PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

by

MUSTAFA ÇOBAN

Submitted to the Graduate School of Engineering and Natural Sciences

in partial fulfillment of

the requirements for the degree of

Master of Science

Sabancı University

Spring 2003

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

APPROVED BY

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

Prof. Dr. Alev TOPUZOĞLU .....

Assist. Prof. Albert LEVİ .....

DATE OF APPROVAL: August 29th, 2003

Anneme, babama

ve

biricik ağabeyime...

Acknowledgments

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

I also would like to thank Ismail Çoban, Mehmet Özdemir, Mustafa Parlak, and Ayça Çeşmelioğlu for their friendship and endless support.

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

Abstract

Arithmetic of finite fields is not only important for other branches of mathematics but also widely used in applications such as coding and cryptography. A primitive element of a finite field is of particular interest since it enables one to represent all other elements of the field. Therefore an extensive research has been done on primitive elements, especially those satisfying extra conditions.

We are interested in the existence of primitive elements in extensions of finite fields with prescribed trace value. This existence problem can be settled by means of two important theories. One is character sums and the other is the theory of algebraic function fields. The aim of this thesis is to introduce some important properties of these two topics and to show how they are used in answering the existence problem mentioned above.

Keywords: Finite field, primitive element, trace, character sum, algebraic function field.

SONLU CİSİMLERDE HERHANGİ TRACE DEĞERİNE SAHİP İLKEL ELEMANLAR

Özet

Sonlu cisimlerin aritmetiği matematiğin diğer alanlarındaki önemi dışında kodlama ve şifreleme gibi uygulamalarda da sıkça kullanılır. Cismin tüm diğer elemanlarının gösterilişine imkan verdiği için sonlu cisimlerin ilkel elemanlarına özellikle ilgi duyulmaktadır. Bu sebepten genelde ilkel elemanlar, özellikle de bazı şartları sağlayan ilkel elemanlar konularında kapsamlı araştırmalar yapılmaktadır.

Biz, sonlu cisimlerin genişlemelerinde herhangi bir trace değerine sahip ilkel elemanların varlığı problemiyle ilgileneceğiz. Bu varlık problemi iki önemli kuram yoluyla çözülebilir. Bunlardan birincisi karakter toplamları diğeri ise cebirsel fonksiyon cisimleridir. Bu tezin amacı sözü geçen iki önemli kuramın bazı temel özelliklerini açıklamak ve yukarda tanımlanan varlık probleminin cevaplanmasında nasıl kullanıldıklarını göstermektir.

Anahtar kelimeler: Sonlu cisim, ilkel eleman, trace, karakter toplamı, cebirsel fonksiyon cismi.

TABLE OF CONTENTS

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

by

MUSTAFA ÇOBAN

Submitted to the Graduate School of Engineering and Natural Sciences

in partial fulfillment of

the requirements for the degree of

Master of Science

Sabancı University

Spring 2003

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

APPROVED BY

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

Prof. Dr. Alev TOPUZOĞLU .....

Assist. Prof. Albert LEVİ .....

DATE OF APPROVAL: August 29th, 2003

Anneme, babama

ve

biricik ağabeyime...

Acknowledgments

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

I also would like to thank Ismail Çoban, Mehmet Özdemir, Mustafa Parlak, and Ayça Çeşmelioğlu for their friendship and endless support.

PRIMITIVE ELEMENTS IN FINITE FIELDS WITH ARBITRARY TRACE

Abstract

Arithmetic of finite fields is not only important for other branches of mathematics but also widely used in applications such as coding and cryptography. A primitive element of a finite field is of particular interest since it enables one to represent all other elements of the field. Therefore an extensive research has been done on primitive elements, especially those satisfying extra conditions.

We are interested in the existence of primitive elements in extensions of finite fields with prescribed trace value. This existence problem can be settled by means of two important theories. One is character sums and the other is the theory of algebraic function fields. The aim of this thesis is to introduce some important properties of these two topics and to show how they are used in answering the existence problem mentioned above.

Keywords: Finite field, primitive element, trace, character sum, algebraic function field.

SONLU CİSİMLERDE HERHANGİ TRACE DEĞERİNE SAHİP İLKEL ELEMANLAR

Özet

Sonlu cisimlerin aritmetiği matematiğin diğer alanlarındaki önemi dışında kodlama ve şifreleme gibi uygulamalarda da sıkça kullanılır. Cismin tüm diğer elemanlarının gösterilişine imkan verdiği için sonlu cisimlerin ilkel elemanlarına özellikle ilgi duyulmaktadır. Bu sebepten genelde ilkel elemanlar, özellikle de bazı şartları sağlayan ilkel elemanlar konularında kapsamlı araştırmalar yapılmaktadır.

Biz, sonlu cisimlerin genişlemelerinde herhangi bir trace değerine sahip ilkel elemanların varlığı problemiyle ilgileneceğiz. Bu varlık problemi iki önemli kuram yoluyla çözülebilir. Bunlardan birincisi karakter toplamları diğeri ise cebirsel fonksiyon cisimleridir. Bu tezin amacı sözü geçen iki önemli kuramın bazı temel özelliklerini açıklamak ve yukarda tanımlanan varlık probleminin cevaplanmasında nasıl kullanıldıklarını göstermektir.

Anahtar kelimeler: Sonlu cisim, ilkel eleman, trace, karakter toplamı, cebirsel fonksiyon cismi.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Arithmetic of finite fields is not only important for other branches of mathematics but also widely used in applications such as coding and cryptography. A primitive element of a finite field is of particular interest since it enables one to represent all other elements of the field, i.e. it generates the multiplicative group of the finite field. Therefore an extensive research has been done on primitive elements, especially those satisfying extra conditions.

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_{q^n}$ denote the degree n extension of $\mathbb{F}_q$. The primitive normal basis theorem, the complete proof of which was given by Lenstra-Schoof ([11]), states that for any $n \geq 2$, there exists a primitive element w in $\mathbb{F}_{q^n}$ such that $\{w, w^q, \ldots, w^{q^{n-1}}\}$ forms an $\mathbb{F}_q$-basis for the n dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. If $q = 2$, then $w + w^2 + \cdots + w^{2^{n-1}}$ is simply the trace of w relative to extension $\mathbb{F}_{2^n}/\mathbb{F}_2$. Hence, the value of this sum is either 0 or 1, two elements of $\mathbb{F}_2$. If zero, then one gets a contradiction to $\mathbb{F}_2$-linear independence of the basis elements $w, w^2, \ldots, w^{2^{n-1}}$. Hence we can conclude that there exists a primitive element in $\mathbb{F}_{2^n}$ whose trace relative to $\mathbb{F}_{2^n}/\mathbb{F}_2$ is one.

Since the proof of the primitive normal basis theorem is rather complicated, MacWilliams-Sloane ([13], Research Problem 4.1) asked for a simpler and more direct proof of the fact that there exists primitive elements in extensions of $\mathbb{F}_2$ with trace one. This was accomplished by Moreno ([15]). From this point on the problem was generalized to extensions of arbitrary finite fields $\mathbb{F}_q$ and any trace value t in

$\mathbb{F}_q$, including zero trace. Jungnickel-Vanstone ([10]) proved this general version of the problem for nonzero trace values with certain exceptions all of which arise in quadratic extensions. The complete answer was given by Cohen in a series of papers ([1], [2], [3]).

At this point one could think that the above existence problem was no longer of interest since it was settled completely. The common feature of all the works mentioned above is that they use character sums. Using the theory of algebraic function fields, Özbudak ([16]) showed that a more general result for the nonzero trace case can be found. This thesis focuses on the works of Cohen, inparticular [3], and Özbudak.

In this chapter we introduce some of the basic concepts in finite fields, character sums and function fields, which will be used in the subsequent chapters and which also make the above discussion meaningful. For the proofs of results and a complete introduction to subjects above, we refer the reader to excellent books of Lidl-Niederreiter [12], Stichtenoth [17] and Jungnickel [9].

1.1. Primitive Elements and the Trace Map in Finite Fields

For a finite field $\mathbb{F}_q$, we denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements in $\mathbb{F}_q$. It is known that $\mathbb{F}_q^*$ is a cyclic group with $q-1$ elements.

A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$. Since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, $\mathbb{F}_q$ clearly has $\varphi(q-1)$ primitive elements, where φ is the Euler phi function that counts the numbers between 1 and $q-1$ which are relatively prime to $q-1$.

Let $\mathbb{F}_{q^m}$ be the finite field with q^m elements which can be viewed as a degree m field extension of $\mathbb{F}_q$. Note that a primitive element α of $\mathbb{F}_{q^m}$ is a *defining element* for the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$, i.e. $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$.

Definition 1.1.1 A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $m \geq 1$ is called a *primitive polynomial* over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^m}$.

For any finite Galois extension F/E, there is an important mapping called the *trace map* from F to E. It is denoted by $Tr_{F/E}$ and defined as

$$Tr_{F/E}(x) = \sum_{\sigma \in Gal(F/E)} \sigma(x), \forall x \in F.$$

The trace map can be defined for any finite field extension F/E by slightly changing the above description. Since an extension of finite fields $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic (Galois) extension of degree n, where the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated by the Frobenious automorphism $\sigma(x) = x^q$, the description of the trace map for finite fields can be given as follows:

Definition 1.1.2 For an extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, *trace map* is a mapping from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ defined by

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \sum_{k=0}^{n-1} x^{q^k}, \forall x \in \mathbb{F}_{q^n}. \tag{1.1}$$

We list some properties of the trace in the following theorem. When there is no ambiguity, we ignore the related extension and just write Tr for trace.

Theorem 1.1.1 *The trace function $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is an $\mathbb{F}_q$-linear mapping from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ with the following properties:*
(a) $Tr(u^q) = Tr(u)$ for all $u \in \mathbb{F}_{q^n}$;
(b) $Tr(u) = nu$ for all $u \in \mathbb{F}_q$;
(c) If $\alpha \in \mathbb{F}_{q^n}$ with the minimal polynomial $f_\alpha(t) = t^m + a_{m-1}t^{m-1} + \ldots + a_1 t + a_0 \in \mathbb{F}_q[t]$ over $\mathbb{F}_q$, then $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -\frac{n}{m}a_{m-1}$;
(d)(Transitivity of trace) Let $\mathbb{F}_{q^m}$ be a finite extension of $\mathbb{F}_{q^n}$. Then

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\alpha)) \text{ for all } \alpha \in \mathbb{F}_{q^m};$$

(e)(Additive Hilbert's Theorem 90) $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) = 0$ for $b \in \mathbb{F}_{q^n}$ if and only if $b = a^q - a$ for some $a \in \mathbb{F}_{q^n}$.

1.2. Character Sums

Let G be a multiplicatively written finite abelian group with identity element 1_G. A *character* χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. In other words χ is a mapping from G to U satisfying $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for any $g_1, g_2 \in G$. Note that $\chi(1_G) = 1$. Since $(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$ for every $g \in G$, $\chi(g)$ is a complex $|G|^{th}$ root of unity. Among the characters of G, there is the *trivial character* χ_0 which is defined by $\chi_0(g) = 1$ for all $g \in G$. All other characters of G are *nontrivial* . With each character χ of G there is an associated *conjugate character* $\bar{\chi}$ defined by $\bar{\chi}(g) = \overline{\chi(g)}$, where $\overline{\chi(g)}$ denotes the complex conjugate of $\chi(g) \in U$. Note that for an element in U, the complex conjugate is the multiplicative inverse. Hence, $\bar{\chi}(g) = \overline{\chi(g)} = \chi(g)^{-1} = \chi(g^{-1})$.

