ON THE ASYMPTOTIC THEORY OF TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

APPROVED BY

Prof. Dr. Henning Stichtenoth ....
(Thesis Supervisor)

Assoc. Prof. Stéphane Ballet ....

Assoc. Prof. Cem Güneri ....

Prof. Dr. Ferruh Özbudak ....

Assoc. Prof. Erkay Savaş ....

DATE OF APPROVAL: May 31, 2012

ON THE ASYMPTOTIC THEORY OF TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

by

SEHER TUTDERE

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

Sabancı University
Spring 2012

ON THE ASYMPTOTIC THEORY OF TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

APPROVED BY

Prof. Dr. Henning Stichtenoth ....
(Thesis Supervisor)

Assoc. Prof. Stéphane Ballet ....

Assoc. Prof. Cem Güneri ....

Prof. Dr. Ferruh Özbudak ....

Assoc. Prof. Erkay Savaş ....

DATE OF APPROVAL: May 31, 2012

ON THE ASYMPTOTIC THEORY OF TOWERS OF FUNCTION FIELDS OVER FINITE FIELDS

Seher Tutdere

Mathematics, PhD Thesis, 2012

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: towers of function fields, number of places, genus.

Abstract

In this thesis we consider a tower of function fields $\mathcal{F} = (F_n)_{n\geq 0}$ over a finite field $\mathbb{F}_q$ and a finite extension E/F_0 such that the sequence $\mathcal{E} := E \cdot \mathcal{F} = (EF_n)_{n\geq 0}$ is a tower over the field $\mathbb{F}_q$. Then we study invariants of $\mathcal{E}$, that is, the asymptotic number of the places of degree r in $\mathcal{E}$, for any $r \geq 1$, if those of $\mathcal{F}$ are known. We give a method for constructing towers of function fields over any finite field $\mathbb{F}_q$ with finitely many prescribed invariants being positive. For certain q, we prove that with the same method one can also construct towers with at least one positive invariant and certain prescribed invariants being zero. Our method is based on explicit extensions of function fields. Moreover, we show the existence of towers over a finite field $\mathbb{F}_q$ attaining the Drinfeld-Vladut bound of order r, for any $r \geq 1$ with q^r a square. Finally, we give some examples of recursive towers with various invariants being positive and towers with exactly one invariant being positive.

SONLU CİSİMLER ÜZERİNDE TANIMLANAN FONKSİYON CİSİMLERİ KULELERİNİN ASİMPTOTİK TEORİSİ ÜZERİNE

Seher Tutdere

Matematik, Doktora Tezi, 2012

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: fonksiyon cisimleri kuleleri, yerlerin sayısı, cins.

Özet

Bu tezde, herhangi bir sonlu cisim $\mathbb{F}_q$ üzerinde tanımlanan bir fonksiyon cisimleri kulesi $\mathcal{F} = (F_n)_{n\geq 0}$ ve $\mathcal{E} := E \cdot \mathcal{F} = (EF_n)_{n\geq 0}$ dizisinin $\mathbb{F}_q$ üzerinde tanımlanmasını sağlayan herhangi bir sonlu genişleme E/F_0 ele alınmıştır. Bu $\mathcal{F}$ kulesinin değişmezlerinin (yani derecesi herhangi bir $r \geq 1$ olan $\mathcal{F}$'teki yerlerin asimptotik sayılarının) bilindiği varsıyılarak, $\mathcal{E}$'nin değişmezleri üzerinde çalışılmıştır. Herhangi bir $\mathbb{F}_q$ üzerinde tanımlanan ve belirlenen sonlu sayıdaki değişmezi pozitif olan fonksiyon cisimleri kulelerinin inşa edilebilmesi için bir metod verilmiştir. Ayrıca, aynı metod kullanılarak, bazı q değerleri için, en az bir tane pozitif değişmezi ve bazı belirlenmiş değişmezleri sıfır olan kulelerinin inşa edilebileceği ispatlanmıştır. Bu metod, fonksiyon cisimlerinin açık genişlemelerine dayanmaktadır. Ayrıca, herhangi bir $r \geq 1$ ve q öyle ki q^r bir kare olduğu durumlarda, $\mathbb{F}_q$ üzerinde tanımlanan ve r mertebeli Drinfeld-Vladut sınırına ulaşan fonksiyon cisimleri kulelerinin var olduğu gösterilmiştir. Son olarak, çeşitli değişmezleri pozitif olan veya sadece bir değişmezi pozitif olan bazı özyineli fonksiyon cisimleri kuleleri örnekleri verilmiştir.

to my mother

Acknowledgments

First I am very grateful to my thesis father Henning Stichtenoth, for his motivation, invaluable advice and encouragement throughout this thesis.

I would like to express my sincere gratitude to Stéphane Ballet for fruitful discussions we made and being a member of my thesis committee.

It is a pleasure to thank Florian Hess for his hospitality in Germany for one year and for all his help. I also wish to thank Osmanbey Uzunkol for his support and encouragement during my stay in Germany.

I thank my family who have supported and encouraged me throughout my whole life.

Furthermore, I would like to thank all my friends in Sabancı University, especially Alp Bassa, Kağan Kurşungöz, Matteo Paganin, Leyla Işık, and Buket Özkaya for all the useful discussions we made and enjoyable moments we shared.

Lastly, I would also like to thank Albert Erkip for his support.

Table of Contents

Introduction

Let $\mathbb{F}_q$ be a finite field and $F/\mathbb{F}_q$ be an algebraic function field with the field $\mathbb{F}_q$ as its full constant field. Throughout this thesis, we shall simply refer to $F/\mathbb{F}_q$ as a function field. In this thesis the main aim is to construct towers of function fields over $\mathbb{F}_q$ and estimate their invariants, by using explicit extensions.

In 1992, M. Tsfasman [25] introduced the notion of asymptotically exact sequences of function fields over $\mathbb{F}_q$. For any such sequence $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$, M. Tsfasman [25] and M. Tsfasman, S. Vladut [26] studied invariants of $\mathcal{F}$ defined as follows: for any $r \geq 1$,

$$\beta_r(\mathcal{F}) := \lim_{n\to\infty} \frac{B_r(F_n)}{g(F_n)},$$

where $B_r(F_n)$ denotes the number of places of $F_n/\mathbb{F}_q$ of degree r, and $g(F_n)$ denotes the genus of $F_n/\mathbb{F}_q$.

The sequences for which β_r exists and is large are useful to obtain both good algebraic geometric codes and bounds for multiplication complexity in $\mathbb{F}_q$. In [1], S. Ballet and R. Rolland showed that these particular sequences have large asymptotic class number. In particular, explicitely defined exact sequences are quite useful in application.

In 2007, T. Hasegawa [13] and P. Lebacque [17] independently gave a proof of the existence of towers of function fields over $\mathbb{F}_q$ with finitely many prescribed invariants β_r being positive. Their method is based on class field theory. Note that M. Tsfasman, S. Vladut [26] and T. Hasegawa [12] showed that any tower of function fields over $\mathbb{F}_q$ is an exact sequence. However, the existence of exact sequences of function fields over $\mathbb{F}_q$ with at least one nonzero invariant and certain prescribed invariants being zero is in general not known (c.f. [20, p.64]).

The following open problem is stated in [1]: find asymptotically exact sequences $\mathcal{F}$ of function fields over $\mathbb{F}_q$, attaining the Drinfeld-Vladut bound of order r, for any $r \geq 1$, which is as follows:

$$\beta_r(\mathcal{F}) \leq \frac{q^{r/2}-1}{r}. \tag{0.1}$$

In [1], when $r = 4$ and $q = 2$, an exact sequence attaining the bound (0.1) is given. In the particular case, when q is a square and $r = 1$, there are several examples, namely maximal (or optimal) towers attaining this bound (for instance, see [8]). In [1], S. Ballet and R. Rolland proved that for any prime power q, there exists a tower attaining the bound (0.1) with $r = 2$.

The organization of this thesis is as follows:

In Chapter 1 we recall the basic definitions and introduce the notations. Moreover, we give some basic results.

In Chapter 2 we firstly give some bounds for the invariants of towers of function fields over $\mathbb{F}_q$. We then give a method for constructing towers with many prescribed invariants being positive. Furthermore, for certain q, we prove that by the same method, one can construct towers over $\mathbb{F}_q$ with at least one positive invariant and certain prescribed invariants being zero.

In Chapter 3 we give some examples of non-maximal recursive towers with all but one invariants equal to zero. This is analogous to the following open problem given in [19, p.3]: Are there any infinite number fields (i.e., towers of number fields) with all but one invariants equal to zero? Moreover, we show that for any integer $r \geq 1$ and a prime power q such that q^r is a square, there are towers of function fields over $\mathbb{F}_q$ attaining the Drinfeld-Vladut bound of order r. In this chapter we give also several examples of recursive towers with many invariants being positive. We also estimate the *deficiency*, i.e., the difference between the right hand side and the left hand side of (0.1), and the class number $h(F_n)$ for each new tower $\mathcal{F} = (F_n)_{n\geq 0}$.

In Chapter 4 we discuss constant field extensions of asymptotically exact sequences of function fields. Moreover, we give some basic results concerning Ihara's constant $A_r(q)$, for any $r \geq 1$ and prime power q, which is defined as follows:

$$A_r(q) := \limsup_{g\to\infty} \frac{B_r(F)}{g},$$

where F runs over all function fields over $\mathbb{F}_q$ with genus $g > 0$.

1

Preliminaries

Let us first fix some notation. Throughout this thesis, $\mathbb{F}_q$ will denote the finite field with $q = p^r$ elements, where p is a prime and $r \geq 1$ is an integer. We will consider function fields $F/\mathbb{F}_q$ of one variable over $\mathbb{F}_q$; in all cases, $\mathbb{F}_q$ will be the full constant field of F. We denote by $g(F)$ and $\mathbb{P}(F)$ the genus and the set of all places of $F/\mathbb{F}_q$, respectively. For any integer $r \geq 1$, define

$$B_r(F) := \#\{P \in \mathbb{P}(F) : \deg P = r\}.$$

For a rational function field $\mathbb{F}_q(x)$ we will write $(x = a)$ for the place which is the zero of $x - a$ (where $a \in \mathbb{F}_q$) and $(x = \infty)$ for the pole of x. For a place $P \in \mathbb{P}(F)$, we will use the following notations:

- $v_P :=$ the discrete valuation of $F/\mathbb{F}_q$ associated to the place P,
- $\mathcal{O}_P :=$ the valuation ring of P,
- $k(P) :=$ the residue class field of P.

Let E/F be a finite separable extension and Q be a place of E/F_q. We will write $Q|P$ if the place Q lies above the place $P \in \mathbb{P}(F)$. In this case, we will denote by

$$e(Q|P), f(Q|P), d(Q|P)$$

the ramification index, the relative degree, and the different exponent, respectively, of $Q|P$.

1.1 Asymptotically exact sequences of function fields

In [25], M. A. Tsfasman studied asymptotic properties of the numbers $B_r(F)$ in sequences of function fields over $\mathbb{F}_q$. Specifically, he introduced the following notion:

Definition 1.1.1. A sequence $\mathcal{S} = (F_n)_{n\geq 0}$ of function fields $F_n/\mathbb{F}_q$ is called asymptotically exact if $g(F_n) \to \infty$ as $n \to \infty$, and for all $r \geq 1$, the limit

$$\beta_r(\mathcal{S}) := \lim_{n\to\infty} \frac{B_r(F_n)}{g(F_n)}$$

exists.

For the numbers $\beta_r(\mathcal{S})$ one obtains the following bound [25, Corollary 1], [22, Theorem 3]:

Theorem 1.1.2 (**Generalized Drinfeld-Vladut bound**). *For an asymptotically exact sequence $\mathcal{S}$ of function fields over a finite field $\mathbb{F}_q$ the following holds:*

$$\sum_{r=1}^{\infty} \frac{r\beta_r(\mathcal{S})}{q^{r/2}-1} \leq 1. \tag{1.1}$$

Definition 1.1.3. For every $r \geq 1$, the real number

$$A_r(q) := \limsup_{g(F)\to\infty} \frac{B_r(F)}{g(F)},$$

where F runs over all function fields over $\mathbb{F}_q$ of genus $g(F) > 0$ is called the r-th Ihara's constant.

In particular, $A_1(q) = A(q)$, which is called *Ihara's constant.* The difference between the right hand side and the left hand side of the inequality (1.1) is called the *deficiency* of the sequence $\mathcal{S}$. This is related to the limit distribution of zeroes of zeta functions. For details see [26].

As a consequence of Theorem 1.1.2, one has

Corollary 1.1.4.

$$A_r(q) \leq \frac{q^{r/2}-1}{r}.$$

An exact sequence $\mathcal{S}$ over $\mathbb{F}_q$ is called

asymptotically good if there exists an $r \geq 1$ such that $\beta_r(\mathcal{S}) > 0$,

asymptotically bad if $\beta_r(\mathcal{S}) = 0$ for all $r \geq 1$, and

maximal if the bound (1.1) is attained.

For a sequence $\mathcal{S} = (F_n)_{n\geq 0}$ of function fields over $\mathbb{F}_q$, denote by $h_n := h(F_n)$ the *class number* of $F_n/\mathbb{F}_q$. Next, we give some results concerning the relation between the invariants $\beta_r(\mathcal{S})$ and the numbers h_n, with $r, n \geq 1$.

Theorem 1.1.5. *Suppose that the sequence $\mathcal{S} = (F_n)_{n\geq 0}$ of function fields over $\mathbb{F}_q$ is asymptotically exact. Then the limit*

$$H(\mathcal{S}) := \lim_{n\to\infty} \frac{\log_q h_n}{g(F_n)}$$

exists and

$$H(\mathcal{S}) = 1 + \sum_{r=1}^{\infty} \beta_r(\mathcal{S}) \log_q\left(\frac{q^r}{q^r-1}\right).$$

Proof. See [25, Corollary 2]. □

Recently, for the non-asymptotic case, S. Ballet and R. Rolland gave the following result in [2]:

Theorem 1.1.6. *Let $\mathcal{S} = (F_n)_{n\geq 0}$ be a sequence of function fields over a finite field $\mathbb{F}_q$ such that $B_1(F_n) \geq 1$ for all $n \geq 0$. Let further α be a positive real number. Suppose that there exists an integer $r \geq 1$ such that* *(i)* $\liminf_{n\to\infty} \frac{B_r(F_n)}{g(F_n)} > \alpha$ *or*

(ii) $\frac{1}{r} \liminf_{n\to\infty} \sum_{i|r} \frac{iB_i(F_n)}{g(F_n)} > \alpha$.

Then there exists a constant $C > 0$ *such that for all* $n \geq 0$, *one has*

$$h(F_n) > C\left(\left(\frac{q^r}{q^r - 1}\right)^{\alpha} q\right)^{g(F_n)}.$$

As a consequence of Theorems 1.1.5 and 1.1.6, it is clear that in a sequence $\mathcal{S} = (F_n)_{n\geq 0}$ with various positive invariants $\beta_r(\mathcal{S})$, the numbers h_n are large.

In this thesis we will consider specific sequences of function fields over $\mathbb{F}_q$, namely towers. We will show that they are asymptotically exact and then study their invariants defined in Definition 1.3.1. We will give an elementary method to construct towers with various invariants being positive.

1.2 Towers of function fields

In this section we introduce towers of function fields and discuss some of their general properties.

Definition 1.2.1. An infinite sequence $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ is called a *tower* if the following hold:

(a) $F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \ldots$,

(b) for each $n \geq 0$, the extension F_{n+1}/F_n is finite and separable,

(c) the genus $g(F_n) \to \infty$ as $n \to \infty$.

Note that we always assume that $\mathbb{F}_q$ is the full constant field of F_n for all $n \geq 0$.

Definition 1.2.2. Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over $\mathbb{F}_q$ and $f(X,Y) \in \mathbb{F}_q[X,Y]$ be a non-constant polynomial. Suppose that there exist elements $x_n \in F_n$ (for $n \geq 0$) such that

$$F_{n+1} = F_n(x_{n+1}) \text{ with } f(x_n, x_{n+1}) = 0 \text{ for all } n \geq 0.$$

Then we say that the tower $\mathcal{F}$ is *recursively* defined over F_q by the polynomial $f(X,Y)$.

In the subsequent chapters, we will give many examples of recursive towers and study their invariants.

Proposition 1.2.3. *Let* $\mathcal{F} = (F_n)_{n\geq 0}$ *be a tower over* $\mathbb{F}_q$. *Then the following hold:*

(i) The sequence $\big(g(F_n)/[F_n : F_0]\big)_{n\geq 0}$ *is convergent in* $\mathbb{R}^{>0} \cup \{\infty\}$.

(ii) Let $P \in \mathbb{P}(F_0)$, *and* $r \geq 1$. *Set*

$$B_r(P, F_n) := \#\left\{Q \in \mathbb{P}(F_n) : Q|P \text{ and } \deg Q = r\right\}.$$

Then the sequence $\big(B_r(P, F_n)/[F_n : F_0]\big)_{n\geq 0}$ *is convergent in* $\mathbb{R}^{\geq 0}$.

Proof.

(i) See [10, Proposition 2.4(i)].

(ii) Our proof is similar to T. Hasegawa's proof that the sequence $(B_r(F_n)/g(F_n))_{n\geq 0}$ is convergent (cf. [12, Proposition 2.2]). We proceed by induction over r. For $r = 1$, the sequence $(B_1(P, F_n)/[F_n : F_0])_{n\geq 0}$ is monotonically decreasing, and so convergent (cf. [24, Lemma 7.2.3(a)]). Now let $r \geq 1$ and assume that for all $1 \leq s < r$, the sequence $(B_s(P, F_n)/[F_n : F_0])_{n\geq 0}$ is convergent. Let $d := \deg P$. If $d \nmid r$, then $B_r(P, F_n) = 0$ for all $n \geq 0$. Hence, we can assume that $d \mid r$.

Consider the constant field extension of $\mathcal{F}$ with the field $\mathbb{F}_{q^r}$; i.e.,

$$\mathcal{F} \cdot \mathbb{F}_{q^r} := (F_n\mathbb{F}_{q^r})_{n\geq 0}.$$

This is clearly a tower over $\mathbb{F}_{q^r}$. The place $P \in \mathbb{P}(F_0)$ splits into $P_1, \ldots, P_d \in \mathbb{P}(F_0\mathbb{F}_{q^r})$ of degree one, and all places of F_n of degree $s \mid r$ split into s degree one places of $F_n\mathbb{F}_{q^r}/\mathbb{F}_{q^r}$. Hence, the following formula holds (cf. [24, p. 206]):

$$\sum_{s|r} s \cdot B_s(P, F_n) = \sum_{j=1}^{d} B_1(P_j, F_n\mathbb{F}_{q^r}). \tag{1.2}$$

By the induction hypothesis, the sequences

$$\left(\frac{B_s(P, F_n)}{[F_n : F_0]}\right)_{n\geq 0} \quad \text{and} \quad \left(\frac{B_1(P_j, F_n\mathbb{F}_{q^r})}{[F_n : F_0]}\right)_{n\geq 0}$$

are convergent for $s < r$. Hence, the sequence $(B_r(P, F_n)/[F_n : F_0])_{n\geq 0}$ also converges. □

Corollary 1.2.4. *Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over $\mathbb{F}_q$, P a place of F_0 and $r \geq 1$. Then the sequences*

$$\left(\frac{B_r(P, F_n)}{g(F_n)}\right)_{n\geq 0}, \quad \left(\frac{B_r(F_n)}{[F_n : F_0]}\right)_{n\geq 0}, \quad \textit{and} \quad \left(\frac{B_r(F_n)}{g(F_n)}\right)_{n\geq 0}$$

are convergent in $\mathbb{R}^{\geq 0}$.

Proof. It is clear from Proposition 1.2.3(i) that $([F_n : F_0]/g(F_n))$ is convergent in $\mathbb{R}^{\geq 0}$. Hence, the convergence of the sequence $(B_r(P, F_n)/g(F_n))_{n\geq 0}$ follows immediately from Proposition 1.2.3(ii) and the equality

$$\frac{B_r(P, F_n)}{g(F_n)} = \frac{B_r(P, F_n)}{[F_n : F_0]} \cdot \frac{[F_n : F_0]}{g(F_n)}.$$

Since

$$B_r(F_n) = \sum_{P\in\mathbb{P}(F_0)} B_r(P, F_n), \tag{1.3}$$

the other sequences in Corollary 1.2.4 are convergent as well. Note that the sum (1.3) is finite since for any fixed $r \geq 1$ there are only finitely many places of F_0 of degree dividing r. □

1.3 Invariants of towers

As a consequence of Proposition 1.2.3(i) and Corollary 1.2.4, the following definitions make sense:

Definition 1.3.1. Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over $\mathbb{F}_q$, $P \in \mathbb{P}(F_0)$ and $r \geq 1$.

