KUMMER EXTENSIONS OF FUNCTION FIELDS WITH MANY RATIONAL PLACES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BURCU GÜLMEZ TEMUR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

JULY 2005

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan ÖZGEN
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Şafak ALPAY
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Prof.Dr. Mehpare BİLHAN Co-Supervisor	Assoc. Prof.Dr. Ferruh ÖZBUDAK Supervisor

Examining Committee Members

Prof. Dr. Halil İbrahim KARAKAŞ	(BAŞKENT UNIV.)	
Assoc. Prof. Dr. Ferruh ÖZBUDAK	(METU, MATH)	
Prof. Dr. Ersan AKYILDIZ	(METU, MATH)	
Assoc. Prof. Dr. Yıldıray OZAN	(METU, MATH)	
Assist.Prof. Dr. Feza ARSLAN	(METU, MATH)	

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Burcu Gülmez Temur
Signature :

ABSTRACT

KUMMER EXTENSIONS OF FUNCTION FIELDS WITH MANY RATIONAL PLACES

GÜLMEZ TEMUR, Burcu
Ph.D., Department of Mathematics
Supervisor: Assoc. Prof. Dr. Ferruh ÖZBUDAK
Co-Supervisor: Prof. Dr. Mehpare BİLHAN

July 2005, 33 pages

In this thesis, we give two simple and effective methods for constructing Kummer extensions of algebraic function fields over finite fields with many rational places. Some explicit examples are obtained after a practical search. We also study fibre products of Kummer extensions over a finite field and determine the exact number of rational places. We obtain explicit examples with many rational places by a practical search. We have a record (i.e the lower bound is improved) and a new entry for the table of van der Geer and van der Vlugt.

Keywords: Function Fields, Kummer Extensions, Rational Places

ÖZ

FONKSİYON CİSİMLERİNİN RASYONEL ASAL BÖLENİ ÇOK OLAN KUMMER GENİŞLEMELERİ

GÜLMEZ TEMUR, Burcu
Doktora, Matematik Bölümü
Tez Yöneticisi: Doç. Dr. Ferruh ÖZBUDAK
Ortak Tez Yöneticisi: Prof. Dr. Mehpare BİLHAN

Temmuz 2005, 33 sayfa

Bu tezde, sonlu cisimler üzerinde tanımlanmış cebirsel fonksiyon cisimlerinin rasyonel asal böleni çok olan Kummer genişlemelerinin inşası için basit ve etkili iki metot veriyoruz. Pratik bir araştırma sonucunda bazı açık örnekler elde ettik. Ayrıca, sonlu bir cisim üzerinde Kummer genişlemelerinin lif çarpımlarını çalıştık ve rasyonel asal bölenlerinin kesin sayısını belirledik. Pratik bir araştırmayla rasyonel asal böleni çok olan açık örnekler elde ettik. Van der Geer ve van der Vlugt'un tablosu için bir rekor (alt sınır iyileştirildi) ve yeni bir kayıt elde ettik.

Anahtar Kelimeler: Fonksiyon Cisimleri, Kummer Genişlemeleri, Rasyonel Asal Bölenler

To my husband,
Haydar Temur

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor, Assoc. Prof. Dr. Ferruh Özbudak for his encouragement, attentive insight throughout the research and constant guidance during this work.

I would also like to express my sincere appreciation to my co-supervisor, Prof. Dr. Mehpare Bilhan for her guidance, continuous support and motivation throughout my education at Middle East Technical University.

I offer thanks to Assoc. Prof. Dr. Tuncay Başkaya for his tolerance and support.

I want to thank Ümit Akın Aksoy, Celalettin Kaya, Erol Serbest, Abdullah Özbekler and Gülay Karadoğan for their friendship.

I offer thanks to my family for their love and moral support.

Finally, I want to express my deepest love and appreciation to my husband, Haydar Temur for his patience, encouragement and love all through the way.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION AND PRELIMINARIES

1.1 Introduction

Let F be an algebraic function field defined over a finite field $\mathbb{F}_q$ with q elements. Let $N(F)$ denote the number of rational places of F and $g(F)$ denote the genus of F. The Hasse-Weil bound implies that

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

It was improved later by J. P. Serre substituting $2\sqrt{q}$ by its integer part $[2\sqrt{q}]$. If q is a square then the function field F over $\mathbb{F}_q$ is called maximal if $N(F) = q + 1 + 2g(F)\sqrt{q}$.

The number of rational places of a function field F of genus g over $\mathbb{F}_q$ have attracted pure mathematicians for many years. But after Goppa's construction of algebraic-geometric codes in 1980, see [3], the interest in the area was greatly renovated. The books of Stepanov [7] and Tsfasman and Vladut [9] are devoted to algebraic-geometric codes. There are also many important applications for function fields over finite fields in cryptography and related areas. The book of Niederreiter and Xing [5] not only gives the applications to coding theory but also cyrptography and low-discrepancy sequences.

There are many books written on function fields but there is an excellent reference, the book of Stichtenoth [8], which gives a detailed and self-contained interpretation of the theory of algebraic function fields.

In recent years, many mathematicians searched for function fields over finite fields with many rational points. In [2], van der Geer and van der Vlugt constructed a table of results for $0 \leq g(F) \leq 50$ and q a small power of 2 or 3. There are good examples of explicitly defined algebraic function fields with many rational places in [1], [4], [6] which are constructed by Kummer extensions.

In this thesis, we concentrate on a Kummer extension of the rational function field $\mathbb{F}_q(x)$, which can be expressed as $y^m = f(x) \in \mathbb{F}_q(x)[y]$ where m is a divisor of $q-1$.

In Chapter 2, we will give two methods for constructing Kummer extensions of algebraic function fields with many rational places. Some explicitly defined examples with many rational points found by the given methods will also be presented in details.

In Chapter 3, we shall study fibre products of Kummer extensions over a finite field. In Section 1, the exact number of rational places is determined, in Section 2 there are good examples of fibre products of Kummer extensions with many rational places. Example 3.2.1 is a record (i.e the lower bound is improved) and Example 3.2.13 is a new entry in the table [2] of van der Geer and van der Vlugt.

1.2 Preliminaries

In this section we will introduce some basic definitions and fundamental properties of algebraic function fields that will be used in the following chapters. We will follow the book of Stichtenoth [8]. Throughout the section k denotes an arbitrary field.

1.2.1 Algebraic Function Fields and Valuations

Definition 1.2.1. *A finite algebraic extension F of $k(x)$ for some element $x \in F$ is called an algebraic function field of one variable over k, if x is transcendental over k. Moreover, k is called the full constant field of F if every element of F that is algebraic over k is in k.*

Definition 1.2.2. *A discrete valuation of F/k is a surjective map*

$$v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$$

satisfying the following:

(i) $v(x) = \infty$ *iff* $x = 0$.

(ii) $v(xy) = v(x) + v(y)$ *for all* $x, y \in F$.

(iii) $v(x + y) \geq min\{v(x), v(y)\}$ *for all* $x, y \in F$.

(iv) $v(u) = 0$ *for any* $0 \neq u \in k$.

Definition 1.2.3. *(a) A subring $\mathcal{O}$ such that $k \subset \mathcal{O} \subset F$ is called a valuation ring of the function field F/k if for any $z \in F$, either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. $\mathcal{O}$ is a local ring.*
(b) A place P is the maximal ideal of some valuation ring $\mathcal{O}$ of F/k.
(c) $F_P = \mathcal{O}/P$ is called the residue class field of P.
(d) $\deg P = [F_P : k]$ is called the degree of P. Moreover, a place of degree one is called rational.

Let P be a place of F and $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ be the discrete valuation corresponding to the place P in F. Then its valuation ring is

$$\mathcal{O}_P = \{x \in F : v_P(x) \geq 0\}$$

and its maximal ideal is

$$P = \{x \in F : v_P(x) > 0\}.$$

Definition 1.2.4. *Let $x \in F$. P is called a zero of x if $v_P(x) > 0$ and a pole of x if $v_P(x) < 0$.*

1.2.2 The Rational Function Field

An algebraic function field F/k is called rational if $F = k(x)$ where x is transcendental over k. Let $p(x) \in k[x]$ be an arbitrary monic, irreducible polynomial. Then we can uniquely determine a discrete valuation v_P of F by defining:

$$v_P(r(x)) = n \ \text{ if } \ r(x) = p(x)^n \frac{f(x)}{g(x)} \in k(x) \backslash \{0\}$$

where $f(x), g(x) \in k[x]$ with $p(x) \nmid f(x)$, $p(x) \nmid g(x)$ and $n \in \mathbb{Z}$. Then

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ p(x) \nmid g(x) \right\}$$

is a valuation ring of $k(x)/k$ with maximal ideal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ p(x)|f(x),\ p(x) \nmid g(x) \right\}. \tag{1.1}$$

Thus $p(x)$ produces a place $P_{p(x)}$ for $k(x)/k$. There is another uniquely determined discrete valuation v_{P_∞} of F which is defined as:

$$v_{P_\infty}\left(\frac{f(x)}{g(x)}\right) = \deg g(x) - \deg f(x)$$

where $f(x), g(x) \in k[x]$. Then

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ \deg f(x) \leq \deg g(x) \right\}$$

is a valuation ring of $k(x)/k$ with maximal ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in k[x],\ \deg f(x) < \deg g(x) \right\}. \tag{1.2}$$

P_∞ is called the infinite place of $k(x)$.