For finitely many characters $\chi_1, \ldots, \chi_n$ of G, we can define the *product character* $\chi_1 \cdots \chi_n$ by $(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g)$ for all $g \in G$. We denote the set of all characters of G by $\hat{G}$. Clearly $\hat{G}$ is an abelian group under this multiplication of characters. Since the values of characters of G are complex $|G|^{th}$ roots of unity, $\hat{G}$ is a finite abelian group. In fact, $\hat{G}$ is isomorphic to G and hence $\mid \hat{G} \mid = \mid G \mid$.

Example 1.2.1 Let G be a finite cyclic group of order n, and let g be a generator of G. All characters of G are defined by $\chi_j(g^k) = e^{2\pi ijk/n}$, $k = 0, 1, \ldots, n-1$ for a fixed integer j, $0 \leq j \leq n-1$. $\hat{G}$ consists exactly of the characters $\chi_0, \chi_1, \ldots, \chi_{n-1}$.

In the following theorem, we list some basic properties of characters which will be used later.

Theorem 1.2.2 *Let G be a finite abelian group. For all $g, h \in G$ and all characters χ, ψ of G, we have the following properties:*

(i) $\sum_{g\in G}\chi(g)=0$ *if* $\chi\neq\chi_0$.

(ii) $\sum_{\chi\in\hat{G}}\chi(g)=0$ *for* $1_G\neq g\in G$.

(iii)

$$\sum_{\chi\in\hat{G}}\chi(g)\chi^{-1}(h)=\begin{cases}\mid G\mid & \text{if } g=h\\ 0 & \text{otherwise}\end{cases}$$

(iv)

$$\sum_{g\in G}\psi(g)\chi^{-1}(g)=\begin{cases}\mid G\mid & \text{if } \chi=\psi\\ 0 & \text{otherwise}\end{cases}$$

Last two properties are called *orthogonality relations for characters.*

In a finite field $\mathbb{F}_q$ there are two important finite abelian groups, i.e. the additive group and the multiplicative group of the field. The characters associated to these two group structures are different. We use the term, *additive character* for the characters of the additive group of $\mathbb{F}_q$ and the term *multiplicative character* for the characters of the multiplicative group $\mathbb{F}_q^*$. Let p be the characteristic of $\mathbb{F}_q$ and let Tr denote the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then the function χ_1 defined by $\chi_1(c)=e^{2\pi iTr(c)/p}$ for all $c\in\mathbb{F}_q$ is called the *canonical additive character* of $\mathbb{F}_q$. All additive characters of $\mathbb{F}_q$ can be given by $\chi_b(c)=\chi_1(bc)$ for all $c\in\mathbb{F}_q$ and for some $b\in\mathbb{F}_q$. Since the multiplicative group $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, multiplicative characters can be easily determined using Example 1.2.1. Let g be a generator of $\mathbb{F}_q^*$. For each $j=0,1,\ldots,q-2$, the function ψ_j with

$$\psi_j(g^k)=e^{2\pi ijk/(q-1)}\ for\ k=0,1,\ldots,q-2$$

defines a multiplicative character of $\mathbb{F}_q$. Every multiplicative character of $\mathbb{F}_q$ is in this form. Since $\hat{\mathbb{F}}_q^*\simeq\mathbb{F}_q^*$, $\hat{\mathbb{F}}_q^*$ is a cyclic group of order $q-1$.

If λ is a multiplicative character of $\mathbb{F}_q$, then λ is defined for all nonzero elements of $\mathbb{F}_q$. But, for convenience, we can extend the definition of λ by setting $\lambda(0)=1$ if λ is the trivial character and $\lambda(0)=0$ if λ is a nontrivial character. Then we have

$$\sum_{c\in\mathbb{F}_q}\lambda(c)=\begin{cases}q & \text{if } \lambda \text{ is trivial}\\ 0 & \text{if } \lambda \text{ is nontrivial}\end{cases},$$

which justifies the above conventions for $\lambda(0)$ values.

Clearly, the restriction of a character to a subgroup H of G is a character of H. It is often useful to consider the subgroup $H^{\perp}$ of all characters of G which restrict to the trivial character of H, i.e.

$$H^{\perp} := \{\chi \in \hat{G} : \chi(h) = 1 \ for \ all \ h \in H\}. \tag{1.2}$$

Similarly, given a subgroup S of $\hat{G}$, we also define an associated subgroup $S^{\perp}$ of G:

$$S^{\perp} := \{g \in G : \chi(g) = 1 \ for \ all \ \chi \in S\}. \tag{1.3}$$

The final theorem of this section describes the structure of the character groups of subgroups of G and $\hat{G}$, respectively.

Theorem 1.2.3 ***(Duality Theorem)*** *Let G be a finite abelian group. Then one has the following for all subgroups H and S of G and $\hat{G}$, respectively.*

$$\hat{H} \cong \hat{G}/H^{\perp} \ and \ H^{\perp} \cong \widehat{(G/H)}; \tag{1.4}$$

$$\hat{S} \cong G/S^{\perp} \ and \ S^{\perp} \cong \widehat{(\hat{G}/S)}. \tag{1.5}$$

1.3. Algebraic Function Fields

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

Example 1.3.2 The simplest example of an algebraic function field is the rational function field $F = K(x)$, where x is a transcendental element over K. Any element $0 \neq z \in K(x)$ has a unique representation

$$z = a \prod_i p_i(x)^{n_i}, \tag{1.6}$$

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

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

Definition 1.3.3 A *valuation ring* of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties :
(i) $K \subsetneq \mathcal{O} \subsetneq F$,
(ii) for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

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

Definition 1.3.4 A *place* P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Any element $t \in P$ such that $P = t\mathcal{O}$ is called a *prime element* for P.

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

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

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

Definition 1.3.5 A *discrete valuation* of F/K is a function $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties :
(i) $v(x) = \infty \Longleftrightarrow x = 0$.
(ii) $v(xy) = v(x) + v(y)$ for any $x, y \in F$.
(iii) (Triangle inequality) $v(x + y) \geq min\{v(x), v(y)\}$ for any $x, y \in F$.
(iv) There exists an element $z \in F$ with $v(z) = 1$.
(v) $v(a) = 0$ for any $0 \neq a \in K$.

The triangle inequality is an equality in some cases.

Lemma 1.3.4 ***(Strict Triangle Inequality)*** *Let v be a discrete valuation of F/K and $x, y \in F$ with $v(x) \neq v(y)$. Then*

$$v(x + y) = min\{v(x), v(y)\}. \tag{1.7}$$

Now we describe how v_P is defined for a given valuation ring $\mathcal{O}_P$ or a place $P \in \mathbb{P}_F$. If t is a prime element for P, then every $0 \neq z \in F$ has a unique representation $z = t^n u$ for some $u \in \mathcal{O}_P^*$ and integer n. We define $v_P(z) = n$. This function is a discrete valuation associated to the given place $P \in \mathbb{P}_F$. Conversely, let v be a discrete valuation of F/K. The set $\{z \in F | v(z) > 0\}$ determines a place P of F/K. Corresponding valuation ring $\mathcal{O}_P$ is $\{z \in F |\ v(z) \geq 0\}$.

Example 1.3.3 If F/K is a function field, where $\widetilde{K} = K$, then note that any $0 \neq k \in K$ is contained in $\mathcal{O}_P^*$ for any $P \in \mathbb{P}_F$. Therefore, $k = t^0 k$ is the unique representation mentioned above. Hence, $v_P(k) = 0$, for any $P \in \mathbb{P}_F$ and any $k \in K - \{0\}$.

For a valuation ring $\mathcal{O}_P$, the quotient ring $\mathcal{O}_P\ /P$ is a field, since P is maximal in $\mathcal{O}_P$. This field is denoted by F_P and it is called the *residue class field* of P. For an element $z \in \mathcal{O}_P$, we denote the coset $z + P \in \mathcal{O}_P\ /P$ by $z(P)$. For $z \in F - \mathcal{O}_P$,

we set $z(P) = \infty$. Hence, we have a map from F to $F_P \cup \{\infty\}$ via the assignment $z \longmapsto z(P)$ for any $z \in F$. Under this map, $K \subset \mathcal{O}_P$ is mapped injectively into F_P, i.e. there exists an isomorphic copy of K in F_P. Therefore, F_P can be viewed as a K-vector space. In fact, F_P is a finite dimensional vector space over K.

Definition 1.3.6 For a place P of F/K, *the degree of* P is defined by

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

Definition 1.3.7 Let $0 \neq z \in F$ and $P \in \mathbb{P}_F$. We say that P is a *zero* of z of order m if $v_P(z) = m > 0$ and P is a *pole* of z of order m if $v_P(z) = -m < 0$.

For a nonzero element $x \in F$, there are finitely many zeros and poles. Note that there are, in fact, no zeros or poles for an element $0 \neq k \in K$, by Example 1.3.3. We try to explain the meanings of these fundamental concepts for the simplest function field, that is the rational function field.

Example 1.3.4 Let $F = K(x)$ be the rational function field over K. K is clearly the full constant field of $K(x)/K$ since every element in $K(x) - K$ is transcendental over K. For any monic, irreducible polynomial $p(x) \in K[x]$, there is an *affine place* $P_{p(x)}$ of $K(x)$ defined by

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \middle| \ f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}. \tag{1.8}$$

Its corresponding valuation ring is given by

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \middle| \ f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \tag{1.9}$$

We can describe the corresponding discrete valuation v_P for $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ as follows: Any $z \in K(x) - \{0\}$ can be uniquely written as $z = p(x)^n (f(x)/g(x))$ with $n \in \mathbb{Z}$ and $f(x), g(x) \in K[x]$ both of which are not divisible by $p(x)$. Then $v_P(z) = n$. The residue class field $K(x)_P = \mathcal{O}_P/P$ of P is isomorphic to $K[x]/(p(x))$. Therefore, $\deg P = \deg(p(x))$. If $p(x)$ is linear, i.e. $p(x) = x - \alpha$ for some $\alpha \in K$, we denote its affine place by $P_\alpha = P_{x-\alpha} \in \mathbb{P}_{K(x)}$. In this case the degree of $P = P_\alpha$

is one. Another place of the rational function field $K(x)$ is the *infinite place* which is

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \Big| \ f(x), g(x) \in K[x], \deg(f(x)) < \deg(g(x)) \right\}. \tag{1.10}$$

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

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \Big| \ f(x), g(x) \in K[x], \deg(f(x)) \leq \deg(g(x)) \right\}. \tag{1.11}$$

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

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

Definition 1.3.8 The (additively written) free abelian group which is generated by the places of F/K is denoted by $\mathcal{D}_F$ and it is called *divisor group* of F/K. The elements of $\mathcal{D}_F$ are called *divisors* of F/K. In other words, a divisor is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_p P, \tag{1.12}$$

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

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

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

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \tag{1.13}$$

and the *pole divisor* of x by

$$(x)_\infty := \sum_{P \in N} -v_P(x)P. \tag{1.14}$$

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

$$(x) = (x)_0 - (x)_\infty. \tag{1.15}$$

An important fact is that $\deg(x)_0 = \deg(x)_\infty = [F : K(x)] < \infty$, if $x \in F - K$. This means that any nonconstant function has as many poles as zeros, counted with multiplicities. For a nonzero constant function $k \in K$, $(k)_0 = (k)_\infty = (k) = 0$ by Example 1.3.3. We now associate an important space to a divisor of F/K.