(a) The *local invariants* of $\mathcal{F}$ at P are defined as

$$\nu_r(P,\mathcal{F}) := \lim_{n\to\infty} \frac{B_r(P,\mathcal{F})}{[F_n : F_0]} \quad \text{and} \quad \beta_r(P,\mathcal{F}) := \lim_{n\to\infty} \frac{B_r(P,F_n)}{g(F_n)}.$$

(b) The *global invariants* of $\mathcal{F}$ are defined as

$$\nu_r(\mathcal{F}) := \lim_{n\to\infty} \frac{B_r(\mathcal{F})}{[F_n : F_0]} \quad \text{and} \quad \beta_r(\mathcal{F}) := \lim_{n\to\infty} \frac{B_r(F_n)}{g(F_n)}.$$

(c) The *genus* $\gamma(\mathcal{F})$ of $\mathcal{F}$ is defined as

$$\gamma(\mathcal{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F]}.$$

Note that the definition of $\beta_r(\mathcal{F})$ is consistent with Definition 1.1.1. The sets

$$\mathrm{Supp}(\mathcal{F}) := \{P \in \mathbb{P}(F_0) : \nu_r(P,\mathcal{F}) > 0 \text{ for some } r \in \mathbb{N}\} \text{ and}$$

$$\mathcal{P}(\mathcal{F}) := \{r \in \mathbb{N} : \ \nu_r(\mathcal{F}) > 0\}$$

are called the *support* and the set of the *positive parameters* of $\mathcal{F}$, respectively.

We summarize as follows:

Theorem 1.3.2. *Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over $\mathbb{F}_q$. Then one has the following:*

(i) For all $r \geq 1$, the limit

$$\beta_r(\mathcal{F}) := \lim_{n\to\infty} \frac{B_r(F_n)}{g(F_n)}$$

exists; i.e., the tower is asymptotically exact.

(ii) (Generalized Drinfeld-Vladut bound and Deficiency)

$$\sum_{r=1}^{\infty} \frac{r\beta_r(\mathcal{F})}{q^{r/2}-1} \leq 1,$$

and the difference between the right hand side and the left hand side of this inequality is called the deficiency of $\mathcal{F}$.

(iii) (Drinfeld-Vladut bound of order r) For all $r \geq 1$,

$$\beta_r(\mathcal{F}) \leq A_r(q) \leq \frac{q^{r/2}-1}{r},$$

where $A_r(q)$ is the r-th Ihara's constant.

(iv) Let $P \in \mathbb{P}(F_0)$ and $r \geq 1$. Then

$$\beta_r(P, \mathcal{F}) = \frac{\nu_r(P, \mathcal{F})}{\gamma(\mathcal{F})} \text{ and } \beta_r(\mathcal{F}) = \frac{\nu_r(\mathcal{F})}{\gamma(\mathcal{F})}.$$

(v) For all $r \geq 1$,

$$\nu_r(\mathcal{F}) = \sum_{P \in \mathbb{P}(F_0)} \nu_r(P, \mathcal{F}) \text{ and } \beta_r(\mathcal{F}) = \sum_{P \in \mathbb{P}(F_0)} \beta_r(P, \mathcal{F}).$$

Note that obviously for a tower $\mathcal{F}$ when $\gamma(\mathcal{F}) < \infty$, by using Theorem 1.3.2(iv), one can define the set of positive parameters of $\mathcal{F}$ as follows:

$$\mathcal{P}(\mathcal{F}) = \{r \in \mathbb{N} : \beta_r(\mathcal{F}) > 0\} = \{r \in \mathbb{N} : \nu_r(\mathcal{F}) > 0\}.$$

Lemma 1.3.3. *Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a tower over $\mathbb{F}_q$ and for each $r \geq 1$ set $F_r := F_0\mathbb{F}_{q^r}$. Then the following holds:*

$$0 \leq \nu_r(\mathcal{F}) \leq \frac{B_1(F_r)}{r},$$

where $B_1(F_r)$ denotes the number of rational places of $F_r/\mathbb{F}_{q^r}$.

Proof. The first inequality is clear, so we prove the second one. For $n \geq 2$, let Q be a place of F_n of degree r and set $P := Q \cap F_0$. Since F_n and F_0 have the same constant field, we have

$$f(Q|P) \cdot \deg P = \deg Q = r, \tag{1.4}$$

which implies that $\deg P | r$. Thus, in order to find the number of places $Q \in \mathbb{P}(F_n)$ of degree r, we take a place P of F_0 of degree d dividing r, and define

$$s_P := \#\left\{Q \in \mathbb{P}(F_n) |\ Q \text{ lies above } P\ ,\ \deg Q = r\right\}.$$

From (1.4), for all such places Q, the relative degree $f(Q|P) = \frac{r}{d}$, and so we get

$$\begin{aligned} s_P = \sum_{\substack{Q|P \\ \deg Q = r}} 1 &= \frac{d}{r} \cdot \sum_{\substack{Q|P \\ \deg Q = r}} f(Q|P) \\ &\leq \frac{d}{r} \sum_{Q|P} e(Q|P) \cdot f(Q|P) \\ &= \frac{d}{r} \cdot [F_n : F_0] \qquad \text{(by the Fundamental Equality)} \end{aligned}$$

Then by this inequality, we obtain that

$$\begin{aligned} B_r(F_n) &= \sum_{\deg P | r} s_P = \sum_{d|r} \sum_{\substack{P \\ \deg P = d}} s_P \\ &\leq \sum_{d|r} \sum_{\substack{P \\ \deg P = d}} \frac{d}{r}[F_n : F_0] = \sum_{d|r} \frac{[F_n : F_0]}{r} \cdot d \cdot \sum_{\substack{P \\ \deg P = d}} 1 \\ &= \sum_{d|r} \frac{[F_n : F_0]}{r} \cdot d \cdot B_d(F_0). \end{aligned}$$

Now in the above inequality, dividing both of the sides by $[F_n : F_0]$, and then taking the limit yields the desired result:

$$\nu_r(\mathcal{F}) \leq \frac{1}{r} \cdot \left(\sum_{d|r} d \cdot B_d(F_0) \right) = \frac{B_1(F_r)}{r}.$$

□

Thus, the following consequence is immediate:

Corollary 1.3.4. *Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over $\mathbb{F}_q$. Then for any $r \geq 1$ and $P \in \mathbb{P}(F_0)$, the limit $\beta_r(P, \mathcal{F}) > 0$ if and only if $\nu_r(P, \mathcal{F}) > 0$ and $\gamma(\mathcal{F}) < \infty$.*

Proof. By Theorem 1.3.2(iv), we have $\beta_r(P, \mathcal{F}) = \nu_r(P, \mathcal{F})/\gamma(\mathcal{F})$. Hence, by using Proposition 1.2.3 and Lemma 1.3.3, the corollary follows. □

Definition 1.3.5. Let $\mathcal{F} = (F_n)_{n\geq 0}$ and $\mathcal{E} = (E_n)_{n\geq 0}$ be towers over $\mathbb{F}_q$. Then $\mathcal{F}$ is said to be a *subtower* of $\mathcal{E}$ if for each $i \geq 0$ there exists a $j \geq 0$ and an embedding $\phi_i : F_i \to E_j$ over $\mathbb{F}_q$.

For the proof of the following result see [24, Proposition 7.2.8]:

Lemma 1.3.6. *Let $\mathcal{F}$ be a subtower of $\mathcal{E}$. Then $\beta_1(\mathcal{F}) \geq \beta_1(\mathcal{E})$.*

We note here that Lemma 1.3.6 is in general not true for β_r with $r \geq 2$. For instance, see examples in Chapter 3.

Furthermore, by [19, Theorem C], the *deficiency* is an increasing function with respect to inclusion, i.e., we have the following:

Lemma 1.3.7. *If $\mathcal{F}$ is a subtower of $\mathcal{E}$, then*

$$\delta(\mathcal{F}) \leq \delta(\mathcal{E}).$$

1.4 Infinite function fields

An *infinite function field* $\Omega/\mathbb{F}_q$ is an infinite separable extension of the rational function field $\mathbb{F}_q(x)$ such that $\mathbb{F}_q$ is algebraically closed in Ω. In other words,

$$\Omega = \bigcup_{n\geq 0} F_n, \quad \text{for some tower } \mathcal{F} = (F_n)_{n\geq 0} \text{ over } \mathbb{F}_q.$$

In this case, the tower $\mathcal{F}$ is called a *representative* for the field Ω.

Lemma 1.4.1. *Suppose that $\mathcal{F} = (F_n)_{n\geq 0}$ and $\mathcal{H} = (H_n)_{n\geq 0}$ are two towers, with $F := F_0 = H_0$, representing the same infinite function field Ω. Then the following hold:*

(i) $\gamma(\mathcal{F}) = \gamma(\mathcal{H})$.

(ii) For any $P \in \mathbb{P}(F)$ and $r \geq 1$, one has that

$$\nu_r(P, \mathcal{F}) = \nu_r(P, \mathcal{H}) \text{ and } \beta_r(P, \mathcal{F}) = \beta_r(P, \mathcal{H}).$$

Moreover,

$$\nu_r(\mathcal{F}) = \nu_r(\mathcal{H}) \text{ and } \beta_r(\mathcal{F}) = \beta_r(\mathcal{H}) \text{ for all } r \geq 1. \tag{1.5}$$

Proof.

(i) As $\Omega = \bigcup_{n\geq 0} F_n = \bigcup_{n\geq 0} H_n$, and each F_n is finitely generated over $\mathbb{F}_q$, there is an $m \geq n$ such that F_n is contained in H_m. Hence, by using the Hurwitz Genus Formula [24], we obtain that

$$g(H_m) - 1 \geq [H_m : F_n] \cdot (g(F_n) - 1).$$

Then dividing both sides of this inequality by $[H_m : F]$ yields

$$\frac{g(H_m) - 1}{[H_m : F]} \geq \frac{g(F_n) - 1}{[F_n : F]}.$$

Hence, $\gamma(\mathcal{H}) \geq \gamma(\mathcal{F})$, and similarly, vice versa.

(ii) Let $P \in \mathbb{P}(F)$. It is enough to prove that $\nu_r(P, \mathcal{F}) = \nu_r(P, \mathcal{H})$ for any $r \geq 1$. Then by (i) and Theorem 1.3.2(iv),(v), the other invariants of $\mathcal{F}$ and $\mathcal{H}$ are also equal. As in (i), for any $n \geq 1$, we have $F_n \subseteq H_m$ for some $m \geq n$. We prove our assertion by induction over r. For $r = 1$, we have that

$$B_1(P, H_m) \leq [H_m : F_n] B_1(P, F_n).$$

Hence, as $n \to \infty$, we obtain that

$$\nu_1(P, \mathcal{H}) = \lim_{m\to\infty} \frac{B_1(P, H_m)}{[H_m : F]} \leq \lim_{n\to\infty} \frac{B_1(P, F_n)}{[F_n : F]} = \nu_1(P, \mathcal{F}).$$

Similarly, since $H_m \subseteq F_k$ for some $k \geq m$, we obtain that $\nu_1(P, \mathcal{F}) \leq \nu_1(P, \mathcal{H})$. Hence,

$$\nu_1(P, \mathcal{F}) = \nu_1(P, \mathcal{H}).$$

Now let $r \geq 1$ and assume that for all $1 \leq s < r$, we have that $\nu_s(P, \mathcal{F}) = \nu_s(P, \mathcal{H})$. Consider the constant field extensions $\mathcal{F} \cdot \mathbb{F}_{q^r} = (F_n \mathbb{F}_{q^r})_{n\geq 0}$ and $\mathcal{H} \cdot \mathbb{F}_{q^r} = (H_n \mathbb{F}_{q^r})_{n\geq 0}$ of the towers $\mathcal{F}$ and $\mathcal{H}$, respectively. Let $d := \deg P$. From the Formula (1.2), we have that

$$\sum_{s|r} s B_s(P, F_n) = \sum_{j=1}^{d} B_1(P_j, F_n \mathbb{F}_{q^r}), \tag{1.6}$$

where $P_1, \ldots, P_d$ are the extensions of P in $F\mathbb{F}_{q^r}$. Dividing Eq. (1.6) by $[F_n : F]$ and then taking the limit as $n \to \infty$ gives that

$$\begin{aligned} \sum_{s|r} s\nu_s(P, \mathcal{F}) &= \sum_{j=1}^{d} \nu_1(P_j, \mathcal{F} \cdot \mathbb{F}_{q^r}) && (1.7) \\ &= \sum_{j=1}^{d} \nu_1(P_j, \mathcal{H} \cdot \mathbb{F}_{q^r}) = \sum_{s|r} s\nu_s(P, \mathcal{H}). && (1.8) \end{aligned}$$

By the induction hypothesis, $\nu_s(P, \mathcal{F}) = \nu_s(P, \mathcal{H})$ for all $1 \leq s < r$. Therefore,

$$\nu_r(P, \mathcal{F}) = \nu_r(P, \mathcal{H}).$$

□

Lemma 1.4.2. *Let Ω be an infinite function field represented by a tower $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ and $\Omega^{'}$ be a finite separable extension of Ω. Suppose that $\mathbb{F}_q$ is algebraically closed in $\Omega^{'}$. Then for some $k \geq 0$, there exists a finite separable extension E of F_k such that the following hold:*

(i) The fields E and F_n are linearly disjoint over F_k for all $n \geq 0$.

(ii) The sequence $\mathcal{E} := (EF_n)_{n\geq k}$ is a tower over $\mathbb{F}_q$ representing the field $\Omega^{'}$.

Proof. We will prove just the first assertion. The second assertion will clearly follow. Since $\Omega^{'}/\Omega$ is finite and separable, there exists an element $\alpha \in \Omega^{'}$ such that $\Omega^{'} = \Omega(\alpha)$. The coefficients of the minimal polynomial of α over Ω lie in F_k for some $k \geq 0$. Let $E := F_k(\alpha)$ and $E_n := EF_n$ for all $n \geq k$. Then, $\Omega' = \bigcup_{n\geq k} E_n$ and for all $n \geq k$, we have that

$$[E_k : F_k] = [E_n : F_n] = [\Omega^{'} : \Omega].$$

This means that the fields E_k and F_n are linearly disjoint over F_k for all $n \geq k$. Then obviously

$$[E_{n+1} : E_n] = [F_{n+1} : F_n] \text{ for all } n \geq k.$$

Next, as $\mathbb{F}_q$ is algebraically closed in $\Omega^{'}$ and F_n, for all $n \geq 0$, it is the full constant field of E_n. Hence, $\mathcal{E} = (E_n)_{n\geq k}$ is a tower over $\mathbb{F}_q$. □

2

Invariants of Towers

In this chapter, unless otherwise stated, we consider a tower $\mathcal{F} = (F_n)_{n\geq 0}$ of function fields over $\mathbb{F}_q$ and a finite separable extension E of F_0. For convenience, we assume that $E, F_0, F_1, \ldots$ are all contained in a fixed algebraically closed field Ω. For simplicity, we set $F := F_0$ and denote by $\mathcal{E} := E \cdot \mathcal{F}$ the sequence $\mathcal{E} = (E_n)_{n\geq 0}$, with $E_n := EF_n$, of function fields over $\mathbb{F}_q$.

Remark. If E and F_n are linearly disjoint over F and $\mathbb{F}_q$ is algebraically closed in E_n for all $n \geq 0$, then the sequence $\mathcal{E}$ is a tower over $\mathbb{F}_q$.

Our goal is as follows: For a given tower $\mathcal{F}/\mathbb{F}_q$ we want to construct an appropriate extension E of F such that $\mathcal{E}$ is a tower over $\mathbb{F}_q$ and to estimate the invariants of $\mathcal{E}$ depending on those of $\mathcal{F}$. Recall that by Theorem 1.3.2(iv), for any $r \in \mathbb{N}$, we have $\beta_r(\mathcal{E}) = \frac{\nu_r(\mathcal{E})}{\gamma(\mathcal{E})}$. Hence, in order to get bounds for $\beta_r(\mathcal{E})$, we estimate $\nu_r(\mathcal{E})$ and $\gamma(\mathcal{E})$.

2.1 Bounds for the invariants of a tower

In this section we assume that $\mathcal{E} = (EF_n)_{n\geq 0}$ is a tower over $\mathbb{F}_q$. We begin with a lemma concerning the splitting of places in the compositum of function fields, [24, Proposition 3.9.6(a)].

Lemma 2.1.1. *Let E/F and F'/F be finite separable extensions of function fields contained in an algebraic closure of F. Suppose that P is a place of F which splits completely in the extension F'. Then every place Q of E lying above P splits completely in the compositum EF'.*

Proposition 2.1.2. *For any $s \geq 1$, one has*

$$\nu_s(\mathcal{E}) \geq \# \left\{ Q \in \mathbb{P}(E) |\ \deg Q = s \text{ and } Q \cap F \text{ splits completely in } \mathcal{F} \right\}.$$

Proof. Let $Q \in \mathbb{P}(E)$ such that $P := Q \cap F$ splits completely in $\mathcal{F}$. Then by Lemma 2.1.1, Q splits completely in E_n for all $n \geq 1$. Hence,

$$B_s(Q, E_n) = [E_n : E] \text{ where } s = \deg Q,$$

which yields $\nu_s(Q, \mathcal{E}) = 1$, and so by Theorem 1.3.2(v) the proposition follows. □

Remark 2.1.3. For any $d \geq 1$ and $P \in \mathbb{P}(F)$, the following holds:

$$\sum_{r=1}^{m} \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P,\ s=rd}} \nu_s(Q, \mathcal{E}) \geq \nu_d(P, \mathcal{F}). \tag{2.1}$$

Proof. The proof follows from the following argument. Let P_n be a place of F_n lying above P of $\deg P_n = d$ for some $d \geq 1$. Then for any extension Q_n of P_n in E_n, we have $f(Q_n|P_n) = r$ for some $1 \leq r \leq m$, and so $\deg Q_n = rd$. $\square$

Proposition 2.1.4. *Let $Q \in \mathbb{P}(E)$ and $P := Q \cap F$. Then for all $s > 0$, we have the following:*

(i) $$\nu_s(Q,\mathcal{E}) \leq \sum_{\substack{d\in\mathcal{P}(\mathcal{F})\\ d|s, d\geq \frac{s}{m}}} \frac{md}{s}\nu_d(P,\mathcal{F}) \text{ and } \beta_s(Q,\mathcal{E}) \leq \sum_{\substack{d\in\mathcal{P}(\mathcal{F})\\ d|s, d\geq \frac{s}{m}}} \frac{d}{s}\beta_d(P,\mathcal{F}).$$

(ii) $$\nu_s(\mathcal{E}) \leq \sum_{\substack{d\in\mathcal{P}(\mathcal{F})\\ d|s, d\geq \frac{s}{m}}} \frac{md}{s}\nu_d(\mathcal{F}) \text{ and } \beta_s(\mathcal{E}) \leq \sum_{\substack{d\in\mathcal{P}(\mathcal{F})\\ d|s, d\geq \frac{s}{m}}} \frac{d}{s}\beta_d(\mathcal{F}).$$

Proof. (i) Fix $n \geq 1$ and let Q_n be an extension of Q in E_n of degree s and $P_n := Q_n \cap F_n$. Then clearly $P_n|P$ and $\deg P_n = d$ with d dividing s and $d \geq \frac{s}{m}$, since $f(Q_n|P_n) \leq m$. Conversely, any place P_n of F_n lying above P with $\deg P_n = d$, and satisfying $d \geq \frac{s}{m}$ has at most $\frac{md}{s}$ extensions of degree s in E_n, by the Fundamental Equality [24]. Hence,

$$B_s(Q,E_n) \leq \sum_{\substack{d\in\mathbb{N}\\ d|s,\ d\geq \frac{s}{m}}} \frac{md}{s} B_d(P,F_n) \tag{2.2}$$

Dividing (2.2) by $[E_n : E]$ yields the bound for $\nu_s(Q,\mathcal{E})$. Next, by using the Hurwitz Genus Formula [24], one obtains that

$$g(E_n) \geq mg(F_n) - m \text{ for all } n \geq 0, \text{ and so } \gamma(\mathcal{E}) \geq m\gamma(\mathcal{F}). \tag{2.3}$$

Dividing the LHS and the RHS of (2.2) by $\gamma(\mathcal{E})$ and $m\gamma(\mathcal{F})$), respectively, gives the desired bound for $\beta_s(Q,\mathcal{E})$. The assertion (ii) then follows by using Theorem 1.3.2(v). $\square$

The following consequence follows easily from Proposition 2.1.4:

Corollary 2.1.5. *For the tower $\mathcal{E}$, we obtain that*

(i) $\mathrm{Supp}(\mathcal{E}) \subseteq \{Q \in \mathbb{P}(E) :\ Q \cap F \in \mathrm{Supp}(\mathcal{F})\}$.

(ii) If $\mathcal{P}(\mathcal{F})$ is finite, then $\mathcal{P}(\mathcal{E})$ is also finite.

Since for a given integer $r > 0$ there are finitely many places of F of degree dividing r, if $\mathcal{P}(\mathcal{F})$ is finite, then the set $\mathrm{Supp}(\mathcal{F})$ is also finite. Furthermore, when $\gamma(\mathcal{F}) < \infty$, by Theorem 1.3.2(iv), for any $r \in \mathcal{P}(\mathcal{F})$, we have $\beta_r(\mathcal{F}) > 0$. Moreover, by Theorem 2.3.3, $\gamma(\mathcal{E}) < \infty$, and hence $\beta_s(\mathcal{E}) > 0$ for all $s \in \mathcal{P}(\mathcal{E})$.