Theorem 1.2.5. *[8, p. 10] There are no places of the rational function field $k[x]/k$ other than the places $P_{p(x)}$ and P_∞, defined by (1.1) and (1.2).*

Proposition 1.2.6. *[8, p.9]*
(a) Let $P = P_{p(x)}$ be the place defined by (1.1), where $p(x) \in k[x]$ is an irreducible polynomial. The residue class field $k(x)_P = \mathcal{O}_P/P$ is isomorphic to $k[x]/(p(x))$. Consequently, $\deg P = \deg p(x)$*. In the special case $p(x) = x-u$ with $u \in k$, we write $P_u = P_{x-u}$ and deg $P_u = 1$.*
(b) Let $P = P_\infty$ be the infinite place of $k[x]/k$ defined by (1.2). Then $\deg P_\infty = 1$*.*

1.2.3 Algebraic Extensions of Function Fields

Let F/k be an algebraic function field of one variable with full constant field k.

Definition 1.2.7. *If $F^{'} \supseteq F$ is an algebraic field extension and $k' \supseteq k$ then $F^{'}/k^{'}$ is called an algebraic extension of F/k.*

Definition 1.2.8. *Let $F^{'}/k^{'}$ be an algebraic extension of F/k. Let $P^{'}$ be a place of $F^{'}/k^{'}$ and P a place of F/k. $P^{'}$ lies over P if $P \subseteq P^{'}$.*

Proposition 1.2.9. *[8, p.60] If $P^{'}$ lies over P, then there exists an integer $e \geq 1$ with $v_{P'}(x) = e.v_P(x)$ for all $x \in F$.*

Definition 1.2.10. *(a) The integer e in Proposition 1.2.9 is called the ramification index of $P^{'}$ over P. It is denoted by $e(P^{'}|P)$. $P^{'}$ is said to be ramified if $e > 1$, unramified if $e = 1$.*
(b) Let $F^{'}_{P^{'}}$ and F_P be the residue class fields of $P^{'}$ and P respectively. The extension degree $[F^{'}_{P^{'}} : F_P]$ is called the relative degree of $P^{'}$ over P, denoted by $f(P^{'}|P)$.

Theorem 1.2.11. *[8, p.64] Let $F^{'}/k^{'}$ be a finite extension of F/k, P a place of F/k and $P_1, ..., P_m$ all the places of $F^{'}/k^{'}$ lying over P. Then*

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

Theorem 1.2.12. *[5, p.15] Suppose that $F^{'}/F$ is a finite Galois extension. Let P a place of F/k and $P_1, ..., P_m$ all the places of $F^{'}/k^{'}$ lying over P. Then for $1 \leq i, j \leq m$ we have*

$$e(P_i|P) = e(P_j|P), \;\; f(P_i|P) = f(P_j|P).$$

CHAPTER 2

SOME KUMMER EXTENSIONS WITH MANY RATIONAL PLACES

In this chapter we will present two methods for the construction of Kummer extensions with many rational places and we will give some explicit examples.

2.1 First Method

Let $f(x)$ and $l(x)$ be two polynomials in $\mathbb{F}_q[x]$ and m be a divisor of $(q-1)$ such that $\deg f(x)^m \geq \deg l(x)$. By the Euclidean division of $f(x)^m$ by $l(x)$ we get

$$f(x)^m = h(x).l(x) + r(x)$$

for some polynomials $h(x), r(x) \in \mathbb{F}_q[x]$ with $\deg r(x) < \deg l(x)$. We assume that $f(x)^m$ is not a multiple of $l(x)$, i.e. $r(x) \neq 0$.
Let $F = \mathbb{F}_q(x, y)$ be the algebraic function field defined by

$$y^m = r(x) \quad , \quad \text{with } \ m \ \text{ a divisor of } (q-1). \tag{2.1}$$

Let $u \in \mathbb{F}_q$ and $P_u = P_{x-u}$ be the rational place of $\mathbb{F}_q(x)$ corresponding to the zero of $x - u$. Let m_u be an integer. Then we can write (2.1) as

$$y^m = (x-u)^{m_u} k(x), \tag{2.2}$$

or equivalently

$$\left(\frac{y^{m/d_u}}{(x-u)^{m_u/d_u}} \right)^{d_u} = k(x)$$

where $k(x) \in \mathbb{F}_q[x]$ with $k(u) \neq 0$ and $d_u = \gcd(m, m_u)$.

Theorem 2.1.1. *There exist either no or exactly d_u rational places of F over P_u. There exists a place of F over P_u if and only if $k(u)$ is a d_u-power in $\mathbb{F}_q$.*

Proof. By [8, Proposition III.7.3], the ramification index of a place lying over P_u is

$$e_u = \frac{m}{\gcd(m, v_{P_u}(r(x)))} = \frac{m}{\gcd(m, m_u)} = \frac{m}{d_u}.$$

Let $P_1, P_2, ..., P_r$ be the rational places of F lying over P_u. By Theorem 1.2.12, we know that the relative degrees, say f_u, of $P_1, P_2, ..., P_r$ are the same and $r.e_u.f_u = m$. Since $\deg P_i = 1$ for all $i = 1, ..., r$; the residue class field of each P_i is $\mathbb{F}_q$. Therefore $f_u = 1$. Then we get

$$r.e_u.f_u = r.\frac{m}{d_u}.1 = m.$$

This implies that $r = d_u = \gcd(m, m_u)$. So there are either no or exactly d_u rational places lying over P_u.
For the second part of the theorem let F_1 be the subfield of F given by

$$F_1 = \mathbb{F}_q(x, y_0), \quad y_0^{d_u} = r(x),$$

or equivalently

$$\left(\frac{y_0}{(x-u)^{m_u/d_u}}\right)^{d_u} = k(x). \tag{2.3}$$

As $\gcd(d_u, v_{P_u}(k(x)) = d_u$, P_u is unramified in $F_1/\mathbb{F}_q(x)$. So there exists a rational place of F_1 over P_u if and only if $k(u)$ is a d_u-power in $\mathbb{F}_q$. Assume that $k(u)$ is a d_u power in $\mathbb{F}_q$. Let $P_u^{'}$ be a place of F_1 over P_u. We have

$$v_{P_u^{'}}(x-u) = 1, \quad v_{P_u^{'}}(y_0) = \frac{m_u}{d_u}$$

Let F_2 be the intermediate field with $F_1 \subseteq F_2 \subseteq F$ given by

$$F_2 = \mathbb{F}_q(x, y_0, y) \quad , \quad y^{m/d_u} = y_0.$$

We observe that $F_2 = F$. Note that $\gcd(\frac{m}{d_u}, v_{P'_u}(y_0)) = \gcd(\frac{m}{d_u}, \frac{m_u}{d_u}) = 1$, since $d_u = \gcd(m, m_u)$ and hence P'_u is totally ramified in F_2/F_1. This completes the proof. □

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. We define $m_\infty = \deg r(x) = -v_{P_\infty}(r(x))$. Let $d_\infty = \gcd(m, m_\infty)$. By [8, Proposition III.7.3], the ramification index of a place lying over P_∞ is

$$e_\infty = \frac{m}{\gcd(m, v_{P_\infty}(r(x)))} = \frac{m}{\gcd(m, m_\infty)} = \frac{m}{d_\infty}.$$

Assume that $r(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_n \in \mathbb{F}_q \setminus \{0\}$.

