2^{r-1}(2^r-1), r, 2^{2r-2}]$. By the Griesmer bound, these codes are optimal.

Remark 4.2.10 *The above constructions can be similarly generalized to any positive divisor D in which ∞ is not in the support of D. Notice further that if $D = e_1P_1 + e_2P_2 + \cdots + e_tP_t$, where $P_1, \ldots, P_t$ are distinct places of F different from ∞, then the code $C(S, D)$ can be viewed as a direct sum of the codes $C(S, P_1^{e_1}), \ldots, C(S, P_t^{e_t})$.*

The next theorem examines the minimum distance of the dual code $C(S, P^n)^\perp$ for any integer n.

Theorem 4.2.11 *Let $S \subseteq \mathbf{P}_F - \{P, \infty\}$ consist of all the rational places of F different from ∞ and possibly P when $\deg P = 1$. Then, the code $C(S, P^n)^\perp$ has minimum distance δ', where*

$$\delta' \geq \begin{cases} nd + 1 - 2g(F) & \text{if } p|n, \\ (n-1)d + 1 - 2g(F) & \text{otherwise} \end{cases}$$

Proof: Let $\mathbf{c}$ be a codeword of $C(S, P^n)^\perp$ with $w(\mathbf{c}) = \mathbf{w}$. Without loss of generality, we may assume that the first w coordinates of $\mathbf{c}$ are nonzero. Write $\mathbf{c} = (c_1, \ldots, c_w, 0, \ldots, 0)$. Since $\mathcal{G}(S, P^n)$ is a parity-check matrix of $C(S, P^n)^\perp$,

$$\mathrm{c}\mathcal{G}(S, P^n)^T = (c_1, \ldots, c_w, 0, \ldots, 0)[P_1 P_2 \ldots P_N] = 0,$$

i.e.

$$\sum_{i=1}^{w} c_i P_i = 0.$$

This implies that there is a divisor D' of F such that the divisor $X = \sum_{i=1}^{w} c_i(P_i - \infty)$ and $X' = pD' - p \deg D' \infty$ are equivalent in the group $C\ell_{nP}^+(F)$. Furthermore, by Lemma 1.4.5, we may assume that D' is effective and $Supp(D') \cap \{\infty, P, P_1, \ldots, P_N\} = \emptyset$. We can therefore find an element $z \in F$ with

$$X - X' = \mathrm{div}(z)$$

and $z \equiv 1 \bmod nP$. Consider the subfield $F_0 = \mathbf{F}_q(z)$. We claim that the extension F/F_0 is separable. Suppose not. Then, $z \in F^p$, i.e. there is a $u \in F$ with $z = u^p$. This means that

$$\mathrm{div}(z) = \mathrm{div}(u^p) = p\mathrm{div}(u) \equiv 0 \bmod p.$$

Thus $X - X' \equiv 0 \bmod p$ which shows that $p|c_i$ for all $1 \leq i \leq w$. This clearly contradicts our assumption that $\mathbf{c}$ is nonzero. Consequently, F/F_0 is separable. Since $\mathrm{div}(z) = \sum_{Q \in \mathbf{P}_{F'}} \nu_Q(z)Q$, the ramification index of any place Q in $Supp(\mathrm{div}(z))$ lying over the zero place of z is just $|\nu_Q(z)|$. Hence, Proposition 1.1.10 yields the corresponding different exponents d_Q for Q lying over z as follows:

$$\begin{aligned} d_{P_i} &\geq c_i - 1, i = 1, \ldots, w, \\ d_Q &\geq p \deg Q \text{ for } Q \in Supp(D'), \\ d_\infty &\geq |p \deg D' - \sum_{i=1}^{w} c_i| - 1. \end{aligned}$$

Similarly, the ramification index of P lying over the place $z - 1$ is at least n which makes the different exponent d_P to be $d_P \geq n'$, where

$$n' = \begin{cases} n & \text{if } p|n, \\ n - 1 & \text{otherwise} \end{cases}$$

Applying the Hurwitz genus formula, we obtain

$$\begin{aligned} 2g(F) - 2 &= [F : F_0](-2) + \sum_{Q \in \mathbf{P}_F} d_Q \deg Q \\ &\geq -2|p \deg D' - \sum_{i=1}^{w} c_i| + \sum_{i=1}^{w}(c_i - 1) + p \deg D' + |p \deg D' - \sum_{i=1}^{w} c_i| - 1 + n'd \\ &\geq -w + n'd + 1. \end{aligned}$$

As a result, $w \geq n'd + 1 - 2g$ which in turn implies that the minimum distance of C must satisfy

$$\delta \geq n'd + 1 - 2g.$$

□

Remark 4.2.12 *The dual codes $C(S, P^n)^\perp$ are introduced by Xing in [88] for $n = p$.*

4.3 Function Fields Constructed from Linear Codes

We have seen how the minimum distance of the codes $C(S, D)$ can be estimated from bounds on the number of rational places of suitable global function fields. Conversely, by using the same construction discussed in the previous section, we can use known bounds on the minimum distance of codes to estimate the number of rational places that the associated global function fields contain. In some cases, these global function fields have sufficiently many rational places as compared to their genera.

In this section, we will use two examples to illustrate how this can be achieved. In both of our examples, the global function fields constructed have more rational places than currently known ones with the same genera.

We first quote, without proof, a lemma from [55, Chapter 1].

Lemma 4.3.1 *Let $F/\mathbf{F}_q$ be a global function field of genus g. Suppose that for some integer $d \geq 2$ we have*

$$q^d - 2gq^{d/2} > \sum_{r|d, r<d} (q^r + 2gq^{r/2}).$$

Then there exists at least one place of F of degree d.

Example 4.3.2 $g(L/\mathbf{F}_2) = 52, N(L/\mathbf{F}_2) \geq 36$. Consider the function field $F/\mathbf{F}_2$ in which $g(F) = 19$ and $N(F) = 20$. Such an F exists by [82]. Fix a rational place $\infty \in \mathbf{P}_F^1$ and

let $S = \mathbf{P}_F^1 - \{\infty\}$. By Lemma 4.3.1, we can find a place P of F with degree 15. Then the code $C(S, P^2)$ is a binary code with length 19 and dimension at least 15. Consider the parity-check matrix $\mathcal{H}(S, P^2)$ of $C(S, P^2)$. Clearly, $\mathcal{H}(S, P^2)$ is a $t \times 19$ matrix over $\mathbf{F}_2$ with $t \leq 4$. As there are at most 15 distinct nonzero t-tuples, we conclude from Theorem 4.1.5 that $C(S, P^2)$ has minimum distance at most 2. Consequently, by Corollary 4.1.9, there are 17 columns of $\mathcal{G}(S, P^2)$ of rank at most 14. With $d = 2$ and using these 17 columns, construct the field L as in Lemma 4.2.4. Then, all the 17 places represented by these columns as well as ∞ split completely in L/F. Thus, L has at least $2(17 + 1) = 36$ rational places. By the proof of Theorem 4.2.5, the genus of L is

$$g(L) = 2(19 - 1) = 36$$

or

$$g(L) = 2(19) + 14 = 52.$$

Since $N_2(36) = 31 < 36$ according to the table in [82], we conclude that $g(L) = 52$. The Oesterl*é* bound for $N_2(52)$ is 42. Note that this example improves the bound of $N_2(52) \geq 34$ given in [55, Table 4.5.2].

Example 4.3.3 $g(L/\mathbf{F}_{128}) = 13, N(L/\mathbf{F}_{128}) \geq 308$. Consider the function field $F/\mathbf{F}_{128}$ in which $g(F) = 4$ and $N(F) = 215$. Such an F exists by [82]. Fix a rational place $\infty \in \mathbf{P}_F^1$ and let $S = \mathbf{P}_F^1 - \{\infty\}$. By Lemma 4.3.1, we can find a place P of F with degree 6. Then the code $C(S, P^2)$ is a binary code with length 214 and dimension at least 42. Now, by Brouwer's table [7], the lower bound on the minimum distance of a $[214, 42]$-code is 61 while the upper bound is 82. Let δ be the minimum distance of $C(S, P^2)$. Thus, $\delta \leq 82$. By Corollary 4.1.9, there are $214 - \delta$ columns in the matrix $\mathcal{G}(S, P^2)$ with rank at most

41. With these $214 - \delta$ columns, construct the field L as in Lemma 4.2.4. Then all the $214 - \delta$ places represented by these columns as well as ∞ split completely in L/F. It follows that

$$N(L) \geq 2(215 - \delta) = 430 - 2\delta \geq 266.$$

From the proof of Theorem 4.2.5, the genus of L is given by

$$g(L) = 2(4 - 1) = 6$$

or

$$g(L) = 2(4) + 5 = 13.$$

Since $N_{128}(6) \leq 258$ according to the table [82], we conclude that $g(L) = 13$. Now, since the best known code of length 214 and dimension 42 has minimum distance 61, we may assume that $\delta \leq 61$. In this case, $N(L) \geq 308$. By the Oesterlé bound, $N_{128}(13) = 428$. Since $\lceil 428/\sqrt{2} \rceil = 299$, the field L constructed here has more rational places than the criteria for the lower entry of $N_{128}(13)$ in [82].