By using Proposition 2.1.4, we obtain the following generalization of Lemma 1.3.6.

Lemma 2.1.6. *Let $\mathcal{E}$ be a tower over $\mathbb{F}_q$ and $\mathcal{F}$ be a subtower of $\mathcal{E}$. Then*

$$\beta_s(\mathcal{E}) \leq \sum_{\substack{d\in\mathcal{P}(\mathcal{F})\\ d|s, d\geq \frac{s}{m}}} \frac{d}{s}\beta_d(\mathcal{F}).$$

Proof. We use a similar method as used for the proof of Lemma 1.3.6 (cf. [24, Proposition 7.2.8]). Set

$$m := \min_i \{[E_{j(i)} : \varphi_i(F_i)] | \ \varphi_i : F_i \to E_{j(i)} \text{ is an embedding and } g(F_i) \geq 2\}.$$

Let H_i be the subfield of $E_{j(i)}$ which is uniquely determined by the following properties:

- $\varphi_i(F_i) \subseteq H_i \subseteq E_{j(i)}$,
- $H_i/\varphi_i(F_i)$ is separable, and
- $E_{j(i)}/H_i$ is purely inseparable.

By using the Hurwitz Genus Formula [24] for the extension $H_i/\varphi_i(F_i)$, for any $i \geq 1$, with $g(F_i) \geq 2$, we obtain that

$$g(H_i) - 1 \geq m(g(F_i) - 1).$$

By [24, Proposition 3.10.2(c)], the field H_i is isomorphic to $E_{j(i)}$. Hence, by using the formula (2.2) for $H_i/\varphi_i(F_i)$, for any $s \in \mathbb{N}$,

$$\begin{aligned}\frac{B_s(E_{j(i)})}{g(E_{j(i)}) - 1} &= \frac{B_s(H_i)}{g(H_i)} \leq \frac{1}{m(g(F_i) - 1)} \sum_{\substack{d \in \mathbb{N} \\ d|s, d \geq \frac{s}{m}}} \frac{md}{s} B_d(F_i) \\ &= \sum_{\substack{d \in \mathbb{N} \\ d|s, d \geq \frac{s}{m}}} \frac{d}{s}\left(\frac{B_d(F_i)}{g(F_i) - 1}\right) = \sum_{\substack{d \in \mathbb{N} \\ d|s, d \geq \frac{s}{m}}} \frac{d}{s}\left(\frac{B_d(F_i)}{g(F_i) - 1}\right)\end{aligned}$$

By taking the limit as $i \to \infty$ in this inequality, the lemma follows. □

2.2 Construction of towers with prescribed invariants being positive

We say that a tower $\mathcal{F} = (F_n)_{n \geq 0}$, with $F := F_0$, is *pure*, if for all $P \in \mathbb{P}(F)$ and $r \in \mathbb{N}$, the inequality $\nu_r(P, \mathcal{F}) > 0$ implies $\deg P = r$ and $\nu_s(P, \mathcal{F}) = 0$ for all $s \neq r$. In this section we will prove our main result:

Theorem 2.2.1. *Let $\mathcal{F} = (F_n)_{n \geq 0}$ be a tower over $\mathbb{F}_q$ with a finite support and let $N \subset \mathbb{N}$ be a non-empty finite set. Then there exists a finite separable extension E/F such that $\mathcal{E} := E \cdot \mathcal{F}$ is a tower with the following properties:*

(i) for all $s \in \mathbb{N}$,

$$\nu_s(\mathcal{E}) = \sum_{\substack{f \in N \\ d \in \mathbb{P}(\mathcal{F})}} \frac{f}{s} \sum_{\substack{P \in \mathrm{Supp}(\mathcal{F}) \\ lcm(f \deg P, d) = s}} d \cdot \nu_d(P, \mathcal{F}).$$

Moreover,

$$\mathrm{Supp}(\mathcal{E}) = \big\{Q \in \mathbb{P}(E) : Q \cap F \in \mathrm{Supp}(\mathcal{F})\big\} \ \textit{and} \tag{2.4}$$

$$\mathcal{P}(\mathcal{E}) = \big\{s \in \mathbb{N} : s = lcm(f \deg P, d) \textit{ with } f \in N,\ d \in \mathbb{N},\ P \in \mathrm{Supp}(\mathcal{F})\big\}.$$

(ii) If furthermore $\mathcal{F}/F$ is pure, then for all $s \in \mathbb{N}$,

$$\nu_s(\mathcal{E}) = \sum_{\substack{f\in N,\ d\in \mathbb{P}(\mathcal{F})\\ fd=s}} \nu_d(\mathcal{F}) \qquad \textit{and}$$

$$\mathcal{P}(\mathcal{E}) = \big\{s \in \mathbb{N} : s = fd \textit{ with } f \in N,\ d \in \mathcal{P}(\mathcal{F})\big\}.$$

To be able to prove Theorem 2.2.1, we first give some results which will be used to construct an appropriate extension E/F such that $\mathcal{E} := E \cdot \mathcal{F}$ is a tower over $\mathbb{F}_q$ with certain properties.

Proposition 2.2.2. *Let $F/\mathbb{F}_q$ be a function field, $S \subseteq \mathbb{P}(F)$ a finite set of places of $F/\mathbb{F}_q$ and $R \in \mathbb{P}(F) \setminus S$. Assume that for each $P \in S$ there is given a finite set $N_P \subseteq \mathbb{N}$ such that $\sum_{f\in N_P} f = \sum_{f\in N_Q} f$ for all $P, Q \in S$. Then there is a finite separable extension E of F such that*

(i) $[E : F] = m$ where $m := \sum_{f\in N_P} f$ and R is totally ramified in E.

(ii) For each $P \in S$, $f \in N$, there exists exactly one extension Q of P in $E/\mathbb{F}_q$ with $f(Q|P) = f$.

(iii) There is $y \in E$ such that $E = F(y)$ and $\{1, y, \dots, y^{m-1}\}$ is an integral basis for E/F at all $P \in S$.

Proof. For each $P \in S$, set

$$\varphi_P(T) := \prod_{f\in N_P} g_f(T) = \sum_{k=0}^{m} a_{kP}T^k \in \mathcal{O}_P[T],$$

where $g_f \in \mathcal{O}_P[T]$ is a monic polynomial which is irreducible over $k(P)$ of $\deg g_f = f$. Then by the Weak Approximation Theorem [24], for each $k = 0, \dots, m$, there exist elements $b_1, \dots, b_m \in F$ such that

- $v_P(b_i - a_{iP}) > 0$ for all $i = 1, \dots, m-1$ and $P \in S$, and
- $v_R(b_m) = 0$,
  $gcd(m, v_R(b_0)) = 1$ and either

$$v_R(b_i) \ge v_R(b_0) > 0 \text{ for } i = 1, \dots, m-1 \qquad \text{or}$$

$$v_R(b_0) < 0,\ v_R(b_i) \ge 0 \text{ for } i = 1, \dots, m-1.$$

Note that w.l.o.g. we can take $b_m := 1$. Now we set $\varphi(T) := \sum_{k=0}^{m} b_kT^k \in \bigcap_{P\in S} \mathcal{O}_P[T]$. Then

$$\varphi(T) \equiv \varphi_P(T) \text{ over } k(P) \text{ for } P \in S, \text{ and}$$

by the generalized Eisenstein's Irreducibility Criterion [24] with the place R, the polynomial $\varphi(T)$ is irreducible over F. Set $E := F(y)$ where y is a root of $\varphi(T)$. Hence, $[E : F] = m$ and by the same irreducibility criterion, R is totally ramified in E, and so assertion (i) follows. Then by applying Kummer's Theorem [24], assertion (ii) follows. Note that E/F is separable, since by Kummer's Theorem each $P \in S$ is unramified in E. Assertion (iii) is clear from the factorization of $\varphi(T)$ over $k(P)$. □

Remark 2.2.3. In Proposition 2.2.2, the elements in the set N_P do not need to be distinct if the following holds: for each $P \in S$ and $f \in N_P$, there are monic polynomials $g(T) \in \mathcal{O}_P[T]$ which are pairwise distinct and irreducible over $k(P)$ of $\deg g(T) = f$.

Lemma 2.2.4. *Let E/F and F'/F be finite separable extensions of function fields in some algebraic closure of F. Suppose that $\mathbb{F}_q$ is algebraically closed in F and F', and there is a place P of F that is totally ramified in E/F and unramified in F'/F. Then E/F and F'/F are linearly disjoint and $\mathbb{F}_q$ is algebraically closed in EF'.*

Proof. The linear disjointness follows from the existence of P and Abhyankar's Lemma [24]. Let $L/\mathbb{F}_q$ be a finite extension of $\mathbb{F}_q$. Then P is unramified in the constant field extension $F'L$. Hence, again by applying Abhyankar's Lemma, we obtain that EF'/F' and $F'L/F'$ are linearly disjoint, and so

$$EF' \cap F'L = F'.$$

This gives that $EF' \cap L = \mathbb{F}_q$, as $\mathbb{F}_q$ is algebraically closed in F'. Since this holds for any finite extension $L/\mathbb{F}_q$, we obtain that $\mathbb{F}_q$ is algebraically closed in EF'. □

Lemma 2.2.5. *Let $F/\mathbb{F}_q$ be an algebraic function field and let E, F' and E' be finite extensions of F such that $E' = EF'$. Let Q and P' be places of E and F', respectively, lying above a place P of F. Suppose that there exists a place Q' of E' lying above both Q and P'. Then*

$$e(Q'|P') \leq e(Q|P) \text{ and } k(Q') \supseteq k(Q)k(P').$$

If furthermore $e(Q|P)$ and $e(P'|P)$ are coprime, then

$$e(Q'|P') = e(Q|P) \text{ and } k(Q') = k(Q)k(P').$$

Proof. We first set $k := k(Q)k(P')$, then clearly $k(Q') \supseteq k$. Consider the constant field extensions $F_1 := Fk, E_1 := Ek, F'_1 = F'k$ and $E'_1 := E'k$. Let $Q'_1 \in \mathbb{P}(E'_1)$ be an extension of Q'. Then obviously $P_1 := Q'_1 \cap F$, $Q_1 := Q'_1 \cap E$, and $P'_1 := Q'_1 \cap F'$ lie above P, Q and P', respectively. We denote the completions of F_1, E_1, F'_1 and E'_1 with respect to P_1, Q_1, P'_1 and Q'_1 by the symbol $\hat{}$. As Q'_1 is lying above P_1,Q_1 and P'_1, we can regard $\hat{F}_1, \hat{E}_1, \hat{F}'_1$ as subfields of $\hat{E}'_1$ such that $\hat{E}'_1 = \hat{E}_1\hat{F}'_1$. We note that by [21, p.30, Theorem 1], the corresponding ramification indices and the relative degrees are preserved by completion. Moreover, by [24, Theorem 3.6.3], the corresponding ramification indices do not change after taking the constant field extensions. Consequently, we obtain that

$$f(\hat{Q}_1|\hat{P}_1) = f(\hat{P'}_1|\hat{P}_1) = f(Q_1|P_1) = f(P'_1|P_1) = 1.$$

Thus,

$$e(\hat{Q}'_1|\hat{P}'_1)e(\hat{P}'_1|\hat{P}_1) \leq [\hat{E}'_1 : \hat{F}_1] \leq [\hat{E}_1 : \hat{F}_1] \cdot [\hat{F}'_1 : \hat{F}_1] = e(\hat{Q}_1|\hat{P}_1)e(\hat{P}'_1|\hat{P}_1). \tag{2.5}$$

Therefore,

$$e(Q'|P') = e(\hat{Q}'_1|\hat{P}'_1) \leq e(\hat{Q}_1|\hat{P}_1) = e(Q|P).$$

Now suppose that $e(Q|P)$ and $e(P'|P))$ are coprime. By Abhyankar's Lemma [24], we get

$$e(Q'|P') = e(Q|P) \text{ and } e(Q'|Q) = e(P'|P).$$

Thus, in Eq.(2.5), equalities hold, and so

$$e(\hat{Q}'_1|\hat{P}_1) = [\hat{E}'_1 : \hat{F}_1] = e(\hat{Q}'_1|\hat{P}_1)f(\hat{Q}'_1|\hat{P}_1).$$

Hence,

$$1 = f(\hat{Q}_1'|\hat{P}_1 = [k(\hat{Q}_1') : k(\hat{P}_1)] = [k(Q_1') : k(P_1)].$$

This means that $k(Q_1') = k(P_1) = k$. As $k(Q') \supseteq k$ and by [24, Theorem 3.6.3(g)], $k(Q_1') = k \cdot k(Q')$, we obtain that $k(Q') = k$. □

Lemma 2.2.6. *Let $F/\mathbb{F}_q$ be an algebraic function field and let E, F' and E' be finite separable extensions of F such that $E' = EF'$. Suppose that E/F and F'/F are linearly disjoint. Set $E := F(y)$, $m := [E : F]$, and consider the set*

$$M := \{P \in \mathbb{P}(F) : \{1, y, \dots, y^{m-1}\} \text{ is an integral basis for } E/F \text{ at } P\}.$$

Let $P \in M, P' \in \mathbb{P}(F')$ with $P'|P$. Suppose that $e(P'|P)$ is coprime to any ramification index of P in E. Then above P' and each $Q \in \mathbb{P}(E)$ with $Q|P$ there are exactly $\gcd(f(Q|P), f(P'|P))$ places $Q' \in \mathbb{P}(E')$. Moreover, for each such place Q',

$$f(Q'|P) = [k(Q)k(P') : k(P)]. \tag{2.6}$$

Proof. We first note that by [24, Theorem 3.3.6], the set M contains almost all places of F. Fix a place $P \in M$ with an extension P' in E' satisfying the given assumption. Let $\varphi(T) \in \mathcal{O}_P[T]$ be the minimal polynomial of y over F and

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \bar{g}_i(T)^{\epsilon_i} \tag{2.7}$$

be the decomposition of $\bar{\varphi}(T)$ into irreducible factors over $k(P)$. By Kummer's Theorem [24], for $1 \le i \le r$, there are places $Q_i \in \mathbb{P}(E)$ satisfying

$$Q_i|P,\ g_i(y) \in Q_i,\ e(Q_i|P) = \epsilon_i,\ f(Q_i|P) = \deg g_i, \tag{2.8}$$

and these are all extensions of P in E. For each $1 \le i \le r$, set

$$k_i := [k(Q_i)k(P') : k(P')]. \tag{2.9}$$

Then as $\bar{g}_i(T)$ is irreducible over $k(P)$, it is separable, and so

$$\bar{g}_i(T)^{\epsilon_i} = \prod_{j=1}^{s_i} \bar{h}_{ij}(T)^{\epsilon_i} \in k(P')[T],$$

where $\bar{h}_{i1}(T), \dots, \bar{h}_{is_i}(T)$ are pairwise distinct, monic, irreducible polynomials in $k(P')[T]$ of $\deg \bar{h}_{ij}(T) = k_i$ for all $1 \le j \le s_i$, and

$$s_i = \gcd(f(Q_i|P), f(P'|P)), \tag{2.10}$$

Again by Kummer's Theorem, for $1 \le j \le s_i$, there are places $Q_{ij} \in \mathbb{P}(E')$ satisfying

$$Q_{ij}|P',\ h_{ij}(y) \in Q_{ij},\ f(Q_{ij}|P') \ge \deg h_{ij} = k_i. \tag{2.11}$$

Moreover, as $h_{ij}(T) \mid g_i(T)$, it follows that each $Q_{ij}|Q_i$. Since by assumption $e(Q_i|P)$ and $e(P'|P)$ are coprime, by Lemma 2.2.5, we have

$$k(Q_{ij}) = k(Q_i)k(P').$$

Hence,

$$f(Q_{ij}|P') = [k(Q_{ij}) : k(P')] = [k(Q_i)k(P') : k(P')] = k_i.$$

Now we just need to prove that Q_{ij}'s are all extensions of Q_i and P', then by (2.10) the lemma follows. By Abhyankar's Lemma [24], we have that

$$e(Q_{ij}|P') = e(Q_i|P) = \epsilon_i \text{ for all } 1 \leq j \leq s_i. \tag{2.12}$$

As this holds for all $1 \leq i \leq r$, by using (2.8), (2.11) and (2.12), we obtain that

$$\begin{aligned}
[E : F] &= \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P}} e(Q|P) f(Q|P) = \sum_{i=1}^{r} \epsilon_i \deg g_i(T) = \sum_{i=1}^{r} \epsilon_i \sum_{j=1}^{s_i} k_i \\
&= \sum_{i=1}^{r} \sum_{j=1}^{s_i} e(Q_{ij}|P') f(Q_{ij}|P') \leq \sum_{\substack{Q' \in \mathbb{P}(E') \\ Q'|P'}} e(Q'|P') f(Q'|P') = [E' : F'].
\end{aligned}$$

Hence, as $[E : F] = [E' : F']$, the above equality holds. Then for each $1 \leq i \leq r$, we obtain that $Q_{i1}, \ldots Q_{is_i}$ are all places of E' lying over Q_i and P'. □

Theorem 2.2.7. *Suppose that $\mathcal{E} := E \cdot \mathcal{F}$ is a tower of $\mathcal{F}/\mathbb{F}_q$. With the same notations as in Lemma 2.2.6, let $P \in M$, and suppose that $e(Q|P)$ is coprime to any ramification index of P in $\mathcal{F}$, for all $Q \in \mathbb{P}(E)$ with $Q|P$. Then for any $Q|P$ and $s \geq 1$,*

$$\nu_s(Q, \mathcal{E}) = \frac{f(Q|P)}{s} \sum_{\substack{d \in \mathbb{N} \\ lcm(\deg Q, d) = s}} d \cdot \nu_d(P, \mathcal{F}).$$

Proof. Set $E' := E_n$, $F' := F_n$, for any $n \geq 1$. By Lemma 2.2.6, there are $\gcd(f(Q|P), f(P'|P))$ places $Q' \in \mathbb{P}(E')$ above any fixed Q and P' lying over $P \in M$, and moreover for each such place Q', one has

$$f(Q'|P) = [k(Q)k(P') : k(P)].$$

In particular, $s := f(Q'|P) = \operatorname{lcm}((f(Q|P), f(P'|P))$, and so $d := f(P'|P)$ divides s. Conversely, any P' lying over P with $d = f(P'|P)$ such that $s = \operatorname{lcm}(f(Q|P), d)$ has at least one extension Q' in E' with $f(Q'|P) = s$. Hence,

$$\begin{aligned}
\sum_{\substack{Q'|Q \\ f(Q'|P)=s}} 1 &= \sum_{\substack{d \in \mathbb{N} \\ \operatorname{lcm}(f(Q|P),d)=s}} \sum_{\substack{P'|P \\ f(P'|P)=d}} \sum_{\substack{Q'|P' \\ Q'|Q}} 1 \\
&= \sum_{\substack{d \in \mathbb{N} \\ \operatorname{lcm}(f(Q|P),d))=s}} \sum_{\substack{P'|P \\ f(P'|P)=d}} \gcd(f(Q|P), d) \\
&= \sum_{\substack{d \in \mathbb{N} \\ \operatorname{lcm}(f(Q|P),d)=s}} \frac{d \cdot f(Q|P)}{s} \sum_{\substack{P'|P \\ f(P'|P)=d}} 1.
\end{aligned}$$

Since $\operatorname{lcm}(af, ad) = as$ if and only if $\operatorname{lcm}(f, d) = s$, we can write the summation indices in terms of absolute degrees instead of relative degrees with respect to P as base place.

Then we get

$$\begin{aligned} B_s(Q,E') &= \sum_{\substack{Q'|Q \\ \deg Q'=s}} 1 = \frac{f(Q|P)}{s} \sum_{\substack{d\in\mathbb{N} \\ \operatorname{lcm}(\deg Q,d)=s}} d \sum_{\substack{P'|P \\ \deg P'=d}} 1 \\ &= \frac{f(Q|P)}{s} \sum_{\substack{d\in\mathbb{N} \\ \operatorname{lcm}(\deg Q,d)=s}} d\cdot B_d(P,F'). \end{aligned}$$

Dividing this equation by $[E':E]$ and then taking the limit as $n\to\infty$ proves the theorem. $\square$

Proof of Theorem 2.2.1. It is enough to prove (i), then (ii) is immediate. By applying Lemma 2.2.4 and Proposition 2.2.2 with the set $S := \mathrm{Supp}(\mathcal{F})$ and $N_P := N$ for each $P \in \mathrm{Supp}(\mathcal{F})$, one can construct an extension E/F such that the following hold:

(i) $\mathcal{E} := E\cdot\mathcal{F}$ is a tower of $\mathcal{F}$ with E/F.

(ii) For each $f\in N$, any $P\in S$ has exactly one extension Q in E with $f(Q|P)=f$ and these are the only extensions of P in E.

(iii) All places $P\in S$ are unramified in E and S is contained in the set M defined in Lemma 2.2.6.