Theorem 2.1.2. *There exists either no or exactly d_∞ rational places of F over P_∞. There exists a rational place of F over P_∞ if and only if a_n is a d_∞-power in $\mathbb{F}_q$.*

Proof. We write

$$r(x) = x^n(a_n + a_{n-1}\frac{1}{x} + ... + a_1\frac{1}{x^{n-1}} + a_0\frac{1}{x^n}).$$

Let $t = \dfrac{1}{x}$. Then we can write (2.1) as

$$y^m = \frac{a_n + a_{n-1}t + ... + a_1 t^{n-1} + a_0 t^n}{t^n}$$

or equivalently,

$$y^m = t^{-n}(a_n + a_{n-1}t + ... + a_1 t^{n-1} + a_0 t^n).$$

Now we can apply the proof of Theorem 2.1.1 for $t = 0$ and we get the result. □

We will now compute the genus of the function field F. By [8, Proposition III.7.3] we have:

$$g(F) = 1 + m. \left[-1 + \frac{1}{2} \sum_{P} \left(1 - \frac{\gcd(m, v_P(r(x)))}{m} \right) \deg P \right] \qquad (2.4)$$

where P runs through all places of $\mathbb{F}_q(x)$.

We know by Theorem 1.2.5 that the only places of the rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$ are $P_{p(x)}$ and P_∞, where $p(x) \in \mathbb{F}_q[x]$ is an irreducible polynomial and $\deg P_{p(x)} = deg\, p(x)$, $\deg P_\infty = 1$ by Proposition 1.2.6.

If $p(x) \in \mathbb{F}_q[x]$ does not divide $r(x)$, then $v_P(r(x)) = 0$, which implies that $\gcd(m, v_P(r(x))) = m$. This means the sum over P is a finite sum over only the zeros and poles of $r(x)$.

2.2 Examples Based on Section 1

Example 2.2.1. *This is an example of a function field $F = \mathbb{F}_8(x, y)$ given by*

$$y^7 = x(x+1)(x^2+x+1)^2$$

with $g(F) = 9$ and $N(F) = 45$. This is the best value known in [2].

Proof. Taking $f(x) = x^2 + x$, $l(x) = x^8 - x$ and $m = 7$, by the Euclidean division of $f(x)^m$ by $l(x)$, we get

$$r(x) = x(x+1)(x^2+x+1)^2.$$

Let $p_1(x) = x$, $p_2(x) = x + 1$, $p_3(x) = x^2 + x + 1$ and P_1, P_2, P_3 be the corresponding places of $\mathbb{F}_8(x)$ where $\deg P_1 = \deg P_2 = 1$ and $\deg P_3 = 2$. We have $v_{P_i}(r(x)) = 1$ for $i = 1, 2$ and $v_{P_3}(r(x)) = 2$. Then

$$\gcd(m, v_{P_i}(r(x))) = \gcd(7, 1) = 1 \text{ for } i = 1, 2$$

and $\gcd(m, v_{P_3}(r(x))) = \gcd(7,2) = 1$. For P_∞, $\gcd(m, m_\infty) = gcd(7,6) = 1$, where $m_\infty = \deg r(x) = 6$.
Thus $g(F)$ can be computed using (2.4) as follows:

$$g(F) = 1 + 7\left[-1 + \frac{1}{2}\sum_{i=1}^{3}\left(1 - \frac{1}{7}\right) + \frac{1}{2}\left(1 - \frac{1}{7}\right)2\right] = 9$$

We observe that P_1, P_2 and P_∞ are the only rational places of $\mathbb{F}_8(x)$ which are zeros and poles of $r(x)$. There exists one place lying over P_1 and also one place lying over P_2. Both of them are rational places of $F/\mathbb{F}_8(x)$. There is one place of $F/\mathbb{F}_8(x)$ lying over P_∞ which is rational. We have computed the number of rational places which are neither zeros nor poles of $r(x)$ by a computer search. This gives 42 extra rational places. Adding all these rational places we get $N(F) = 45$. □

Example 2.2.2. *This is an example of a function field $F = \mathbb{F}_{16}(x,y)$ given by*

$$y^5 = x^2(x+w^4)^2(x+w^9)^2(x+w^{14})^2$$

where $w^4 + w + 1 = 0$, with $g(F) = 6$ and $N(F) = 65$. This is a maximal function field.

Proof. Taking $f(x) = x^4 + w^{12}x$, $\quad l(x) = x^{16} - x$ and $m = 5$, by the Euclidean division of $f(x)^m$ by $l(x)$ we get

$$r(x) = x^2(x+w^4)^2(x+w^9)^2(x+w^{14})^2.$$

Let $p_1(x) = x$, $p_2(x) = x+w^4$, $p_3(x) = x+w^9$, $p_4(x) = x+w^{14}$ and P_1, P_2, P_3, P_4 be the corresponding places of $\mathbb{F}_{16}(x)$ where $\deg P_i = 1$ for $i = 1,2,3,4$. We have $v_{P_i}(r(x)) = 2$ for $i = 1,2,3,4$. Then

$$\gcd(m, v_{P_i}(r(x))) = \gcd(5,2) = 1 \text{ for } i = 1,2,3,4.$$

For P_∞, $d_\infty = \gcd(m, m_\infty) = gcd(5, 8) = 1$, where $m_\infty = \deg r(x) = 8$. Thus $g(F)$ can be computed using (2.4) as follows:

$$g(F) = 1 + 5\left[-1 + \frac{1}{2}\sum_{i=1}^{5}\left(1 - \frac{1}{5}\right)\right] = 6$$

We observe that P_1, P_2, P_3, P_4 and P_∞ are the only rational places of $\mathbb{F}_{16}(x)$ which are zeros and poles of $r(x)$. Each P_i has only one extension in F for $i = 1, 2, 3, 4$ and they are all rational over $\mathbb{F}_{16}$. There is one place of $F/\mathbb{F}_{16}(x)$ lying over P_∞ which is rational. We have computed the number of rational places which are neither zeros nor poles of $r(x)$ by a computer search. This gives 60 extra rational places. Adding all these rational places we get $N(F) = 65$. $\square$

Example 2.2.3. *This is an example of a function field $F = \mathbb{F}_{16}(x, y)$ given by*

$$y^{15} = (x + w^8)(x + w^{13})(x^3 + w^8x^2 + w^{11}x + w^{14})^2(x^3 + w^{13}x^2 + wx + w^4)^2$$

where $w^4 + w + 1 = 0$, with $g(F) = 49$ and $N(F) = 213$. This is the best value known in [2].

Proof. Taking $f(x) = x^4 + w^9x^2 + w^8x + 1$, $l(x) = x^{16} - x$ and $m = 15$, by the Euclidean division of $f(x)^m$ by $l(x)$ we get

$$r(x) = (x + w^8)(x + w^{13})(x^3 + w^8x^2 + w^{11}x + w^{14})^2(x^3 + w^{13}x^2 + wx + w^4)^2.$$

Let $p_1(x) = x + w^8$, $p_2(x) = x + w^{13}$, $p_3(x) = x^3 + w^8x^2 + w^{11}x + w^{14}$, $p_4(x) = x^3 + w^{13}x^2 + wx + w^4$ and P_1, P_2, P_3, P_4 be the corresponding places of $\mathbb{F}_{16}(x)$ where $\deg P_i = 1$ for $i = 1, 2$ and $\deg P_i = 3$ for $i = 3, 4$. We have $v_{P_i}(r(x)) = 1$ for $i = 1, 2$ and $v_{P_i}(r(x)) = 2$ for $i = 3, 4$. Then

$$\gcd(m, v_{P_i}(r(x))) = \gcd(15, 1) = 1 \text{ for } i = 1, 2$$

and

$$\gcd(m, v_{P_i}(r(x))) = \gcd(15, 2) = 1 \text{ for } i = 3, 4$$

For P_∞, $d_\infty = \gcd(m, m_\infty) = \gcd(15, 14) = 1$, where $m_\infty = \deg r(x) = 14$. Thus $g(F)$ can be computed using (2.4) as follows:

$$g(F) \;=\; 1 + 15\left[-1 + \frac{1}{2}\sum_{i=1}^{3}\left(1 - \frac{1}{15}\right) + \frac{1}{2}\sum_{i=1}^{2}\left(1 - \frac{1}{15}\right)3\right] = 49$$

We observe that P_1, P_2 and P_∞ are the only rational places of $\mathbb{F}_{16}(x)$ which are zeros and poles of $r(x)$. Each P_i has only one extension in F for $i = 1, 2$ and both of them are rational over $\mathbb{F}_{16}$. There is one place of $F/\mathbb{F}_{16}(x)$ lying over P_∞ which is rational. We have computed the number of rational places which are neither zeros nor poles of $r(x)$ by a computer search. This gives 210 extra rational places. Adding all these rational places we get $N(F) = 213$. $\square$

Example 2.2.4. *This is an example of a function field $F = \mathbb{F}_9(x, y)$ given by*

$$y^8 = 2(x + w^3)(x + w^5)^5$$

where $w^2 + 2w + 2 = 0$, with $g(F) = 3$ and $N(F) = 28$. This is a maximal function field.