Remark 4.3.4 *In Example* 4.3.3*, notice that for* $61 \leq \delta \leq 65$*, L has sufficient rational places that meet the criteria for the lower entry of* $N_{128}(13)$ *in [82]. In this case, both the code* $C(S, P^2)$ *and the field L are better than the existing code and field with the same parameters. For* $66 \leq \delta \leq 82$*, the code* $C(S, P^2)$ *has minimum distance that improves the current lower bound.*

Chapter 5

More on Cyclotomic Function Fields

Thus far, we have developed numerous results on cyclotomic function fields, particularly in Chapters 2 and 3. We recall that cyclotomic function fields are special examples of narrow ray class fields with the base field being the rational function field. In this present chapter, we will make use of these results, as well as the interplay between error-correcting codes and function fields established in the preceding chapter, to construct subfields of cyclotomic function fields, thereby obtaining several new global function fields with improved lower bounds on the number of rational places for various genera.

The idea of using cyclotomic function fields to construct global function fields with many rational places was first suggested by Quebbemann [59]. Subsequently, extensive search among this family of class fields was conducted by a number of other researchers, including Niederreiter and Xing [41, 42, 46], Keller [30], Lauter [34] and Gebhardt [38]. In particular, Keller carried out an exhaustive search for cyclotomic function fields over $\mathbf{F}_2$ while Gebhardt extended the search to fields over $\mathbf{F}_q$ for small powers of 2, 3 and 5.

An advantage of using cyclotomic function fields is that its Galois group can be explic-

itly expressed, namely, it is the unit group of the ring of polynomials factored by its modulus. More specifically, using all the notations introduced in Section 2.4, the cyclotomic function field $F' = F(\Lambda_M)$ with modulus M has Galois group $\mathrm{Gal}(F'/F) = (R/(M))^*$. Thus, all rational places can be identified with linear polynomials and our problem is now reduced to finding the orders of subgroups generated by a set of linear polynomials $\mathcal{S}^*$ in this group.

Besides those notations of Section 2.4, we fix a few more notations to be used throughout this chapter. $\mathcal{S}^*$ will always denote the set of rational places (excluding ∞) that will generate the subgroup G_M of $(R/(M))^*$. For any factor M' of M, $\Omega(M')$ will denote the ratio $\Phi(M')/|G_{M'}|$, where $G_{M'}$ is the subgroup of $(R/(M'))^*$ generated by the places in $\mathcal{S}^*$ and $\mathbf{F}_q^*$. Finally, L will be the fixed field of F_M generated by the group G_M.

5.1 Cyclotomic Function Fields over $\mathbf{F}_p$

First of all, we let $q = p$ and concentrate on cyclotomic function fields over the prime field $\mathbf{F}_p$. In this case, F has p rational places apart from ∞.

The three examples below illustrate the construction in Theorem 3.5.1.

Example 5.1.1 $g(L/\mathbf{F}_3) = 44, N(L/\mathbf{F}_3) = 48$. Let $F = \mathbf{F}_3(x)$ be the rational function field. Let

$$M = (x^2+1)^2(x^2+x+2)^2(x^4+x^3+2x+1) = P_1^2P_2^2P_3 \in \mathbf{F}_3[x].$$

Consider the set $\mathcal{S}^* = \{x, x+1, x+2\}$. Then, the following give the relevant values of

$\Omega(M')$:

$$\Omega(M) = 12, \qquad \Omega(P_1^2P_2^2) = 3, \qquad \Omega(P_1P_2^2P_3) = 4,$$
$$\Omega(P_2^2P_3) = 2, \quad \Omega(P_1^2P_2P_3) = 4, \Omega(P_1^2P_3) = 1.$$

By Theorem 3.5.1, we have

$$2g(L) - 2 = 12(-2 + 12) - 4 \cdot 3 - 2 \cdot 4 - 2 \cdot 1 - 2 \cdot 4 - 2 \cdot 2 = 86,$$

thereby giving $g(L) = 44$. Moreover, $N(L) \geq 4[L : F] = 4 \cdot 12 = 48$. The Oesterlé bound gives $N_3(44) = 61$. Since $\lceil 61/\sqrt{(2)} \rceil = 44$, the field just constructed meets the criteria for the lower entry of the table in [82].

Example 5.1.2 $g(L/\mathbf{F}_7) = 4, N(L/\mathbf{F}_7) = 24$. Let $F = \mathbf{F}_7(x)$ be the rational function field. Consider

$$M = x^3 - 1 = (x + 3)(x + 5)(x + 6) \in \mathbf{F}_7[x].$$

Then, $\Phi(M) = 6^3 = 216$. Since $x^3 \equiv 1 \bmod M$, $|G_M| = 18$ and so $[L : F] = \Omega(M) = 12$. Direct computations show that

$$\Omega((x + 3)(x + 5)) = \Omega((x + 3)(x + 6)) = \Omega((x + 5)(x + 6)) = 2.$$

Therefore, Theorem 3.5.1 gives

$$g(L) = 1 + \frac{1}{2}(12(-2) + 3(12) - 2 - 2 - 2) = 4$$

and $N(L) = 24$. The Oesterlé bound for $N_7(4)$ is 25.

Example 5.1.3 $g(L/\mathbf{F}_7) = 7, N(L/\mathbf{F}_7) = 32$. Let $F = \mathbf{F}_7(x)$ be the rational function field. Let $M = (x^2 + 2)(x^2 + 4) \in \mathbf{F}_7[x]$. Consider $\mathcal{S}^* = \{x, x + 1\}$. Clearly, $\Phi(M) = 48^2$.

Since $|G_M| = 288$, we have $[L : F] = \Omega(M) = 8$. Further, direct computations show that $\Omega(x^2 + 2) = \Omega(x^2 + 4) = 1$ and G_M contains the rational places $x, x + 1$ and $x + 5$. Consequently, by Theorem 3.5.1,we have

$$g(L) = 1 + \frac{1}{2}(8(-2) + 4(8) - 2(1) - 2(1)) = 7$$

and $N(L) = 32$. The Oesterlé bound for $N_7(7)$ is 36.

Using a similar approach as the above examples, we record, in Table 5.1.1 below, some cyclotomic function fields over $\mathbf{F}_7$ for several other genera. Note that the fields listed have more number of rational places than those constructed from subfields of Hilbert class fields and having the same genera (see [74]). In the table, $\mathcal{S}^*$ always denotes the minimum set of linear polynomials that generate the group G_M for a modulus M. The number $l(\mathcal{S}^*)$ refers to the number of linear polynomials in the group G_M. Hence, $N(L) = (l(\mathcal{S}^*) + 1)[L : F]$. To allow for comparison, we provide the Oesterlé bound $N_7(g)$ for the genus g in the last column.

Table 5.1.1. Bounds for $N_7(g)$

M	$\mathcal{S}^*$	$l(\mathcal{S}^*)$	$[L:F]$	g	$N(L)$	$N_7(g)$
$6+x^3$	$\{x\}$	1	12	4	24	25
$1+2x^2+x^4+x^6$	$\{x, x+1, x+2\}$	5	4	5	24	29
$1+3x+2x^2+3x^3+x^4$	$\{x\}$	2	8	6	24	32
$1+6x^2+x^4$	$\{x, x+1\}$	3	8	7	32	36
$2+x^3$	$\{x\}$	1	19	9	38	42
$1+3x^2+x^3+3x^5+x^6$	$\{x, x+1\}$	5	12	10	36	45
$3+6x+6x^2+4x^3+x^4+x^5$	$\{x, x+1\}$	2	12	11	36	49
x^6	$\{x+1, x+2, x+3, x+4\}$	4	7	12	36	52
$1+x+5x^2+6x^3+6x^4+2x^5+x^6$	$\{x\}$	4	8	14	40	57
$4+2x+3x^2+2x^3+x^4$	$\{x\}$	2	16	15	48	60
$6+6x+5x^2+3x^3+x^4$	$\{x\}$	1	16	16	48	63
$5+5x+3x^3+x^4$	$\{x\}$	1	16	20	48	74
$6+2x+3x^4+6x^5+x^6$	$\{x, x+1, x+2\}$	3	16	21	64	77
$1+4x+2x^2+4x^3+x^4$	$\{x, x+1\}$	2	24	22	72	79
$3+x+5x^2+6x^3+2x^4+x^5+x^6$	$\{x\}$	3	16	23	64	82
$2+3x+x^2+6x^4+x^5$	$\{x, x+1\}$	2	24	25	72	87
$3+3x+2x^3+x^4$	$\{x\}$	1	36	28	72	95
$3+4x^2+5x^4+2x^5$	$\{x, x+1\}$	2	24	29	72	98
$2+2x+3x^3+x^4+x^6$	$\{x, x+1\}$	4	19	36	95	117

Next, let us consider the case when $M = P^n$ for a certain place P of F of degree d.