By Corollary 2.1.5 and the construction of E/F, and Theorem 2.2.7, the statement (2.4) is immediate. Therefore, for any $s\geq 1$, by using Theorems 2.2.7 and 1.3.2(v), we get

$$\nu_s(\mathcal{E}) = \sum_{\substack{f\in N, d\in\mathbb{N} \\ P\in S}} \sum_{\substack{f(Q|P)=f \\ \operatorname{lcm}(\deg Q,d)=s}} \nu_s(Q,\mathcal{E}) = \sum_{\substack{f\in N \\ d\in\mathbb{N}}} \frac{f}{s} \sum_{\substack{P\in S \\ \operatorname{lcm}(f\deg P,d)=s}} d\cdot\nu_d(P,\mathcal{F}).$$

$\square$

We note here that when $\mathrm{Supp}(\mathcal{F})$ is infinite, one can apply Theorem 2.2.1 with a finite subset $S\subseteq \mathrm{Supp}(\mathcal{F})$ and get a finite subset of $\mathrm{Supp}(\mathcal{E})$.

As there are many towers over a given finite field $\mathbb{F}_q$ with non-empty finite support, such as many of the class field towers and the recursive towers (see Chapter 3), Theorem 2.2.1 can be often applied. More specifically, let $\mathcal{F}$ be a tower over $\mathbb{F}_{q^2}$ attaining the Drinfeld-Vladut bound of order one. Note that there are many such towers, for instance see Section 3.2. Then obviously $\mathcal{P}(\mathcal{F})=\{1\}$. Hence, by using Theorem 2.2.1(ii) one gets immediately the following consequence:

Corollary 2.2.8. *For any given finite set $N\subseteq\mathbb{N}$, there exists a tower of function fields $\mathcal{E}$ over $\mathbb{F}_{q^2}$ with*

$$\mathcal{P}(\mathcal{E}) = N.$$

Proof. Consider a tower $\mathcal{F}=(F_n)_{n\geq 0}$ over $\mathbb{F}_{q^2}$ with $\mathcal{P}(\mathcal{F})=\{1\}$. Then by Theorem 2.2.1(ii), there is an extension E of F_0 such that $\mathcal{E}:=E\cdot\mathcal{F}$ is a tower over $\mathbb{F}_{q^2}$ with $\mathcal{P}(\mathcal{E})=N$. $\square$

Corollary 2.2.9. *For any given set $M\subsetneq\mathbb{N}$, there exists an asymptotically good tower of function fields $\mathcal{E}$ over $\mathbb{F}_{q^2}$ with*

$$\mathcal{P}(\mathcal{E})\cap M=\emptyset.$$

Proof. Let $N \subseteq \mathbb{N} \setminus M$ be a finite set. By Corollary 2.2.8, there exists a tower $\mathcal{E}$ over $\mathbb{F}_{q^2}$ with $\mathcal{P}(\mathcal{E}) = N$, and hence the corollary follows. $\square$

Remark 2.2.10. For a finite field $\mathbb{F}_q$, when q is non-prime, there are many recursive towers $\mathcal{F}/\mathbb{F}_q$ with $\beta_1(\mathcal{F}) > 0$ (for instance see Chapter 3). Hence, for any finite set $N \subseteq \mathbb{N}$, by using Theorem 2.2.1, one can construct many recursive towers $\mathcal{E}$ over $\mathbb{F}_q$ with

$$\mathcal{P}(\mathcal{E}) = \{r \in \mathbb{N} : \beta_r(\mathcal{E}) > 0\} \supseteq N.$$

In Chapter 3 we will construct some such towers $\mathcal{E}$ over $\mathbb{F}_q$. However, in the case that q is a prime, the existence of recursive towers $\mathcal{F}$ over $\mathbb{F}_q$ with $\beta_1(\mathcal{F}) > 0$ is not known.

2.3 Computation of the genus of a tower

Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over a finite field $\mathbb{F}_q$ and E be a finite separable extension of F_0. In this section we suppose that $\mathcal{E} = (EF_n)_{n\geq 0}$ is a tower over $\mathbb{F}_q$ and estimate the genus $\gamma(\mathcal{E})$ of the tower $\mathcal{E}$, under certain conditions.

Definition 2.3.1. Let $\mathcal{F} = (F_n)_{n\geq 0}$ be a tower over $\mathbb{F}_q$. Then the set

$$R(\mathcal{F}) := \{P \in \mathbb{P}(F_0) : \ P \text{ is ramified in } F_n \text{ for some } n \geq 0\}.$$

is called the *ramification locus* of $\mathcal{F}$.

The proof of the following lemma is omitted; for the proof see [11, Lemma 3.4].

Lemma 2.3.2. *Suppose that the set $R(\mathcal{F})$ is finite. For any $n \geq 1$, set*

$$A_n := \sum_{\substack{P\in\mathbb{P}(F_n)\\ P\cap F\in R(\mathcal{F})}} P.$$

Then the following limit exists:

$$\alpha(\mathcal{F}) := \lim_{n\to\infty} \frac{\deg A_n}{[F_n : F]}.$$

Theorem 2.3.3. *For the genus $\gamma(\mathcal{E})$ of the tower $\mathcal{E}$ the following hold:*

(i) Set $m := [E : F]$. Then $m \cdot \gamma(\mathcal{F}) \leq \gamma(\mathcal{E}) \leq g(E) - 1 + m(1 - g(F) + \gamma(\mathcal{F}))$. If furthermore all $P \in R$ are unramified in E, then

$$\gamma(\mathcal{E}) = g(E) - 1 + m(1 - g(F) + \gamma(\mathcal{F})).$$

(ii) If R is finite, $\alpha(\mathcal{F}) = 0$ and all $P \in R$ are tame in E, then

$$\gamma(\mathcal{E}) = g(E) - 1 - s/2 + m(1 - g(F) + \gamma(\mathcal{F})),$$

where $s := \sum_{\substack{Q\in\mathbb{P}(E)\\ Q\cap F\in R}} d(Q|Q\cap F) \cdot \deg Q.$

For the proof of Theorem 2.3.3 we need the following lemma:

Lemma 2.3.4. *Let $F/\mathbb{F}_q$ be a function field and let E, F' and E' be finite separable extensions of F such that $E' = EF'$. Set $n := [F' : F]$ and $m := [E : F]$. Then*

(i) for any $Q' \in \mathbb{P}(E')$ with $P' := Q' \cap F'$, $Q := Q' \cap E$, and $P := Q' \cap F$, one has

$$d(Q'|P') \leq e(Q'|Q)d(Q|P).$$

(ii) Suppose that E/F and F'/F are linearly disjoint. Then

$$m(g(F') - 1) + 1 \leq g(E') \leq mg(F') + ng(E) - nmg(F) + (n-1)(m-1).$$

In order to prove Lemma 2.3.4, we will use the following proposition. Its proof follows from [21, p.52, Proposition 10], [21, p.57, Proposition 12], and [21, p.56, Corollary 2].

Proposition 2.3.5. *Let $K/\mathbb{F}_q$ be a function field and L be a finite separable extension of K with a place Q and $P := Q \cap K$. Consider the completions $\hat{K}$, $\hat{L}$ of the fields K, L with respect to the places P, Q, respectively. Then one has*

(i) $\mathcal{O}_{\hat{Q}} = \mathcal{O}_{\hat{P}}[\alpha]$ for some $\alpha \in \hat{L}$.

(ii) $d(Q|P) = d(\hat{Q}|\hat{P}) = v_{\hat{Q}}(f'(\alpha))$, where $f(T) \in \mathcal{O}_{\hat{P}}[T]$ is the minimal polynomial of α over $\mathcal{O}_{\hat{P}}$.

Proof of Lemma 2.3.4.

(i) First we fix a place Q' with the restrictions P, Q, and P' to the fields F, E and F', respectively. Consider the completions $\hat{F}$, $\hat{E}$, $\hat{F'}$ and $\hat{E'}$ with respect to the places P, Q, P' and Q', respectively. By Proposition 2.3.5(ii), the different is preserved by completion, and so it suffices to prove it in the completed setting. By Proposition 2.3.5(i), there is an element $\alpha \in \hat{E}$ such that $\mathcal{O}_{\hat{Q}} = \mathcal{O}_{\hat{P}}[\alpha]$. Let $f(T) \in \mathcal{O}_{\hat{P}}[T]$, (resp. $g(T) \in \mathcal{O}_{\hat{P'}}[T]$) be the minimal polynomial of α over $\hat{F}$ (resp. over $\hat{F'}$). By the Lemma of Gauss [14], we can write $f(T) = g(T)h(T)$ in $\mathcal{O}_{\hat{P'}}[T]$, then

$$f'(\alpha) = g'(\alpha)h(\alpha) + h'(\alpha)g(\alpha) = g'(\alpha)h(\alpha).$$

Thus, by applying [24, Theorem 3.5.10(a)] and Proposition 2.3.5(ii), the desired result follows:

$$d(\hat{Q'}|\hat{P'}) \leq v_{\hat{Q'}}(g'(\alpha)) \leq v_{\hat{Q'}}(f'(\alpha)) = e(\hat{Q'}|\hat{Q})v_{\hat{Q}}(f'(\alpha)) = e(\hat{Q'}|\hat{Q})d(\hat{Q}|\hat{P}).$$

Note that by [21, p.30, Theorem 1], the ramification indices are preserved by completion.

(ii) By using the Hurwitz Genus Formula [24] for the extension E'/F', we obtain that

$$g(E') \geq m(g(F') - 1) + 1.$$

Next, we prove the second inequality. By using (i), we have that

$$\begin{aligned} \mathrm{Diff}(E'/F') &= \sum_{P' \in \mathbb{P}(F')} \sum_{Q'|P'} d(Q'|P')Q' \leq \sum_{\substack{Q \in \mathbb{P}(E) \\ P = Q \cap F}} \sum_{Q'|Q} e(Q'|Q)d(Q|P)Q' \\ &= \mathrm{Con}_{E'/E}(\mathrm{Diff}(E/F)), \end{aligned}$$

where $\mathrm{Con}_{E'/E}$ is the conorm map and Diff is the different. Hence, by [24, Corollary 3.1.14],

$$\deg \mathrm{Diff}(E'/F') \leq [E' : E] \deg \mathrm{Diff}(E/F). \tag{2.13}$$

By using the Hurwitz Genus Formula for the extension E/F, we obtain that

$$\deg \mathrm{Diff}(E/F) = 2g(E) - 2 - m(2g(F) - 2). \tag{2.14}$$

By using (2.13), (2.14) and the Hurwitz Genus Formula for the extensions E'/F', it follows that

$$\begin{aligned} 2g(E') - 2 &= m(2g(F') - 2) + \deg \mathrm{Diff}(E'/F') \\ &\leq m(2g(F') - 2) + n \deg \mathrm{Diff}(E/F) \\ &= m(2g(F') - 2) + n\big(2g(E) - 2 - m(2g(F) - 2)\big) \\ &= 2[mg(F') - m + ng(E) - n - nmg(F) + nm], \end{aligned}$$

Therefore, the second inequality follows. □

Proof of Theorem 2.3.3.

(i) By applying Lemma 2.3.4(ii), with $E' := E_n$, $F' := F_n$, for any $n \geq 1$, we have that

$$m(g(F') - 1) \leq g(E') \leq mg(F') + [F' : F]g(E) - m[F' : F]g(F) + ([F' : F] - 1)(m - 1).$$

Dividing both sides of those inequalities by $[E' : E] = [F' : F]$, and then taking the limit as $n \to \infty$ gives the first part of the assertion.

Now assume that all places $P \in R(\mathcal{F})$ are unramified in E. For simplicity, we first denote by P (resp. Q, P', Q') the places of F (resp. E, F_n, E_n), and set $R := R(\mathcal{F})$. The Hurwitz Genus Formula for the extension E_n/F yields that

$$2g(E_n) - 2 = [E_n : F](2g(F) - 2) + s_1 + s_2, \tag{2.15}$$

where

$$s_1 := \sum_{P \notin R} \sum_{Q'|P} d(Q'|P) \cdot \deg Q' \quad \text{and} \quad s_2 := \sum_{P \in R} \sum_{Q'|P} d(Q'|P) \cdot \deg Q'.$$

By applying the transitivity of the different in $F \subseteq E \subseteq E_n$, we obtain that

$$\begin{aligned} s_1 &= \sum_{P \notin R} \sum_{Q|P} \sum_{Q'|Q} (e(Q'|Q) \cdot d(Q|P) + d(Q'|Q)) \cdot \deg Q' \\ &= \sum_{P \notin R} \sum_{Q|P} \sum_{Q'|Q} d(Q|P) \cdot f(Q'|Q) \cdot \deg Q \quad \text{(by the Fundamental Equality)} \\ &= [E_n : E] \cdot \sum_{P \notin R} \sum_{Q|P} d(Q|P) \cdot \deg Q \\ &= [E_n : E] \cdot \deg \mathrm{Diff}(E/F). \end{aligned}$$

Next, we apply the transitivity of the different in $F \subseteq F_n \subseteq E_n$:

$$\begin{aligned} s_2 &= \sum_{P \in R} \sum_{P'|P} \sum_{Q'|P'} (e(Q'|P') \cdot d(P'|P) + d(Q'|P')) \cdot \deg Q' \\ &= \sum_{P \in R} \sum_{P'|P} \sum_{Q'|P'} d(P'|P) \cdot f(Q'|P') \cdot \deg P' \\ &= [E : F] \cdot \sum_{P \in R} \sum_{P'|P} d(P'|P) \cdot \deg P' \quad \text{(by the Fundamental Equality)} \\ &= [E : F] \cdot \deg \mathrm{Diff}(F_n/F). \end{aligned}$$

Now by substituting s_1 and s_2 in (2.15), we obtain that

$$\begin{aligned}
2g(E_n) - 2 &= [E_n : F] \cdot (2g(F) - 2) + [E_n : E] \cdot \deg \mathrm{Diff}(E/F) \\
&+ [E : F] \cdot \deg \mathrm{Diff}(F_n/F) \\
&= [E_n : F] \cdot (2g(F) - 2) + [E_n : E] \cdot (2g(E) - 2 - [E : F] \cdot (2g(F) - 2)) \\
&+ [E : F] \cdot (2g(F_n) - 2 - [F_n : F] \cdot (2g(F) - 2))\,.
\end{aligned}$$

Dividing both of the sides of this equation by $2 \cdot [E_n : E]$, and letting $n \to \infty$, we obtain that

$$\begin{aligned}
\gamma(\mathcal{E}) &= [E : F] \cdot (g(F) - 1) + g(E) - 1 - [E : F] \cdot (g(F) - 1) \\
&+ [E : F] \cdot (\gamma(\mathcal{F}) - g(F) + 1) \\
&= g(E) - 1 + [E : F] \cdot (\gamma(\mathcal{F}) - g(F) + 1)\,.
\end{aligned}$$

(ii) For the proof see [11, Theorem 3.6]. The proof is similar to our proof for the second part of assertion (i). □

Remark 2.3.6. Let $K/\mathbb{F}_q$ be a function field and K_1, K_2 be two subfields of K. Suppose that $K = K_1K_2$ and $[K : K_i] = n_i$ for $i = 1, 2$. Then Castelnouvo's Inequality [24] gives the following bound for the genus $g(K)$ of K:

$$g(K) \leq n_1 g(K_1) + n_2 g(K_2) + (n_1 - 1)(n_2 - 1).$$

In Theorem 2.3.3, when $g(F) = 0$, the equality in Castelnouvo's Inequality holds for the function fields $E/\mathbb{F}_q$ and $F_n/\mathbb{F}_q$ with their compositum $E_n = EF_n$.

Remark 2.3.7. In Theorem 2.3.3(ii), if $\alpha(\mathcal{F})$ is not zero, then

$$\gamma(\mathcal{E}) \leq g(E) - 1 - s/2 + [E : F](1 - g(F) + s + \gamma(\mathcal{F})), \tag{2.16}$$

where $s := \sum_{P \in R(\mathcal{F})} \deg P$.

However, the bound (2.16) is not better than the one obtained by using Castelnouvo's Inequality for E, F_n and E_n, which yields that

$$\gamma(\mathcal{E}) \leq g(E) - 1 + [E : F](1 + \gamma(\mathcal{F})).$$

A tower $\mathcal{F} = (F_n)_{n \geq 0}$ is called *tame* if F_{n+1}/F_n is a tame extension for all $n \geq 0$.

Lemma 2.3.8. *Suppose that $\mathcal{F}$ is a tame tower. Then the tower $\mathcal{E}$ is also tame, and hence*

$$\gamma(\mathcal{E}) \leq \frac{2g(E) - 2 + s}{2} \quad \text{where } s := \sum_{P \in R(\mathcal{E})} \deg P. \tag{2.17}$$

Proof. By Abhyankar's Lemma [24], it is clear that the tower $\mathcal{E}$ is tame. Then by [11, Theorem 2.1],the ineaulity (2.17) holds. □

2.4 Towers with infinitely many positive invariants

In this section we investigate the situation where we can estimate $\nu_r(\mathcal{F})$ for infinitely many $r \geq 1$.

Theorem 2.4.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p. Then there is a tower $\mathcal{F}$ over $\mathbb{F}_q$ and a strictly increasing sequence $(k_i)_{i\geq 0}$ of positive integers with $k_0 := 1$ such that*

$$\nu_{k_i}(\mathcal{F}) \geq \frac{1}{p^i} \text{ for all } i \geq 0.$$

Proof. Let $F_0 := \mathbb{F}_q(x_0)$ be the rational function field. Set

$$Q_0 := (x_0 = \infty),\ S_0 := \{P_0\} \text{ where } P_0 := (x_0 = 0),\ \text{and } k_0 := 1.$$

Choose an element $z_0 \in F_0$ with the following properties:

$$z_0(P) = 0 \text{ for } P \in S_0, \text{ and } z_0 \text{ has a simple pole at } Q_0.$$

Note that by the Weak Approximation Theorem [24] such an element z_0 always exists. Let $F_1 := F_0(x_1)$ where x_1 satisfies the equation

$$x_1^p - x_1 = z_0.$$

Then Q_0 is totally ramified in F_1, and hence $\mathbb{F}_q$ is algebraically closed in F_1. Denote by Q_1 the place of F_1 lying above Q_0. Set

$$S_1 := \{P \in \mathbb{P}(F_1) : P \cap F_0 \in S_0\} \cup \{P_1\},$$

where $P_1 \in \mathbb{P}(F_1)$ of $\deg P_1 = k_1$ for some $k_1 > 1$. Next, choose an element $z_1 \in F_1$ such that

$$z_1(P) = 0 \text{ for all } P \in S_1, \text{ and } z_1 \text{ has a simple pole at } Q_1.$$

Let $F_2 := F_1(x_2)$ where x_2 satisfies the equation

$$x_2^p - x_2 = z_1.$$

Then Q_1 is totally ramified in F_2, and so $\mathbb{F}_q$ is algebraically closed in F_2. We continue on this process inductively for $n \geq 2$. Set

$$S_{n-1} := \{P \in \mathbb{P}(F_{n-1}) : P \cap F_{n-2} \in S_{n-2}\} \cup \{P_{n-1}\}$$

where $P_{n-1} \in \mathbb{P}(F_{n-1})$ of $\deg P_{n-1} = k_{n-1}$ for some $k_{n-1} > k_{n-2}$. Choose an element $z_{n-1} \in F_{n-1}$ such that the following hold:

(i) $z_{n-1}(P) = 0$ for all $P \in S_{n-1}$,

(ii) z_{n-1} has a simple pole at Q_{n-1} where $Q_{n-1}|Q_{n-2}$.

Let $F_n := F_{n-1}(x_n)$ where x_n satisfies the following equation:

$$x_n^p - x_n = z_{n-1}.$$

Then Q_{n-1} is totally ramified in F_n, and hence $\mathbb{F}_q$ is algebraically closed in F_n.

Now it follows from the construction of $F_n/\mathbb{F}_q$, for $n \geq 0$, that the sequence $\mathcal{F} := (F_n)_{n\geq 0}$ is a tower over $\mathbb{F}_q$ with $[F_n : F_{n-1}] = p$ for all $n \geq 0$. Moreover, for all $i \geq 0$, by applying Kummer's Theorem [24], each place $P \in S_i$ splits in F_n, for any sufficiently large $n \geq 1$. Thus, for all $i \geq 0$, we obtain that

$$B_{k_i}(F_n) \geq [F_n : F_i] = p^{n-i},\ \text{and so}\ \nu_{k_i}(\mathcal{F}) \geq \frac{1}{p^i}.$$

□

Remark 2.4.2. It is not yet known if there exist towers of function fields over finite fields with infinitely many β_r being positive.

2.5 Towers with all invariants being zero

For any tower $\mathcal{F}/\mathbb{F}_q$, it is clear that when either the genus $\gamma(\mathcal{F})$ of $\mathcal{F}$ is infinite or $\nu_r(\mathcal{F}) = 0$, the invariants $\beta_r(\mathcal{F})$ are all zero, for any $r \geq 1$. We know that there are many towers with infinite genus. For instance, see Lemma 4.1.10. We now prove the existence of towers with $\nu_r(\mathcal{F}) = 0$ for all $r \geq 1$. First, recall that for any function field extension E/F, if $Q \in \mathbb{P}(E)$ lies above $P \in \mathbb{P}(F)$, then $\deg P$ divides $\deg Q$.