Proof. Taking $f(x) = x^3 + 2x^2 + w^3x + w^3$, $l(x) = 2x^9 + 2x^3$ and $m = 8$, by the Euclidean division of $f(x)^m$ by $l(x)$ we get

$$r(x) = 2(x + w^3)(x + w^5)^5.$$

Let $p_1(x) = x + w^3$, $p_2(x) = x + w^5$ and P_1, P_2 be the corresponding places of $\mathbb{F}_9(x)$ where $\deg P_i = 1$ for $i = 1, 2$. We have $v_{P_1}(r(x)) = 1$ and $v_{P_2}(r(x)) = 5$. Then

$$\gcd(m, v_{P_1}(r(x))) = \gcd(8, 1) = 1 \text{ and } \gcd(m, v_{P_2}(r(x))) = \gcd(8, 5) = 1.$$

For P_∞, $d_\infty = \gcd(m, m_\infty) = \gcd(8, 6) = 2$, where $m_\infty = \deg r(x) = 6$. Thus $g(F)$ can be computed using (2.4) as follows:

$$g(F) = 1 + 8\left[-1 + \frac{1}{2}\sum_{i=1}^{2}\left(1 - \frac{1}{8}\right) + \frac{1}{2}\left(1 - \frac{2}{8}\right)\right] = 3$$

We observe that P_1, P_2 and P_∞ are the only rational places of $\mathbb{F}_9(x)$ which are zeros and poles of $r(x)$. Each P_i has only one extension in F for $i = 1, 2$ and both of them are rational over $\mathbb{F}_9$. There are two places of $F/\mathbb{F}_9(x)$ lying over P_∞ which are rational. We have computed the number of rational places which are neither zeros nor poles of $r(x)$ by a computer search. This gives 24 extra rational places. Adding all these rational places we get $N(F) = 28$. $\square$

Example 2.2.5. *This is an example of a function field $F = \mathbb{F}_9(x, y)$ given by*

$$y^8 = w^2(x + w^6)^2(x^2 + w^2x + w^5)$$

where $w^2 + 2w + 2 = 0$, with $g(F) = 5$ and $N(F) = 32$. This is the best value known in [2].

Proof. Taking

$$f(x) = x^2 + 1 \ \ , \ \ l(x) = \frac{x^9 - x}{x(x+1)(x+w)(x+w^2)}$$

and $m = 8$, by the Euclidean division of $f(x)^m$ by $l(x)$ we get

$$r(x) = w^2(x + w^6)^2(x^2 + w^2x + w^5).$$

Let $p_1(x) = x + w^6$, $p_2(x) = x^2 + w^2x + w^5$ and P_1, P_2 be the corresponding places of $\mathbb{F}_9(x)$ where $\deg P_1 = 1$ and $\deg P_2 = 2$. We have $v_{P_1}(r(x)) = 2$ and $v_{P_2}(r(x)) = 1$. Then

$$\gcd(m, v_{P_1}(r(x))) = \gcd(8, 2) = 2 \ \text{ and } \ \gcd(m, v_{P_2}(r(x))) = \gcd(8, 1) = 1.$$

For P_∞, $\quad d_\infty = \gcd(m, m_\infty) = \gcd(8, 4) = 4$, where $m_\infty = \deg r(x) = 4$. Thus $g(F)$ can be computed using (2.4) as follows:

$$g(F) = 1 + 8\left[-1 + \frac{1}{2}\left(1 - \frac{2}{8}\right) + \frac{1}{2}\left(1 - \frac{1}{8}\right)2 + \frac{1}{2}\left(1 - \frac{4}{8}\right)\right] = 5$$

We observe that P_1 and P_∞ are the only rational places of $\mathbb{F}_9(x)$ which are zeros and poles of $r(x)$. There are no rational places of $F/\mathbb{F}_9(x)$ lying over P_1 and P_∞. We have computed the number of rational places which are neither zeros nor poles of $r(x)$ by a computer search. This gives 32 rational places. We get $N(F) = 32$. $\square$

2.3 Second Method

Let $f(x)$, $l(x)$, $l_1(x)$ be polynomials in $\mathbb{F}_q[x]$, m be a divisor of $(q-1)$ and s be an integer such that $\deg f(x)^{m+s} \geq \deg l(x)$ and $\deg f(x)^s \geq \deg l_1(x)$. By the Euclidean division of $f(x)^{m+s}$ by $l(x)$ we get

$$f(x)^{m+s} = h(x).l(x) + r(x)$$

for some polynomials $h(x), r(x) \in \mathbb{F}_q[x]$ with $\deg r(x) < \deg l(x)$. We assume that $f(x)^{m+s}$ is not a multiple of $l(x)$, i.e. $r(x) \neq 0$. By the Euclidean division of $f(x)^s$ by $l_1(x)$ we get

$$f(x)^s = h_1(x).l_1(x) + r_1(x)$$

for some polynomials $h_1(x), r_1(x) \in \mathbb{F}_q[x]$ with $\deg r_1(x) < \deg l_1(x)$. We assume that $f(x)^s$ is not a multiple of $l_1(x)$, i.e. $r_1(x) \neq 0$.
Let $F = \mathbb{F}_q(x, y)$ be the algebraic function field given by

$$y^m = \frac{r(x)}{r_1(x)} \quad , \quad \text{with } m \text{ a divisor of } (q-1). \tag{2.5}$$

Let $u \in \mathbb{F}_q$ and $P_u = P_{x-u}$ be the rational place of $\mathbb{F}_q(x)$ corresponding to the zero of $x - u$. Let m_u be an integer. Then we can write (2.5) as

$$y^m = (x-u)^{m_u} k(x), \tag{2.6}$$

or equivalently

$$\left(\frac{y^{m/d_u}}{(x-u)^{m_u/d_u}} \right)^{d_u} = k(x),$$

where $k(x) \in \mathbb{F}_q(x)$ with $k(u) \neq 0$, $k(u) \neq \infty$ and $d_u = \gcd(m, m_u)$.

Theorem 2.3.1. *There exist either no or exactly d_u rational places of F over P_u. There exists a place of F over P_u if and only if $k(u)$ is a d_u-power in $\mathbb{F}_q$.*

Proof. The proof of Theorem 2.1.1 can be applied, since in both cases we assume that m_u is an integer. $\square$

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. We define

$$m_\infty = \deg r(x) - \deg r_1(x) = -\, v_{P_\infty}\left(\frac{r(x)}{r_1(x)}\right).$$

Let $d_\infty = \gcd(m, m_\infty)$. By [8, Proposition III.7.3], the ramification index of a place lying over P_∞ is

$$e_\infty = \frac{m}{\gcd(m, v_{P_\infty}(r(x)))} = \frac{m}{\gcd(m, m_\infty)} = \frac{m}{d_\infty}.$$

Assume that $r(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{F}_q[x]$, with $a_n \in \mathbb{F}_q \setminus \{0\}$ and $r_1(x) = b_s x^s + b_{s-1}x^{s-1} + ... + b_1 x + b_0 \in \mathbb{F}_q[x]$, with $b_s \in \mathbb{F}_q \setminus \{0\}$.

Theorem 2.3.2. *There exists either no or exactly d_∞ rational places of F over P_∞. There exists a rational place of F over P_∞ if and only if $\frac{a_n}{b_s}$ is a d_∞-power in $\mathbb{F}_q$.*

Proof. We write

$$r(x) = x^n(a_n + a_{n-1}\frac{1}{x} + ... + a_1\frac{1}{x^{n-1}} + a_0\frac{1}{x^n})$$

and

$$r_1(x) = x^s(b_s + b_{s-1}\frac{1}{x} + ... + b_1\frac{1}{x^{s-1}} + b_0\frac{1}{x^s}).$$

Let $t = \frac{1}{x}$. Then we can write (2.5) as

$$y^m = \left(\frac{a_n + a_{n-1}t + ... + a_1 t^{n-1} + a_0 t^n}{t^n}\right)\left(\frac{t^s}{b_s + b_{s-1}t + ... + b_1 t^{s-1} + b_0 t^s}\right).$$

or equivalently,

$$y^m = t^{s-n}\,\frac{(a_n + a_{n-1}t + ... + a_1 t^{n-1} + a_0 t^n)}{(b_s + b_{s-1}t + ... + b_1 t^{s-1} + b_0 t^s)}.$$

Now we can apply the proof of Theorem 2.1.1 for $t = 0$ and we get the result. $\square$

We will now compute the genus of the function field F. By [8, Proposition III.7.3] we have:

$$g(F) = 1 + m. \left[-1 + \frac{1}{2} \sum_{P} \left(1 - \frac{\gcd\left(m, v_P(\frac{r(x)}{r_1(x)})\right)}{m} \right) \deg P \right], \qquad (2.7)$$

where P runs through all places of $\mathbb{F}_q(x)$.