Definition 5.1.4 A finite set $\mathcal{S}^* \subseteq \mathbf{P}_F - \{P, \infty\}$ is said to be **independent mod** P^n if it is $\mathbf{F}_p$/-linearly independent in the vector space V_{P^n} (refer to Section 4.2 for the definition of V_{P^n}.)

Let S consist of all the rational places of F other than ∞ and possibly P, when $\deg P = 1$. As such, $|S| = p - \epsilon$, where

$$\epsilon = \begin{cases} 1 & \text{if } d = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Consider the code $C(S, P^n)$. Then, $C(S, P^n)$ is a $[p-\epsilon, \kappa \leq d(n-1-\lfloor (n-1)/p \rfloor]$-code over $\mathbf{F}_p$. First, consider $n < \lfloor (p-\epsilon)/d \rfloor + 1 < p$. Now by Theorem 4.2.11, $C(S, P^n)^\perp$ has minimum distance at least $(n-1)d+1$. Applying Theorem 4.1.5, and since the number of linearly independent vectors cannot exceed the dimension $\kappa \leq d(n-1)$, we can conclude that $C(S, P^n)^\perp$ has minimum distance exactly $(n-1)d+1$. Consequently, any subset of $\leq d(n-1)$ rational places of F must be independent mod P^n and $\kappa = d(n-1)$. On the other hand, for $n \geq \lfloor (p-\epsilon)/d \rfloor + 1$, it is clear that the generator matrix $\mathcal{G}(S, P^n)$ is a $(p-\epsilon) \times (p-\epsilon)$ invertible matrix, i.e. all $p-\epsilon$ rational places are independent mod P^n. Together with Proposition 3.5.2, we can easily prove the following lemma.

Lemma 5.1.5 *Let $\mathcal{S}^* \subset \mathbf{P}_F - \{\infty, P\}$ consist of k rational places of F, where $k \leq p-\epsilon$. Write $k = ad+b$, where $0 \leq b < d$. Then for any positive integer $n > 1$, we have*

$$\Omega(P^n) = \omega \frac{p^{n-1}}{(n/(a+1))_p^b \prod_{i=1}^a (n/i)_p^d},$$

where $\omega = \Omega(P)$.

Proof: Let $\mathcal{S}^* = \{P_1, P_2, \ldots, P_k\}$. For $i = 1, \ldots, d$, it is clear from Proposition 3.5.2 that $|\langle P_i \rangle_n| = \omega_i n_p$, where $\omega_i = |\langle P_i \rangle_1|$. Thus,

$$|\langle P_1, \ldots, P_d \rangle_n| = \omega' n_p^d,$$

where $\omega' = |\langle P_1, \ldots, P_d \rangle_1|$. From our above discussion, $P_{d+1} \in \langle P_1, \ldots, P_d \rangle_2$ but $P_{d+1} \notin \langle P_1, \ldots, P_d \rangle_3$. Applying Proposition 3.5.2 yields $|\langle P_1, \ldots, P_{d+1} \rangle_n| = \omega' |\langle P_1, \ldots, P_d \rangle_n| (n/2)_p = \omega' n_p^d (n/2)_p$. Continuing in this way for $i = d+2, \ldots, k$ and recalling that $\Phi(P^n) = (p^d - 1)p^{d(n-1)}$, we obtain

$$|\langle P_1, \ldots, P_k \rangle_n| = \omega' (n/(a+1)_p \prod_{i=1}^{b} (n/i)_p^d.$$

Consequently,

$$\Omega(P^n) = \omega \frac{p^{n-1}}{(n/(a+1))_p^b \prod_{i=1}^{a} (n/i)_p^d},$$

where $\omega = (p^d - 1)/\omega' = \Omega(P)$. □

With these computations, the genus and number of rational places of the field L constructed in Theorem 3.5.1 can be written down explicitly.

Corollary 5.1.6 *Let $\mathcal{S}^* \subset \mathbf{P}_F - \{\infty, P\}$ consist of k rational places of F, where $k \leq p - \epsilon$. Write $k = ad + b$, where $0 \leq b < d$. Then the subfield L of the cyclotomic function field $F(\Lambda_{P^n})/F$ constructed as the fixed field of G_{P^n} has genus*

$$2g(L) - 2 = \Omega(P^n)(dn - 2) - d(1 + \sum_{i=1}^{n-1} \Omega(P^i)),$$

where $\Omega(P^j) = \Omega(P) \frac{p^{d(j-1)}}{(j/(a+1))_p^b \prod_{i=1}^{a} (j/i)_p^d}$ for $n \geq 2$. Further, L has exactly

$$N(L) = (k+1)\Omega(P^n) + \epsilon$$

rational places.

Example 5.1.7 Put $d = 1$ in the above corollary. Then

$$g(L) = \frac{p^{n-1}}{2\prod_{i=1}^{k} (n/i)_p}(n-2) - \sum_{j=2}^{n-1} \frac{p^{j-1}}{2\prod_{i=1}^{k} (j/i)_p}$$

and

$$N(L) = \frac{p^{n-1}}{\prod_{i=1}^{k} (n/i)_p}(k+1) + 1.$$

5.2 Cyclotomic Function Fields over $\mathbf{F}_{p^r}$

In this section, we return to the situation of $q = p^r$. We will construct several subfields of cyclotomic function fields in which the number of rational places improves the lower bounds given in [82].

We begin with an example.

Example 5.2.1 $g(L/\mathbf{F}_{16}) = 29, N(L/\mathbf{F}_{16}) = 162$. Let F be the rational function field $F = \mathbf{F}_{16}(x)$ and let α be a primitive element of $\mathbf{F}_{16}^*$ with $\alpha^4 + \alpha + 1 = 0$. Put $M = (x+\alpha^7)^2(x+\alpha^8)^2(x+\alpha^{14})^2 = (x^2+\alpha)(x^2+\alpha^{13})(x^2+\alpha^{14})$. Consider the cyclotomic function field $F_M = F(\Lambda_M)$. With $\mathcal{S}^* = \{x+\alpha^i : 0 \le i \le 6\} \cup \{x\}$, construct the field L as in Theorem 3.5.1. We compute the relevant values of $\Omega(M')$ below.

$$\begin{aligned}
\Omega(M) &= [L:F] = 16, \\
\Omega((x+\alpha^7)(x+\alpha^8)^2(x+\alpha^{14})^2) &= \Omega((x+\alpha^8)^2(x+\alpha^{14})^2) = 2, \\
\Omega((x+\alpha^7)^2(x+\alpha^8)(x+\alpha^{14})^2) &= \Omega((x+\alpha^7)^2(x+\alpha^{14})^2) = 1, \\
\Omega((x+\alpha^7)^2(x+\alpha^8)^2(x+\alpha^{14})) &= \Omega((x+\alpha^7)^2(x+\alpha^8)^2) = 1.
\end{aligned}$$

Thus, the genus of L is given by

$$g(L) = 1 + \frac{1}{2}(16(-2+6) - 2 - 2 - 1 - 1 - 1 - 1) = 29.$$

Further, it can be checked that apart from the places in $\mathcal{S}^*$, G_M contains $x+\alpha^{10}$ as well. Since both $x+\alpha^8$ and $x+\alpha^{14}$ are totally ramified in L/F,

$$N(L) = 10(16) + 2 = 162.$$

This example improves the lower bound of $N_{16}(29) \ge 161$ given in [82].

Next for a positive integer $n \geq 2$, consider $M = x^n$. Let α be a fixed primitive element of $\mathbf{F}_q^*$. We denote by P_i the zero of $x - \alpha^i, i = 0, \ldots, q-2$. Let $S = \{P_0, P_1, \ldots, P_{N-1}\}$, where $N = q-1$ and construct the code $C(S, x^n)$. Write the generator matrix of $C(S, x^n)$ as

$$\mathcal{G}(S, x^n) = [P_0 P_1 \ldots P_{N-1}].$$

We will prove in Proposition 5.2.3 that $C(S, x^n)$ is the dual of a narrow-sense BCH code. To do this, let us first recall the Newton's formulas involving the sums of powers of roots of a polynomial.