Definition 1.3.9 For a divisor $A \in \mathcal{D}_F$ we set

$$\mathcal{L}(\mathcal{A}) := \{x \in F \Big| \ (x) \geq -A\} \cup \{0\}. \tag{1.16}$$

$\mathcal{L}(\mathcal{A})$ is a finite dimensional K-vector space for any $A \in \mathcal{D}_F$. It is called the *Riemann-Roch space of* A and we define the *dimension of a divisor* to be $\dim A := \dim_K \mathcal{L}(\mathcal{A})$. Computing the dimension of a divisor is a challenging problems in general. The main tool for this is the Riemann-Roch Theorem ([17], Theorem I.5.15). Now we are ready to give the definition of an important invariant of a function field.

Definition 1.3.10 The *genus* of F/K is defined by

$$g(F) = max\{\deg A - \dim A + 1| \ A \in \mathcal{D}_F\}. \tag{1.17}$$

The genus of the rational function field is zero. In general, genus is a nonnegative integer.

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

Theorem 1.3.5 *Let F'/K' be an algebraic extension of F/K. Let P (respectively P') be a place of F/K (respectively F'/K') and let $\mathcal{O}_P \subseteq F$ (respectively $\mathcal{O}_{P'} \subseteq F'$) be the corresponding valuation rings. Suppose that v_P, $v_{P'}$ are corresponding discrete valuations. Then the following are equivalent:*
(a) $P' \mid P$.
(b) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.
(c) There exists an integer $e \geq 1$ such that $v_{P'}(x) = e.v_P(x)$ for all $x \in F$.
If $P' \mid P$, we have $P = P' \cap F$ and $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. An important fact is that any place $P \in \mathbb{P}_F$ has finitely many places in $\mathbb{P}_{F'}$ over it.

Definition 1.3.11 Let F'/K' be an algebraic extension of F/K, and let $P' \in \mathbb{P}'_F$ be a place of F'/K' lying over $P \in \mathbb{P}_F$.
(i) The integer $e(P'|P) := e$ with $v_{P'}(x) = e.v_P(x)$ for any $x \in F$ is called the *ramification index* of P' over P.
(ii) $f(P'|P) := [F'_{P'} : F_P]$ is called the *relative degree* of P' over P.

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

The following important fact is sometimes called the fundamental equality.

Theorem 1.3.6 *Let F'/K' be a finite extension of F/K, P a place of F/K and*

$P_1, \ldots, P_m$ all the places of F'/K' lying over P. Let $e_i = e(P_i \mid P)$ denote the ramification index and $f_i = f(P_i \mid P)$ the relative degree of P_i over P for all $i = 1, \ldots, m$. Then

$$\sum_{i=1}^{m} e_i f_i = [F' : F]. \tag{1.18}$$

The following theorem is useful in determining extensions of places in function field extensions.

Theorem 1.3.7 ***(Kummer's Theorem)*** *Let $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + \ldots + f_0(x) \in K(x)[T]$ be an irreducible polynomial over the rational function field $K(x)$. We consider the function field $K(x, y)/K$ where y satisfies the equation $\varphi(y) = 0$, and an element $\alpha \in K$ such that $f_j(\alpha) \neq \infty$ for any j, $0 \leq j \leq n-1$. Let $P_\alpha \in \mathbb{P}_{K(x)}$ be the zero of $x-\alpha$ in $K(x)$. Assume that $\varphi_\alpha(T) := T^n + f_{n-1}(\alpha)T^{n-1} + \ldots + f_0(\alpha) \in K[T]$ can be decomposed in $K[T]$ as $\varphi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T)$ with irreducible, monic, pairwise distinct polynomials $\psi_i(T) \in K[T]$. Then we have :*
(a) For any $i = 1, \ldots, r$, there is a uniquely determined place $P_i \in \mathbb{P}_{K(x,y)}$ such that $x - \alpha \in P_i$ and $\psi_i(y) \in P_i$. The element $x - \alpha$ is a prime element of P_i (i.e. $e(P_i|P_\alpha) = 1$), and the residue class field of P_i is isomorphic to $K[T]/(\psi_i(T))$. Hence $f_i(P_i|P_\alpha) = \deg \psi_i(T)$.
(b) If $\deg \psi_i(T) = 1$ for at least one $i \in \{1, \ldots, r\}$, then K is the full constant field of $K(x, y)$.
(c) If $\varphi_\alpha(T)$ has $n = \deg \varphi_\alpha(T)$ distinct roots in K, then there is, for any β with $\varphi_\alpha(\beta) = 0$, a unique place $P_{\alpha,\beta} \in P_{K(x,y)}$ such that $x - \alpha \in P_{\alpha,\beta}$ and $y - \beta \in P_{\alpha,\beta}$. $P_{\alpha,\beta}$ is a place of $K(x, y)$ of degree 1.

We finish the introduction of algebraic function fields with an important theorem. It provides a bound (upper and lower) for the number of degree one (rational) places of a function field over a finite field.

Theorem 1.3.8 ***(Hasse-Weil Bound)*** *Let $F/\mathbb{F}_q$ be a function field with full constant field $\mathbb{F}_q$ of genus g. The number N of places of $F/\mathbb{F}_q$ of degree one satisfies*

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

CHAPTER 2

PRIMITIVE ELEMENTS WITH ARBITRARY TRACE USING CHARACTER SUMS

Let $\mathbb{F}_{q^n}$ be a degree n extension of the finite field $\mathbb{F}_q$ for an arbitrary integer $n \geq 2$. In this chapter, we prove the existence of primitive elements w of $\mathbb{F}_{q^n}$ with prescribed trace t in $\mathbb{F}_q$. The result is due to Cohen ([3]). If $f(x) \in \mathbb{F}_q[x]$ denotes the minimal polynomial of w over $\mathbb{F}_q$, i.e. a primitive polynomial, then, as noted in Section 1.1, this is equivalent to proving that the coefficient of x^{n-1} in $f(x)$ is $-t$, where t is the prescribed element in $\mathbb{F}_q$.

The above existence result is valid for all q, n pairs and all $t \in \mathbb{F}_q$ with two exceptions. For $n = 2$, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w) = 0$ is impossible for any q. If so, then $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(w) = w + w^q = 0$ implies that $w^{q-1} = -1$ which gives $w^{2q-2} = 1$. Since w is primitive in $\mathbb{F}_{q^2}$, its order is $q^2 - 1$. But $2q - 2 \leq q^2 - 1$ for any prime or prime power q. So, there is no primitive element with zero trace in quadratic extensions of finite fields. The second exception is the case $n = 3$, $q = 4$. There are twelve primitive polynomials of degree 3 over $\mathbb{F}_4$ and none of them have zero coefficient for the x^2 term (see [12], Ch. 10).

2.1. Strategy

The following is what we want to prove in this chapter.

Theorem 2.1.1 *Let $n \geq 2$ and $t \in \mathbb{F}_q$ be an arbitrary member with $t \neq 0$ if $n = 2$ or if $n = 3$, $q = 4$. Then there exists a primitive element in $\mathbb{F}_{q^n}$ with trace t.*

The proof of Theorem 2.1.1 is easy after a simple lemma and another theorem. We denote the trace map $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ simply as Tr.

Lemma 2.1.2 *There exists a basis $\{w_1, \ldots, w_n\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with*

$$Tr(w_i) = 0, \ i = 1, \ldots, n-1$$

$$Tr(w_n) = 1 \ .$$

Proof: Since Tr is onto mapping, as noted in Section 1.1, there exists $\xi \in \mathbb{F}_{q^n}$ with $Tr(\xi) \neq 0$. Let $w_n = \frac{\xi}{Tr(\xi)}$. Note that $Tr(w_n) = \frac{1}{Tr(\xi)} Tr(\xi) = 1$, since $Tr(\xi) \in \mathbb{F}_q$ and Tr is $\mathbb{F}_q$-linear. Now let $\{w'_1, \ldots, w'_{n-1}, w_n\}$ be a basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$ extending $\{w_n\}$. Let $w_i = w'_i - Tr(w'_i)w_n$ for all $i = 1, \ldots, n-1$. Then $Tr(w_i) = Tr(w'_i) - Tr(w'_i)Tr(w_n) = 0$ for all i.

□

Theorem 2.1.3 *Let n and t be as in Theorem 2.1.1 and let $\{w_1, \ldots, w_n\}$ be any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then there exists elements $a_1, \ldots, a_{n-1}$ in $\mathbb{F}_q$ such that $a_1 w_1 + \ldots + a_{n-1} w_{n-1} + t w_n$ is a primitive element of $\mathbb{F}_{q^n}$.*

Remark 2.1.1 The geometric interpretation of the above theorem sometimes is very useful. Note that $\mathbb{F}_{q^n}$ can be regarded as an n-dimensional affine space over $\mathbb{F}_q$, $n \geq 2$. Theorem 2.1.3 implies that, with the exception of hyperplanes through the origin when $n = 2$ or when $n = 3$ and $q = 4$, every hyperplane contains a point corresponding to a primitive element of $\mathbb{F}_{q^n}$.

Assuming the validity of Theorem 2.1.3, we can now prove the main result easily.
Proof of Theorem 2.1.1 : Let $\{w_1, \ldots, w_n\}$ be the basis constructed in Lemma 2.1.2. From Theorem 2.1.3 let w be a primitive element of the form $a_1 w_1 + \ldots +$

$a_{n-1}w_{n-1}+tw_n$. Then $Tr(w) = Tr(a_1w_1+\ldots+a_{n-1}w_{n-1}+tw_n)$. Since $a_1,\ldots,a_{n-1},t \in \mathbb{F}_q$, we have $Tr(w) = a_1Tr(w_1)+\ldots+a_{n-1}Tr(w_{n-1})+tTr(w_n)$. From Lemma 2.1.2, $Tr(w_i) = 0$, $i = 1,\ldots,n-1$ and $Tr(w_n) = 1$. Therefore, $Tr(w) = t$.

□

2.2. Estimate for a Character Sum and Proof of Theorem 2.1.3

In this section t is a non-zero element of $\mathbb{F}_q$ while throughout $\{w_1,\ldots,w_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. As shorthand we write $\mathbf{a}$ for $(a_1,\ldots,a_{n-1}) \in \mathbb{F}_q^{n-1}$ etc., and put $\mathbf{w}$ for $(w_1,\ldots,w_{n-1})$ and $\mathbf{a.w}$ for the inner product $a_1w_1+\ldots+a_{n-1}w_{n-1}$.