We know by Theorem 1.2.5 that the only places of the rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$ are $P_{p(x)}$ and P_∞, where $p(x) \in \mathbb{F}_q[x]$ is an irreducible polynomial and $\deg P_{p(x)} = \deg p(x)$, $\deg P_\infty = 1$ by Proposition 1.2.6. If $p(x) \in \mathbb{F}_q[x]$ does not divide $r(x)$ and $r_1(x)$, then we get

$$v_{P_{p(x)}} \left(\frac{r(x)}{r_1(x)} \right) = 0,$$

which implies that $\gcd(m, v_{P_{p(x)}}(r(x)/r_1(x))) = m$. This means the sum over P is a finite sum over only the zeros and poles of $r(x)/r_1(x)$.

2.4 Examples Based on Section 3

Example 2.4.1. *This is an example of a function field $F = \mathbb{F}_8(x, y)$ given by*

$$y^7 = \frac{(x+1)^4(x+w)^2}{w^4},$$

where $w^3 + w + 1 = 0$, with $g(F) = 3$ and $N(F) = 24$. This is the best value known in [2].

Proof. Taking $f(x) = x^3 + wx^2 + x + w$, $\quad l(x) = x^8 - x$, $\quad l_1(x) = x + w^6$, $m = 7$ and $s = 2$, by the Euclidean division of $f(x)^{m+s}$ by $l(x)$ we get

$$r(x) = (x+1)^4(x+w)^2.$$

By Euclidean division of $f(x)^s$ by $l_1(x)$ we get $r_1(x) = w^4$.
Let $p_1(x) = x + 1$, $p_2(x) = x + w$, and P_1, P_2 be the corresponding places of

$\mathbb{F}_8(x)$ where $\deg P_1 = \deg P_2 = 1$. We have

$$v_{P_1}(r(x)/r_1(x)) = 4 \text{ and } v_{P_2}(r(x)/r_1(x)) = 2.$$

Then

$$\gcd(m, v_{P_1}(r(x)/r_1(x))) = \gcd(7,4) = 1$$

and

$$\gcd(m, v_{P_2}(r(x)/r_1(x))) = \gcd(7,2) = 1.$$

For P_∞, $\gcd(m, m_\infty) = \gcd(7,6) = 1$, where $m_\infty = \deg r(x) - \deg r_1(x) = 6$. Thus $g(F)$ can be computed using (2.7) as follows:

$$g(F) = 1 + 7\left[-1 + \frac{1}{2}\sum_{i=1}^{3}\left(1 - \frac{1}{7}\right)\right] = 3$$

We observe that P_1, P_2 and P_∞ are the only rational places of $\mathbb{F}_8(x)$ which are zeros and poles of $r(x)/r_1(x)$. There exists one place lying over P_1 and also one place lying over P_2. Both of them are rational places of $F/\mathbb{F}_8(x)$. There is one place of $F/\mathbb{F}_8(x)$ lying over P_∞ which is rational. We have computed the number of rational places which are neither zeros nor poles of $r(x)/r_1(x)$ by a computer search. This gives 21 extra rational places. Adding all these rational places we get $N(F) = 24$. □

Example 2.4.2. *This is an example of a function field $F = \mathbb{F}_{16}(x,y)$given by*

$$y^5 = \frac{w^9(x + w^7)^3}{(x+1)(x+w^2)^2}$$

where $w^4 + w + 1 = 0$, with $g(F) = 2$ and $N(F) = 33$. This is a maximal function field.

Proof. Taking $f(x) = x^6 + w^5x^5 + w^{14}x^3 + w^{11}x^2 + w^7x + w^{13}$, $l(x) = x^4 + x^3 + x^2 + x + 1$, $m = 5$ and $s = 7$, by the Euclidean division of $f(x)^{m+s}$ by $l(x)$ we get $r(x) = w^9(x + w^7)^3$. By Euclidean division of $f(x)^s$ by $l(x)$ we get $r_1(x) = (x+1)(x+w^2)^2$. Let $p_1(x) = x + w^7$, $p_2(x) = x + 1$,

$p_3(x) = x + w^2$ and $P_1,\ P_2,\ P_3$ be the corresponding places of $\mathbb{F}_{16}(x)$ where $\deg P_1 = \deg P_2 = \deg P_3 = 1$. We have

$$v_{P_1}(r(x)/r_1(x)) = 3\ \ ,\ \ v_{P_2}(r(x)/r_1(x)) = -1 \text{ and } v_{P_3}(r(x)/r_1(x)) = -2.$$

Then

$$\gcd(m, v_{P_1}(r(x)/r_1(x))) = \gcd(5,3) = 1,$$

$$\gcd(m, v_{P_2}(r(x)/r_1(x))) = \gcd(5,-1) = 1$$

and

$$\gcd(m, v_{P_3}(r(x)/r_1(x))) = \gcd(5,-2) = 1.$$

For P_∞, $\gcd(m, m_\infty) = \gcd(5,0) = 5$, where $m_\infty = \deg r(x) - \deg r_1(x) = 0$. Thus $g(F)$ can be computed using (2.7) as follows:

$$g(F) = 1 + 5\left[-1 + \frac{1}{2}\sum_{i=1}^{3}\left(1 - \frac{1}{5}\right)\right] = 2$$

We observe that P_1, P_2, P_3 and P_∞ are the only rational places of $\mathbb{F}_{16}(x)$ which are zeros and poles of $r(x)/r_1(x)$. There exists one place lying over P_1, one place lying over P_2 and also one place lying over P_3. All of them are rational places of $F/\mathbb{F}_{16}(x)$. There are no rational places of $F/\mathbb{F}_{16}(x)$ lying over P_∞. We have computed the number of rational places which are neither zeros nor poles of $r(x)/r_1(x)$ by a computer search. This gives 30 extra rational places. Adding all these rational places we get $N(F) = 33$. $\square$

Example 2.4.3. *This is an example of a function field $F = \mathbb{F}_9(x,y)$ given by*

$$y^4 = \frac{1}{w^3(x+w^7)^2(x^2+w^3x+2)(x^2+w^3x+w^7)}$$

where $w^2+2w+2 = 0$, with $g(F) = 5$ and $N(F) = 32$. This is the best value known in [2].

Proof. Taking $f(x) = x^3 + wx + w^3$, $l(x) = \frac{x^9-x}{x+w^7}$, $m = 4$ and $s = 4$, by the Euclidean division of $f(x)^{m+s}$ by $l(x)$ we get $r(x) = 1$. By Euclidean division of $f(x)^s$ by $l(x)$ we get $r_1(x) = w^3(x+w^7)^2(x^2+w^3x+2)(x^2+w^3x+w^7)$. Let $p_1(x) = x+w^7$, $p_2(x) = x^2+w^3x+2$, $p_3(x) = x^2+w^3x+w^7$ and P_1, P_2, P_3 be the corresponding places of $\mathbb{F}_9(x)$ where $\deg P_1 = 1$ and $\deg P_2 = \deg P_3 = 2$. We have

$$v_{P_1}(r(x)/r_1(x)) = -2 \ \text{ and } \ v_{P_i}(r(x)/r_1(x)) = -1 \ \text{ for } \ i = 2, 3.$$

Then

$$\gcd(m, v_{P_1}(r(x)/r_1(x))) = \gcd(4, -2) = 2$$

and

$$\gcd(m, v_{P_i}(r(x)/r_1(x))) = \gcd(4, -1) = 1$$

for $i = 2, 3$. For P_∞, $\gcd(m, m_\infty) = \gcd(4, -6) = 2$, where

$$m_\infty = \deg r(x) - \deg r_1(x) = -6.$$

Thus $g(F)$ can be computed using (2.7) as follows:

$$g(F) = 1 + 4\left[-1 + \frac{1}{2}\sum_{i=1}^{2}\left(1 - \frac{2}{4}\right) + \frac{1}{2}\sum_{i=1}^{2}\left(1 - \frac{1}{4}\right)2\right] = 5$$

We observe that P_1 and P_∞ are the only rational places of $\mathbb{F}_9(x)$ which are zeros and poles of $r(x)/r_1(x)$. There are no rational places of $F/\mathbb{F}_9(x)$ lying over P_1 and P_∞. We have computed the number of rational places which are neither zeros nor poles of $r(x)/r_1(x)$ by a computer search. This gives 32 rational places. We get $N(F) = 32$. □

CHAPTER 3

FIBRE PRODUCTS OF KUMMER EXTENSIONS

3.1 Main Theorems

Let $u \in \mathbb{F}_q$ and P_0 be the rational place of $\mathbb{F}_q(x)$ corresponding to the zero of $x-u$. Let $n_1, n_2 \geq 2$ be integers with $\gcd(n_1, q) = \gcd(n_2, q) = 1$. Let $f_1(x), f_2(x) \in \mathbb{F}_q(x)$ with $v_{P_0}(f_1(x)) = v_{P_0}(f_2(x)) = 0$. Let a_1, a_2 be integers. Let $E = \mathbb{F}_q(x, y_1, y_2)$ be the algebraic function field with

$$\begin{aligned} y_1^{n_1} &= (x-u)^{a_1} f_1(x), \\ y_2^{n_2} &= (x-u)^{a_2} f_2(x). \end{aligned} \tag{3.1}$$

We assume that $\mathbb{F}_q$ is the full constant field of E and $[E : \mathbb{F}_q(x)] = n_1 n_2$. Let $\bar{n}_1 = \gcd(n_1, a_1)$, $\bar{n}_2 = \gcd(n_2, a_2)$ and $m = \gcd(\frac{n_1}{\bar{n}_1}, \frac{n_2}{\bar{n}_2})$.