Lemma 5.2.2 (Newton's formula) *Let $f(x) = \sum_{i=0}^{l} \beta_i x^i$ be a polynomial over $\mathbf{F}_p$ with reciprocal roots $\alpha_1, \alpha_2, \ldots, \alpha_l$, i.e.*

$$f(x) = \prod_{i=1}^{l} (1 - \alpha_i x).$$

For any integer u, let $y_u = \sum_{i=1}^{l} \alpha_i^u$. Then

$$s\beta_s + \sum_{i=1}^{s} \beta_i y_{s-i} = 0$$

for any positive integer s.

Proposition 5.2.3 *The code $C(S, x^n)^\perp$ is a narrow-sense* BCH *code with designed distance $\delta_0 = n$.*

Proof: Let $\mathbf{c} = (c_0, c_1, \ldots, c_{N-1}) \in \mathbf{C}(\mathbf{S}, \mathbf{x^n})^\perp$. We need to show that α^s is a root of $c(x) = \sum_{i=0}^{N-1} c_i x^i$ for all $s = 1, 2, \ldots, n-1$. Since $\mathcal{G}(S, x^n)$ is a parity-check matrix of $C(S, x^n)^\perp$, we have

$$\sum_{i=0}^{N-1} c_i P_i = 0.$$

By identifying $c_i \in \mathbf{F}_p$ with the corresponding integer $c_i \in \mathbf{Z}$, it follows that there exists a polynomial $f(x) \in (\mathbf{F}_q[x]/(x^n))^*$ such that

$$\prod_{i=0}^{N-1}(x-\alpha^i)^{c_i} \equiv f(x)^p \equiv f(x^p) \bmod (p, x^n).$$

Factoring out the constants, the above is equivalent to

$$\prod_{i=0}^{N-1}(1-\alpha^i x)^{c_i} \equiv f'(x^p) \bmod (p, x^n)$$

for some $f'(x)$. Now write $\prod_{i=0}^{N-1}(1-\alpha^i x)^{c_i} = \sum_{j=0}^{\infty}\beta_j x^j$. Clearly, $\beta_0 = 1$ and $\beta_j \equiv 0 \bmod p$ for all $j = 1, \ldots, n-1$ and $\gcd(j,p) = 1$. We claim that for integers $s = 1, \ldots, n-1$,

$$c(\alpha^s) = \sum_{i=0}^{N-1} c_i \alpha^{is} = 0.$$

We prove this by induction on $s < n$. By the Newton's formulas,

$$\beta_1 \equiv -\beta_0 c(\alpha) \equiv -c(\alpha) \equiv 0 \bmod p.$$

The result is thus true for $s = 1$. So assume that the result holds for all positive integers $\leq s-1 < n$. By the Newton's formulas again,

$$s\beta_s = -\sum_{j=1}^{s}\beta_j c(\alpha^{s-j}) \bmod p.$$

By our induction hypothesis, this becomes $c(\alpha^s) \equiv -s\beta_s \bmod p$. But $s\beta_s \equiv 0 \bmod p$ for all $s < n$. Hence our claim is shown. Consequently, $C(S, x^n)^\perp$ is a narrow-sense BCH code with designed distance at least n. By the arguments just discussed, it is clear that if $c(x)$ is the lcm of all the minimal polynomials of α^j for $j = 1, \ldots, n-1$, then the codeword $\mathbf{c}$ corresponding to $c(x)$ is a codeword in $C(S, x^n)^\perp$. From the definition of a narrow-sense BCH code, this shows that the designed distance of $C(S, x^n)^\perp$ is exactly n. $\square$

Corollary 5.2.4 *$C(S, x^n)$ is a cyclic code with generator polynomial $g(x) = x^N h(1/x)$, where*

$$h(x) = \mathrm{lcm}(m_1(x), \ldots, m_{n-1}(x)).$$

Proof: This is an immediate consequence of Propositions 5.2.3 and 4.1.12. □

Corollary 5.2.5 *The code $C(S, x^n)$ has dimension $\kappa = r(n-1-\lfloor (n-1)/p \rfloor)$ if $n \leq p^{\lceil r/2 \rceil}$.*

Proof: By Corollary 4.1.18 and our assumption on n,, $C(S, x^n)^{\perp}$ has dimension $q-1-r(n-1-\lfloor (n-1)/p \rfloor)$. Hence, the dimension of $C(S, x^n)$ is $r(n-1-\lfloor (n-1)/p \rfloor)$. □

Remark 5.2.6 *The rank of $C(S, x^n)$ was first shown by Lauter in [34] using generalized Witt vectors. However, our proof follows that given in [2].*

In Section 4.3, we have seen that upper bounds on the minimum distances of the codes $C(S, D)$ can be used to estimate the number of rational places of the fields constructed by means of Lemma 4.2.4. Unfortunately, this method does not often lead to "good' global function fields as large minimum distances necessarily result in fewer rational places (see for example Theorems 4.2.5 and 4.2.8).

For the codes discussed in this section, we have shown that their structures are explicitly known. As such, we can exploit Mathematical software packages such as Mathematica or magma to look for subsets of S of different ranks, and then construct fields based on Lemma 4.2.4. Lemma 4.1.8 suggests how we can search for good subsets.

More specifically, we define recursively the codes $C_0, C_1, \dots$ and their respective fields $L_0, L_1, \dots$ as follows. Let $C_0 = C(S, x^n), S_0 = S, \delta_0 = d(C_0)$, and $\mathrm{c}_0 \in C_0$ with weight $w(\mathbf{c_0}) = \delta_\mathbf{0}$. Construct L_0 by the method in Lemma 4.2.4 with $\mathcal{S}^* = S - \mathrm{supp}(\mathbf{c_0})$ as the generating set. Now, assume that $C_i, S_i, \delta_i, \mathbf{c_i}$ and L_i have been constructed. Let $S_{i+1} = S_i - \mathrm{supp}(\mathbf{c_i})$, C_{i+1} be the residual code of C_i at $\mathbf{c_i}$, $\delta_{i+1} = d(C_{i+1}), \mathrm{c}_{i+1} \in C_{i+1}$ with $w(\mathbf{c_{i+1}}) = \delta_\mathbf{i+1}$ and L_{i+1} as the field constructed with $\mathcal{S}^* = S_{i+1} - \mathrm{supp}(\mathbf{c_{i+1}})$ as the generating set.

Proposition 5.2.7 *Suppose that $C(S, x^n)$ has dimension $n - 1 - \lfloor (n-1)/p \rfloor$. With $C_i, S_i, \delta_i, \mathbf{c_i}$ and L_i as above, the following are true.*

(i) *For $i = 0, \dots, r-1$, $[L_i : F] = p^{i+1}$.*

(ii) *All places in S_{i+1} split completely in L_i/F. In particular, L_i has $(|S_{i+1}|+1)p^i + 1 = (q - \sum_{i=0}^{i} \delta_i)p^{i+1} + 1$ rational places*

(iii) *The genus of L_i is given by*

$$g(L_i) \leq (p^i - 1)(n-2)/2$$

and equality holds if the places in S_{i+1} generate $C(S, x^{n-1})$.

Proof: All the assertions can be proven by induction on i by using Lemma 4.2.4 and Lemma 4.1.8. For the genus, we apply the genus formula given in Theorem 3.5.1. □

With this procedure, we use the Mathematica to determine the sequences $(\delta_0, \delta_1, \dots)$ and their respective sets $(S_0, S_1, \dots)$ for $q = 27, 32, 64, 81$ and 128. The following new function fields are obtained. As in [82], we restrict our search for fields with genus at

most 50. In addition, we give values for $N_{27}(51), N_{27}(52), N_{81}(51)$ and $N_{81}(52)$. Note that to compute the genus of L_i, we need to know the rank of the places in S_{i+1} with respect to the codes $C(S, x^j), j < n$. Clearly, if the places in S_{i+1} generate $C(S, x^j)$, they generate $C(S, x^{j'})$ for all $j' < j$. In Table 5.2.1, κ_j refers to the rank S_{i+1} with respect to the code $C(S, x^j)$. In the last column, we give the range of $N_q(g)$ taken from [82]. In the case where no entry is entered in that table, we provide the Oesterlé bound for comparison.