Lemma 2.2.4 *For all ξ in $\mathbb{F}_{q^n}-\mathbb{F}_q$, there are q^{n-2} solutions $(\boldsymbol{x},\boldsymbol{y}) \in \mathbb{F}_q^{2n-2}$ of the equation*

$$(\boldsymbol{x.w}+tw_n)/(\boldsymbol{y.w}+tw_n) = \xi. \tag{2.1}$$

Proof: Since $\{w_1,\ldots,w_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we can write $\xi w_i = \sum_{j=1}^n a_{ij}w_j$ for all i, where $a_{ij} \in \mathbb{F}_q$ for all i and j. Then (2.1) holds if and only if

$$\begin{aligned}
\xi\Big(\sum_{i=1}^n y_iw_i\Big) \quad &= \quad \sum_{i=1}^n\Big(\sum_{j=1}^n y_ja_{ij}\Big)w_j = \sum_{j=1}^n x_jw_j,\ x_n = y_n = t,\\
&\iff\ x_1 - a_{11}y_1 - \ldots - a_{n-1}y_{n-1} = a_{n1}t\\
&\quad\ \vdots\\
&\quad\ x_{n-1} - a_{1n-1}y_1 - \ldots - a_{n-1n-1}y_{n-1} = a_{nn-1}t\\
&\quad\ -a_{1n}y_1 - \ldots - a_{n-1n}y_{n-1} = (a_{nn}-1)t.
\end{aligned}$$

This linear system has n equations in $2n-2$ unknowns. Hence the rank of the linear system is $2n-2-n = n-2$ unless $a_{jn} = 0$, $j = 1,\ldots,n-1$ which, however, implies that $\xi = a_{nn}$. This is a contradiction since $\xi \notin \mathbb{F}_q$. Therefore the linear system has $n-2$ free unknowns. Since these variables are in $\mathbb{F}_q$, we have q choices for each one. Then there are q^{n-2} solutions.

□

Remark 2.2.2 If $\xi \in \mathbb{F}_q$, then equation (2.1) can be written as

$$x_1w_1 + \ldots + x_{n-1}w_{n-1} + tw_n = \xi(y_1w_1 + \ldots + y_{n-1}w_{n-1} + tw_n).$$

Since $\{w_1, \ldots, w_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and x_i, y_j, $t \in \mathbb{F}_q$, for all i,j, we conclude that $x_i = \xi y_i$ for $i = 1, \ldots, n-1$ and $t = \xi t$. Since $t \neq 0$, we get $\xi = 1$ and hence $x_i = y_i$ for all $i = 1, \ldots, n-1$. Therefore, $\mathbf{x} = \mathbf{y}$ and the value of (2.1) is 1. Since $\mathbf{x} \in \mathbb{F}_q^{n-1}$, there are q^{n-1} such $\mathbf{x}$.

Now let χ be a multiplicative character of $\mathbb{F}_{q^n}$ and define

$$S(\chi) = \sum_{\mathbf{a} \in \mathbb{F}_q^{n-1}} \chi(\mathbf{a}.\mathbf{w} + tw_n). \tag{2.2}$$

Also let $Q = (q^n - 1)/(q - 1)$. We compute $|S(\chi)|$ next.

Lemma 2.2.5 *Suppose χ is a* non-trivial *character of order $d(> 1)$, where $d \mid q^n - 1$. Then*

$$|S(\chi)| = \begin{cases} q^{(n-2)/2}, & \text{if } d \mid Q, \\ q^{(n-1)/2}, & \text{otherwise.} \end{cases}$$

Proof: Let $\bar{\chi}$ be the conjugate of χ. Then

$$\begin{aligned} |S(\chi)|^2 &= S(\chi)S(\bar{\chi}) \\ &= \sum_{\mathbf{a} \in \mathbb{F}_q^{n-1}} \chi(\mathbf{a}.\mathbf{w} + tw_n) \sum_{\mathbf{b} \in \mathbb{F}_q^{n-1}} \chi((\mathbf{b}.\mathbf{w} + tw_n)^{-1}) \\ &= \sum_{\mathbf{a},\mathbf{b} \in \mathbb{F}_q^{n-1}} \chi((\mathbf{a}.\mathbf{w} + tw_n)/(\mathbf{b}.\mathbf{w} + tw_n)) \\ &= q^{n-2} \sum_{\xi \in \mathbb{F}_{q^n}^* - \mathbb{F}_q^*} \chi(\xi) + q^{n-1}\chi(1), \end{aligned}$$

where the last equality follows from Lemma 2.2.4 and Remark 2.2.2. From the fact that $\sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) = 0$ (cf. Theorem 1.2.2) for non-trivial characters and $\chi(1) = 1$, we have

$$|S(\chi)|^2 = -q^{n-2} \sum_{\xi \in \mathbb{F}_q^*} \chi(\xi) + q^{n-1}. \tag{2.3}$$

For trivial multiplicative character, we have $\sum_{\xi\in\mathbb{F}_q^*}\chi(\xi) = q-1$. Note that the multiplicative characters χ of $\mathbb{F}_{q^n}$ of order d dividing Q are precisely the characters in $(\mathbb{F}_q^*)^\perp$, since we have

$$(\mathbb{F}_q^*)^\perp \cong (\widehat{\mathbb{F}_{q^n}^*/\mathbb{F}_q^*}) \cong \mathbb{F}_{q^n}^*/\mathbb{F}_q^* \cong \mathbb{Z}_Q$$

by Theorem 1.2.3. Now the sum in (2.3) is zero if the restriction of χ to $\mathbb{F}_q^*$ is non-trivial, i.e. if $d \nmid Q$ and otherwise, the right side of (2.3) has the value $-q^{n-2}(q-1)+q^{n-1} = q^{n-2}$. Taking square roots on both sides of (2.3), we are done.

□

Let e be a divisor of q^n-1 and define $N(e)$ to be the number of elements of the form $\xi = \mathbf{a}.\mathbf{w} + tw_n$ (i.e. on a given hyperplane) for which $\xi \neq 0$ and the integer defined by $(q^n-1)/(\textit{order of } \xi)$ and e are relatively prime. When $e = q^n-1$, clearly order of ξ is q^n-1. Hence $N(q^n-1)$ is simply the number of primitive elements on the hyperplane. To calculate this number, we use the Vinogradov Formula in [10]. Recall that The *Möbius function* is the function on $\mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes}, \\ 0 & \text{if } n \text{ is divisible by the square of a prime.} \end{cases}$$

Lemma 2.2.6 (The Vinogradov Formula) *Let U be a subset of $\mathbb{F}_{q^n}$ such that $U = \{\boldsymbol{a} \in \mathbb{F}_q^{n-1} \mid \boldsymbol{a}.\boldsymbol{w} + tw_n\}$. Let $N(q^n-1)$ be the number of primitive elements $\mathbb{F}_{q^n}$ contained in U. Then one has*

$$\frac{q^n-1}{\varphi(q^n-1)} N(q^n-1) = \sum_{d|(q^n-1)} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x), \tag{2.4}$$

where φ and μ are the functions of Euler and Möbius and ψ_d runs over all multiplicative characters of order exactly d.

Proof: Let $x \in \mathbb{F}_{q^n}$, and write $x = w^k$ for some fixed primitive element w of $\mathbb{F}_{q^n}$. Since both the Möbius and the Euler function are multiplicative functions, we have

$$\sum_{d|(q^n-1)} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \psi_d(x) = \prod_{p|q^n-1} \Big(1 + \frac{\mu(p)}{\varphi(p)} \sum_{\psi_p} \psi_p(x) \Big) ,$$

where p runs over the prime divisors of $q^n - 1$.

Note that $\mu(p) = -1$ and $\varphi(p) = p - 1$, which follow directly from definition. Since $\psi_p(w)^p = 1$ and w is primitive in $\mathbb{F}_{q^n}$, then $\xi_p = \psi_p(w)$ is a primitive p^{th} root of unity in multiplicative group of complex numbers. Each ψ_p is determined by the image of w. Hence, number of characters of order p are equal to primitive p^{th} roots of unity in multiplicative group of complex numbers. Therefore, $\sum_{\psi_p} \psi_p(x) = \sum_{\xi_p} \xi_p^k$. Hence,

$$\prod_{p|q^n-1} \Big(1 + \frac{\mu(p)}{\varphi(p)} \sum_{\psi_p} \psi_p(x) \Big) = \prod_{p|q^n-1} \Big(1 - \frac{1}{p-1} \sum_{\xi_p} \xi_p^k \Big) \, ,$$

where ξ_p runs over the primitive p^{th} roots of unity in multiplicative group of complex numbers.

Note that there are $\varphi(p) = p - 1$ primitive p^{th} roots of unity. Since $\xi_p^p = 1$, then $\xi_p^k = 1$ for $p \mid k$. Hence, $\sum_{\xi_p} \xi_p^k = p - 1$ if $p \mid k$. Also note that ξ_p^k is again a primitive p^{th} root of unity for $p \nmid k$. Therefore, $\sum_{\xi_p} \xi_p^k$ is equal to sum of all different $p - 1$ powers of ξ_p except for 1. This is equal to -1. Hence,

$$\sum_{\xi_p} \xi_p^k = \begin{cases} p - 1, & \text{if } p \mid k, \\ -1, & p \nmid k. \end{cases}$$

Hence,

$$\prod_{p|q^n-1} \Big(1 - \frac{1}{p-1} \sum_{\xi_p} \xi_p^k \Big) = \begin{cases} 0, & \text{if some } p \text{ divides } k, \\ \prod_{p|q^n-1} \Big(1 + \frac{1}{p-1} \Big), & \text{if } (q^n - 1, k) = 1 \, . \end{cases}$$

By multiplicativity of φ again, we have

$$\prod_{p|q^n-1} \Big(1 + \frac{1}{p-1} \Big) = \prod_{p|q^n-1} \frac{p}{\varphi(p)} = \frac{q^n - 1}{\varphi(q^n - 1)} \, .$$

Thus the assertion follows by summing the equation just obtained over all $x \in U$.

□

Remark 2.2.3 In fact, Vinogradov Formula holds for more general subsets of $\mathbb{F}_{q^n}$. We just state the version which is sufficient for our purpose.

We set $N(q,n) = \frac{q^n-1}{\varphi(q^n-1)}N(q^n-1)$ and $W(e) = 2^{w(e)}$, where $w(e)$ denotes the number of distinct primes dividing e.

Lemma 2.2.7 *If*

$$q^{n-1} - (W(q^n-1) - W(Q))q^{(n-1)/2} - (W(Q)-1)q^{(n-2)/2} > 0, \tag{2.5}$$

then $N(q,n)$ is positive, i.e. $N(q^n-1) > 0$ and hence U contains a primitive element of $\mathbb{F}_{q^n}$.