Let $f_1(u)$ and $f_2(u)$ be the evaluations of $f_1(x)$ and $f_2(x)$ at P_0.

Theorem 3.1.1. *There exist either no or exactly $\bar{n}_1 \bar{n}_2 m$ rational places of E over P_0. There exists a rational place of E over P_0 if and only if the following conditions C1, C2, C3 and C4 hold simultaneously:*

C1: $f_1(u)$ is an $\bar{n}_1$-power in $\mathbb{F}_q$.

C2: $f_2(u)$ is an $\bar{n}_2$-power in $\mathbb{F}_q$.

C3: $(m.\mathrm{lcm}\ (\bar{n}_1, \bar{n}_2)) \big| (q-1)$.

C4: Under the assumptions of C1 and C2, let α and β be elements of $\mathbb{F}_q$ with $\alpha^{\bar{n}_1} = f_1(u)$ and $\beta^{\bar{n}_2} = f_2(u)$. Let A and B be integers satisfying

$$A\frac{n_1}{\bar{n}_1} + B\frac{a_1}{\bar{n}_1} = 1. \tag{3.2}$$

Then we have

$$\frac{\beta}{\alpha^{\frac{a_2}{\bar{n}_2}B}} \ \text{ is an } m\text{-power in } \mathbb{F}_q. \tag{3.3}$$

Proof. Let P be a place of $\mathbb{F}_q(x, y_1)$ lying over P_0. Then by [8, Proposition III.7.3], the ramification index of P is

$$e_P = \frac{n_1}{gcd(n_1, v_{P_0}((x-u)^{a_1} f_1(x)))} = \frac{n_1}{gcd(n_1, a_1)} = \frac{n_1}{\bar{n}_1}.$$

Let P' be a place of $\mathbb{F}_q(x, y_2)$ lying over P_0. Then again by [8, Proposition III.7.3], the ramification index of P' is

$$e_{P'} = \frac{n_2}{gcd(n_2, v_{P_0}((x-u)^{a_2} f_2(x)))} = \frac{n_2}{gcd(n_2, a_2)} = \frac{n_2}{\bar{n}_2}.$$

Let P'' be a place of E lying over P_0. It follows from Abhyankar's Lemma ([8, Proposition III.8.9]) that the ramification index of P'' is

$$e_{P''} = lcm(e_P, e_{P'}) = lcm\left(\frac{n_1}{\bar{n}_1}, \frac{n_2}{\bar{n}_2}\right)$$

Let $P_1, P_2, ..., P_r$ be the rational places of E lying over P_0. By [8, Corollary III.7.2], we know that the relative degrees, say f_{P_i}, of $P_1, P_2, ..., P_r$ are the same and $r.e_{P_i}.f_{P_i} = n_1 n_2$. Since $degP_i = 1$ for all $i = 1, ..., r$, the residue class field of P_i is $\mathbb{F}_q$, so the relative degree f_{P_i} is 1. Then we get

$$r.e_{P_i}.f_{P_i} = r.lcm\left(\frac{n_1}{\bar{n}_1}, \frac{n_2}{\bar{n}_2}\right).1 = n_1 n_2.$$

That is

$$r = \bar{n}_1\bar{n}_2.gcd\left(\frac{n_1}{\bar{n}_1}, \frac{n_2}{\bar{n}_2}\right) = \bar{n}_1\bar{n}_2 m.$$

This implies that there are either no or exactly $\bar{n}_1\bar{n}_2 m$ rational places of E lying over P_0.

Now we will prove the second part of the theorem. Let E_1 be the subfield of E given by

$$E_1 = \mathbb{F}_q(x, z_1), \ \ z_1^{\bar{n}_1} = (x-u)^{a_1} f_1(x),$$

or equivalently

$$\left(\frac{z_1}{(x-u)^{a_1/\bar{n}_1}}\right)^{\bar{n}_1} = f_1(x). \tag{3.4}$$

As $\gcd(\bar{n}_1, v_{P_0}(f_1(x))) = \bar{n}_1$, P_0 is unramified in $E_1/\mathbb{F}_q(x)$. There exists a rational place of E_1 over P_0 if and only if C1 holds. Assume that C1 holds. Let P_1 be a place of E_1 over P_0. We have

$$v_{P_1}(x-u) = 1, \ v_{P_1}(z_1) = \frac{a_1}{\bar{n}_1}.$$

Let E_2 be the intermediate function field with $E_1 \subseteq E_2 \subseteq E$ given by

$$E_2 = \mathbb{F}_q(x, z_1, z_2), \ \ z_2^{\bar{n}_2} = (x-u)^{a_2} f_2(x),$$

or equivalently

$$\left(\frac{z_2}{(x-u)^{a_2/\bar{n}_2}}\right)^{\bar{n}_2} = f_2(x). \tag{3.5}$$

As $gcd(\bar{n}_2, v_{P_1}(f_2(x))) = \bar{n}_2$, P_1 is unramified in E_2/E_1. There exists a rational place of E_2 over P_1 if and only if C2 holds. Assume that C2 holds. Let P_2 be a place of E_2 over P_1. We have

$$v_{P_2}(x-u) = 1, \ v_{P_2}(z_1) = \frac{a_1}{\bar{n}_1}, \ v_{P_2}(z_2) = \frac{a_2}{\bar{n}_2}.$$

Let E_3 be the intermediate function field with $E_2 \subseteq E_3 \subseteq E$ given by

$$E_3 = \mathbb{F}_q(x, z_1, z_2, y_1), \ \ y_1^{n_1/\bar{n}_1} = z_1.$$

Note that $\gcd(\frac{n_1}{\bar{n}_1}, v_{P_2}(z_1)) = \gcd(\frac{n_1}{\bar{n}_1}, \frac{a_1}{\bar{n}_1}) = 1$, hence P_2 is totally ramifed in E_3/E_2. Let P_3 be the place of E_3 over P_2. We have

$$v_{P_3}(x-u) = \frac{n_1}{\bar{n}_1},\ v_{P_3}(z_1) = \frac{a_1}{\bar{n}_1}\frac{n_1}{\bar{n}_1},\ v_{P_3}(z_2) = \frac{a_2}{\bar{n}_2}\frac{n_1}{\bar{n}_1},\ v_{P_3}(y_1) = \frac{a_1}{\bar{n}_1}.$$

Now, since $\gcd(\frac{n_1}{\bar{n}_1}, \frac{a_1}{\bar{n}_1}) = 1$, we can choose integers A and B such that

$$A\frac{n_1}{\bar{n}_1} + B\frac{a_1}{\bar{n}_1} = 1.$$

Let $t = (x-u)^A y_1^B$. We have

$$v_{P_3}(t) = 1,\ v_{P_3}\left(\frac{x-u}{t^{\frac{n_1}{\bar{n}_1}}}\right) = 0$$

and

$$\frac{x-u}{t^{\frac{n_1}{\bar{n}_1}}} = \left(\frac{(x-u)^{\frac{a_1}{\bar{n}_1}}}{y_1^{\frac{n_1}{\bar{n}_1}}}\right)^B = \left(\frac{(x-u)^{\frac{a_1}{\bar{n}_1}}}{z_1}\right)^B.$$

Therefore the evaluation $\mathrm{Ev}_{P_3}\left(\frac{x-u}{t^{\frac{n_1}{\bar{n}_1}}}\right)$ of $\frac{x-u}{t^{\frac{n_1}{\bar{n}_1}}}$ at P_3 is in the set

$$\{c^{-B} : c^{\bar{n}_1} = f_1(u)\}.$$

Using (3.5) we obtain that $v_{P_3}\left(\frac{z_2}{t^{\frac{n_1}{\bar{n}_1}\frac{a_2}{\bar{n}_2}}}\right) = 0$ and for its evaluation at P_3 we have

$$\mathrm{Ev}_{P_3}\left(\frac{z_2}{t^{\frac{n_1}{\bar{n}_1}\frac{a_2}{\bar{n}_2}}}\right) \in \{dc^{-\frac{a_2}{\bar{n}_2}B} : c^{\bar{n}_1} = f_1(u),\ d^{\bar{n}_2} = f_2(u)\}. \tag{3.6}$$