Table5.2.1. Improved lower bounds on $N_q(g)$

q	n	i	$(\delta_0, \dots, \delta_i)$	$(\kappa_{n-1}, \kappa_{n-2}, \dots)$	g	$N(L)$	$N_q(g)$
64	6	2	$(16, 8, 8)$	$(12, \dots)$	14	257	$241 - -284$
64	8	2	$(14, 7, 6)$	$(18, \dots)$	21	297	$281 - -396$
64	8	3	$(14, 7, 6, 5)$	$(17, 17, 12, \dots)$	44	513	695
128	6	3	$(48, 24, 14, 7)$	$(13, 13, 7, \dots)$	29	561	785
27	6	2	$(9, 3, 3)$	$(8, 6, \dots)$	51	361	423
27	6	2	$(9, 3, 1)$	$(9, \dots)$	52	379	430
81	3	2	$(48, 16, 6)$	(4)	13	298	$256 - 312$
81	8	1	$(30, 10)$	$(15, 15, 12, \dots)$	22	370	478
81	8	1	$(30, 10)$	$(16, \dots)$	24	370	514
81	3	3	$(48, 16, 6, 2)$	(3)	39	730	769
81	6	2	$(30, 15, 8)$	$(11, 8, \dots)$	51	757	923
81	6	2	$(30, 10, 13)$	$(12, \dots)$	52	757	936

Chapter 6

Bounds on $A(q)$

In this final chapter, we turn to a somewhat different topic, namely, we will investigate the behaviour of the ratio $N_q(g)/g$ as g tends to infinity.

6.1 Some general results on $A(q)$

In [28], Ihara introduced the following quantity

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

This asymptotic quantity, which we simply refer to as $A(q)$ is of interest as it has significant and direct applications to the construction of good algebraic-geometric codes.

As a consequence of the Serre bound on $N_q(g)$(1.5.9), we immediately obtain an upper bound on $A(q)$, namely,

$$A(q) \leq \lfloor 2q^{1/2} \rfloor$$

for all prime powers q. Vladut and Drinfeld established an improved upper bound on

$A(q)$ in [84]. They showed that for all q,

$$A(q) \leq q^{1/2} - 1.$$

By constructing an explicit tower of class fields, Garcia and Stichtenoth proved that this bound is in fact sharp when q is a square [13], [15].

However for nonsquares q, the exact value of $A(q)$ remains a challenge. As such, Mathematicians have concentrated on providing general results on the lower bounds on $A(q)$. For instance, by employing class field towers, Serre [66, 69] showed that there is a constant $c > 0$ such that $A(q) \geq c \log q$. This was later improved by Li and Maharaj [37] and Temkine [73] who proved that there exists an effective absolute constant $c > 0$ such that for any prime power q and any integer $m \geq 1$, we have

$$A(q^m) \geq \frac{cm^2(\log q)^2}{\log m + \log q}.$$

Moreover, Zink [97] gave a lower bound on $A(p^3)$ for any prime p, which states that

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}.$$

For more classes of composite q, Perret [58] proved that if m is a prime and $q = p^r$ is a prime power with $q > 4m + 1$ and $q \equiv 1 \pmod{m}$, then

$$A(q^m) \geq \frac{m^{1/2}(q-1)^{1/2} - 2m}{m-1}.$$

Subsequently, Niederreiter and Xing generalized and improved this bound to the following (refer to [50, 55]) :

Theorem 6.1.1 (i) *If $q = p^r$ with an odd prime p and an odd integer $r \geq 3$, then*

$$A(q) \geq \frac{2q^{1/m} + 2}{\lceil 2(2q^{1/m} + 3)^{1/2} \rceil + 1},$$

where m is the least prime dividing r.

(ii) *If $q = 2^r$ with an odd composite integer $r \geq 3$, then*

$$A(q) \geq \frac{q^{1/m} + 1}{\lceil 2(2q^{1/m} + 2)^{1/2} \rceil + 2},$$

where m is the least prime dividing r.

Further refinements of the above theorem are given in Li and Maharaj [37] and in Niederreiter and Xing [50].

So far, no general results on lower bounds on $A(p)$ for primes p have been established. Instead, attempts have been made to provide explicit lower bounds on $A(p)$ for small primes p. In the next section, we will present improved lower bounds on $A(p)$ for $p = 2, 5, 7$ and 11.We summarize the results in the table below.

Table 6.1.1. Lower bounds on $A(p)$

p	Existing bound	Source	Improved bound
2	0.2555...	[48]	0.257979...
3	$0.4705\ldots$	[1], [73]	—
5	$0.7272\ldots$	[1], [73]	$0.7333\ldots$
7	0.9	[37]	0.9375
11	$1.0909\ldots$	[37]	$1.1666\ldots$
13	$1.333\ldots$	[37]	—
17	1.6	[37]	—

Finally, we will discuss, in the next section, an improvement to Theorem 6.1.1 (i), i.e. the lower bound on $A(q)$ for odd, composite and nonsquares q.

6.2 Improved lower bounds on $A(q)$

The proofs on the lower bounds of $A(q)$ that follow will essentially depend on the lower bounds for the l-rank of fractional ideal class groups as the next theorem shows.

Theorem 6.2.1 *Let $F/\mathbf{F}_q$ be a global function field of genus $g(F) > 1$ and let $\mathcal{S}$ be a subset of $\mathbf{P}_F$ such that $\mathcal{S}' := \mathbf{P}_F - \mathcal{S}$ is a nonempty set of rational places of F. Suppose that there exists a prime number l such that*

$$d_l(\mathrm{Cl}(O_{\mathcal{S}})) \geq 2 + 2(|\mathcal{S}'| + \varepsilon_l(q))^{1/2},$$

where $\varepsilon_l(q) = 1$ if $l|(q-1)$ and $\varepsilon_l(q) = 0$ otherwise. Then we have

$$A(q) \geq \frac{|\mathcal{S}'|}{g(F) - 1}.$$

In view of this theorem, it is obvious that a good lower bound on the l-rank of the $\mathcal{S}$-ideal class group will inevitably lead to better lower bounds of $A(q)$. As such, the next result, proven by Niederreiter and Xing using cohomology in [48], or alternatively proven by Li and Maharaj via the properties of narrow ray class fields [37], will be useful.

Proposition 6.2.2 *Let $F/\mathbf{F}_q$ be a global function field and F'/F a finite abelian extension. Let $\mathcal{T}$ be a proper subset of $\mathbf{P}_F$ such that $\mathcal{T}' := \mathbf{P}_F - \mathcal{T}$ is finite and let $\mathcal{S}$ be the over-set of $\mathcal{T}$ with respect to F'/F. Then for any prime number l we have*

$$d_l(Cl(O_{\mathcal{S}})) \geq \sum_P d_l(G_P) - (|\mathcal{T}'| - 1 + \varepsilon_l(q)) - d_l(G),$$

where $\varepsilon_l(q)$ is defined as in Theorem 6.2.1*, $G = \mathrm{Gal}(F'/F)$, and G_P is the inertia group of the place P in F'/F. The sum is extended over all places P of F.*

A close examination of Proposition 6.2.2 reveals that a larger l-rank of the $\mathcal{S}$-ideal class group requires a sufficient number of ramified places, but this will in turn increase the genus of the field. Since the lower bound of $A(q)$ given in Theorem 6.2.1 depends on both the l-rank and the genus, we need to construct the fields carefully to achieve better bounds. In fact, all the improved bounds have been achieved by looking for function fields with a bigger ratio of $|\mathcal{S}'|$ to the genus $g(L)$.

In the ensuing examples, cyclotomic function fields will be employed to construct our field when $p = 2$ while all other fields will be constructed from Kummer extensions.

Proposition 6.2.3

$$A(2) \geq 97/376 = 0.257979\ldots.$$

Proof: As in [48], our field is constructed as the compositum of the subfields of cyclotomic function fields. Let $F = \mathbf{F}_2(x)$ be the rational function field.

(i) Let $F_1 = F(\Lambda_M)$, with the modulus $M = (x^4 + x^3 + x^2 + x + 1)^2$ and let L_1 be the subfield of F_1/F fixed by the subgroup of $(\mathbf{F}_2[x]/(M))^*$ generated by x. Since $\Phi(M) = 240$ and $x^{10} \equiv 1 \bmod M$, it follows that $\Omega(M) = [L_1 : F] = 24$. Since $\Omega(x^4 + x^3 + x^2 + x + 1) = 3$, the genus formula in Theorem 3.5.1 gives

$$g(L_1) = 1 + \frac{1}{2}(24(-2 + 8) - 4 \cdot 3 - 4) = 65.$$

Notice that since x and ∞ split completely in L_1/F, L_1 has 48 rational places, with 24 places lying over each of x and ∞.

(ii) Next consider the cyclotomic function field $F_2 = F(\Lambda_N)$, where $N = x^4$. Let L_2 be the subfield of F_2 fixed by the subgroup of $(\mathbf{F}_2[x]/(N))^*$ generated by $x^2 + 1$. Since

$(x^2+1)^2 \equiv 1 \bmod x^4$, it follows that $\Omega(N) = [L_2 : F] = 4$. In addition, we have $\Omega(x^3) = \Omega(x^2) = 2$ and $\Omega(x) = 1$. So if P denotes a place of L_2 lying over x, we see from Theorem 1.3.3 and the fact that x is totally ramified in L_2/F that

$$d(P|x) = 4 \cdot 4 - 2 - 2 - 1 - 1 = 10.$$

Observe that $\mathrm{Gal}(L_2/F)$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$.