Lemma 2.5.1. *For any finite field $\mathbb{F}_q$, there exists a tower $\mathcal{F}$ over $\mathbb{F}_q$ with*

$$\nu_r(\mathcal{F}) = 0 \textit{ for all } r \in \mathbb{N}.$$

Proof. The proof is similar to that of Theorem 2.4.1. Let p be the characteristic of $\mathbb{F}_q$. We first claim that there exists an element $\alpha_1 \in F_q^*$ such that the polynomial $T^p - T - \alpha_1$ is irreducible over $\mathbb{F}_q$.
Proof of the claim: We first recall that for any $a \in \mathbb{F}_q$, the polynomial $T^p - T - a$ is irreducible over $\mathbb{F}_q$ if and only if it has no root in $\mathbb{F}_q$. Consider the map $\gamma : \mathbb{F}_q \to \mathbb{F}_q$ with $\gamma(b) = b^p - b$ for any $b \in \mathbb{F}_q$. This map is clearly $\mathbb{F}_p$-linear and its kernel is $\operatorname{Ker}\gamma = \mathbb{F}_p$. Hence, γ is not surjective, and so there exists an α_1 such that the polynomial $T^p - T - \alpha_1$ has no roots in $\mathbb{F}_q$. Then the claim follows.

Now let $F_0 := \mathbb{F}_q(x_0)$ be the rational function field and set

$$Q_0 := (x_0 = \infty), \quad S_0 := \{P \in \mathbb{P}(F_0) \setminus \{Q_0\} : \deg P = 1\}.$$

Choose an element $z_0 \in F_0$ with the following properties:

$$z_0(P) = \alpha_1 \text{ for all } P \in S_0 \text{ and } Q_0 \text{ is a simple pole of } z_0.$$

Let $F_1 := F_0(z_0)$ with

$$x_1^p - x_1 = z_0. \tag{2.18}$$

Then Q_0 is totally ramified in F_1 and hence $\mathbb{F}_q$ is algebraically closed in F_1. Moreover, it follows from Kummer's Theorem [24] and our claim that all places $P \in S_0$ are inert in F_1. Thus,

$$B_1(F_1) = 1.$$

Next, denote by Q_1 the extension of Q_0 in F_1 and set

$$S_1 := \{P \in \mathbb{P}(F_1) : \deg P = 2\}.$$

By using our claim, there exists an element $\alpha_2 \in \mathbb{F}_{q^2}$ such that the polynomial $T^p - T - \alpha_2$ is irreducible over $\mathbb{F}_{q^2}$. Choose an element $z_1 \in F_1$ such that the following hold:

$$z_1(P) = \alpha_2 \text{ for all } P \in S_1 \text{ and } z_2 \text{ has a simple pole at } Q_1.$$

Let $F_2 := F_1(x_2)$ where x_2 satisfies the equation

$$x_2^p - x_2 = z_1.$$

Then Q_1 is totally ramified in F_n, and so $\mathbb{F}_q$ is algebraically closed in F_2. By Kummer's Theorem, all $P \in S_1$ are inert in F_2. Hence,

$$B_2(F_2) = 1 \quad \text{and} \quad B_2(F_2) = 0.$$

We proceed by induction over n. Suppose that there is an extension F_{n-1}/F_0, with $n \geq 3$, such that

(a) $B_1(F_{n-1}) = 1$ and $B_r(F_{n-1}) = 0$ for all $2 \leq r \leq n-1$,

(b) Q_0 is totally ramified in F_{n-1},

(c) $\mathbb{F}_q$ is algebraically closed in F_{n-1}.

Let $Q_{n-1} \in \mathbb{P}(F_{n-1})$ be the extension of Q_0 in F_{n-1}. Set

$$S_{n-1} := \{P \in \mathbb{P}(F_{n-1}) : \deg P = n\}.$$

Using our claim, there exists an element $\alpha_n \in \mathbb{F}_{q^n}^*$ such that the polynomial $T^p - T - \alpha_n$ is irreducible over $\mathbb{F}_q^n$. Choose an element $z_{n-1} \in F_{n-1}$ with the following properties:

$$z_{n-1}(P) = \alpha_n \text{ for all } P \in S_{n-1} \text{ and } z_{n-1} \text{ has a simple pole at } Q_{n-1}.$$

Let $F_n := F_{n-1}(x_n)$ with

$$x_n^p - x_n = z_{n-1}.$$

Then Q_{n-1} is totally ramified in F_n, and so $\mathbb{F}_q$ is algebraically closed in F_n. By Kummer's Theorem, all $P \in S_{n-1}$ are inert in F_n (notice that $k(P) = \mathbb{F}_{q^n}$ for all $P \in S_{n-1}$). Hence, by combining this observation with (a), we get that

$$B_1(F_n) = 1 \quad \text{and} \quad B_r(F_n) = 0 \text{ for all } 2 \leq r \leq n.$$

Now by the construction of $F_n/\mathbb{F}_q$, it follows that the sequence $\mathcal{F} := (F_n)_{n \geq 0}$ is a tower over $\mathbb{F}_q$ with

$$\nu_r(\mathcal{F}) = 0 \text{ for all } r \in \mathbb{N}.$$

□

3

Examples

In this chapter we are interested in the following problems concerning the invariants of a tower over any finite field $\mathbb{F}_q$.
Problem 1. For a given tower (an asymptotically exact sequence) $\mathcal{F}$ over $\mathbb{F}_q$, describe the set of positive parameters $\mathcal{P}(\mathcal{F}) = \{r \in \mathbb{N} : \beta_r(\mathcal{F}) > 0\}$.
Problem 2. Describe the set of possible values of the deficiency for towers (asymptotically exact sequences) of function fields over $\mathbb{F}_q$.
Problem 3. Find towers (asymptotically exact sequences) of function fields over $\mathbb{F}_q$ with small deficiency.

We will construct some new towers $\mathcal{E} = (E_n)_{n\geq 0}$ of function fields over $\mathbb{F}_q$ and then find the set $\mathcal{P}(\mathcal{E})$ and the deficiency $\delta(\mathcal{E})$. Moreover, we will estimate the class numbers $h_n := h(E_n)$, for $n \geq 0$, and the value $H(\mathcal{E})$ for these new towers $\mathcal{E}$ over $\mathbb{F}_q$. We note that to estimate the numbers h_n, we compute the genus $g(E_n)$, and then by Theorem 1.1.6, one can easily estimate these numbers.

3.1 Non-maximal recursive towers with all but one invariants being zero

We first recall that a *non-maximal* tower is a tower which does not attain the generalized Drinfeld-Vladut bound given in Theorem 1.3.2(ii). We begin with some simple remarks, which we will apply in the subsequent examples.

Remark 3.1.1. Let $\mathcal{F} = (F_n)_{n\geq 0}$. For any $n \geq 1$, we have that

$$rB_r\left(F_n/\mathbb{F}_q\right) = \sum_{d|r} \mu(\frac{r}{d}) B_1(F_n\mathbb{F}_{q^d}/\mathbb{F}_{q^d}),$$

where μ denotes the Mobius function (see [24, p.207]). Therefore,

$$r\beta_r\left(\mathcal{F}/\mathbb{F}_q\right) = \sum_{d|r} \mu(\frac{r}{d}) \beta_1(\mathcal{F}\mathbb{F}_{q^d}/\mathbb{F}_{q^d}).$$

Remark 3.1.2. For any $r, t \geq 1$, we have

$$\sum_{t|d|r} \mu(\frac{r}{d}) = \begin{cases} 1 & \text{if } r = t, \\ 0 & \text{else.} \end{cases}$$

Proof. We know that

$$\sum_{d|r}\mu(d)=\begin{cases}1 & \text{if } r=1,\\ 0 & \text{else.}\end{cases}$$

Clearly, if $t\nmid r$, then there is nothing to prove. So we assume that $r=t^n s$ for some $n\geq 1$ and $t\nmid s$, where s is an integer. Set $d:=tk$ where k is a factor of $\frac{r}{t}$. Then

$$\begin{aligned}\sum_{t|d|r}\mu(\frac{r}{d}) &= \sum_{tk|t^n s}\mu\left(\frac{r}{d}\right)=\sum_{k|t^{n-1}s}\mu\left(\frac{t^{n-1}s}{k}\right)\\ &= \sum_{k|t^{n-1}s}\mu\left(k\right)=\begin{cases}1 & \text{if } t^{n-1}s=1\\ 0 & \text{else.}\end{cases}\end{aligned}$$

Hence, since $r=t^n s$, the result follows. □

Example 3.1.3. Let $\mathcal{F}$ be the tower defined by the equation $y^2+y=x+1+1/x$ over a finite field $\mathbb{F}_{2^e}$ for some $e\geq 1$. Then by Example 5.8 in [4], we have

$$\beta_1(\mathcal{F})=\begin{cases}3/2 & \text{if 3 divides } e,\\ 0 & \text{else.}\end{cases}$$

Now we consider the tower $\mathcal{F}$ over $\mathbb{F}_q$, with $q=2^e$ where $3\nmid e$. Then by using Remark 3.1.1, we obtain that

$$r\beta_r(\mathcal{F}/\mathbb{F}_q)=\sum_{3|d|r}\mu(\frac{r}{d})\beta_1(\mathcal{F}\mathbb{F}_{q^d}/\mathbb{F}_{q^d})=\frac{3}{2}\sum_{3|d|r}\mu(\frac{r}{d}).$$

This equality and an application of Remark 3.1.2 with $t=3$ yields

$$r\beta_r(\mathcal{F})=\begin{cases}3/2 & \text{if } r=3,\\ 0 & \text{else.}\end{cases}$$

Hence,

$$\mathbb{P}(\mathcal{F}/\mathbb{F}_q)=\{3\} \text{ with } \beta_3(\mathcal{F}/\mathbb{F}_q)=\frac{1}{2}.$$

Then the deficiency and $H(\mathcal{F})=\lim_{n\to\infty}\log_q h_n/g(F_n)$, as defined in Theorem 1.1.5, are as follows:

$$\delta(\mathcal{F}/\mathbb{F}_q)=\frac{2q^{3/2}-5}{2(q^{3/2}-1)} \text{ and } H(\mathcal{F}/\mathbb{F}_q)=1+\frac{1}{2}loq_q\left(\frac{q^3}{q^3-1}\right).$$

This example implies that for $q=2^e$ where $3\nmid e$, we get

$$A_3(q)\geq\frac{1}{2}.$$

Notice that for $q=2$, we get a lower bound close to the Drinfeld-Vladut bound of order 3 with the *deficiency* $\delta(\mathcal{F}/\mathbb{F}_2)=0.17962$ and $H(\mathcal{F}/\mathbb{F}_2)=1.0850$.

Example 3.1.4. Let $q = 3^e$ for some $e \geq 1$ and $\mathcal{F}$ be the tower given in [10], which is defined by the equation $y^2 = \frac{x(x-1)}{x+1}$ over $\mathbb{F}_q$. Then by Example 2.4.3 in [13], we have

$$\beta_1(\mathcal{F}) = \begin{cases} 2/3 & \text{if } e \text{ is even,} \\ 0 & \text{if } e = 1. \end{cases}$$

Now by applying Remark 3.1.2 with $t = 1$, we obtain that

$$\mathbb{P}(\mathcal{F}/\mathbb{F}_9) = \{1\} \text{ with } \beta_1(\mathcal{F}/\mathbb{F}_9) = \frac{2}{3}.$$

Thus,

$$\delta(\mathcal{F}/\mathbb{F}_9) = \frac{2}{3} \approx 0.66 \text{ and } H(\mathcal{F}/\mathbb{F}_9) = 1.0357.$$

Example 3.1.5. Let q be a power of 3, and $\mathcal{F}$ be the tower given in [10], which is defined by the equation $y^2 = \frac{x(x+1)}{x-1}$ over $\mathbb{F}_q$. Then by a remark in [13, p.46], we have

$$\beta_1(\mathcal{F}/\mathbb{F}_{81^n}) = 2 \text{ for all } n \geq 1.$$

Now by applying Remark 3.1.2 with $t = 1$, we get that

$$\mathbb{P}(\mathcal{F}/\mathbb{F}_{81}) = \{1\} \text{ with } \beta_1(\mathcal{F}/\mathbb{F}_{81}) = 2.$$

Hence,

$$\delta(\mathcal{F}/\mathbb{F}_{81}) = 0.75 \text{ and } H(\mathcal{F}/\mathbb{F}_{81}) = 1.0057.$$

Example 3.1.6. Let $p \geq 3$ be a prime number and $\mathcal{F}$ be the tower over $\mathbb{F}_{p^e}$ defined by the equation $y^2 = (x^2+1)/2x$. Then by Example 5.9 in [4], we have

$$\beta_1(\mathcal{F}) = \begin{cases} p-1 & \text{if 2 divides } e, \\ 0 & \text{else.} \end{cases}$$

We consider the tower $\mathcal{F}$ over $\mathbb{F}_q$, where $q := p^e$ with 2 not dividing e. Then by applying Remark 3.1.2 with $t = 2$, we obtain that

$$\mathbb{P}(\mathcal{F}/\mathbb{F}_q) = \{2\} \text{ with } \beta_2(\mathcal{F}) = \frac{p-1}{2}.$$

Thus,

$$\delta(\mathcal{F}/\mathbb{F}_q) = p^{e-1} + p^{e-2} + \ldots + p \text{ and } H(\mathcal{F}/\mathbb{F}_q) = 1 + \left(\frac{p-1}{2}\right) \log_q\left(\frac{q^2}{q^2-1}\right).$$

Thus, the tower $\mathcal{F}$ over $\mathbb{F}_p$ attains the Drinfeld-Vladut bound of order 2.

Corollary 3.1.7. *In the following cases there exists a non-maximal recursive tower over* $\mathbb{F}_q$ *with exactly one nonzero invariant:*

(i) $q = 2^e$ *with* 3 *not dividing* e,

(ii) $q = 3^e$ *with* $e = 2$ *or* 4,

(iii) $q = p^e$ *with* $p \geq 3$, $e > 2$ *and* 2 *not dividing* e.

Proof. See Examples 3.1.3, 3.1.4, 3.1.5, and 3.1.6, respectively. □

3.2 Towers attaining the Drinfeld-Vladut bound of order r

Example 3.2.1. Let q^r be a square and $\mathcal{F}$ be the tower defined by the equation

$$y^{q^{r/2}} + y = \frac{x^{q^{r/2}}}{x^{q^{r/2}-1} + 1} \tag{3.1}$$

over a finite field $\mathbb{F}_{p^e}$, for some $e \geq 1$. Then by Example 5.7 in [4], we have

$$\beta_1(\mathcal{F}) = \begin{cases} q^{r/2} - 1 & \text{if } \mathbb{F}_{q^r} \subseteq \mathbb{F}_{p^e}, \\ 0 & \text{else} \end{cases}$$

Now consider the tower $\mathcal{E}/\mathbb{F}_{q^r}$ defined by (3.1), which is studied in [9]. Using Remark 3.1.1, we have that

$$r\beta_r(\mathcal{E}/\mathbb{F}_q) = \sum_{d|r} \mu(\frac{r}{d})\beta_1(\mathcal{E}/\mathbb{F}_{q^d}),$$

from which it follows that

$$\beta_r(\mathcal{E}/\mathbb{F}_q) = \frac{q^{r/2} - 1}{r} = A_r(q), \text{ and so } \mathcal{P}(\mathcal{E}/\mathbb{F}_q) = \{r\}.$$

Thus,

$$\delta(\mathcal{E}/\mathbb{F}_q) = 0 \text{ and } H(\mathcal{E}/\mathbb{F}_q) = 1 + \frac{q^r - 1}{r} \log_q \left(\frac{q^r}{q^r - 1} \right).$$

Example 3.2.2. Consider the tower $\mathcal{T}$ defined by the equation

$$y^{q^{r/2}} x^{q^{r/2}-1} + y = x^{q^{r/2}}$$

over $\mathbb{F}_{q^r}$, with q^r a square. This tower is studied in [8]. It is maximal and from [9, Remark 3.11, Corollary 2.4], we have that $\beta_1(\mathcal{E}) \geq \beta_1(\mathcal{T})$, where $\mathcal{E}/\mathbb{F}_{q^r}$ is the tower defined in Example 3.2.1. Hence,

$$\beta_1(\mathcal{T}) = \begin{cases} q^{r/2} - 1 & \text{over } \mathbb{F}_{q^r}, \\ 0 & \text{over } \mathbb{F}_{p^e} \text{ where } \mathbb{F}_{q^r} \nsubseteq \mathbb{F}_{p^e}. \end{cases}$$

Then by the same way as in the previous example, we get that

$$\mathcal{P}(\mathcal{T}/\mathbb{F}_q) = \{r\} \text{ with } \beta_r(\mathcal{T}/\mathbb{F}_q) = \frac{q^{r/2} - 1}{r} = A_r(q).$$

Note that

$$\delta(\mathcal{T}/\mathbb{F}_q) = \delta(\mathcal{E}/\mathbb{F}_q) \text{ and } H(\mathcal{T}/\mathbb{F}_q) = H(\mathcal{E}/\mathbb{F}_q).$$

3.3 Recursive towers with various invariants being positive

In this section we will construct some recursive towers $\mathcal{E} = (E_n)_{n\geq 0}$ over $\mathbb{F}_q$ and estimate the deficiency $\delta(\mathcal{E})$, the class numbers $h_n := h(E_n)$, and $H(\mathcal{E}) = \lim_{n\to\infty} \log_q h_n/g(E_n)$. By Theorems 2.2.1, 2.3.3, and Examples 3.2.1, 3.2.2, 3.1.3, 3.1.6, we have the following:

Theorem 3.3.1. *Let $N \subseteq \mathbb{N}$ be a finite set and q be a prime number. Then there exists a recursive tower of function fields $\mathcal{F}/\mathbb{F}_q$ such that the set*

$$\mathcal{P}(\mathcal{F}) := \big\{r \in \mathbb{N} : \beta_r(\mathcal{F}) > 0\big\} \supseteq N.$$

Moreover, in the following cases there exists a recursive tower $\mathcal{F}/\mathbb{F}_q$ with $\mathcal{P}(\mathcal{F}) = N$:

(i) q is any prime power and N is a finite set with each $k \in N$ a multiple of r for some r such that q^r is a square,

(ii) $q = 2^e$ with $3 \nmid e$ and each element $k \in N$ is a multiple of 3,

(iii) $q = p^e$ with $p \geq 3$, $e > 2$ and $2 \nmid e$, and each $k \in N$ is an even integer.

We will mainly use the following proposition to construct some new towers with various invariants being positive.

Proposition 3.3.2. *Let $F/\mathbb{F}_q$ be a function field with a finite set of places S and F'/F be a finite separable extension. Further let $N \subseteq \mathbb{N}$ be a finite set with $m := \sum_{f\in N} f$. Suppose that $F/\mathbb{F}_q$ has a rational place Q which has a rational extension Q' in F' such that $(m, e(Q'|Q)) = 1$. Define $E := F(z)$ where z is a root of the polynomial*

$$\varphi(T) := \prod_{f\in N} g_f(T) - \alpha \in F[T]$$

which has the following properties:

(a) each $g_f(T)$ is a monic, irreducible polynomial in $\mathbb{F}_q[T]$ of $\deg g_f(T) = f$,

(b) $\alpha \in F$ and $\alpha(P) = 0$ for all $P \in S$,

(c) $v_Q(\alpha) < 0$ and $(v_q(\alpha), m) = 1$.

Set $E' := EF'$. Then the following hold:

(i) the place Q is totally ramified in E, $[E : F] = [E' : F'] = m$, and $\mathbb{F}_q$ is algebraically closed in E'.

(ii) Each place $P \in S$ has exactly one extension $Q_f \in E$ with

$$\deg Q_f = f \deg P \text{ for all } f \in N.$$

(iii) If P splits completely in F', then each extension of P in E splits completely in E'.

Proof. (i) By applying the generalized Eisenstein's Irreducibility Criterion [24] with the place Q and using (c), we obtain that $\varphi(T)$ is irreducible over F and Q is totally ramified in E. Since $(m, e(Q'|Q)) = 1$ for some rational place Q' of F' lying over Q, it follows from Abhyankar's Lemma [24] that Q' is totally ramified in $E' = EF'$. Thus, assertion (i) follows.
(ii) The proof is clear by Kummer's Theorem [24], and the properties (a) and (b).
(iii) See Lemma 2.1.1. □

We here compute the class numbers by using Theorem 1.1.6. Hence, we need to compute the genus $g(E_n)$. For this we will use the following lemma (recall that we have $F := F_0$):

Lemma 3.3.3. *Suppose that $\mathcal{F} = (F_n)_{n\geq 0}$ is a tower over $\mathbb{F}_q$ with finite ramification locus $R(\mathcal{F})$. Let E/F be a finite separable extension such that all $P \in R(\mathcal{F})$ are tame in E. Assume that $\mathcal{E} = (E_n)_{n\geq 0}$, with $E_n := EF_n$, is a tower over $\mathbb{F}_q$. Set $m := [E : F]$. Then*

$$g(E_n) = \left(g(E) - mg(F) + m - \frac{s+2}{2}\right)[E_n : E] + m(g(F_n) - 1) + \frac{r(n)}{2} + 1,$$

where

$$\begin{aligned} s &= \sum_{\substack{Q\in\mathbb{P}(E)\\ Q\cap F\in R(\mathcal{F})}} d(Q|Q\cap F)\deg Q \quad \text{and} \\ r(n) &= \sum_{P\in R(\mathcal{F})} \sum_{\substack{P_n\in\mathbb{P}(F_n)\\ P_n|P}} \deg P_n \sum_{\substack{Q_n\in\mathbb{P}(E_n)\\ Q_n|P_n}} (e(Q_n|P_n) - 1) f(Q_n|P_n). \end{aligned}$$

Proof. See [11, Theorem 3.6]. □

A tower $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ is called an *Artin-Schreier tower* if each extension F_{n+1}/F_n is an Artin-Schreier extension.