Proof: Assume that U does not contain a primitive element of $\mathbb{F}_{q^n}$. Then, from Lemma 2.2.6,

$$\sum_{d|(q^n-1)} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x) = 0 \ .$$

We split up the preceding sum as

$$\sum_{d|(q^n-1),\ d\nmid Q} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x) + \sum_{d|Q,\ d\neq 1} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x) + \sum_{d=1} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x) = 0 \ .$$

Note that φ_1 is the trivial character. Hence, $\sum_{x\in U} \varphi_1(x) = \mid U \mid = q^{n-1}$. Therefore, we get

$$\sum_{d|(q^n-1),\ d\nmid Q} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x) + \sum_{d|Q,\ d\neq 1} \frac{\mu(d)}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \psi_d(x) = -q^{n-1}. \tag{2.6}$$

Taking absolute values in (2.6) and using the triangle inequality yields

$$\sum_{d|(q^n-1),\ d\nmid Q} \frac{\mid \mu(d) \mid}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \mid \psi_d(x) \mid + \sum_{d|Q,\ d\neq 1} \frac{\mid \mu(d) \mid}{\varphi(d)} \sum_{\psi_d} \sum_{x\in U} \mid \psi_d(x) \mid \geq q^{n-1}. \tag{2.7}$$

Note that the multiplicative characters ψ_d of $\mathbb{F}_{q^n}$ of order d dividing Q are precisely the characters in $(\mathbb{F}_q^*)^\perp$, since we have $(\mathbb{F}_q^*)^\perp \cong (\widehat{\mathbb{F}_{q^n}^*/\mathbb{F}_q^*}) \cong \mathbb{F}_{q^n}^*/\mathbb{F}_q^* \cong \mathbb{Z}_Q$, by Theorem 1.2.3 in Section 1.2. Hence we can apply Lemma 2.2.5 to substitute for the absolute values of the character sums appearing in (2.7). We also note that there are exactly $\varphi(d)$ multiplicative characters of order d. We obtain

$$q^{(n-1)/2} \sum_{d|(q^n-1),\ d\nmid Q} \mid \mu(d) \mid \ + q^{(n-2)/2} \sum_{d|Q,\ d\neq 1} \mid \mu(d) \mid \geq q^{n-1}. \tag{2.8}$$

We now require the following auxiliary formula:

$$\sum_{d|m} \mid \mu(d) \mid = 2^{w(m)}. \tag{2.9}$$

This result is an immediate consequence of the definition of the Möbius function, since one can form exactly $2^{w(m)}$ squarefree divisors of m from the $w(m)$ distinct prime divisors of m. Using (2.9), we obtain from (2.8) the inequality

$$(W(q^n-1)-W(Q))q^{(n-1)/2}+(W(Q)-1)q^{(n-2)/2} \geq q^{n-1},$$

contradicting the hypothesis in the statement. This proves the lemma.

□

Proof of Theorem 2.1.3 : There exists a primitive root of $\mathbb{F}_{q^2}$ of the form $a_1w_1 + tw_2$ for some $a_1 \in \mathbb{F}_q$ by Theorem 1.1 of [1]. Hence Theorem 2.1.3 is true for $n = 2$. For $n \geq 3$ and $t = 0$, the result follows from Theorem 1 of [2]. This theorem conclude that every cyclic (v, k, λ)-difference set contains a residue prime to v, i.e. it has generator of the additive group of integers modulo v with two exceptions. Namely, two $(21, 5, 1)$-difference sets do not contain a generator of the additive group of integers modulo v. For $q \neq 4$ and $n \geq 3$ every hyperplane in projective n-space over $\mathbb{F}_q$ contains an element of order Q. This implies that every hyperplane *through the origin* in affine n-space contains an element ξ whose index with respect to any primitive element is prime to Q, so that $(q^n - 1)/(order\ of\ \xi)$ is prime to Q. Hence, we can find a suitable element $a \in \mathbb{F}_q$ such that $a\xi$ is a primitive element which gives the conclusion in Remark 2.1.1. Therefore we assume that $n \geq 3$ and $t \neq 0$.

Our mail tool is Lemma 2.2.7. We must check that (2.5) in Lemma 2.2.7 is generally effective when $n = 3$. After that, verification of this equation is easier for greater n. We therefore concentrate on this case.

Suppose that $n = 3$. Note first that if a prime p divides $Q = q^2 + q + 1$ then, either $p = 3$ (in which case $q \equiv 1(mod 3)$) or $p \equiv 1(mod 6)$(and $\nmid (q-1)$). Now we

set $r = w(q^3-1)(\geq 1)$, $s = w(Q)(\geq 1)$ and $t = w(q-1)$. We have

$$t = \begin{cases} r-s & \text{if } q \not\equiv 1(mod 3) \\ r-s+1 & \text{if } q \equiv 1(mod 3) \end{cases} \tag{2.10}$$

With this setting, (2.5) in Lemma 2.2.7 is true if

$$q > 2^r - 2^s + (2^s - 1)q^{-\frac{1}{2}}. \tag{2.11}$$

Since $r = s$ for $q = 2$, we can easily see that (2.11) holds when $r = 1$ or 2. Moreover, if $r = 3$ or 4, then (2.11) is satisfied when $q > 5$ or $q > 13$, respectively. Further, we gain (2.11) for all $q \leq 13$ by direct verification except when $q = 11$ in which case $q^3 - 1 = 1330 = 2.5.7.19$, $r = 4$ and $s = 2$. This case is investigated separately at the end.

Now we define integers $A(m)$ and $B(m)$ as the product of the first m primes and the first m primes which are congruent to 1 modulo 6 for each positive integer m, respectively. We have $q > A(t)$ and

$$Q \geq \begin{cases} B(s), & \text{if } q \not\equiv 1(mod 3), \\ 3B(s-1), & \text{if } q \equiv 1(mod 3). \end{cases} \tag{2.12}$$

If

$$A(m) \geq 2^r - 2, \tag{2.13}$$

we can conclude that (2.11) is satisfied for $t \geq m$. Note that for $s = 1$ it is satisfied since q is an integer.

If $r = 5$, then (2.13) holds with $m = 3$ and so we can assume $t \leq 2$. By (2.10),(2.12) we have $s \geq 3$, $Q \geq B(3) = 1729$ and $q > 41$. Note that this is stronger than (2.11).

If $r = 6$, then (2.13) holds with $m = 4$ and we can take $t \leq 3$. Indeed if $t = 3$ and $q \not\equiv 1(mod 3)$ then $q \geq 71$ which implies (2.11). Otherwise we have $s \geq 4$ from (2.10) and hence we have $Q \geq 5187$ by (2.12). Hence,it yields $q > 71$. The method for the cases $r = 7$ and 8 is similar to that of $r = 5$ and 6, respectively. Note that $B(4) = 7.13.19.31 = 53599$. Hence, we obtain $q > 230$ for $r = 7$ and $q \geq 771$ and $q > 400$ for $r = 8$.

For $r \geq 9$ we use the following facts which can be proved by induction for $m \geq 5$, namely,

$$A(m) \geq 2^m,\ B(m) > 6^m(m+1)!/3 > 2^{4m}\ (m \geq 5). \tag{2.14}$$

Recall that $[x]$ denotes the integral part of a real number x. Selecting $m = [\frac{1}{2}(r+1)]$, we obtain from (2.14) that $t < m$ and so $s \geq m$. From (2.14), were (2.11) to be false, we would have

$$2^{4m} \geq 2^{2r} \geq (q+1)^2 > Q > B(m) > 2^{4m},$$

a contradiction. With the exception $q = 11$ noted above, this completes the proof for $n = 3$.

For greater n, the verification is easier than that for small values of n. Let $n = 4$. If q is odd, then 16 divides $q^4 - 1$. Hence we are done. For example, if $w(q^4-1) = 4$ then $q^4 - 1 \geq 16.3.5.7 = 1680$ which implies $q^{\frac{3}{2}} > 14$ and this is enough. When $n = 5$ it is sufficient to prove that $q^2 > W(q^5 - 1)$. It can be seen from the fact that $p \equiv 1 (mod\ 10)$ for all $p\ (> 5)$ dividing Q. Therefore, we omit further details.

From the above for the completion of the proof of Theorem 2.1.3 the only lack is the case which is $q = 11$ and $n = 3$. For this case, note that there are eleven primitive polynomials of degree 3 over $\mathbb{F}_{11}$. These are

$$5 + 6x + x^3$$
$$4 + 6x + x^2 + x^3$$
$$4 + 7x + 2x^2 + x^3$$
$$9 + 4x + 3x^2 + x^3$$
$$9 + 2x + 4x^2 + x^3$$
$$5 + 5x + 5x^2 + x^3$$
$$3 + 6x^2 + x^3$$
$$5 + 2x + 7x^2 + x^3$$
$$9 + x + 8x^2 + x^3$$
$$4 + 9x^2 + x^3$$
$$5 + 5x + 10x^2 + x^3$$

(See [10]). Looking at the coefficients of x^2 in these polynomials, we realize that all possible trace values are taken in this case. Hence, we are done.

□

CHAPTER 3

"GENERALIZATION" VIA ALGEBRAIC FUNCTION FIELDS

Cohen's result (cf. Theorem 2.1.1) guarantees the existence of a primitive element in $\mathbb{F}_{q^n}$ with prescribed trace $t \in \mathbb{F}_q$ with two exceptions. Namely, as seen in Chapter 2, t cannot be zero if $n = 2$ or $(n, q) = (3, 4)$. In this chapter, we will prove a "generalization" of this result, which is due to Özbudak ([16]). It is valid not only for the trace map but for any additive polynomial, with some technical details which will be explained. The reason why we call this a "generalization" is that it only guarantees a nonzero prescribed trace. The technique used in Özbudak's work is the theory of algebraic function fields rather than character sums, which was the main tool for Cohen's work. In the first section we describe some properties of important class of function fields called Artin-Schreier extensions. The second section contains the proof of Özbudak's theorem.

3.1. Artin-Schreier Extensions

Let K be a field of char $K = p > 0$. A polynomial of the form

$$A(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \ldots + a_1 T^p + a_0 T \in K[T] \tag{3.1}$$

is called an *additive* (or *linearized*) polynomial over K. $A(T)$ is separable iff $A(T)$ and its derivative $A'(T)$ have no common factor of degree > 0. Since $A'(T) = a_0$, then the polynomial (3.1) is separable iff $a_0 \neq 0$. An additive polynomial has the following important property :

$$A(u + v) = A(u) + A(v) \tag{3.2}$$

for any u, v in some extension field of K. In particular, if $A(T)$ is an additive and separable polynomial over K all of whose roots are in K, then these roots form a subgroup of the additive group of K of order $p^n = \deg A(T)$. This easily follows from equation (3.2). The converse of this is also true, which gives a nice criteria for additivity of separable polynomials.

Lemma 3.1.1 *Let K be an algebraically closed field. Let $P(x) \in K[x]$ be a separable polynomial. Let*

$$\{w_1, \ldots, w_m\} \subset K$$

be the set of its roots. Then $P(x)$ is additive *if and only if $\{w_1, \ldots, w_m\}$ is an additive subgroup in K.*

Proof: What must be shown is the following: Let $W = \{w_1, \ldots, w_m\}$ be an additive subgroup of K and let

$$P(x) := P_W(x) := \prod_{i=1} m(x - w_i) \ .$$

Then $P(x)$ is additive.

Note that if $w \in W$, then $P(x + w) = P(x)$. Now let $y \in K$ and put

$$H(x) = P(x + y) - P(x) - P(y).$$

Clearly deg $H(x) <$ deg $P(x)$. On the other hand, it is now trivial to see that $H(w) = 0$ for $w \in W$. As $m =$deg $P >$deg H, we conclude that $H(x) \equiv 0$.

Let y now be an arbitrary indeterminate and put

$$H_1(y) = P(x + y) - P(x) - P(y) \in K[x][y].$$

We conclude that $H_1(\alpha) = 0$ for $\alpha \in K$. As K is infinite, we see that $H_1(y) \equiv 0$, which completes the proof.

□

Before defining Artin-Schreier extensions, we need an important technical lemma.