Now, let L be the compositum of L_1 and L_2. By considering the ramification behaviour of x, it is clear that both L_1 and L_2 are linearly disjoint. Further, only the places of L_1 lying over x can ramify in L/L_1. If Q_1 is a place of L_1 lying over x, and Q is a place of L lying over Q_1, it follows from (ii) and the tower formula for different exponents that $d(Q|Q_1) = 10$. Hence, the genus of L can now be calculated as

$$g(L) = 1 + \frac{1}{2}(4(2 \cdot 65 - 2) + 24 \cdot 10) = 377.$$

Let $\mathcal{T}' \subseteq \mathbf{P}_{L_1}$ consist of all the 24 places lying over ∞ as well as 1 place lying over x and let $\mathcal{S}'$ be the overset of $\mathcal{T}'$ with respect to L/L_1 so that $|\mathcal{T}'| = 25$ and $|\mathcal{S}'| = 97$. By Proposition 6.2.2,

$$d_2(\mathrm{Cl}(O_{\mathcal{S}})) \geq 24(2) - (25-1) - 2 = 22 \geq 2 + 2\sqrt{|\mathcal{S}'|}.$$

Since the condition in Theorem 6.2.1 is satisfied, we may apply its result to yield

$$A(2) \geq \frac{|\mathcal{S}'|}{g(L) - 1} = \frac{97}{376} = 0.257979\ldots$$

□

Proposition 6.2.4

$$A(5) \geq 11/15 = 0.7333...$$

Proof: Let F be the rational function field $\mathbf{F}_5(x)$. Consider the field $F' = F(y)$, where

$$y^2 = f(x) = x^5 + 4x + 1.$$

Then, F' is a Kummer extension of F as in Theorem 2.2.2. Since $\deg f$ is odd and $f(a) \equiv 1 \bmod 5$ for all $a \in \mathbf{F}_5$, Corollary 2.2.3 and Theorem 2.2.6 imply that $g(F') = 2$ and all the 5 finite rational places split completely in F'/F while ∞ is totally ramified in F'/F. Further, the following five places of degree 2 split completely in F'/F as well:

$$P_1 = x^2 + 2, \quad P_2 = x^2 + x + 1, \quad P_3 = x^2 + 2x + 3,$$
$$P_4 = x^2 + 3x + 3, \quad P_5 = x^2 + 4x + 1.$$

Let

$$z^2 = g(x) = x(x+1)(x+3)P_1P_2P_3P_4P_5$$

and put $L = F'(z)$. L/F' is again a Kummer extension with $[L : F'] = 2$. From Theorem 2.2.2 again, we see that all the 16 places lying above $x, x+1, x+3, P_i, 1 \leq i \leq 5$ ramify in L/F'. Thus the genus of L is given by

$$2g(L) - 2 = 2 \cdot 2 \cdot (2-1) + 2 \cdot 3 + 2 \cdot 10,$$

thereby yielding $g(L) = 16$. Now, let $\mathcal{T}'$ be the set consisting of the following 6 places of F':

(i) The two places lying above $x + 2$;

(ii) The two places lying above $x + 4$;

(iii) P_∞, the unique place lying above ∞

(iv) One of the places lying above x. Since $z^2 \equiv 1 \pmod{x+2}$ and $z^2 \equiv 4 \pmod{x+4}$, the 4 places lying over $x+2$ and $x+4$ split completely in L/F'. Moreover, since

$$\nu_{P_\infty}(g(x)) = 2\nu_\infty(g(x)) = -26$$

which is even, P_∞ splits completely in L/F' too. Hence, if $\mathcal{S}'$ is the overset of $\mathcal{T}'$ with respect to the extension L/F', we apply Proposition 6.2.2 to obtain

$$d_2(\mathrm{Cl}(O_{\mathcal{S}})) \geq 16 - 6 - 1 = 9 \geq 2 + 2\sqrt{2 \cdot 5 + 1 + 1} = 8.9282.$$

Consequently, we conclude from Theorem 6.2.1 that

$$A(5) \geq \frac{|\mathcal{S}'|}{g(L) - 1} = \frac{11}{15} = 0.7333...$$

□

We use a similar approach in Proposition 6.2.4 to prove the next two propositions.

Proposition 6.2.5

$$A(7) \geq 15/16 = 0.9375.$$

Proof: Let F' be the elliptic function field in Example 2.2.7. Then, F has 13 rational places and 13 places of degree 2. Let

$$z^2 = x(x+1)(x+3)(x+6)P_1P_2P_3P_4P_5P_6,$$

where $P_i, 1 \leq i \leq 6$ are as in the example. Put $L = F'(z)$. L/F' is a Kummer extension with $[L : F'] = 2$. Then, we have 19 places ramifying in L/F'. By the Hurwitz genus

formula, the genus of L is given by

$$2g(L) - 2 = 2 \cdot 2 \cdot (1 - 1) + 2 \cdot 3 + 2 \cdot 13,$$

thus yielding $g(L) = 17$. Let $\mathcal{T}'$ be the set consisting of 7 places of F' lying over $x + 2$, $x+4$, $x+5$ and ∞ together with one place above x. It can be easily verified that all places in $\mathcal{T}'$ apart from the place above x split completely in L/F'. Hence, if $\mathcal{S}'$ is the overset of $\mathcal{T}'$ with respect to the extension L/F', Proposition 6.2.2 gives

$$d_2(\mathrm{Cl}(\mathcal{O}_{\mathcal{S}})) \geq 19 - 8 - 1 = 10 \geq 2 + 2\sqrt{2 \cdot 7 + 1 + 1}.$$

Consequently, Theorem 6.2.1 yields

$$A(7) \geq \frac{|\mathcal{S}'|}{g(L) - 1} = \frac{15}{16} = 0.9375.$$

□

Proposition 6.2.6

$$A(11) \geq 7/6 = 1.1666...$$

Proof: Let F be the rational function field $\mathbf{F}_{11}(x)$. Consider the field $F' = F(y_1, y_2)$, where

$$y_1^2 = 2x(x^2 + 7x + 2)$$

and

$$y_2^2 = 2x(x - 10)(x^2 + 9x + 5).$$

Then, for $1 \leq i \leq 8$, the place $x - i$ splits completely in F'/F. Moreover, the place ∞ is totally ramified in $F(y_1)/F$ and splits completely in $F'/F(y_1)$. Thus, F' has genus 4 and

34 rational places. Next, let

$$z^2 = (x-1)(x-3)(x-4)(x-5)(x-6)(x-7)$$

and put $L = F'(z)$. Noting that there are 24 rational places of F' ramifying in L, and using the Hurwitz genus formula, we obtain $g(L) = 19$. Let $\mathcal{T}'$ consist of the 8 places of F' lying above $x-2$ and $x-8$, 2 places above ∞ together with 1 place above $x-1$, i.e. $|\mathcal{T}'| = 11$. Since all the places in $\mathcal{T}'$ except the place above $x-1$ split completely in L/F', $\mathcal{S}'$ has 21 places, where $\mathcal{S}'$ is the overset of $\mathcal{T}'$ with respect to the extension L/F'. Now, from Proposition 6.2.2,

$$d_2(\mathrm{Cl}(\mathcal{O}_{\mathcal{S}})) \geq 24 - 11 - 1 = 12 \geq 2 + 2\sqrt{2 \cdot 10 + 1 + 1} = 11.381.$$

Consequently, Theorem 6.2.1 yields

$$A(11) \geq 21/18 = 7/6 = 1.1666...$$

□

To conclude, we apply the method in the examples to give a general lower bound for $A(q^m)$, where q is an odd prime power and m is a prime.