Here we first consider the tower $\mathcal{F}$ over $\mathbb{F}_{q^2}$ which is defined as follows: $F := F_0 = \mathbb{F}_{q^2}(x_0)$ is the rational function field and $F_{n+1} = F_n(x_{n+1})$ with

$$x_{n+1}^q x_n^{q-1} + x_{n+1} = x_n^q \tag{3.2}$$

for all $n \geq 0$. This tower is studied in [8]. It has the following properties:

- $\mathrm{Supp}(\mathcal{F}) = \{P \in \mathbb{P}(F) |\ x_0(P) = \alpha \text{ for some } 0 \neq \alpha \in \mathbb{F}_{q^2}\}$ and

  $$\mathcal{P}(\mathcal{F}) = \{1\} \text{ and } \nu_1(P, \mathcal{F}) = 1 \text{ for all } P \in \mathrm{Supp}(\mathcal{F}).$$

- $R(\mathcal{F}) = \{P_0, P_\infty\} \subseteq \mathbb{P}(F)$, where P_0 (resp. P_∞) is the zero (resp. the pole) of x_0, is the set of ramified places in $\mathcal{F}$.
- P_∞ is totally ramified in $\mathcal{F}$, and $\gamma(\mathcal{F}) = q + 1$.
- $\beta_1(\mathcal{F}) = q - 1$, i.e., $\mathcal{F}$ attains the Drinfeld-Vladut bound of order one.
- $$g(F_n) = \begin{cases} (q+1)q^n - (q+2)q^{\frac{n}{2}} + 1 & \text{if } n \equiv 0 \mod 2 \\ (q+1)q^n - \frac{1}{2}(q^2+3q+1)q^{\frac{n-1}{2}} + 1 & \text{if } n \equiv 1 \mod 2. \end{cases} \tag{3.3}$$

Example 3.3.4. Let $N \subseteq \mathbb{N}$ be a finite set and set $m := \sum_{f\in N} f$. Consider the tower $\mathcal{F} = (F_n)_{n\geq 0}$ defined by Eq. (3.2) over $\mathbb{F}_{q^2}$, with $(m, q) = 1$. Let t be an integer such that $1 \leq t \leq q^2 - 1$ and $(t, m) = 1$. Further let $E := F(z)$ where z is a root of the polynomial

$$\varphi(T) := \prod_{f \in N} g_f(T) - \prod_{j=1}^{t}(x_0 - \alpha_j) \text{ with } 0 \neq \alpha_j \in \mathbb{F}_{q^2},$$

where each g_f is a monic and irreducible polynomial in $\mathbb{F}_{q^2}[T]$ having $\deg g_f(T) = f$. Let

$$S := \{P \in \mathbb{P}(F) : x_0(P) = \alpha_j \text{ for some } j = 1, \ldots, t\}.$$

By applying Proposition 3.3.2 with $Q := P_\infty$ and the set S, and using Abhyankar's Lemma [24], we obtain the following:

- E/F is separable of degree $[E : F] = \deg \varphi(T) = m$,
- E and F_n are linearly disjoint over F for all $n \geq 0$,
- $\mathbb{F}_{q^2}$ is algebraically closed in E_n for all $n \geq 0$,
- each $P \in S$ has exactly one extension Q_f in E with $\deg Q_f = f$ for all $f \in N$.

Thus, the sequence $\mathcal{E} = (E_n)_{n \geq 0}$, with $E_n := EF_n$, is a tower over $\mathbb{F}_{q^2}$ such that $[E_{n+1} : E_n] = q$ for all $n \geq 0$. Moreover, since for all $P \in S$ we have that $\nu_1(P, \mathcal{F}) = 1$, i.e., P splits completely in $\mathcal{F}$, by Propositon 3.3.2(iii), each place Q_f splits completely in $\mathcal{E}$. Hence,

$$\nu_f(Q_f, \mathcal{E}) = 1 \text{ for all } f \in N.$$

Then by Theorem 1.3.2(v), for each $f \in N$, we have that

$$\nu_f(\mathcal{E}) \geq \sum_{\substack{P \in S \\ Q_f | P}} \nu_f(Q_f, \mathcal{E}) = \#S = t. \tag{3.4}$$

Moreover, since $\gamma(F) < \infty$, by Theorem 2.3.3(i), the genus $\gamma(\mathcal{E}) < \infty$. Therefore, by Theorem 1.3.2(iv) and Eq. (3.4), we obtain that

$$\beta_f(\mathcal{E}) \geq \frac{t}{\gamma(\mathcal{E})} > 0 \text{ for all } f \in N. \tag{3.5}$$

It is obvious that

$$\mathcal{P}(\mathcal{F}) \supseteq N.$$

Next, we compute the genus of the tower $\mathcal{E}$ in some specific cases:
Case-1: Let $t := 1$, $q := p$ for some prime p, $\alpha_1 := 1$, and $N := \{1, r\}$ where $r \geq 2$ with $(r + 1, p) = 1$. For simlicity, we set $l := p^2$. We have

$$\varphi(T) = g_r(T)(T - 1) - x_0 + 1 \in F[T], \tag{3.6}$$

where $g_r(T) \in \mathbb{F}_{q^2}[T]$ is a monic and irreducible polynomial of degree r. Assume that $(\varphi(T), \varphi'(T)) = 1$ at P_0. To estimate $g(E_n)$, we apply Lemma 3.3.3. It is clear that $g(E) = 0$. From the defining equation (3.6), we have that the place P_∞ is totally ramified in E. Let $Q \in \mathbb{P}(E)$ lying above P_∞. Then the different exponent $d(Q|P) = e(Q|P) - 1 = r$.

Since $(\varphi(T), \varphi'(T)) = 1$ at P_0, the polynomial $\varphi(T)$ has no multiple factors over the residue class field of P_0. Hence, by Kummer's Theorem [24], P_0 is unramified in E. Then the sum s defined in Lemma 3.3.3 is

$$s = r.$$

Since P_∞ is totally ramified in E and $\mathcal{F}$, by Abhyankar's Lemma [24], it is totally ramified in E_n for all $n \geq 0$. Hence, the value $r(n)$ defined in Lemma 3.3.3 is

$$r(n) = r \text{ for all } n \geq 0.$$

Then by using the same lemma and (3.3), we obtain that

$$\begin{aligned}
g(E_n) &= \left(r + 1 - \frac{r+2}{2}\right)[E_n : E] + (r+1)(g(F_n) - 1) + \frac{r+2}{2} \\
&= \frac{r}{2}p^n + (r+1)g(F_n) - r - 1 + \frac{r+2}{2} \\
&= \begin{cases} \frac{1}{2}(2rp + 2p + 3r + 2)p^n - (r+1)(p+2)p^{\frac{n}{2}} + \frac{r+2}{2} & \text{if } n \equiv 0 \mod 2 \\ \frac{1}{2}(2rp + 2p + 3r + 2)p^n - Ap^{\frac{n-1}{2}} + \frac{r+2}{2} & \text{if } n \equiv 1 \mod 2. \end{cases}
\end{aligned}$$

where

$$A := \frac{1}{2}(r+1)(p^2 + 3p + 1).$$

Therefore,

$$\gamma(\mathcal{E}) = \frac{1}{2}(2rp + 2p + 3r + 2),$$

and so by substituting in Eq. (3.5), we obtain that

$$\beta_f(\mathcal{E}) \geq \frac{2}{2rp + 2p + 3r + 2} \text{ for } f \in \{1, r\}.$$

Now we estimate the class numbers in both asymptotic and non-asymptotic cases. By Theorem 1.1.5,

$$\begin{aligned}
H(\mathcal{E}) &= 1 + \sum_{r=1}^{\infty} \beta_r(\mathcal{E}) \log_l \left(\frac{l^r}{l^r - 1}\right) \\
&\geq 1 + \frac{2}{2rp + 2p + 3r + 2}\left(\log_l \left(\frac{l^{r+1}}{(l-1)(l^r - 1)}\right)\right).
\end{aligned}$$

By using Theorem 1.1.6, for each $0 < \alpha < \frac{2}{2rp+2p+3r+2}$, we obtain that there exists a constant $C > 0$ such that for all $n \geq 0$ the following holds:

$$h(E_n) > C\left(\left(\frac{l^r}{l^r - 1}\right)^{\alpha} l\right)^{g(E_n)}.$$

Case-2: Let $t := q^2 - 1$ where q is any prime power, $N \subseteq \mathbb{N}$ be a finite set such that $m := \sum_{f \in N} f$ is coprime to q. For simplicity, set $l := q^2$. Define $E := F(z)$ with z a root of the polynomial

$$\varphi(T) := \prod_{f \in N} g_f(T) - x_0^{q^2} + x_0 \in F[T], \tag{3.7}$$

where each $g_f(T)$ is a monic and irreducible polynomail in $\mathbb{F}_{q^2}[T]$. We first note that all conditions in Proposition 3.3.2 are satisfied with the set $S := \mathrm{Supp}(\mathcal{F})$ and the place $Q := P_\infty$. We also have the following:

(i) The extension $E/\mathbb{F}_{q^2}(z)$ is an elementary abelian extension. Hence, we can easily conclude from Eq. (3.7) that only the pole of z, say Q_∞, is ramified in $E/\mathbb{F}_{q^2}(z)$. Let Q'_∞ be the extension of Q_∞ in E. Then

$$e(Q'_\infty|Q_\infty) = q^2 \text{ and } d(Q'_\infty|Q_\infty) = (m+1)(q^2-1).$$

For details see [24, Proposition 3.7.10]. Now it follows from the Hurwitz Genus Formula for the extension $E/\mathbb{F}_{q^2}(z)$ that the genus of E is

$$g(E) = \frac{(m-1)(q^2-1)}{2}. \tag{3.8}$$

(ii) By using Kummer's Theorem [24], the place P_0 is unramified and by Proposition 3.3.2(i), P_∞ is totally ramified in E/F. Hence, the sum s defined in Lemma 3.3.3 is

$$s = m-1. \tag{3.9}$$

(iii) Since P_∞ is totally ramified in E and $\mathcal{F}$, by using Abhyankar's Lemma [24], P_∞ is totally ramified in E_n for all $n \geq 0$. Hence, the sum $r(n)$ defined in Lemma 3.3.3 is

$$r(n) = m-1 \text{ for all } n \geq 0. \tag{3.10}$$

Now by combining (3.8), (3.9),(3.10), (3.3) and applying Lemma 3.3.3, we obtain that

$$\begin{aligned} g(E_n) &= \left(\frac{(m-1)(q^2-1)+m-1}{2}\right)[E_n:E] + m(g(F_n)-1) + \frac{m-1}{2} + 1 \\ &= \frac{(mq^2-q^2)}{2}q^n + m(g(F_n)-1) + \frac{m+1}{2} \\ &= \begin{cases} \frac{1}{2}(m(q^2+2q+2)-q^2)q^n - m(q+2)q^{\frac{n}{2}} + \frac{m+1}{2} & \text{if } n \equiv 0 \mod 2 \\ \frac{1}{2}(m(q^2+2q+2)-q^2)q^n - \frac{m}{2}(q^2+3q+1)q^{\frac{n-1}{2}} + \frac{m+1}{2} & \text{if } n \equiv 1 \mod 2. \end{cases} \end{aligned}$$

Hence,

$$\gamma(\mathcal{E}) = \frac{1}{2}(m(q^2+2q+2)-q^2). \tag{3.11}$$

Then by (3.4),

$$\nu_f(\mathcal{E}) \geq t = q^2-1 \text{ for all } f \in N. \tag{3.12}$$

Since the tower $\mathcal{F}$ is pure and $S = \mathrm{Supp}(\mathcal{F})$, by Theorem 2.2.1(ii),

$$\nu_f(\mathcal{E}) = q^2-1 \text{ for all } f \in N \text{ and } \mathcal{P}(\mathcal{E}) = N. \tag{3.13}$$

Now by combining (3.11) and (3.13), and Theorem 1.3.2(iv), we obtain that

$$\beta_f(\mathcal{E}) = \frac{2(q^2-1)}{m(q^2+2q+2)-q^2} \text{ for all } f \in N.$$

Now by Theorem 1.1.5, in the asymptotic case, we get

$$H(\mathcal{E}) = 1 + \frac{2(q^2-1)}{m(q^2+2q+2)-q^2} \sum_{f\in N} \log_l\left(\frac{l^f}{l^f-1}\right).$$

By Theorem 1.1.6, for each $0 < \alpha < \frac{2(q^2-1)}{m(q^2+2q+2)-q^2}$, there exists a constant $C > 0$ such that for all $n \geq 0$, we have

$$h(E_n) > C\left(\left(\frac{l^r}{l^r-1}\right)^{\alpha} l\right)^{g(E_n)}.$$

In this case, one can obtain the exact value of the *deficiency*:

$$\delta(\mathcal{E}) = 1 - \frac{2(q^2-1)}{m(q^2+2q+2)-q^2} \sum_{f \in N} \frac{f}{q^f - 1},$$

which depends on m, q and the set N. Thus, by an appropriate choice of m, q and N, one can construct many different towers $\mathcal{E}/\mathbb{F}_{q^2}$ with distinct δ.

A tower $\mathcal{F} = (F_n)_{n \geq 0}$ is called a *tame tower* if each extension F_{n+1}/F_n is a tame extension.

Next, we construct some tame towers of function fields over $\mathbb{F}_q$ with many invariants β_r being positive and estimate the class numbers in these towers. First of all, for any tower $\mathcal{F} = (F_n)_{n \geq 0}$, set

$$a_n := \sum_{P \in R(\mathcal{F})} \sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P}} \deg Q.$$

Lemma 3.3.5. *Let l be a prime power, $q = l^r$ with $r \geq 2$, and $d := \frac{q-1}{l-1}$. Let $\mathcal{F} = (F_n)_{n \geq 0}$, with the rational function field $F_0 := \mathbb{F}_q(x_0)$, be the tower which is recursively defined by the equation*

$$y^d = a(x+b)^d + c \text{ with } a, c \in F_l^*, b \in F_q^* \text{ and } ab^d + c = 0. \tag{3.14}$$

Then the following hold:

(i) the pole (resp. the zero) of x_0, say P_∞ (resp. P_0), splits completely (resp. is totally ramified) in $\mathcal{F}$, and

$$R(\mathcal{F}) = \{P \in \mathbb{P}(F) : x_0(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_q\}.$$

(ii) $\beta_1(\mathcal{F}) = \frac{2}{q-2}$.

(iii) For any $n \geq 1$, the genus

$$g(F_n) = \left(\frac{q-2}{2}\right) d^n - \frac{1}{2} a_n + 1 \quad \text{with} \quad \lim_{n \to \infty} \frac{a_n}{[F_n : F_0]} = 0.$$

Proof. For the proof of (i), see [28, p.37, Theorem 4.1.4 and Lemma 4.2.2]. For that of (ii) and (iii), see [28, Theorem 4.2.3]. □

Example 3.3.6. Consider the tower $\mathcal{F}/\mathbb{F}_q$ given in Lemma 3.3.5. Let $N \subseteq \mathbb{N}$ be a finite set and set $m := \sum_{f \in N} f$. Suppose that $(m, d) = 1$. Let $E := F(z)$ with z a root of the polynomial

$$\varphi(T) := \prod_{f \in N} g_f(T) - \frac{1}{x_0}, \tag{3.15}$$

where each $g_f(T) \in \mathbb{F}_q[T]$ is a monic and irreducible polynomial of $\deg g_f(T) = f$. Suppose further that $\gcd(\varphi(T), \varphi'(T)) = 1$ over the residue class field $k(P)$ for any place $P \in R(\mathcal{F}) \setminus \{P_0\}$, where P_0 is the zero of x_0.

By applying Proposition 3.3.2 with the set $S := \{P_\infty\}$ and $Q := P_0$, we obtain that the sequence $\mathcal{E} := (E_n)_{n\geq 0}$ with $E_n := EF_n$, is a tower over $\mathbb{F}_q$ with the following properties:

(a) $[E : F] = [E_n : F_n] = \deg \varphi(T) = m$ for all $n \geq 0$, (observe that then E/F and F_n/F are linearly disjoint for all $n \geq 0$).

(b) For each $f \in N$, the place P_∞ has exactly one extension Q_f in E with $\deg Q_f = f$ and Q_f splits completely in $\mathcal{E}$.

Hence,

$$B_f(E_n) \geq [E_n : E] = [F_n : F] = d^n \text{ for all } f \in N. \tag{3.16}$$

Next, we estimate $g(E_n)$ for any $n \geq 1$. For this, we will use Lemma 3.3.3. It is clear that $g(E) = 0$. Let $P \in R(F) \setminus \{P_0\}$. By assumption $(\varphi(T), \varphi'(T)) = 1$ at P, and so $\varphi(T)$ has no multiple factors at P. Thus, by Kummer's Theorem [24], P is unramified in E. Now using Abhyankar's Lemma, we obtain that the numbers s and $r(n)$ defined in Lemma 3.3.3 are as follows:

$$s = r(n) = m - 1 \text{ for all } n \geq 1.$$

Then Lemma 3.3.5(iii) and Lemma 3.3.3 yield that

$$g(E_n) = \left(\frac{mq - m - 1}{2}\right) d^n - \frac{m}{2} a_n + \frac{m+1}{2} \quad \text{with } \lim_{n\to\infty} \frac{a_n}{[E_n : E]} = 0.$$

By combining this with Eq. (3.16), we obtain that

$$\beta_f(\mathcal{E}) \geq \frac{2}{mq - m - 1} \text{ for all } f \in N.$$

Moreover, it follows from Lemma 3.3.5(ii) and Theorem 2.2.1(ii) that if $1 \in N$, then

$$\beta_1(\mathcal{E}) = \frac{2}{mq - m - 1}.$$

Lemma 3.3.7. *[10, Theorem 3.11] Let $q = l^r$ with $r \geq 1$ and $l > 2$ a power of the characteristic of $\mathbb{F}_q$. Assume that*

$$r \equiv 0 \mod 2 \text{ or } l \equiv 0 \mod 2.$$

Then the equation

$$y^{l-1} = -(x+b)^{l-1} + 1, \text{ with } b \in \mathbb{F}_l^*, \tag{3.17}$$

defines a recursive tower $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ with the following properties:

(i) letting $F = F_0 := \mathbb{F}_q(x_0)$ the rational function field, we have that

$$R(\mathcal{F}) \subseteq \big\{P \in \mathbb{P}(F_0) : x_0(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_l\big\}.$$

(ii) The pole (resp. the zero) of x_0, say P_∞ (resp. P_0), splits completely (resp. is totally ramified) in $\mathcal{F}$.

(iii) The genus of $\mathcal{F}$ satisfies the inequality

$$\gamma(\mathcal{F}) \leq \frac{l-2}{2}.$$

(iv) $\beta_1(\mathcal{F}) \geq \frac{2}{l-2}$.

Theorem 3.3.8. *Let $\mathcal{F}$ be the tower given in Lemma 3.3.7. Then $\gamma(\mathcal{F}) = \frac{l-2}{2}$. Moreover, when $r = 1$, i.e., l is a power of 2, one has*

$$\beta_1(\mathcal{F}) = \frac{2}{l-2}.$$

We prove Theorem 3.3.8 via the Lemmas 3.3.9, 3.3.10, 3.3.11, 3.3.13 and Proposition 3.3.12. From now on, unless otherwise stated, $\mathcal{F}$ will be the tower defined in Lemma 3.3.7. Additionally, the numbers on the figures denote the corresponding ramification indices. First, by using Eq. (3.17) and Kummer's Theorem, we have the following ramification structure in F_1/F and $F_1/\mathbb{F}_q(x_1)$:

(1) Any place $(x_0 = \alpha)$, with $\alpha \in \mathbb{F}_l \setminus \{-b\}$ is totally ramified in F_1. Let $P_\alpha \in \mathbb{P}(F_1)$ lying above $(x_0 = \alpha)$, then $x_1(P_\alpha) = 0$.

(2) The place $(x_0 = -b)$ splits completely in F_1. Let $P \in \mathbb{P}(F_1)$ be a place lying above $(x_0 = -b)$, then $x_1(P) = \alpha$ for some $\alpha \in \mathbb{F}_l^*$.