Lemma 3.1.2 *Let F/K be an algebraic function field of characteristic $p > 0$. For an arbitrary element $u \in F$ and an arbitrary place $P \in \mathbb{P}_F$, one of the two cases is satisfied:*
(a) There exists an element $z \in F$ such that $v_P(u - (z^p - z)) \geq 0$,
(b) For some $z \in F$, $v_P(u - (z^p - z)) = -m < 0$ with $m \not\equiv 0 \pmod{p}$. In this case, the integer m is uniquely determined by u and P. Namely,

$$-m = max\{v_P(u - (w^p - w)) \mid w \in F\}. \tag{3.3}$$

Proof: Let $x_1, x_2 \in F - \{0\}$ with $v_P(x_1) = v_P(x_2)$. Since $v_P(1/x_2) = -v_P(x_2)$, then $v_P(x_1/x_2) = min\{v_P(x_1), -v_P(x_2)\} \leq 0$ by Strict Triangle Inequality (cf. Lemma 1.3.4). Then $x_1/x_2 \notin P$, i.e. the residue class $(x_1/x_2)(P) \in \mathcal{O}_P/P$ is not zero. Since $\mathcal{O}_P/P$ is perfect field of characteristic $p > 0$, then $(x_1/x_2)(P) = (y(P))^p$ for some $y \in \mathcal{O}_P - P$. Then we have $v_P(y) = 0$ and $v_P(x_1/x_2 - y^p) > 0$, which imply $v_p(x_1 - y^p x_2) > v_P(x_1)$.

Assume that $v_P(u - (z_1^p - z_1)) = -lp < 0$ for some $z_1 \in F$. We can choose $t \in F$ with $v_P(t) = -l$. Then $v_P(u - (z_1^p - z_1)) = v_P(t^p) = -lp$, again by Strict Triangle Inequality. By the arguments in the first paragraph we can find $y \in F$ with $v_P(y) = 0$. By setting $z_2 = z_1 + yt$, we get $v_P(u - (z_2^p - z_2)) > -lp$.

Assume that $v_P(u - (z^p - z)) < 0$ for all $z \in F$. If there exists some l such that $v_P(u - (z^p - z)) = -lp < 0$ for all $z \in F$, then we can find $z_2 \in F$ such that $v_P(u - (z_2^p - z_2)) > -lp$ by arguments above. Continuing this way, we can find z_n such that $v_P(u - (z_n^p - z_n)) \geq 0$ since lp is finite. Then this proves existence of an element $z \in F$ such that (a) holds. if there is no element z of F such that $v_P(u - (z^p - z)) \geq 0$, then we must have an element z such that $v_P(u - (z^p - z)) = -m < 0$ with $m \not\equiv 0 \pmod{p}$. The only lack is the characterization of m. Now

let $v_P(u-(z^p-z)) = -m < 0$ with $m \not\equiv 0 \pmod{p}$. Clearly $pv_P(w-z) \neq -m$ for any $w \in F$. If $pv_P(w-z) > -m$, then $pv_P((w-z)^p-(w-z)) > -m$. From Strict Triangle Inequality we get $v_P(u-(w^p-w)) = -m$. If $pv_P(w-z) < -m$, we obtain $v_P(u-(w^p-w)) < -m$ using Strict Triangle Inequality. Hence, we have $v_P(u-(w^p-w)) \leq -m$. So we proved that characterization of m in (b). Hence, we are done.

□

Definition 3.1.1 Let F/K be an algebraic function field of characteristic $p > 0$. Suppose $u \in F$ is an element with the property

$$u \neq w^p - w, \ \textit{for all } w \in F. \tag{3.4}$$

Let $F' = F(y)$, where $y^p - y = u$. F'/F is called an *Artin-Schreier* extension.

We list some important properties of Artin-Schreier extensions in the following theorem.

Theorem 3.1.3 *Let $F' = F(y)$ with $y^p - y = u$, where $u \in F$, be an Artin-Schreier extension. For a place $P \in \mathbb{P}_F$, define*

$$m_P = \begin{cases} m, & \textit{if there exists } z \in F \textit{ such that } v_P(u-(z^p-z)) = -m < 0 \textit{ and } p \nmid m, \\ -1, & \textit{if } v_P(u-(z^p-z)) \geq 0 \textit{ for some } z \in F. \end{cases} \tag{3.5}$$

Then

(i) F'/F is a cyclic Galois extension of degree p.

(ii) $P \in \mathbb{P}_F$ is unramified in F'/F if and only if $m_P = -1$.

(iii) $P \in \mathbb{P}_F$ is totally ramified in F'/F if and only if $m_P > 0$.

(iv) If $m_Q > 0$ for some $Q \in \mathbb{P}_F$, then K is the full constant field of F' and

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

where g' (respectively g) is the genus of F'/K (respectively F/K).

Proof: See [17], Theorem 3.7.8.

Remark 3.1.1 Note that the number m_P in (3.5) is well - defined by Lemma 3.1.2.

Observe that the equation defining Artin-Schreier extension involves a specific additive polynomial $y^p - y$. A natural question is whether one can say something about extensions defined by a general additive polynomial $A(T)$. The following theorem generalizes Artin-Schreier extensions in this way. We will refer to the extensions of the type described below also as Artin-Schreier extensions, which is commonly done in the literature.

Theorem 3.1.4 *Consider an algebraic function field F/K with full constant field K of characteristic $p > 0$, and an additive separable polynomial $A(T) \in K[T]$ of degree p^n which has all roots in K. Let $u \in F$. Suppose that for any $P \in \mathbb{P}_F$ there is an element $z \in F$ such that*

$$v_P(u - A(z)) \geq 0 \tag{3.6}$$

or

$$v_P(u - A(z)) = -m \text{ with } m > 0 \text{ and } m \not\equiv 0 \pmod{p} \tag{3.7}$$

Define $m_P := -1$ in case (3.6) and $m_P := m$ in case (3.7). Consider the extension field $F' = F(y)$ of F where y satisfies the equation $A(y) = u$. If there exists at least one place $Q \in \mathbb{P}_F$ with $m_Q > 0$, the following holds:

1. *F'/F is a Galois extension of degree p^n and K is the full constant field of F'.*
2. *Any $P \in \mathbb{P}_F$ with $m_P = -1$ is unramified in F'/F.*
3. *Any $P \in \mathbb{P}_F$ with $m_P > 0$ is totally ramified in F'/F.*
4. *Let g' (respectively g) be the genus of F' (respectively F). Then*

$$g' = p^n g + \frac{(p^n - 1)}{2} \Big(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \deg P \Big) .$$

The proof of this theorem can be given by mimicing the arguments in the proof of Theorem 3.1.3. Note the difference in the statements of Theorem 3.1.3 and Theorem 3.1.4, which is of fundamental importance. Namely, the numbers m_P associated with

places $P \in \mathbb{P}_F$ are automatically well-defined for extensions defined by $y^p - y = u$, whereas we make an assumption that they are well-defined when a general additive polynomial is used. So, one has to check this point in the latter case. In the following theorem, we consider a class of Artin-Schreier extensions and determine some properties, which will be used in next section.

Theorem 3.1.5 *Let $L = \mathbb{F}_{q^r}$ be a finite field in which the additive polynomial $A(T) = a_0T + a_1T^q + \ldots + a_nT^{q^n} \in L[T]$ with $a_0a_n \neq 0$ splits. Let $h(x) \in L[x]$ be another polynomial of degree e, where $gcd(e, q) = 1$. Consider the extension $E = L(x, y)$ of the rational function field $L(x)$ defined by equation*

$$A(y) = h(x) \ .$$

We have:
(i) $g(E) = \frac{(q^n-1)(e-1)}{2}$, where g is the genus of E.
(ii) If $P_\infty \in \mathbb{P}_{L(x)}$ is the place at infinity and P_α denotes the zero of $(x - \alpha) \in L(x)$ in $\mathbb{P}_{L(x)}$ (for all $\alpha \in L$), then P_∞ is totally ramified in $E/L(x)$ with a unique degree one extension. For P_α, one of the following holds:

- *$A(T) = h(\alpha)$ has q^n distinct roots in L. In this case P_α has q^n distinct extensions in E, each of which has degree one.*
- *$A(T) = h(\alpha)$ has no root in L. In this case all extensions of P_α in E have degree greater than one.*

Proof: Since $a_0a_n \neq 0$, $A(T)$ is a separable, additive polynomial of degree q^n whose roots are in $\mathbb{F}_{q^r} = L$. Recall that the only places of $L(x)$ are the place at infinity P_∞, the affine places $P_{q(x)}$ associated to irreducible polynomials $q(x) \in L[x]$. We want to use the conclusions of Theorem 3.1.4. However, one needs to check that the assumptions in Theorem 3.1.4 are satisfied for any place of $L(x)$ (cf. Remark 3.1.1).

For any affine place $P_{q(x)} \in \mathbb{P}_{L(x)}$, let $0 = z \in L(x)$. Then $v_{P_{q(x)}}(h(x) - A(0)) = v_{P_{q(x)}}(h(x)) \geq 0$. Is it possible to find $z \in L(x)$ such that $v_{P_{q(x)}}(h(x) - A(z)) = -m < 0$ and $m \not\equiv \pmod p$? We have $v_{P_{q(x)}}(h(x) - A(z)) = v_{P_{q(x)}}(h(x) - (a_0z +$

$a_1z^q + \ldots + a_nz^{q^n})$). For this to be negative, $v_{P_{q(x)}}(a_0z + a_1z^q + \ldots + a_nz^{q^n})$ must be negative by Strict Triangle Inequality (cf. Lemma 1.3.4). Therefore, $v_{P_{q(x)}}(z) < 0$ must hold by Strict Triangle Inequality (cf. Lemma 1.3.4). Then $v_{P_{q(x)}}(A(z)) = min\{v_{P_{q(x)}}(z), \ldots, v_{P_{q(x)}}(z^{q^n})\} = q^n v_{P_{q(x)}}(z) < 0$. Now $v_{P_{q(x)}}(h(x) - A(z)) = v_{P_{q(x)}}(A(z)) = q^n v_{P_{q(x)}}(z) < 0$ but $q^n v_{P_{q(x)}}(z) \equiv 0 \pmod p$. Hence, for any affine place of $L(x)$, the assumptions in Theorem 3.1.4 are satisfied. Therefore, $m_{P_{q(x)}} := -1$.

For P_∞, let $z = 0$. Then $v_{P_\infty}(h(x) - A(0)) = v_{P_\infty}(h(x)) = -\deg(h(x)) = -e$. Since $gcd(e, q) = 1$, then $v_{P_\infty}(h(x) - A(0)) = -e \not\equiv 0 \pmod p$. Then we ask if it is possible to find $z \in L(x)$ such that $v_{P_\infty}(h(x) - A(z)) \geq 0$. If $v_{P_\infty}(A(z)) > -e$, then $v_{P_\infty}(h(x) - A(z)) = v_{P_\infty}(h(x)) = -e < 0$. If $v_{P_\infty}(A(z)) < -e = v_{P_\infty}(h(x))$, then $v_{P_\infty}(h(x) - A(z)) = v_{P_\infty}(A(z)) < -e < 0$. Finally, if $v_{P_\infty}(A(z)) = -e = v_{P_\infty}(h(x))$, then $v_{P_{q(x)}}(z) < 0$. But, as seen in the previous paragraph, this implies $v_{P_\infty}(A(z)) = -e = q^n v_{P_\infty}(z)$. This is impossible since $(e, q) = 1$.