Theorem 6.2.7 *Let q be an odd prime power and m an odd prime. Suppose that m' is the largest integer such that $1 \leq m' \leq m-1$ and $2\sqrt{\lceil 2m'q+3 \rceil} + 3 \leq q$. We have*

$$A(q^m) \geq \frac{2m'q+2}{\lceil 2\sqrt{2m'q+3} \rceil + 1}.$$

Proof: Put $F = \mathbf{F}_{q^m}(x)$ and let $n = \lceil 2\sqrt{2m'q+3} \rceil + 3 \leq q$. Let $\beta \in \mathbf{F}_{q^m} - \mathbf{F}_q$ so that $\beta^q \neq \beta$. For each $\alpha \in \mathbf{F}_q$, let $f_\alpha(x) = (x+\alpha+\beta)(x+\alpha+\beta^q) \in F[x]$. Pick n distinct

elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{F}_q$ and consider the fields $L_i = \mathbf{F}_{q^m}(x, y_i)$, where

$$y_i^2 = f_{\alpha_i}(x),$$

for $i = 1, 2, \ldots, n$. Then, $[L_i : F] = 2$ and $\mathrm{Gal}(L_i/F) \cong \mathbf{Z}/2\mathbf{Z}$ for each $i = 1, 2, \ldots, n$. Let L be the compositum field $L = L_1 L_2 \cdots L_n$. Since the L_i's are linearly disjoint,

$$\mathrm{Gal}(L/F) \cong \prod_{i=1}^{n} \mathrm{Gal}(L_i/F) \cong (\mathbf{Z}/2\mathbf{Z})^n.$$

Now, consider the field $F' = F(y)$, where

$$y^2 = \prod_{i=1}^{n} f_{\alpha_i}(x).$$

Notice that by putting $y = y_1 y_2 \ldots y_n$, F' can be considered as a subfield of L with $[F' : F] = 2$ and $\mathrm{Gal}(L/F') \cong (\mathbf{Z}/2\mathbf{Z})^{n-1}$. Furthermore, the genus of F' is

$$g(F') = n - 1 = \lceil 2\sqrt{2m'q + 3} \rceil + 2.$$

Now, for $1 \leq k \leq m-1$, let s be the inverse of $k \bmod m$, i.e. $sk \equiv 1 \bmod m$ so that $\beta^{q^{sk}} = \beta^q$. Let $s_k = \beta^q + \beta^{q^2} + \cdots + \beta^{q^{(s-1)k}} \in \mathbf{F}_{q^m}$. Consider the set

$$T = \{a + s_k : a \in \mathbf{F}_q, 1 \leq k \leq m'\}$$

and let $\mathcal{T}' = \{P_\gamma = x - \gamma : \gamma \in T\} \cup \{\infty\}$, where ∞ denotes the pole of x. Hence, $|\mathcal{T}'| = m'q + 1$. We wish to show that every place in $\mathcal{T}'$ splits completely in L/F. For $i = 1, 2, \ldots, n$, we have

$$\begin{aligned} f_{\alpha_i}(a + s_k) &= (\alpha_i + a + \beta + s_k)(\alpha_i + a + \beta^q + s_k) \\ &= (\alpha_i + a + \beta + s_k)(\alpha_i + a + s_k + \beta^{q^{sk}}) \\ &= (\alpha_i + a + \beta + s_k)(\alpha_i + a + (\beta + s_k)^{q^k}) \\ &= (\alpha_i + a + \beta + s_k)^{q^k + 1}, \end{aligned}$$

which is a nonzero square in $\mathbf{F}_{q^m}$ since $q^k + 1$ is even. As ∞ splits completely in L_i/F, every place in $\mathcal{T}'$ spits completely in L_i/F, and hence, in L/F. Since only the places $x - \alpha_i + \beta$ or $x - \alpha_i + \beta^q$ ramify in L/F with ramification index 2 and each of these places has ramification index 2 in L_i/F, it follows that L/F' is an unramified extension. Now, let $\mathcal{S}'$ be the overset of $\mathcal{T}'$ with respect to the extension L/F'. Hence, $|\mathcal{S}'| = 2m'q + 2$ and

$$d_2(\mathrm{Cl}(O_{\mathcal{S}})) \geq d_2(\mathrm{Gal}(L/F')) = n - 1 = 2 + \lceil 2\sqrt{2m'q + 3} \rceil \geq 2 + 2(|\mathcal{S}'| + 1).$$

Consequently, Theorem 6.2.1 yields

$$A(q^m) \geq \frac{|\mathcal{S}'|}{g(F') - 1} = \frac{2m'q + 2}{\lceil 2\sqrt{2m'q + 3} \rceil + 1}.$$

□

Bibliography

[1] B. Anglès and C. Maire, A note on tamely ramified towers of global function fields, *Finite Fields Appl.*, **8**, pp. 207–215 (2002).

[2] R. Auer, Ray class fields of global function fields with many rational places, Dissertation, University of Oldenburg, 1999.

[3] R. Auer, Curves over finite fields with many rational points obtained by ray class field extensions, *Algorithmic Number Theory* (W. Bosma, ed.), Lecture Notes in Computer Science, Vol. **1838**, pp. 127–134, Springer, Berlin, 2000.

[4] R. Auer, Ray class fields of global function fields with many rational places, *Acta Arith.* **95**, 97–122 (2000).

[5] I.F. Blake, G. Seroussi, and N.P. Smart, *Elliptic Curves in Cryptography*, London Math. Soc. Lecture Note Series, Vol. **265**, Cambridge University Press, Cambridge, 1999.

[6] L. Carlitz, A class of polynomials, *Trans. Amer. Math. Soc.* **43**, 167–182 (1938).

[7] A. E. Brouwer, Bounds on Minimum Distance of Linear Codes, *Website: http://www.win.tue.nl/ aeb/voorlincod.html*

[8] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.

[9] C.S. Ding, H. Niederreiter, and C.P. Xing, Some new codes from algebraic curves, *IEEE Trans. Inform. Theory* **46**, 2638–2642 (2000).

[10] N. D. Elkies,Excellent nonlinear codes from modular curves, *in STOC'01: Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, Hersonissos, Crete*, 200–208(2001).

[11] R. Fuhrm ann, A. Garcia, and F. Torres, On maximal curves, *J. Number Theory* **67**, 29–51 (1997).

[12] R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* **89**, 103–106 (1996).

[13] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121**, 211–222 (1995).

[14] A. Garcia and A. Garzon, On Kummer covers with many rational points over finite fields., *J. Appl. Algebra* **185**, 177–192(2003).

[15] A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61**, 248–273 (1996).

[16] A. Garcia and H. Stichtenoth, Asymptotically good towers of function fields over finite fields, *C.R. Acad. Sci. Paris Sér. I Math.* **322**, 1067–1070 (1996).

[17] A. Garcia, H. Stichtenoth, and M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3**, 257–274 (1997).

[18] A. Garcia, H. Stichtenoth, and C.P. Xing, On subfields of the Hermitian function field, *Compositio Math.* **120**, 137–170 (2000).

[19] V.D. Goppa, Codes on algebraic curves (Russian), *Dokl. Akad. Nauk SSSR* **259**, 1289–1290 (1981).

[20] V.D. Goppa, Algebraic-geometric codes (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **46**, 762–781 (1982).

[21] V.D. Goppa, *Geometry and Codes*, Kluwer, Dordrecht, 1988.

[22] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, Berlin, 1996.

[23] R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

[24] D.R. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189**, 77–91 (1974).

[25] D.R. Hayes, Explicit class field theory in global function fields, *Studies in Algebra and Number Theory*, Advances in Math. Supp. Studies, Vol. **6**, pp. 173–217, Academic Press, New York, 1979.

[26] D.R. Hayes, Stickelberger elements in function fields, *Compositio Math.* **55**, 209–239 (1985).

[27] D.R. Hayes, A brief introduction to Drinfeld modules, *The Arithmetic of Function Fields* (D. Goss, D.R. Hayes, and M.I. Rosen, eds.), pp. 1–32, W. de Gruyter, Berlin, 1992.

[28] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**, 721–724 (1981).

[29] Y. Ihara, Shimura curves over finite fields and their rational points, *Applications of Curves over Finite Fields* (M.D. Fried, ed.), Contemporary Math., Vol. **245**, pp. 15–23, American Math. Society, Providence, RI, 1999.

[30] A. Keller, Cyclotomic function fields with many rational places, *Finite Fields and Applications* (D. Jungnickel and H. Niederreiter, eds.), Springer, Berlin, 293-303, (2001).

[31] H. Koch, *Algebraic Number Theory*, Springer, Berlin, 1997.

[32] K. Lauter, Ray class field constructions of curves over finite fields with many rational points, *Algorithmic Number Theory* (H. Cohen, ed.), Lecture Notes in Computer Science, Vol. **1122**, pp. 187–195, Springer, Berlin, 1996.

[33] K. Lauter, Deligne-Lusztig curves as ray class fields, *Manuscripta Math.* **98**, 87–96 (1999).

[34] K. Lauter, A formula for constructing curves over finite fields with many rational points, *J. Number Theory* **74**, 56–72 (1999).

[35] K. Lauter, Improved upper bounds for the number of rational points on algebraic curves over finite fields, *C.R. Acad. Sci. Paris Sér. I Math.* **328**, 1181–1185 (1999).

[36] K. Lauter and J.-P. Serre, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, *J. Algebraic Geometry* **10**, 19–36 (2001).

[37] W.-C.W. Li and H. Maharaj, Coverings of curves with asymptotically many rational points, *J. Number Theory*, **96**, pp. 232–256 (2002).

[38] M. Gebhardt, Constructing function with many places via the Carlitz module, *Manuscripta Math.* **107**, 89–99 (2002).