To sum up we have the following:

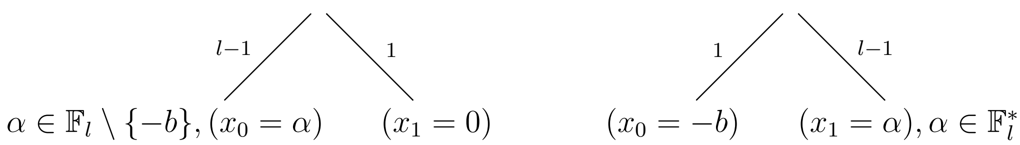

Figure 3.1:

Lemma 3.3.9. *Let $S := \{P \in \mathbb{P}(F) : x_0(P) = \alpha$ for some $\alpha \in \mathbb{F}_l \setminus \{-b\}\}$.*

(i) All $P \in S$ are totally ramified in $\mathcal{F}$.

(ii) $R(\mathcal{F}) = S \cup \{(x_0 = -b)\}$.

Proof. For simplicity, let $f(x) := -(x+b)^{l-1} + 1$. Then for any $n \geq 0$, we have $F_{n+1} = F_n(x_{n+1})$ with

$$x_{n+1}^{l-1} = f(x_n). \tag{3.18}$$

Note that

$$f(\alpha) = 0 \quad \text{if and only if} \quad \alpha \in \mathbb{F}_l \setminus \{-b\}.$$

(i) Let $P \in S$. By Eq. (3.18), and Kummer's Extension Theorem [24], P is totally ramified in F_1. Moreover, for any $Q \in \mathbb{P}(F_1)$ lying above P, we have $x_1(Q) = 0$ and $(x_1 = 0)$ splits in F_1. Then by Eq. (3.18), obviously for any $Q_n \in \mathbb{P}(F_n)$, $n \geq 1$, $Q_n | P$, we have $x_n(Q_n) = 0$. Hence, by using Abhyankar's lemma [24] in Figure 3.2, we obtain that P is totally ramified in F_n for all $n \geq 1$.

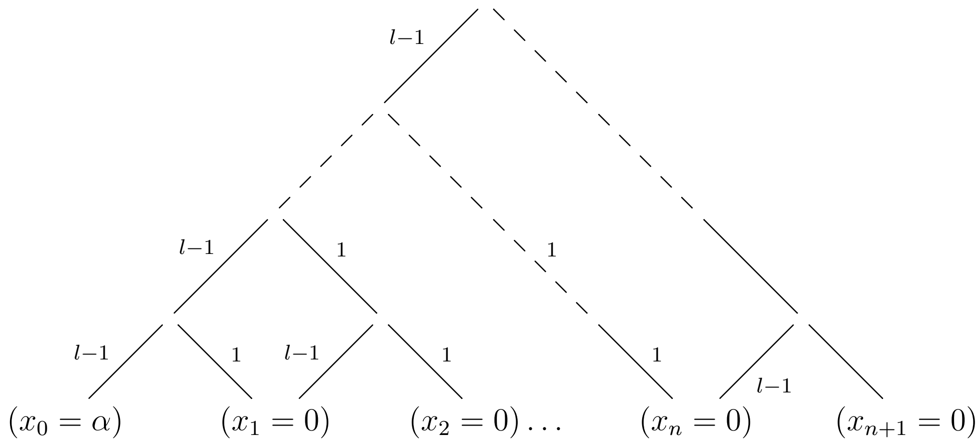

Figure 3.2:

(ii) By (i), $S \subseteq R(\mathcal{F})$. Thus, all we need to do is to check the ramification behaviour of the place $(x_0 = -b) \in \mathbb{P}(F)$ in $\mathcal{F}$. By (2), $(x_0 = -b)$ splits completely in F_1. Let $Q \in \mathbb{P}(F_3)$ lying above $(x_0 = -b)$. Then by using Figure 3.1, we have either

(a) $x_1(Q) \in \mathbb{F}_l^* \setminus \{-b\}$ and $x_2(Q) = 0$ or

(b) $x_1(Q) = -b$ and $x_2(Q) \in \mathbb{F}_l^*$.

W.l.o.g., suppose that (a) holds. Then by drawing a figure and using Abhyankar's Lemma, one can easily see that $e(Q|(x_0 = -b)) = l - 1$, and so the place $(x_0 = -b)$ is ramified in F_3. Thus, $(x_0 = -b) \in R(\mathcal{F})$. □

Lemma 3.3.10. *Let $P := (x_0 = -b)$. Then there exists $k \geq 1$ such that P has an extension $P_k \in \mathbb{P}(F_k)$ with $x_k(P_k) \in \mathbb{F}_l^*$ and the following hold:*

(i) if $x_k(P_k) = -b$, then P_k splits in F_{k+1}.

(ii) If $x_k(P_k) = \alpha$ for some $\alpha \in \mathbb{F}_l^* \setminus \{-b\}$, then P is unramified in F_n for all $n < 2k+1$ and ramified in F_n for all $n \geq 2k+1$. Now suppose that $P_n \in \mathbb{P}(F_n)$ is a place lying over P and P_k. Then for $n \geq 2k+1$, we have

$$e(P_n|P) = (l-1)^{n-2k}.$$

Proof. The existence of k is clear by Figure 3.1. (i) By using Eq. 3.18, P splits completely in $\mathbb{F}_l(x_k, x_{k+1})$, and so by Lemma 2.1.1, P_k splits completely in F_{k+1}, (see Figure 3.3).

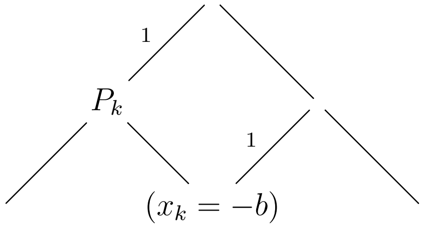

Figure 3.3:

(ii) By using Eq. (3.18), we have the following:

$$\begin{aligned} x_i(P_k) &= -b \text{ for all } i < k \text{ and} \\ x_i(P_k) &= 0 \text{ for all } i > k. \end{aligned}$$

Moreover, for any $i \geq 1$, the following hold:

(a) $(x_i = -b)$ splits completely in $\mathbb{F}_l(x_i, x_{i+1})$ and is totally ramified in $\mathbb{F}_l(x_{i-1}, x_i)$.

(b) $(x_i = \alpha)$, with $\alpha \in \mathbb{F}_l^* \setminus \{-b\}$, is totally ramified in both $\mathbb{F}_l(x_i, x_{i+1})$ and $\mathbb{F}_l(x_{i-1}, x_i)$.

(c) $(x_i = 0)$ splits completely in $\mathbb{F}_l(x_{i-1}, x_i)$ and totally ramified in $\mathbb{F}_l(x_i, x_{i+1})$.

By using (a), (b), (c), and Abhyankar's Lemma, we obtain the following figure, from which (ii) follows:

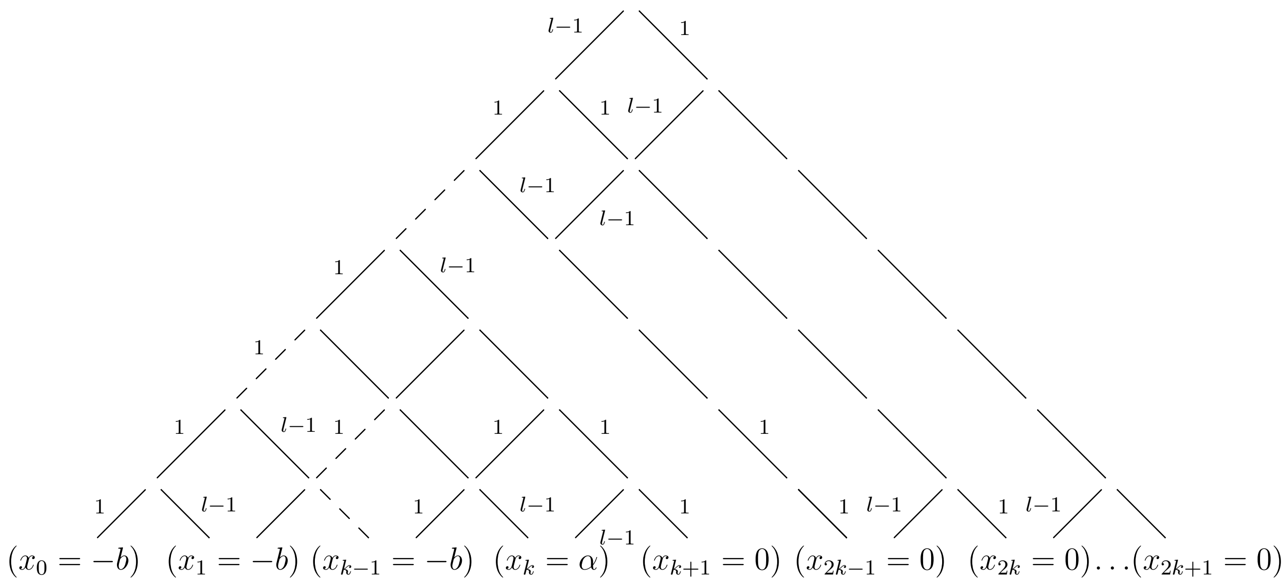

Figure 3.4:

$\square$

Lemma 3.3.11. *For any $k \geq 1$, set $R_k := \{P_k \in \mathbb{P}(F_k) : \; x_k(P_k) = \alpha$ for some $\alpha \in \mathbb{F}_l^* \setminus \{-b\}\}$.*

(i) $(x_k = \alpha)$, with $\alpha \in \mathbb{F}_l^* \setminus \{-b\}$ is totally ramified in F_k for all $k \geq 0$.

(ii) $\#R_k = l - 2$ and $\deg P_k = 1$ for all $k \geq 0$.

(iii)
$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q | P_k \\ P_k \in R_k}} \deg Q = \begin{cases} (l-1)^{n-k} & \text{if } n < 2k+1 \\ (l-1)^k & \text{if } n \geq 2k+1. \end{cases}$$

Proof. Assertion (i) is clear from Figure 3.4. Assertion (ii) follows from (i).
(iii) Let $P_k \in \mathbb{P}(F_k)$ with $x_k(P_k) = \alpha$ for some $\alpha \in \mathbb{F}_l^* \setminus \{-b\}$. Then

$$\begin{aligned} x_i(Q) &= -b \text{ for all } i < k \text{ and} \\ x_i(Q) &= 0 \text{ for all } i > k. \end{aligned}$$

From Figure 3.4 we have the following:

(a) By (ii), $\deg P_k = 1$.

(b) For all $k \leq i \leq 2k$, the place P_k is unramified in F_i, and hence

$$\sum_{\substack{R \in \mathbb{P}(F_i) \\ R | P_k}} \deg R = [F_n : F_k] = (l-1)^{n-k}.$$

(c) Let $R \in \mathbb{P}(F_{2k})$ lying above P_k. Then R is totally ramified in F_n for all $n \geq 2k+1$, i.e., R has only one extension $Q \in \mathbb{P}(F_n)$ and $\deg Q = \deg R$. Therefore, by using (b), for any $n \geq 2k+1$, we have

$$\sum_{\substack{Q \in \mathbb{P}(F_n) \\ Q|P_k}} \deg Q = \sum_{\substack{R \in \mathbb{P}(F_{2k}) \\ R|P_k}} \deg R = [F_{2k} : F_k] = (l-1)^k. \tag{3.19}$$

□

Proposition 3.3.12.

$$g(F_n) = \begin{cases} \left(\frac{l-2}{2}\right)(l-1)^n - \frac{l}{2}(l-1)^{n/2} + 1 & \textit{if } n \equiv 0 \mod 2 \\ \left(\frac{l-2}{2}\right)(l-1)^n - (l-1)^{(n+1)/2} + 1 & \textit{if } n \equiv 1 \mod 2. \end{cases}$$

Proof. Let Q be a place of F_n. By using Lemmas 3.3.9, 3.3.10, and 3.3.11, we obtain that for any $n \geq 1$, the degree of the diferent of F_n/F_0 is as follows:

$$\begin{aligned}
\deg \mathrm{Diff}(F_n/F_0) &= \sum_{\substack{x_0(Q)=\alpha \\ \alpha \in \mathbb{F}_l \setminus \{-b\}}} d(Q|(x_0=\alpha) + \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \#R_k \sum_{\substack{Q|P_k \\ P_k \in R_k}} \deg Q \cdot d(Q|(x_0=-b)) \\
&= (l-1)((l-1)^n - 1) + (l-2) \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{\substack{Q|P_k \\ P_k \in R_k}} \deg Q \cdot d(Q|(x_0=-b)) \\
&= (l-1)^{n+1} - (l-1) + (l-2) \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} (l-1)^k \big[(l-1)^{n-2k} - 1\big] \\
&= (l-1)^{n+1} - (l-1) + (l-2) \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \big[(l-1)^{n-k} - (l-1)^k\big] \\
&= (l-1)^{n+1} - (l-1) + (l-2)(l-1)^n \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor - 1} \frac{1}{(l-1)^{k+1}} \\
&- (l-2) \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor - 1} (l-1)^{k+1} \\
&= (l-1)^{n+1} - (l-1) + (l-2)(l-1)^{n-1} \left(\frac{1}{(l-1)^{\lfloor \frac{n-1}{2} \rfloor}} - 1 \right) \left(\frac{l-1}{2-l} \right) \\
&- (l-2)(l-1) \left(\frac{(l-1)^{\lfloor \frac{n-1}{2} \rfloor} - 1}{l-2} \right) \\
&= l(l-1)^n - (l-1)^{n - \lfloor \frac{n-1}{2} \rfloor} - (l-1)^{\lfloor \frac{n-1}{2} \rfloor + 1} \\
&= \begin{cases} l(l-1)^n - l(l-1)^{n/2} & \text{if } n \equiv 0 \mod 2 \\ l(l-1)^n - 2(l-1)^{(n+1)/2} & \text{if } n \equiv 1 \mod 2\ . \end{cases}
\end{aligned}$$

Now by using the Hurwitz Genus Formula for the extension F_n/F_0, the desired result follows:

$$\begin{aligned} 2g(F_n)-2 &= (l-1)^n(2g(F)-2)+\deg \mathrm{Diff}(F_n/F_0) \\ &= \begin{cases} (l-2)(l-1)^n - l(l-1)^{n/2} & \text{if } n \equiv 0 \mod 2 \\ (l-2)(l-1)^n - 2(l-1)^{(n+1)/2} & \text{if } n \equiv 1 \mod 2. \end{cases} \end{aligned}$$

□

Lemma 3.3.13. *Suppose that $q := l = 2^e$ for some $e > 1$. Then*

$$(l-1)^n + 2(l-1) \le B_1(F_n) \le (l-1)^n + 2(l-1) + A_n,$$

where

$$A_n := \begin{cases} l(l-1)^{n/2} - l & \text{if } n \equiv 0 \mod 2 \\ 2(l-1)^{(n+1)/2} - l & \text{if } n \equiv 1 \mod 2. \end{cases}$$

Proof. We have

$$B_1(F_n) = \sum_{\substack{Q\in\mathbb{P}(F_n) \\ x_0(Q)\in\mathbb{F}_l\setminus\{-b\}}} 1 + \sum_{\substack{Q\in\mathbb{P}(F_n) \\ x_n(Q)=-b}} 1 + \sum_{\substack{Q\in\mathbb{P}(F_n) \\ x_0(Q)=\infty}} 1 + \sum_{\substack{Q\in\mathbb{P}(F_n) \\ Q|P_k \\ P_k\in R_k}} 1. \tag{3.20}$$

By Lemmas 3.3.9, 3.3.10 and 3.3.11, and Lemma 3.3.7(ii), for any $n, k \ge 1$ with $n \ge k$, we have

$$\sum_{\substack{Q\in\mathbb{P}(F_n) \\ x_0(Q)\in\mathbb{F}_l\setminus\{-b\}}} 1 \;=\; l-1, \quad \sum_{\substack{Q\in\mathbb{P}(F_n) \\ x_n(Q)=-b}} = l-1, \quad \sum_{\substack{Q\in\mathbb{P}(F_n) \\ x_0(Q)=\infty}} = (l-1)^n, \quad \text{and}$$

$$\sum_{\substack{Q\in\mathbb{P}(F_n) \\ Q|P_k \\ P_k\in R_k}} 1 \;\le\; \begin{cases} (l-1)^{n-k} \text{ if } n < 2k+1 \\ (l-1)^k \text{ if } n \ge 2k+1\ . \end{cases}$$

Hence,

$$
\begin{aligned}
\sum_{k=1}^{n} \sum_{\substack{Q\in\mathbb{P}(F_n)\\ Q|P_k\\ P_k\in R_k}} 1 &\leq \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor} \#R_k \sum_{\substack{Q\in\mathbb{P}(F_n)\\ Q|P_k\\ P_k\in R_k}} 1 + \sum_{k=\lfloor\frac{n-1}{2}\rfloor+1}^{n} \#R_k \sum_{\substack{Q\in\mathbb{P}(F_n)\\ Q|P_k\\ P_k\in R_k}} 1\\
&= (l-2) \sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor-1} (l-1)^{k+1} + (l-2)(l-1)^n \sum_{k=\lfloor\frac{n-1}{2}\rfloor+1}^{n} \frac{1}{(l-1)^k}\\
&= (l-2)(l-1)\left[\frac{(l-1)^{\lfloor\frac{n-1}{2}\rfloor}-1}{l-2}\right]\\
&+ (l-2)(l-1)^n\left[\frac{1}{(l-1)^{n+1}} - \frac{1}{(l-1)^{\lfloor\frac{n-1}{2}\rfloor+1}}\right]\left(\frac{l-1}{2-l}\right)\\
&= (l-1)\left[(l-1)^{\lfloor\frac{n-1}{2}\rfloor}-1\right] - (l-1)^{n+1}\left[\frac{1}{(l-1)^{n+1}} - \frac{1}{(l-1)^{\lfloor\frac{n-1}{2}\rfloor+1}}\right]\\
&= (l-1)^{\lfloor\frac{n-1}{2}\rfloor+1} - (l-1) - 1 + (l-1)^{n-\lfloor\frac{n-1}{2}\rfloor}\\
&= (l-1)^{\lfloor\frac{n-1}{2}\rfloor+1} + (l-1)^{n-\lfloor\frac{n-1}{2}\rfloor} - l.
\end{aligned}
$$

Now by substituting each value for the sums involved in Eq.(3.20), the lemma follows. □

Proof of Theorem 3.3.8. The proof follows from Proposition 3.3.12 and Lemma 3.3.13. □

Example 3.3.14. Consider the tower $\mathcal{F}$ over $\mathbb{F}_q$ defined in Lemma 3.3.7 with $q = 2^2$. Let $E := F(z)$ with z a root of the polynomial

$$\varphi(T) = (T^4 - T)(T^2 + \mu T + \mu) - \frac{1}{x_0} \in F[T],$$

where μ is a primitive element for $\mathbb{F}_4$. By applying Proposition 3.3.2 with the set $S := \{P_\infty\}$ and $Q := P_0$, we obtain that the sequence $\mathcal{E} = (E_n)_{n\geq 0}$ with $E_n := EF_n$ is a tower over $\mathbb{F}_q$ such that $[E_n : F_n] = \deg\varphi(T) = 6$ for all $n \geq 0$. We want to compute the invariants $\beta_1(\mathcal{E})$ and $\beta_2(\mathcal{E})$.

It follows from Kummer's Theorem [24] and Proposition 3.3.2 that the ramification structure in E/F is as follows:

(a) P_0 is totally ramified.

(b) Since $(\varphi(T), \varphi'(T)) = 1$ at the places $P_\mu := (x_0 = \mu)$ and $P_{\mu^2} := (x_0 = \mu^2)$, these places are unramified in E.

(c) $P_1 := (x_0 = 1)$ has exactly one extension which has degree 2 and ramification index 3 (by using Magma).

(d) P_∞ has 4 rational extensions and one extension of degree 2.

Therefore, by Proposition 3.3.2,

$$B_1(E_n) \geq 4 \cdot [E_n : E] = 4 \cdot 3^n \text{ and } B_2(E_n) \geq 3^n \text{ for all } n \geq 0. \tag{3.21}$$

Next, we want to find $\gamma(\mathcal{E})$. In order to estimate $g(E_n)$, we apply Lemma 3.3.3. It is clear that $g(E) = 0$. By applying Hurwitz Genus Formula for the extension E/F, we have

$$\deg \mathrm{Diff}(E/F_0) = 10. \tag{3.22}$$

Let $Q \in \mathbb{P}(E)$. Then by Dedekind's Different Formula [24], we have that

(i) if $Q|P_1$, then $d(Q|P_1) = e(Q|P_1) - 1 = 2$.

(ii) If $Q|P_0$, then $d(Q|P_0) > e(Q|P_0) - 1 = 5$. Moreover, by (i), (c), and (3.22), we have that $6 \geq d(Q|P_0)$. Hence, $d(Q|P_0) = 6$.