The final thing to check is if the existence $z \in L(x)$ of

$$v_{P_\infty}(h(x) - A(z)) = -\bar{e} < 0,\ \bar{e} \not\equiv 0 \pmod p \text{ and } \bar{e} \neq e\ ,$$

i.e. whether e is well-defined. However our analysis in the previous paragraph shows that for any $z \in L(x)$ and all possible values of $v_{P_\infty}(A(z))$, $v_{P_\infty}(h(x) - A(z))$ is either $-e$ or less than $-e$ but divisible by p. So, e is well-defined and $m_{P_\infty} = e > 0$. Therefore, we can use conclusions of Theorem 3.1.4.

The first conclusion is that P_∞ is the only place of $L(x)$ that is ramified in $E/L(x)$. The ramification index is $q^n = [E : L(x)]$, since P_∞ is totally ramified. Hence, there exists a unique place $Q_\infty \in \mathbb{P}_E$ over P_∞. Note that $e(Q_\infty \mid P_\infty) = q^n$ implies by Theorem 1.3.6, $f(Q_\infty|P_\infty) = 1$. Hence, $\deg(Q_\infty) = [E_{Q_\infty} : L] = \frac{f(Q_\infty|P_\infty)\deg P_\infty}{[L:L]} = 1$.

(i) From Theorem 3.1.4, we have

$$g(E) = q^n g(L(x)) + \frac{q^n - 1}{2}\left(-2 + \sum_{P \in \mathbb{P}_{L(x)}} (m_P + 1)\deg P\right).$$

$g(L(x)) = 0$, $m_{P_\infty} = e$ and $m_P = -1$ for any $P_\infty \neq P \in \mathbb{P}_{L(x)}$. Hence, $g(E) = \frac{(q^n-1)}{2}(-2 + (e + 1)) = \frac{(q^n-1)(e-1)}{2}$.

(ii) Consider the equation $A(T) = h(\alpha)$ for $\alpha \in L$. If $\mu \in L$ is any root of $A(T)$ and β is a root of $A(T) = h(\alpha)$, then $A(\beta + \mu) = A(\beta) + A(\mu) = A(\beta) = h(\alpha)$. Since L contains all roots of $A(T)$ by assumption and $A(T)$ is separable, we conclude that if $A(T) = h(\alpha)$ has one root in L then it must have q^n distinct roots.

If $A(T) = h(\alpha)$ has q^n distinct roots in L, then $A(T) - h(\alpha)$ factors into q^n distinct linear polynomials over L. Then, by Kummer's Theorem (cf. Theorem 1.3.7), there exists q^n degree one extensions of P_α in $\mathbb{P}_E$. If $A(T) - h(\alpha) \in L[T]$ has no root in L, then the irreducible factors over L of this polynomial have degree > 1. Hence, again by Kummer's Theorem, P_α has no degree one extension in $\mathbb{P}_E$.

□

We finish this section with a useful technical lemma of Madden.

Lemma 3.1.6 *Let l and d be two fixed natural numbers with $l \neq 1$. If M is large enough, then there exists integers s and t such that :*

1. *$gcd(s,t) = 1$ and s,t are squarefree,*
2. *r is a prime number. $r \mid (M-1)$ if and only if $r \mid (st)$,*
3. *$\frac{\varphi(t)}{t} > \frac{l-1}{l}.[1 + (d.s-1).\frac{M^{\frac{1}{2}}}{M-1} + \frac{2}{M-1}]$*

where $\varphi(t)$ is the Euler phi function.

Proof: See Madden ([14], page 511).

□

3.2. Additive Polynomials and Primitive Elements

We start with fixing some notation for this section. Let $p = \text{char } \mathbb{F}_q$ and $\bar{K}$ denote the algebraic closure of $\mathbb{F}_q$. Let

$$A(T) = a_0T + a_1T^q + \ldots + a_nT^{q^n} \in \mathbb{F}_{q^m}[T],\ a_0a_n \neq 0 \tag{3.8}$$

be an additive polynomial. Let $\mathbb{F}_{q^{mN}}$ be the smallest extension of $\mathbb{F}_{q^m}$ in which $A(T)$ splits. For $k \geq 1$, we define

$$\begin{aligned} \Phi_k : \mathbb{F}_{q^{mNk}} &\longrightarrow \mathbb{F}_{q^{mNk}} \\ \alpha &\mapsto A(\alpha) \end{aligned}$$

and $B_k(T) := \prod_{\beta \in Im(\Phi_k)}(T - \beta) \in \mathbb{F}_{q^{mNk}}[T]$. For every $k \geq 1$, Φ_k is an additive homomorphism since $A(T)$ is an additive polynomial for which $A(\alpha_1+\alpha_2) = A(\alpha_1)+A(\alpha_2)$ for all $\alpha_1, \alpha_2 \in \mathbb{F}_{q^{mNk}}$. This implies that Im (Φ_k) is an additive subgroup of $\mathbb{F}_{q^{mNk}}$ and, hence, of $\bar{K}$. Since Im (Φ_k) is the set of roots of the separable polynomial $B_k(T)$, and by the above observation that Im (Φ_k) is an additive subgroup of $\bar{K}$, we conclude that $B_k(T)$ is an additive polynomial (cf. Lemma 3.1.1). Note that $|Ker(\Phi_k)| = q^n$ since $A(T)$ is separable of degree q^n which splits over $\mathbb{F}_{q^{mNk}}$. Hence

$$|Im(\Phi_k)| = |\mathbb{F}_{q^{mNk}}/Ker(\Phi_k)| = q^{mNk-n} = \deg(B_k(T))\ .$$

Finally, define for all $k \geq 1$

$$\begin{aligned} \Psi_k : \mathbb{F}_{q^{mNk}} &\longrightarrow \mathbb{F}_{q^{mNk}} \\ \alpha &\mapsto B_k(\alpha) \end{aligned}$$

The following is the result of Özbudak:

Theorem 3.2.7 *With the notations as above, let $f(T) \in \mathbb{F}_{q^{mN}}[T]$ of degree $d \geq 1$ with $f(0) = 0$ and $gcd(d, q) = 1$. If k is sufficiently large and $0 \neq u_k \in Im\Psi_k$, then there exists a primitive root $w_k \in \mathbb{F}_{q^{mNk}}$ such that $B_k(f(w_k)) = u_k$.*

Proof: We use the notation introduced in the paragraph preceding the theorem. Let $L_k = \mathbb{F}_{q^{mNk}}$ and α_k denote a primitive element for L_k for all $k \geq 1$. We consider the function fields

$$\begin{cases} E_k = L_k(x, y) \\ A(y) = f(\alpha_k^t x^s) - v_k \end{cases}$$

where $v_k \in \mathbb{F}_{q^{mNk}}$ such that $\Psi_k(v_k) = u_k \in \mathbb{F}_{q^{mNk}}$ and the numbers t, s are defined for sufficiently large k, using Lemma 3.1.6, as follows:

$$l = q^n, d = \deg(f), M = q^{mNk} \ for \ sufficiently \ large \ k$$

By Lemma 3.1.6, s and t are squarefree relatively prime integers such that a prime number r divides $M-1$ if and only if $r \mid st$. Note that $\deg(f(\alpha_k^t x^s)) = ds$. Since $p = char(\mathbb{F}_q) \nmid q^{mNk} - 1 = M - 1$, $p \nmid s$. Therefore, $(q, ds) = 1$ and E_k/L_k is an Artin-Schreier extension by Lemma 3.1.5. Hence we have $g(E_k) = \frac{(q^n-1)(ds-1)}{2}$, which provides us with a lower bound on the number of degree one places N_k of E_k/L_k via Hasse-Weil bound (cf. Theorem 1.3.8):

$$N_k \geq q^{mNk} + 1 - (q^n - 1)(ds - 1)q^{\frac{mNk}{2}}. \tag{3.9}$$

Let $\lambda_k = \{\alpha_k^t \beta^s : primitive \ in \ L_k; \beta \in L_k - \{0\}\}$. We will determine the cardinality of the set λ_k. Any $\beta \in L_k - \{0\}$ can be written as $\beta = \alpha_k^a$, where $a \in \{1, 2, \ldots, q^{mNk} - 1\}$, since $\alpha_k \in L_k$ is a primitive element. The element $\alpha_k^t \beta^s = \alpha_k^{t+as}$ is primitive in L_k if and only if $(t+as, |L_k - \{0\}|) = (t+as, q^{mNk}-1) = (t + as, M - 1) = 1$. Let us count the number of primes dividing $t + as$ and $M - 1$. Let r be a prime dividing both numbers. Then $r \mid st$ by Lemma 3.1.6. Since s and t are relatively prime by construction, there are two possibilities: Either $r \mid s$ or $r \mid t$. If we assume $r \mid s$, then $r \mid t$ as well since $r \mid (t + as, M - 1)$. This is impossible. Therefore, r must divide t. This implies, again using $r \mid (t + as, M - 1)$ and $(s, t) = 1$, that $r \mid a$. These arguments lead to the following conclusion:

$$(t + as, M - 1) = 1 \Longleftrightarrow (t, a) = 1$$

Therefore, we must count the integers $a \in \{1, 2, \ldots, q^{mNk} - 1\}$ such $(t, a) = 1$ in order to determine $|\lambda_k|$. The number t satisfies $1 \leq t \leq q^{mNk} - 1$ and, by Lemma 3.1.6 (ii), $t \mid q^{mNk} - 1$. Divide the interval of a-values $\{1, 2, \ldots, q^{mNk} - 1\}$ into $\frac{q^{mNk}-1}{t}$ subintervals of length t each. In the first subinterval $\{1, 2, \ldots, t\}$, there exists $\varphi(t)$ a values with $(t, a) = 1$. The second subinterval consists of the numbers $\{t + 1, t + 2, \ldots, 2t\}$. A number $a = t + i$ in this subinterval is relatively prime to t

if and only if $(i,t)=1$. There are, again, $\varphi(t)$ such i values. Continuing this way, we conclude that there are $\varphi(t)\frac{q^{mNk}-1}{t}$ a values in $\{1,2,\ldots,q^{mNk}-1\}$ such that $(a,t)=1$. Therefore

$$|\lambda_k| = \frac{\varphi(t)(q^{mNk}-1)}{t}\,.$$

At this point, observe that if there exists $\beta \in L_k$ such that the corresponding degree one place $P_\beta \in \mathbb{P}_{L_k(x)}$ has a degree one extension in E_k with $\alpha_k^t\beta^s \in \lambda_k$, then, by Kummer's Theorem (cf. Theorem 1.3.7), we conclude that there exists $t_0 \in L_k$, $A(t_0) = f(\alpha_k^t\beta^s) - v_k$. Hence, $B_k(A(t_0)) = B_k(f(\alpha_k^t\beta^s)) - B_k(v_k)$, since B_k is an additive polynomial. Note that $B_k(A(t_0)) = 0$ and $\Psi_k(v_k) = B_k(v_k) = u_k$ by definition of B_k, Ψ_k and v_k. Therefore, we reach the result

there exists $\alpha_k^t\beta^s$: primitive element in $\mathbb{F}_{q^{mNk}}$ such that $B_k(f(\alpha_k^t\beta^s)) = u_k$.

Motivated by the argument in the last paragraph, assume that there exists no degree one place $P_\beta \in \mathbb{P}_{L_k(x)}$ with a degree one extension in E_k such that $\alpha_k^t\beta^s \in \lambda_k$. We want to reach a contradiction to finish the proof.