[39] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[40] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

[41] H. Niederreiter and C.P. Xing, Explicit global function fields over the binary field with many rational places, *Acta Arith.* **75**, 383–396 (1996).

[42] H. Niederreiter and C.P. Xing, Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places, *Acta Arith.* **79**, 59–76 (1997).

[43] H. Niederreiter and C.P. Xing, Drinfeld modules of rank 1 and algebraic curves with many rational points. II, *Acta Arith.* **81**, 81–100 (1997).

[44] H. Niederreiter and C.P. Xing, Global function fields with many rational places over the quinary field, *Demonstratio Math.* **30**, 919–930 (1997).

[45] H. Niederreiter and C.P. Xing, Algebraic curves over finite fields with many rational points, *Number Theory: Diophantine, Computational and Algebraic Aspects* (K. Győry, A. Pethö, and V.T. Sós, eds.), pp. 423–443, W. de Gruyter, Berlin, 1998.

[46] H. Niederreiter and C.P. Xing, Global function fields with many rational places over the ternary field, *Acta Arith.* **83**, 65–86 (1998).

[47] H. Niederreiter and C.P. Xing, Global function fields with many rational places over the quinary field. II, *Acta Arith.* **86**, 277–288 (1998).

[48] H. Niederreiter and C.P. Xing, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound, *Math. Nachr.* **195**, 171–186 (1998).

[49] H. Niederreiter and C.P. Xing, A general method of constructing global function fields with many rational places, *Algorithmic Number Theory* (J.P. Buhler, ed.), Lecture Notes in Computer Science, Vol. **1423**, pp. 555–566, Springer, Berlin, 1998.

[50] H. Niederreiter and C.P. Xing, Curve sequences with asymptotically many rational points, *Applications of Curves over Finite Fields* (M.D. Fried, ed.), Contemporary Math., Vol. **245**, pp. 3–14, American Math. Society, Providence, RI, 1999.

[51] H. Niederreiter and C.P. Xing, Algebraic curves with many rational points over finite fields of characteristic 2, *Number Theory in Progress* (K. Győry, H. Iwaniec, and J. Urbanowicz, eds.), pp. 359–380, W. de Gruyter, Berlin, 1999.

[52] H. Niederreiter and C.P. Xing, Global function fields with many rational places and their applications, *Finite Fields: Theory, Applications, and Algorithms* (R.C. Mullin and G.L. Mullen, eds.), Contemporary Math., Vol. **225**, pp. 87–111, American Math. Society, Providence, RI, 1999.

[53] H. Niederreiter and C.P. Xing, A counterexample to Perret's conjecture on infinite class field towers for global function fields, *Finite Fields Appl.* **5**, 240–245 (1999).

[54] H. Niederreiter and C.P. Xing, Algebraic curves over finite fields with many rational points and their applications, *Number Theory* (R.P. Bambah, V.C. Dumir, and R.J. Hans-Gill, eds.), pp. 287–300, Birkhäuser, Basel, 2000.

[55] H. Niederreiter and C.P. Xing, *Rational points on curves over finite fields: Theory and Applications*, LMS 285, Cambridge, 2001.

[56] H. Niederreiter, C.P. Xing, and K.Y. Lam, A new construction of algebraic-geometry codes, *Applicable Algebra Engrg. Comm. Comput.* **9**, 373–381 (1999).

[57] F. Özbudak and H. Stichtenoth, Constructing codes from algebraic curves, *IEEE Trans. Inform. Theory* **45**, 2502–2505 (1999).

[58] M. Perret, Tours ramifiées infinies de corps de classes, *J. Number Theory* **38**, 300–322 (1991).

[59] H.-G. Quebbemann, Cyclotomic Goppa codes, *IEEE Trans. Inform.Theory* **34**, 1317–1320 (1988).

[60] M. Rosen, The Hilbert Class Field in Function Fields, *Exposition. Math.* **5**, 365–378 (1987).

[61] M. Rosen, *Number Theory in Function Fields*, New York : Springer, 2002.

[62] H.-G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457**, 185–188 (1994).

[63] R. Schoof, Algebraic curves over $\mathbf{F}_2$ with many rational points, *J. Number Theory* **41**, 6–14 (1992).

[64] A. Schweizer, On Drinfeld modular curves with many rational points over finite fields, preprint, Academia Sinica, Taipei, 2000.

[65] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[66] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C.R. Acad. Sci. Paris Sér. I Math.* **296**, 397–402 (1983).

[67] J.-P. Serre, Nombres de points des courbes algébriques sur $\mathbf{F}_q$, *Sém. Théorie des Nombres 1982–1983*, Exp. 22, Université de Bordeaux I, Talence, 1983.

[68] J.-P. Serre, Résumé des cours de 1983–1984, *Annuaire du Collège de France* **1984**, 79–83.

[69] J.-P. Serre, *Rational Points on Curves over Finite Fields*, Lecture Notes, Harvard University, 1985.

[70] S.A. Stepanov, *Arithmetic of Algebraic Curves*, Plenum, New York, 1994.

[71] S.A. Stepanov, *Codes on Algebraic Curves*, Kluwer, New York, 1999.

[72] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[73] A. Temkine, Hilbert class field towers of function fields over finite fields and lower bounds for $A(q)$, *J. Number Theory*, **87**, 189–210(2001).

[74] Teo Kai Meng, Global function fields with many rational places, *Masters thesis, National University of Singapore*, 2003.

[75] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[76] M.A. Tsfasman, S.G. Vladut, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109**, 21–28 (1982).

[77] G. van der Geer and M. van der Vlugt, Curves over finite fields of characteristic 2 with many rational points, *C.R. Acad. Sci. Paris Sér. I Math.* **317**, 593–597 (1993).

[78] G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points, *Arithmetic Geometry* (F. Catanese, ed.), pp. 169–189, Cambridge University Press, Cambridge, 1997.

[79] G. van der Geer and M. van der Vlugt, Generalized Reed-Muller codes and curves with many points, *J. Number Theory* **72**, 257–268 (1998).

[80] G. van der Geer and M. van der Vlugt, Constructing curves over finite fields with many points by solving linear equations, *Applications of Curves over Finite Fields* (M.D. Fried, ed.), Contemporary Math., Vol. **245**, pp. 41–47, American Math. Society, Providence, RI, 1999.

[81] G. van der Geer and M. van der Vlugt, Kummer covers with many points, *Finite Fields Appl.* **6**, 327–341 (2000).

[82] G. van der Geer and M. van der Vlugt, Tables of curves with many points 15, *Website: http://www.science.uva..nl/ geer.*

[83] J.H. van Lint, *Introduction to Coding Theory*, Springer, New York, 1982; 3rd ed., Springer, Berlin, 2000.

[84] S.G. Vladut and V.G. Drinfeld, Number of points of an algebraic curve, *Funct. Anal. Appl.* **17**, 53–54 (1983).

[85] C. Voss and T. Høholdt, An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound: the first steps, *IEEE Trans. Inform. Theory* **43**, 128–135 (1997).

[86] A. Weil, *Basic Number Theory*, 2nd ed., Springer, New York, 1973.

[87] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

[88] C.P. Xing, Linear codes from narrow ray class groups of algebraic curves, *IEEE Trans. on Information Theory*, 50, 541-543(2004).

[89] C.P. Xing and S. Ling, A class of linear codes with good parameters from algebraic curves, *IEEE Trans. Inform. Theory* **46**, 1527–1532 (2000).

[90] C.P. Xing and S. Ling, A class of linear codes with good parameters, *IEEE Trans. Inform. Theory* **46**, 2184–2188 (2000).

[91] S. Ling and C.P. Xing *Coding Theory–A First Course*, Cambridge, 2004.

[92] C.P. Xing and H. Niederreiter, Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels, *C.R. Acad. Sci. Paris Sér. I Math.* **322**, 651–654 (1996).

[93] C.P. Xing and H. Niederreiter, Drinfeld modules of rank 1 and algebraic curves with many rational points, *Monatsh. Math.* **127**, 219–241 (1999).

[94] C.P. Xing, H. Niederreiter, and K.Y. Lam, Constructions of algebraic-geometry codes, *IEEE Trans. Inform. Theory* **45**, 1186–1193 (1999).

[95] C.P. Xing, H. Niederreiter, and K.Y. Lam, A generalization of algebraic-geometry codes, *IEEE Trans. Inform. Theory* **45**, 2498–2501 (1999).

[96] C.P. Xing and H. Stichtenoth, The genus of maximal function fields over finite fields, *Manuscripta Math.* **86**, 217–224 (1995).

[97] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory, *Fundamentals of Computation Theory* (L. Budach, ed.), Lecture Notes in Computer Science, Vol. **199**, pp. 503–511, Springer, Berlin, 1985.