Thus, by using (b), (i), and (ii), we obtain that the number s defined in Lemma 3.3.3 is

$$s = 6 + 2 \cdot 2 = 10 \tag{3.23}$$

Next, we need to find $r(n)$ defined in Lemma 3.3.3. By Abhyankar's Lemma [24] and Lemma 3.3.7(ii), the following hold:

(1) first let $Q \in \mathbb{P}(E)$ lying above P_0. Since P_0 is totally ramified in F_n, it has only one extension, say P_n, in F_n. By Abhyankar's Lemma, $e(Q_n|P_n) = 2$, where $Q_n \in \mathbb{P}(E_n)$ lies over Q.

(2) By (c), P_1 has only one extension, say P_1', in E with $\deg P_1' = 2$ and $e(P_1'|P_1) = 3$, and so Abhyankar's Lemma gives that any extension of P_1 in F_n is unramified in E_n.

(3) Since any $P \in \mathbb{P}(F) \setminus \{P_0, P_1\}$ is unramified in E, by Abhyankar's Lemma their extensions in F_n are unramified in E_n.

Hence, by (1), (2) and (3), for any $n \geq 0$, we have

$$r(n) = e(Q_n|P_n) - 1 = 1. \tag{3.24}$$

Now by applying by Lemma 3.3.3, (3.23), and (3.24), we obtain that for all $n \geq 1$,

$$g(E_n) = 6g(F_n) - \frac{9}{2}. \tag{3.25}$$

Now using Proposition 3.3.12 yields that

$$\gamma(\mathcal{E}) = 6. \tag{3.26}$$

Then by combining (3.21) and (3.26), and since $\mathcal{F}/\mathbb{F}_4$ is maximal with $\beta_1(\mathcal{F}) = 1$, by applying Theorem 2.2.1(ii), we get that

$$\beta_1(\mathcal{E}) = \frac{2}{3} \text{ and } \beta_2(\mathcal{E}) = \frac{1}{6}.$$

Remark 3.3.15. In Example 3.3.14, the deficiency is

$$\delta(\mathcal{E}/\mathbb{F}_4) = 1 - \sum_{r=1}^{\infty} \frac{r\beta_r(\mathcal{E})}{q^{r/2} - 1} = \frac{2}{9} \approx 0.22.$$

Until now, the tower $\mathcal{E}/F_4$ has the smallest δ value among the towers of function fields having at least two positive invariants β_r. Moreover, in comparision with the generalized Drinfeld-Vladut bound of order one (resp. two), one has the following:

$$1 - \beta_1(\mathcal{E}) = \frac{1}{3} \approx 0.33, \text{ (resp. } \frac{1}{2} - \beta_2(\mathcal{E}) = \frac{1}{3} \approx 0.33).$$

Example 3.3.16. Consider the tower $\mathcal{F}$ over $\mathbb{F}_q$ given in Lemma 3.3.7 with $l := 3$ and $r := 2$, i.e., $q = 3^2$, and then $d = 4$. Let $E := F(z)$ with z a root of the polynomial

$$\varphi(T) := (T^2 + \mu^7)(T^9 - T) - \frac{1}{x_0} \in F[T],$$

where μ is a primitive element for $\mathbb{F}_9$. We apply Proposition 3.3.2 with the place $Q := P_0$ and $S := \{P_\infty\}$. We obtain that the sequence $\mathcal{E} = (EF_n)_{n\geq 0}$ is a tower over $\mathbb{F}_9$ and the following hold:

(i) P_0 is totally ramified in E.

(ii) P_∞ has 9 rational extensions and one extension of degree 2 in E.

(iii) Since P_∞ splits completely in $\mathcal{F}$, its all extensions in E splits completely in $\mathcal{E}$.

Note that $\mathcal{F}/\mathbb{F}_9$ is maximal with

$$\beta_1(F) = 2.$$

Hence, $\mathcal{F}/\mathbb{F}_9$ is pure, and so it follows from (iii) and Theorem 2.2.1(ii) that

$$\nu_1(\mathcal{E}) = 9 \text{ and } \nu_2(\mathcal{E}) = 1. \tag{3.27}$$

Next, we want to compute the genus $g(E_n)$. For this, we will apply Lemma 3.3.3. We know that from Lemma 3.3.9 that

$$R(\mathcal{F}) = \{P \in \mathbb{P}(F) : \ x_0(P) = \alpha \text{ for some } \alpha \in \mathbb{F}_3\}.$$

One can easily check that $(\varphi(T), \varphi'(T)) = 1$ at the places $P \in \mathbb{P}(F)$ with $x_0(P) = \alpha$ for some $\alpha \in \mathbb{F}_3^*$. Hence, $\varphi(T)$ has no multiple factor over the residue class field of these places. Then it follows from Kummer's Theorem that these places are unramified in E. Now by applying Lemma 3.3.3, and using assertion (i), since E/F is tame, we obtain that

$$s = d(Q_0|P_0) = e(Q_0|P_0) - 1 = 10 \quad \text{where } Q_0 \text{ is the extension of } P_0 \text{ in } E. \tag{3.28}$$

By using Abhyankar's Lemma, we have that all $P_n \in \mathbb{P}(F_n)$ with $P_n \cap F \in \{P \in \mathbb{P}(F) : x_0(P) \in \mathbb{F}_3^*\}$ are unramified in E_n. Moreover, since P_0 is totally ramified in both extensions E and F_n, again by Abhyankar's Lemma, we have that any extension of P_0 in F_n is totally ramified in E_n. Hence, by Lemma 3.3.3,

$$r(n) = 10 \text{ for all } n \geq 1. \tag{3.29}$$

Now by applying Lemma 3.3.3, (3.28), (3.29), and Proposition 3.3.12, we obtain that

$$g(E_n) = \begin{cases} 21 \cdot 2^{n-1} - 33 \cdot 2^{(n-2)/2} + 6 & \text{if } n \equiv 0 \mod 2 \\ 21 \cdot 2^{n-1} - 11 \cdot 2^{(n+1)/2} + 6 & \text{if } n \equiv 1 \mod 2. \end{cases}$$

Hence,

$$\gamma(\mathcal{E}) = \frac{21}{2}. \tag{3.30}$$

Then by combining (3.27) and (3.30), we get that

$$\beta_1(\mathcal{E}) = \frac{6}{7} \text{ and } \beta_2(\mathcal{E}) = \frac{2}{21}.$$

Note that as $\mathcal{F}$ is pure, by Theorem 2.2.1(ii),

$$\mathcal{P}(\mathcal{E}) = \{1, 2\}.$$

Then the deficiency is given by

$$\delta(E) = \frac{23}{42} \approx 0.54.$$

Moreover, in comparision with the generalized Drinfeld-Vladut bound of order one (resp. two), one has the following:

$$2 - \beta_1(\mathcal{E}) = \frac{8}{7} \approx 1.1 \text{ (resp. } 1 - \beta_2(\mathcal{E}) = \frac{2}{21} \approx 0.9).$$

4

Further Remarks

4.1 Constant field extensions of asymptotically exact sequences of function fields

We first recall that all towers are asymptotically exact sequences, but the converse is not always true.

Lemma 4.1.1. *Let $\mathcal{S} = (F_n)_{n\geq 0}$ be an exact sequence of function fields over $\mathbb{F}_q$ such that $\beta_r(\mathcal{S}) > 0$ for some $r \geq 1$. Then the constant field extension $\mathcal{S} \cdot \mathbb{F}_{q^r}$ of $\mathcal{S}$ has*

$$\beta_1(\mathcal{S} \cdot \mathbb{F}_{q^r}) \geq r\beta_r(\mathcal{S}).$$

Proof. Since $F_n\mathbb{F}_{q^r}$ is a constant field extension of $F_n/\mathbb{F}_q$, we have that

$$B_1(F_n\mathbb{F}_{q^r}) = \sum_{i|r} iB_i(F_n) \quad \text{and} \quad g(F_n\mathbb{F}_{q^r}) = g(F_n). \tag{4.1}$$

Hence,

$$\begin{aligned} \beta_1(\mathcal{S} \cdot \mathbb{F}_{q^r}) &= \lim_{n\to\infty} \frac{B_1(F_n\mathbb{F}_{q^r})}{g(F_n\mathbb{F}_{q^r})} = \lim_{n\to\infty} \frac{1}{g(F_n)} \left(\sum_{i|r} iB_i(F_n) \right) \\ &\geq \lim_{n\to\infty} \frac{rB_r(F_n)}{g(F_n)} = r\beta_r(\mathcal{S}). \end{aligned}$$

□

We note here that if an asymptotically exact sequence $\mathcal{S}/\mathbb{F}_q$ of function fields attains the Drinfeld-Vladut bound of order d for some $d \geq 1$, i.e., $\beta_d(\mathcal{S}) = (q^{d/2} - 1)/d$, then by using (4.1), for any $r \geq 1$ we obtain that

$$\beta_r(\mathcal{S}) = \begin{cases} q^{d/2} - 1 & \text{if } d \mid r \\ 0 & \text{else.} \end{cases} \tag{4.2}$$

By using Lemma 4.1.1, for any integer $r \geq 1$ and prime power q, the following consequence is immediate:

Corollary 4.1.2. $A(q^r) \geq rA_r(q)$.

This fact might be well-known, but we could not find any reference in the literature.

Remark 4.1.3. One can easily conclude from Lemma 4.1.1 that if for some $r \geq 1$ an exact sequence $\mathcal{S}/\mathbb{F}_q$ attains the Drinfeld-Vladut bound of order r, then the sequence $\mathcal{S} \cdot \mathbb{F}_{q^r}/\mathbb{F}_{q^r}$ attains the classical Drinfeld-Vladut bound, i.e., of order one. Furthermore, in that case we have

$$q^{r/2} - 1 \geq A(q^r) \geq \beta_1(\mathcal{S}\mathbb{F}_{q^r}) \geq r\beta_r(\mathcal{S}) = rA_r(q) = r\left(\frac{q^{r/2}-1}{r}\right) = q^{r/2} - 1,$$

which implies that

$$A(q^r) = rA_r(q) = q^{r/2} - 1. \tag{4.3}$$

Theorem 4.1.4. *Let $\mathcal{S} = (F_n)_{n\geq 0}$ be a sequence of function fields over a finite field $\mathbb{F}_q$ and $\mathcal{S}_r := \mathcal{S} \cdot \mathbb{F}_{q^r} = (F_n\mathbb{F}_{q^r})_{n\geq 0}$ be the constant field extension of $\mathcal{S}$, for some $r \geq 1$. Then*

$$\beta_r(\mathcal{S}) = \frac{q^{r/2}-1}{r} \quad \text{if and only if} \quad \beta_1(\mathcal{S}_r) = q^{r/2} - 1.$$

For the proof of Theorem 4.1.4, we need the following results.

Lemma 4.1.5. *[5, Lemma IV.3] Let $\mathcal{S} = (F_n)_{n\geq 0}$ be a sequence of function fields over $\mathbb{F}_q$. If for some $m \geq 1$, one has*

$$\liminf_{n\to\infty} \frac{1}{g(F_n)} \sum_{i=1}^{m} \frac{iB_i(F_n)}{q^{m/2}-1} \geq 1,$$

then

$$\lim_{n\to\infty} \frac{mB_m(F_n)}{g(F_n)} = q^{m/2} - 1.$$

Theorem 4.1.6. *[1, Theorem 2.2] Let $r \in \mathbb{N}$ and $\mathcal{S} = (F_n)_{n\geq 0}$ be a sequence of function fields over $\mathbb{F}_q$ such that $\beta_r(\mathcal{S}) = \frac{q^{r/2}-1}{r}$. Then the sequence $\mathcal{S}/F_q$ is asymptotically exact.*

Proof of Theorem 4.1.4. First, suppose that $\beta_r(\mathcal{S}) = \frac{q^{r/2}-1}{r}$. Then by Theorem 4.1.6, the sequence $\mathcal{S}/\mathbb{F}_q$ is asymptotically exact. Hence, by Remark 4.1.3, $\beta_1(\mathcal{S}_r) = q^{r/2} - 1$. Next, suppose that $\beta_1(\mathcal{S}_r) = q^{r/2} - 1$. Then by using (4.1), we obtain that

$$1 = \lim_{k\to\infty} \frac{B_1(F_k\mathbb{F}_{q^r})}{g_k(q^{r/2}-1)} = \lim_{k\to\infty} \frac{1}{g_k} \sum_{i|r} \frac{iB_i(F_k)}{q^{r/2}-1} \leq \liminf_{k\to\infty} \frac{1}{g_k} \sum_{i=1}^{r} \frac{iB_i(F_k)}{q^{r/2}-1}.$$

Now it follows from Lemma 4.1.5 that

$$\beta_r(\mathcal{S}) = \frac{q^{r/2}-1}{r}.$$

□

By Remark 4.1.3 and Example 3.2.2, the following corollary follows:

Corollary 4.1.7. *For any square prime power q^r, one has*

$$A(q^r) = rA_r(q),$$

hence $A_r(q) = \frac{1}{r}(q^{r/2} - 1)$.

Remark 4.1.8. When q^r is not a square, it is not known whether there are any sequences of function fields $\mathcal{S}$ over $\mathbb{F}_q$ with $\beta_r(\mathcal{S}) = \frac{q^{r/2}-1}{r}$, i.e., attaining the Drinfeld-Vladut bound of order r.

By [23, p.31, Theorem 8], one has the following:

Lemma 4.1.9. *Let $\mathcal{S} = (F_n)_{n\geq 0}$ be a sequence of function fields over $\mathbb{F}_q$ such that each extension F_n/F_0 is an abelian extension. Then $\beta_1(\mathcal{S}) = 0$.*

One can generalize Lemma 4.1.9 as follows:

Theorem 4.1.10. *Let $\mathcal{S} = (F_n)_{n\geq 0}$ be an exact sequence of function fields over $\mathbb{F}_q$ such that each extension F_n/F_0 is an abelian extension. Then $\beta_r(\mathcal{F}) = 0$ for all $r \geq 1$.*

Proof of Theorem 4.1.10. It is obvious that the extension $F_n\mathbb{F}_{q^r}/F_0\mathbb{F}_{q^r}$ is also an abelian extension. Hence, by Lemma 4.1.9, the sequence $\mathcal{S}\cdot\mathbb{F}_{q^r}$ has $\beta_1(\mathcal{S}\cdot\mathbb{F}_{q^r}) = 0$. Then the desired result follows from Lemma 4.1.1. □

Lemma 4.1.11. *Let $\mathcal{F} = (F_k)_{k\geq 0}$ be a tower over a finite field $\mathbb{F}_q$ and $\mathcal{E} := \mathcal{F}\cdot\mathbb{F}_{q^r}$ be the constant field extension of $\mathcal{F}$, for some $r \geq 1$. Set*

$$S := \{P \in \mathbb{P}(F_0) |\deg P = r,\ \textit{all extensions of } P \textit{ in } E \textit{ splits completely in } \mathcal{E}\}.$$

Then

$$\beta_r(\mathcal{F}) \geq \frac{\#S}{\gamma(\mathcal{F})} \quad \textit{and} \quad \gamma(\mathcal{F}) = \gamma(\mathcal{E}).$$

Proof. Since $F_0\mathbb{F}_{q^r}/F_0$ is a constant field extension of degree r, any place $P \in \mathbb{P}(F_0)$ of degree r splits completely in $F_0\mathbb{F}_{q^r}$, and so the lemma is clear. □

Example 4.1.12. Let $q := l^3$ for some prime power l. Consider the tower $\mathcal{H} = (H_k)_{k\geq 0}$ which is recursively defined by the equation

$$(y^l - y)^{l-1} + 1 = \frac{-x^{l(l-1)}}{(x^{l-1}-1)^{l-1}}.$$

This tower is investigated in [3]. Let $H_0 := \mathbb{F}_q(y_0)$ be the rational function field. By [3, Theorems 2.2, 3.4 and 6.5], the following hold:

- $[H_1 : H_0] = l(l-1)$ and $[H_k : H_{k-1}] = l$ for all $k \geq 2$.
- For all $k \geq 0$, the genus $g(F_k) \leq \frac{l^k(l^3+l^2-2l)}{2}$, and $\gamma(\mathcal{H}) \leq \frac{l^2+2l}{2}$.
- The set $Split(\mathcal{H})$ of places of $H_0/\mathbb{F}_q$ which split completely in $\mathcal{H}$ satisfies

$$Split(\mathcal{H}) \supseteq \{(y_0 = \alpha) | \alpha \in \mathbb{F}_{l^3} \setminus \mathbb{F}_l\}.$$

Moreover, by [3, Theorem 2.2], $\mathcal{H}$ is a tower over every constant field $K \supseteq \mathbb{F}_l$. Let $\mathcal{F} = (F_k)_{k\geq 0}$ be the tower over $\mathbb{F}_l$ such that $\mathcal{H} = \mathcal{F}\cdot\mathbb{F}_q$. To estimate $\beta_3(\mathcal{F})$, we first compute the number of degree 3 places of $F_0/\mathbb{F}_l$, then we apply Lemma 4.1.11. It is clear that any degree 3 place $P \in \mathbb{P}(F_0)$ splits completely in H_0 and its extensions are in the set $Split(\mathcal{H}/H_0)$. Now since

$$B_1(H_0) = B_1(F_0) + 3\cdot B_3(F_0),$$

we have $B_3(F_0) = \frac{l^3-l}{3}$, and so

$$\beta_3(\mathcal{F}) \geq \frac{B_3(F_0)}{\gamma(\mathcal{F})} \geq \frac{2(l^3-l)}{3(l^2+2l)}.$$

Bibliography

[1] S. Ballet and R. Rolland, Families of curves over any finite field attaining the generalized Drinfeld-Vladut bound, *Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor.* (2011) Nr. 5-18.

[2] S. Ballet and R. Rolland, Minorations du nombre de classes des corps de fonctions algé briques définis sur un corps fini, *C.R. Acad. Sci. Paris, Ser.* **I 349** (2011) 709-712.

[3] A. Bassa, A. Garcia, and H. Stichtenoth, A new tower over cubic finite fields, *Mosc. Math. J.* **8** (2008), No.3, 401-418.

[4] P. Beelen, Graphs and recursively defined towers of function fields, *J. Number Theory* **108** (2004) 217-240.

[5] I. Cascudo, R. Cramer, C. Xing, and A. Yang, Asymptotic bound for multiplication complexity in the extensions of small finite fields, *To Appear in IEEE Transactions on Information Theory*, DOI:10.1109/TIT.2011.2180696.

[6] V. G. Drinfeld and S. G. Vladut, Number of points of an algebraic curve, *Funct. Anal.* **17** (1983) 53-54.

[7] A. Garcia and H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, *Manuscripta Mathematica* **72** (1991) 67-79.

[8] A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121** (1995) 211-222.

[9] A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61** (1996) 248-273.

[10] A. Garcia, H. Stichtenoth, and H. G. Rück, On tame towers over finite fields, *J. Reine Angew. Math.,* **(557)** (2003) 53-80.

[11] A. Garcia, H. Stichtenoth, and M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3** (1997) 257–274.

[12] T. Hasegawa, A note on optimal towers over finite fields, *Tokyo J. Math.* **30** (2007) No.2.

[13] T. Hasegawa, Asymptotic behavior of higher degree places in towers of function fields over finite fields, PhD Thesis, *Waseda University*, 2007.

[14] T. W. Hungerford, Algebra, Graduate Texts in Mathematics **73** (Springer Verlag, 1974).

[15] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981) 721-724.

[16] S. Lang, Algebraic number theory, 2nd Edition, Graduate Texts in Mathematics **110** (Springer Verlag, 1994).

[17] P. Lebacque, Sur quelques proprietes asymptotiques des corps globaux, PhD Thesis, *Université de Marseille II*, 2007.

[18] P. Lebacque, Quelques résultats effectifs concernant les invariants de Tsfasman-Vladut, *arxiv.org*, (2009).

[19] P. Lebacque, On Tsfasman-Vladut invariants of infinite global fields, *IJNT* **6** (2010) No.6, 1419-1448.

[20] P. Lebacque and A. Zykin, Asymptotic methods in number theory and algebraic geometry, *Publications mathématiques de Basençon* (2011).

[21] J.-P. Serre, Local Fields, Graduate Texts in Mathematics **67** (Springer Verlag, 1979).

[22] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini, *C.R. Acad. Sc. Paris* **t.296** (7 mars 1983).

[23] H. Stichtenoth and M. A. Tsfasman (eds.), Coding theory and algebraic geometry, Lecture Notes in Mathematics **1581** (Springer Verlag, 1991).

[24] H. Stichtenoth, Algebraic function fields and codes, 2nd Edition, Graduate Texts in Mathematics **254** (Springer Verlag, 2009).

[25] M. A. Tsfasman, Some remarks on the asymptotic number of points, *Springer Lect. Notes Math.* **1518** (1992) 178-192.

[26] M. A. Tsfasman and S. G. Vladut, Infinite global fields and the generalized Brauer-Siegel Theorem, *Mosc. Math. J.* **2** (2002), No.2, 329-402.

[27] M. A. Tsfasman, S. G. Vladut, and T. Zink, Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982) 21-28.

[28] J. Wulftange, Zahme Türme algebraischer Funktionenkörper, PhD Thesis, *Essen University* (2002).