Let E_4 be the intermediate function field with $E_3 \subseteq E_4 \subseteq E$ given by

$$E_4 = \mathbb{F}_q(x, z_1, z_2, y_1, w_2),\ \ w_2^m = z_2,$$

or equivalently

$$\left(\frac{w_2}{t^{\frac{a_2}{\bar{n}_2}\frac{n1}{\bar{n}_1 m}}}\right)^m = \frac{z_2}{t^{\frac{n_1}{\bar{n}_1}\frac{a_2}{\bar{n}_2}}}. \tag{3.7}$$

Note that $m|\frac{n_1}{\bar{n}_1}$. Therefore P_3 is unramified in E_4/E_3 and using (3.6) and (3.7) we obtain that there exists a rational place of E_4 over P_0 if and only if

$$\begin{gathered} dc^{-\frac{a_2}{\bar{n}_2}B} \text{ is an } m\text{-power for each } c \text{ and } d \text{ satisfying} \\ c^{\bar{n}_1} = f_1(u) \text{ and } d^{\bar{n}_2} = f_2(u). \end{gathered} \tag{3.8}$$

Let $\theta_1, \theta_2 \in \mathbb{F}_q$ be primitive $\bar{n}_1$-th and $\bar{n}_2$-th roots of 1 respectively, whose existence follow from C1 and C2. Let $\alpha, \beta \in \mathbb{F}_q$ with $\alpha^{\bar{n}_1} = f_1(u)$ and $\beta^{\bar{n}_2} = f_2(u)$. Then (3.8) is equivalent to

$$\begin{gathered} \beta\alpha^{-\frac{a_2}{\bar{n}_2}B}\theta_2^{l_2}\theta_1^{-l_1\frac{a_2}{\bar{n}_2}B} \text{ is an } m\text{-power} \\ \text{for } 0 \le l_1 \le \bar{n}_1 - 1 \text{ and } 0 \le l_2 \le \bar{n}_2 - 1. \end{gathered} \tag{3.9}$$

Substituting $l_1 = 0$ and $l_2 = 1$ in (3.9), we obtain that θ_2 is an m-power in $\mathbb{F}_q$. Note that $m|\frac{n_2}{\bar{n}_2}$ and hence $\gcd(m, \frac{a_2}{\bar{n}_2}) = 1$. From (3.2) we also get that $\gcd(m, B) = 1$. Substituting $l_1 = 1$ and $l_2 = 0$ in (3.9), since $\gcd(m, \frac{a_2}{\bar{n}_2}B) = 1$, we obtain that θ_1 is an m-power in $\mathbb{F}_q$. Therefore, under the assumptions of C1 and C2, (3.9) implies C3 and C4. It is also clear that the assumptions of C1 and C2, C3 and C4 imply (3.9). We assume C3, C4 and let P_4 be a place E_4 over P_3. We have $v_{P_4}(w_2) = \frac{a_2}{\bar{n}_2}\frac{n_1}{\bar{n}_1}\frac{1}{m}$.

Let E_5 be the intermediate function field with $E_4 \subseteq E_5 \subseteq E$ given by

$$E_5 = \mathbb{F}_q(x, z_1, z_2, y_1, w_2, y_2), \quad y_2^{\frac{n_2}{\bar{n}_2 m}} = w_2.$$

We observe that $E_5 = E$. Let ρ be a prime dividing $\frac{n_2}{\bar{n}_2 m}$. Then $\rho \nmid \frac{n_1}{\bar{n}_1 m}$. As $\gcd(\frac{n_2}{\bar{n}_2}, \frac{a_2}{\bar{n}_2}) = 1$, we also have $\rho \nmid \frac{a_2}{\bar{n}_2}$. Therefore $\gcd(\frac{n_2}{\bar{n}_2 m}, \frac{a_2}{\bar{n}_2}\frac{n_1}{\bar{n}_1}\frac{1}{m}) = 1$ and P_4 is totally ramified in E_5/E_4. This completes the proof. $\square$

Remark 3.1.2. *We observe that C4 is independent from the choice of the integers A and B. Indeed let $A', B' \in \mathbb{Z}$ with $A \neq A'$ and $B \neq B'$ satisfying*

$$A'\frac{n_1}{\bar{n}_1} + B'\frac{a_1}{\bar{n}_1} = 1.$$

Then we get

$$(A - A')\frac{n_1}{\bar{n}_1} = (B' - B)\frac{a_1}{\bar{n}_1}.$$

As $\frac{n_1}{\bar{n}_1}$ and $\frac{a_1}{\bar{n}_1}$ are relatively prime, we get that $B' - B$ is divisible by m. This implies that C4 is independent from the choice of A and B.

Remark 3.1.3. *Let $w_1 = y_1^{\frac{n_1}{\bar{n}_1 m}} \in E$. Using the tower $\mathbb{F}_q(x) \subseteq \mathbb{F}_q(x, z_1) \subseteq \mathbb{F}_q(x, z_1, z_2) \subseteq \mathbb{F}_q(x, z_1, z_2, y_2) \subseteq \mathbb{F}_q(x, z_1, z_2, y_2, w_1) \subseteq E$ instead of the tower $\mathbb{F}_q(x) \subseteq E1 \subseteq E_2 \subseteq E_3 \subseteq E_4 \subseteq E$ in the proof of Theorem 3.1.1, we obtain the conditions C1, C2, C3 and C4′ instead of the conditions of the theorem, where*

C4′: Under the assumptions of C1 and C2, let α and β be chosen elements of $\mathbb{F}_q$ with $\alpha^{\bar{n}_1} = f_1(u)$ and $\beta^{\bar{n}_2} = f_2(u)$. Let A' and B' be chosen integers satisfying

$$A' \frac{n_2}{\bar{n}_2} + B' \frac{a_2}{\bar{n}_2} = 1. \tag{3.10}$$

We have

$$\frac{\alpha}{\beta^{\frac{a_1}{\bar{n}_1} B'}} \text{ is an } m\text{-power in } \mathbb{F}_q. \tag{3.11}$$

Now we will show that these two sets of conditions are equivalent using elementary techniques, without algebraic function fields. By (3.2) we have

$$B \frac{a_1}{\bar{n}_1} \equiv 1 \mod m. \tag{3.12}$$

similarly by (3.10) we have

$$B' \frac{a_2}{\bar{n}_2} \equiv 1 \mod m. \tag{3.13}$$

From (3.12) and (3.13) we get that

$$\begin{aligned} \left(\tfrac{a_1}{\bar{n}_1}\right)\left(B\tfrac{a_2}{\bar{n}_2}\right) - \left(\tfrac{a_2}{\bar{n}_2}\right) &\equiv 0 \mod m, \\ \left(\tfrac{a_1}{\bar{n}_1}\right) - \left(\tfrac{a_2}{\bar{n}_2}\right)\left(B'\tfrac{a_1}{\bar{n}_1}\right) &\equiv 0 \mod m. \end{aligned} \tag{3.14}$$

Then (3.14) implies that

$$\left(\frac{\beta}{\alpha^{B\frac{a_2}{\bar{n}_2}}}\right)^{\frac{a_1}{\bar{n}_1}} \left(\frac{\alpha}{\beta^{B'\frac{a_1}{\bar{n}_1}}}\right)^{\frac{a_2}{\bar{n}_2}} \quad \text{is an } m\text{-power in } \mathbb{F}_q. \tag{3.15}$$

Using (3.15), $\gcd(m, \frac{a_1}{\bar{n}_1}) = 1$ *and* $\gcd(m, \frac{a_2}{\bar{n}_2}) = 1$, *under the assumptions of C1, C2 and C3 we prove that C4 is equivalent to C4′.*

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. Using almost the same arguments as in the proof of Theorem 3.1.1, we obtain the following theorem.