We know that $A(T) = h(0) - v_k$ has no solution in L_k. Otherwise if $t_0 \in L_k$ is a solution, then $B_k(A(t_0)) = B_k(h(0)) - B_k(v_k)$. We have $B_k(A(t_0)) = 0$ for any $t_0 \in L_k$. Since $h(0) = 0$, then $B_k(v_k) = 0 = u_k$. By assumption, u_k is a nonzero element of $Im\Psi_k$. This is a contradiction. So $A(T) = h(0) - v_k$ has no solution in L_k. In order to write a lower bound for N_k we need Hasse-Weil bound. However, to write an upper bound for N_k we will rather use the arguments above. Let $S = \{\beta \in L_k : \alpha_k^t\beta^s \in \lambda_k\}$. Note that $|S| \geq |\lambda_k|$ since for distinct $\beta_1, \beta_2 \in L_k$ one might have $\alpha_k^t\beta_1^s = \alpha_k^t\beta_2^s$. Hence, under the assumption made above, at most $q^{mNk} - 1 - |S|$ elements in L_k might have a corresponding degree one place in $\mathbb{P}_{L(x)}$ with a degree one extension in $\mathbb{P}_{E_k}$. By Lemma 3.1.5, each such a place has q^n distinct degree one places in $\mathbb{P}_{E_k}$. Knowing degree one places of E_k must lie over degree one places of L_k, we get

$$N_k \leq 1 + q^n(q^{mNk} - 1 - |\lambda_k|) = 1 + q^n\left(q^{mNk} - 1 - \frac{\varphi(t)(q^{mNk}-1)}{t}\right),$$

where $+1$ in the above upper bound comes from the fact that the place at infinity of $L_k(x)$ is totally ramified (cf. Lemma 3.1.5). Combining lower and upper bounds

for N_k yields

$$q^{mNk} - (q^n - 1)(ds - 1)q^{\frac{mNk}{2}} \leq q^n\left(q^{mNk} - 1 - \frac{\varphi(t)(q^{mNk} - 1)}{t}\right).$$

This implies, after a simple manipulation, that

$$\frac{\varphi(t)}{t} \leq 1 - \frac{q^{mNk-n}}{q^{mNk} - 1} + (ds - 1)\left(1 - \frac{1}{q^n}\right)\frac{q^{\frac{mNk}{2}}}{q^{mNk} - 1}.$$

Since $\frac{1}{q^n} \leq \frac{q^{mNk-n}}{q^{mNk}-1}$, $1 - \frac{q^{mNk-1}}{q^{mNk}-1} \leq \frac{q^n-1}{q^n}$ and we get

$$1 - \frac{q^{mNk-n}}{q^{mNk} - 1} < \frac{q^n - 1}{q^n}\left(1 + \frac{2}{q^{mNk} - 1}\right).$$

From the last two inequalities we get

$$\frac{\varphi(t)}{t} < \frac{q^n - 1}{q^n}\left(1 + (ds - 1)\frac{q^{\frac{mNk}{2}}}{q^{mNk} - 1} + \frac{2}{q^{mNk} - 1}\right).$$

The inequality above yields a contradiction to Lemma 3.1.6 (iii), where one replaces l by q^n and M by q^{mNk}. Hence, we are done.

□

Remark 3.2.2 Let $A(T) = T^q - T$ and $f(T) = T$. Then $A(T)$ splits over $\mathbb{F}_q$. Note that $B_k(T) \in \mathbb{F}_{q^k}[T]$ of degree q^{k-1}. $B_k(\alpha) = 0$ if and only if $\alpha = \gamma^q - \gamma$ for some $\alpha \in \mathbb{F}_{q^k}$ by Hilbert's Theorem 90 (cf. Theorem 1.1.1). Consider the polynomial $Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(T) = T + T^q + \ldots + T^{q^{k-1}}$ of degree q^{k-1}. For a root α of $B_k(T)$, we have

$$\begin{aligned} Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) &= (\gamma^q - \gamma) + (\gamma^q - \gamma)^q + \ldots + (\gamma^q - \gamma)^{q^{k-1}} \\ &= \gamma^q - \gamma + \gamma^{q^2} - \gamma^q + \ldots + \gamma^{q^k} - \gamma^{q^{k-1}} \\ &= \gamma^{q^k} - \gamma = 0 \end{aligned}$$

where the last step follows from the fact that $\gamma \in \mathbb{F}_{q^k}$. Hence, roots of $B_k(T)$ and $Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(T)$ are the same. Since these are polynomials over the same field and of the same degree, we conclude that $B_k(T) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(T)$. Note that $Im(\Psi_k) = \{B_k(\alpha) \colon \alpha \in \mathbb{F}_{q^k}\} = \mathbb{F}_q$ since trace map is onto. Therefore $B_k(w_k) = Tr_{\mathbb{F}_{q^k}/\mathbb{F}_q}(w_k) = u_k$. This shows how Theorem 3.2.7 "specializes" to Theorem 2.1.1.

CHAPTER 4

CONCLUSION AND FURTHER RESEARCH

In this thesis we have given two proofs of the existence of primitive elements in finite fields with arbitrary trace (or equivalently, existence of primitive polynomials whose first coefficient is prescribed). The first proof is due to Cohen and the main tool is character sums. The second is a work of Özbudak who uses algebraic function fields to prove a more general statement.

Since Cohen solved the above problem in all cases in 1990, variants of the problem have been introduced and worked on. The common goal of these later works is to impose more conditions on primitive elements (or primitive polynomials) and still prove existence results. Some of these new problems, which in turn motivate further research, are:

- In addition to the trace, also prescribe the norm of the primitive element. We refer to [8] for research in this direction.

- Cohen-Hachenberger ([5]) proved the existence of a primitive element w in $\mathbb{F}_{q^n}$ which generate a normal basis $\{w, w^q, \ldots, w^{q^{n-1}}\}$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and which has a prescribed nonzero trace value in $\mathbb{F}_q$. Note that having a nonzero trace is not an assumption but necessity since a zero trace for w would imply a zero trace for all elements of $\mathbb{F}_{q^n}$, which is impossible.

- The works of Han ([7]) and Cohen-Mills ([4]) study the existence of primitive polynomials over $\mathbb{F}_q$ of degree n for which the coefficients of the terms x^{n-1}

and x^{n-2} are prescribed. Obviously, this problem can be extended to cover more coefficients with specified values.

The above list can be extended with similar problems all of which arise from the initial problem that is discussed in this thesis. All of these works seem to rely on heavy computational arguments and, usually, the main mathematical tool is character sums. This makes each work quite involved. However, Özbudak's approach was able to simplify the proof, and even obtain a result in more general setting, in the case of primitive elements with specified trace. Therefore, attacking these kinds of problems with techniques brought from algebraic function fields, or other branches of mathematics, with or without the use of character sums would be very interesting. Especially, if such approaches prove to be as simplifying as Özbudak's work they would be quite useful.

Bibliography

[1] Cohen, S. D., *Primitive roots in the quadratic extension of a finite field*, Journal of London Mathematical Society **27** (1983), 221–228.

[2] Cohen, S. D., *Generators in cyclic difference sets*, Journal of Combanatorial Theory Series A **51** (1989), 227–236.

[3] Cohen, S. D., *Primitive elements and polynomials with arbitrary trace*, Discrete Mathematics **83** (1990), 1–7.

[4] Cohen, S.D. and Mills, D., *Primitive polynomials with first and second coefficients prescribed*, Finite Fields and Their Applications **9** (2003), 334–350.

[5] Cohen, S.D. and Hachenberger, D., *Primitive normal bases with prescribed trace*, Applicable Algebra in Engineering, Communication and Computing **9** (1999), 383–403.

[6] Goss, D., *Basic Structures of Function Field Arithmetic*, Springer-Verlag, 1996.

[7] Han, W.B., *Coefficients of primitive polynomials over finite fields*, Mathematics of Computation **65** (1996), 331–340.

[8] Huczynska, S. and Cohen, S.D., *Primitive free cubics with specified norm and trace*, Transactions of American Mathematical Society **355** (2003), 3099–3116.

[9] Jungnickel, D., *Finite Fields : Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[10] Jungnickel, D. and Vanstone, S. A., *On primitive polynomials over finite fields*, Journal of Algebra **124** (1989), 337–353.

[11] Lenstra, H.W. and Schoof, R.J., *Primitive normal bases for finite fields*, Mathematics of Computation **48** (1987), 217–231.

[12] Lidl, R. and Niederreiter, H., *Finite Fields,* Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, 1983.

[13] MacWilliams, F.J. and Sloane, N.J.A., *The theory of error-correcting codes*, North-Holland, 1998.

[14] Madden, D. J., *Polynomials and primitive roots in finite fields*, Journal of Number Theory **13** (1981), 499–514.

[15] Moreno, O., *On primitive elements of trace equal to 1 in* $GF(2^m)$, Discrete Mathematics **41** (1982), 53–56.

[16] Özbudak, F., *Additive Polynomials and Primitive Roots ove Finite Fields*, Communications in Algebra **29** (2001), 987–991.

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

Bibliography

[1] Cohen, S. D., *Primitive roots in the quadratic extension of a finite field*, Journal of London Mathematical Society **27** (1983), 221–228.

[2] Cohen, S. D., *Generators in cyclic difference sets*, Journal of Combanatorial Theory Series A **51** (1989), 227–236.

[3] Cohen, S. D., *Primitive elements and polynomials with arbitrary trace*, Discrete Mathematics **83** (1990), 1–7.

[4] Cohen, S.D. and Mills, D., *Primitive polynomials with first and second coefficients prescribed*, Finite Fields and Their Applications **9** (2003), 334–350.

[5] Cohen, S.D. and Hachenberger, D., *Primitive normal bases with prescribed trace*, Applicable Algebra in Engineering, Communication and Computing **9** (1999), 383–403.

[6] Goss, D., *Basic Structures of Function Field Arithmetic*, Springer-Verlag, 1996.

[7] Han, W.B., *Coefficients of primitive polynomials over finite fields*, Mathematics of Computation **65** (1996), 331–340.

[8] Huczynska, S. and Cohen, S.D., *Primitive free cubics with specified norm and trace*, Transactions of American Mathematical Society **355** (2003), 3099–3116.

[9] Jungnickel, D., *Finite Fields : Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[10] Jungnickel, D. and Vanstone, S. A., *On primitive polynomials over finite fields*, Journal of Algebra **124** (1989), 337–353.

[11] Lenstra, H.W. and Schoof, R.J., *Primitive normal bases for finite fields*, Mathematics of Computation **48** (1987), 217–231.

[12] Lidl, R. and Niederreiter, H., *Finite Fields,* Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, 1983.

[13] MacWilliams, F.J. and Sloane, N.J.A., *The theory of error-correcting codes*, North-Holland, 1998.

[14] Madden, D. J., *Polynomials and primitive roots in finite fields*, Journal of Number Theory **13** (1981), 499–514.

[15] Moreno, O., *On primitive elements of trace equal to 1 in* $GF(2^m)$, Discrete Mathematics **41** (1982), 53–56.

[16] Özbudak, F., *Additive Polynomials and Primitive Roots ove Finite Fields*, Communications in Algebra **29** (2001), 987–991.

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