Theorem 3.1.4. *Let* $f_{1,1}(x), f_{1,2}(x), f_{2,1}(x), f_{2,2}(x)$ *be polynomials in* $\mathbb{F}_q[x]$ *of degrees* $d_{1,1}, d_{1,2}, d_{2,1}, d_{2,2}$. *Let* $d_1 = d_{1,1} - d_{1,2}$ *and* $d_2 = d_{2,1} - d_{2,2}$. *Let* $c_1, c_2 \in \mathbb{F}_q \setminus \{0\}$. *Let* $F = \mathbb{F}_q(x, y_1, y_2)$ *be the algebraic function field with*

$$y_1^{n_1} = c_1 \tfrac{f_{1,1}(x)}{f_{1,2}(x)}, \quad y_2^{n_2} = c_2 \tfrac{f_{2,1}(x)}{f_{2,2}(x)}.$$

We assume that $\mathbb{F}_q$ *is the full constant field of* F *and* $[F : \mathbb{F}_q(x)] = n_1 n_2$. *Let* $\bar{n}_1 = \gcd(n_1, d_1)$, $\bar{n}_2 = \gcd(n_2, d_2)$ *and* $m = \gcd(\frac{n_1}{\bar{n}_1}, \frac{n_2}{\bar{n}_2})$. *There exist either no or exactly* $\bar{n}_1 \bar{n}_2 m$ *rational places of* F *over* P_∞. *There exists a place of* F *over* P_∞ *if and only if the following conditions D1, D2, D3 and D4 hold simultaneously:*

- *D1:* c_1 *is an* $\bar{n}_1$*-power.*
- *D2:* c_2 *is an* $\bar{n}_2$*-power.*
- *D3:* $(m\operatorname{lcm}(\bar{n}_1, \bar{n}_2)) \big| (q-1)$.
- *D4: Under the assumptions of D1 and D2, let* α *and* β *be elements of* $\mathbb{F}_q$ *with* $\alpha^{\bar{n}_1} = c_1$ *and* $\beta^{\bar{n}_2} = c_2$. *Let* A *and* B *be integers satisfying*

  $$A\frac{n_1}{\bar{n}_1} + B\frac{a_1}{\bar{n}_1} = 1.$$

  We have

  $$\frac{\beta}{\alpha^{\frac{a_2}{\bar{n}_2}B}} \quad \text{is an } m\text{-power.}$$

3.2 Examples Based on Section 1

We have done a computer search in order to find function fields with many rational places using Theorem 3.1.1 and Theorem 3.1.4.

Example 3.2.1. *Let $E = \mathbb{F}_8(x, y_1, y_2)$ be the function field over $\mathbb{F}_8$ given by the following equations:*

$$\begin{aligned} y_1^7 &= w^3(x+1)^4(x+w)^2 \\ y_2^7 &= \frac{(x+1)^4(x+w)}{x+w^6} \end{aligned}$$

where $w^3 + w + 1 = 0$. The genus of E is $g(E) = 36$ and $N(E) = 112$. In this case the best known lower bound is 107 in [2].

Example 3.2.2. *Let $E = \mathbb{F}_{16}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{16}$ given by the following equations:*

$$\begin{aligned} y_1^3 &= \frac{w^3x(x+1)}{x+w^{10}} \\ y_2^5 &= x^3(x+1)^3(x^6+x^5+x^3+x+1) \end{aligned}$$

where $w^4 + w + 1 = 0$. The genus of E is $g(E) = 20$ and $N(E) = 127$. This is the best value known in [2].

Example 3.2.3. *Let $E = \mathbb{F}_{16}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{16}$ given by the following equations:*

$$\begin{aligned} y_1^5 &= x^3(x+1)^3(x^6+x^5+x^3+x+1) \\ y_2^3 &= \frac{x^4+x^2+x+w^{10}}{x^2+w^5} \end{aligned}$$

where $w^4 + w + 1 = 0$. The genus of E is $g(E) = 34$ and $N(E) = 183$.This is the best value known in [2].

Example 3.2.4. *Let $E = \mathbb{F}_{64}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{64}$ given by the following equations:*

$$\begin{aligned} y_1^3 &= x^3(x+1)^5(x^3+x+1) \\ y_2^3 &= w^{60}x^2(x+1)^5 \end{aligned}$$

where $w^6+w^4+w^3+w+1 = 0$. The genus of E is $g(E) = 10$ and $N(E) = 225$. This function field is maximal.

Example 3.2.5. *Let $E = \mathbb{F}_9(x, y_1, y_2)$ be the function field over $\mathbb{F}_9$ given by the following equations:*

$$\begin{aligned} y_1^2 &= \frac{x^2+w^7x+w^5}{x+w^3} \\ y_2^2 &= \frac{x^4+w^5x^3+x^2+w^3x+w^3}{x+w^3} \end{aligned}$$

where $w^2+2w+2 = 0$. The genus of E is $g(E) = 5$ and $N(E) = 32$. This is the best value known in [2].

Example 3.2.6. *Let $E = \mathbb{F}_9(x, y_1, y_2)$ be the function field over $\mathbb{F}_9$ given by the following equations:*

$$\begin{aligned} y_1^8 &= -(x^6+x^5+wx^4+2x^3+w^7x^2+x+2) \\ y_2^2 &= \frac{x^4+w^6x^3+w^7x+w^5}{x+w^3} \end{aligned}$$

where $w^2+2w+2 = 0$. The genus of E is $g(E) = 9$ and $N(E) = 48$. This is the best value known in [2].

Example 3.2.7. *Let $E = \mathbb{F}_{27}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{27}$ given by the following equations:*

$$\begin{aligned} y_1^2 &= (x-1)^6(x^3+w^{11}x^2+w^{11}x+w^{15}) \\ y_2^2 &= \frac{x^3+w^{11}x+w^{12}}{x^2} \end{aligned}$$

where $w^3+2w+1 = 0$. The genus of E is $g(E) = 4$ and $N(E) = 64$.

Example 3.2.8. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{10} &= x(x+1) \\ y_2^2 &= \frac{x^2 + w^3 x + w^6}{x} \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 8$ and $N(E) = 226$. This function field is maximal.

Example 3.2.9. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{5} &= x(x+1)^8 \\ y_2^2 &= \frac{x^2 + x + 2}{x + w^{60}} \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 11$ and $N(E) = 220$. This is the best value known in [2].

Example 3.2.10. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{16} &= x(x+1)^8 \\ y_2^2 &= \frac{x^2 + w^{22} x + w^{64}}{x} \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 15$ and $N(E) = 292$. This is the best value known in [2].

Example 3.2.11. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{5} &= x(x-1)^5 \\ y_2^{10} &= x(x-1)^{10}(x + w^{35}) \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 16$ and $N(E) = 370$. This function field is maximal.

Example 3.2.12. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{10} &= (x-1)^2(x+w^{60}) \\ y_2^2 &= \frac{x^2+1}{x+w^{50}} \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 17$ and $N(E) = 288$. This is the best value known in [2].

Example 3.2.13. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{10} &= x(x+1) \\ y_2^2 &= \frac{x(x+w^{18})}{x+w^2} \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 18$ and $N(E) = 306$. This is a new entry for the table in [2].

Example 3.2.14. *Let $E = \mathbb{F}_{81}(x, y_1, y_2)$ be the function field over $\mathbb{F}_{81}$ given by the following equations:*

$$\begin{aligned} y_1^{5} &= x(x+1)^8 \\ y_2^{10} &= \frac{x^2+x+1}{x} \end{aligned}$$

where $w^4 + 2w^3 + 2 = 0$. The genus of E is $g(E) = 36$ and $N(E) = 730$. This function field is maximal.

REFERENCES

[1] A. Garcia and A. Garzon, *On Kummer covers with many rational points over finite fields*, J. Pure Appl. Alg. **185** (2003), no. 1-3, 177–192.

[2] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, updated version January 2005,URL http://www.science.uva.nl/$\sim$ geer.

[3] V.D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290.

[4] M. Q. Kawakita, *Kummer curves and their fibre products with many rational points*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 1, 55–64.

[5] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields*, London Mathematical Society Lecture Note Series, Vol. 285, Cambridge University Press, Cambridge, 2001.

[6] F. Özbudak and H. Stichtenoth, *Curves with many points and configurations of hyperplanes over finite fields*, Finite Fields Appl. **5** (1999), no. 4, 436–449.

[7] S.A. Stepanov, *Codes on Algebraic Curves*, Kluwer Academic Publishers, New York, 1999.

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

[9] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht-Boston-London, 1991.

VITA

PERSONAL INFORMATION

Surname, Name: GÜLMEZ TEMUR, Burcu
Nationality: Turkish (TC)
Date and Place of Birth: 16 December 1973, Ankara
Marital Status: Married
email: bgtemur@atilim.edu.tr

EDUCATION

Degree	**Institution**	**Year of Graduation**
MS	METU Mathematics	1998
BS	METU Mathematics	1995
High School	İzmir Türk Koleji	1991

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2004- Present	Atılım Univ. Mathematics	Instructor
1996-2004	METU Mathematics	Research Assistant

FOREIGN LANGUAGE

Advanced English

FIELD OF STUDY

Algebraic Function Fields