Explicit Constructions of Asymptotically Good Towers of Function Fields

Ernest C. Lötter

Thesis presented in partial fulfilment of the requirements for the degree of
MASTER OF SCIENCE at the UNIVERSITY OF STELLENBOSCH.

Supervisor: Professor B W GREEN
Co-supervisor: Professor A B VAN DER MERWE
December 2003

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Abstract

A tower of global function fields $\mathcal{F} = (F_1, F_2, ...)$ is an infinite tower of separable extensions of algebraic function fields of one variable such that the constituent function fields have the same (finite) field of constants and the genus of these tend to infinity. A study can be made of the asymptotic behaviour of the ratio of the number of places of degree one over the genus of $F_i/\mathbb{F}_q$ as i tends to infinity. A tower is called asymptotically good if this limit is a positive number. The well-known Drinfeld-Vlăduţ bound provides a general upper bound for this limit.

In practise, asymptotically good towers are rare. While the first examples were non-explicit, we focus on explicit towers of function fields, that is towers where equations recursively defining the extensions F_{i+1}/F_i are known. It is known that if the field of constants of the tower has square cardinality, it is possible to attain the Drinfeld-Vlăduţ upper bound for this limit, even in the explicit case. If the field of constants does not have square cardinality, it is unknown how close the limit of the tower can come to this upper bound.

In this thesis, we will develop the theory required to construct and analyse the asymptotic behaviour of explicit towers of function fields. Various towers will be exhibited, and general families of explicit formulae for which the splitting behaviour and growth of the genus can be computed in a tower will be discussed. When the necessary theory has been developed, we will focus on the case of towers over fields of non-square cardinality and the open problem of how good the asymptotic behaviour of the tower can be under these circumstances.

Opsomming

'n Toring van globale funksieliggame $\mathcal{F} = (F_1, F_2, ...)$ is 'n oneindige toring van skeibare uitbreidings van algebraïese funksieliggame van een veranderlike sodat die samestellende funksieliggame dieselfde (eindige) konstante liggaam het en die genus streef na oneindig. 'n Studie kan gemaak word van die asimptotiese gedrag van die verhouding van die aantal plekke van graad een gedeel deur die genus van $F_i/\mathbb{F}_q$ soos i streef na oneindig. 'n Toring word asimptoties goed genoem as hierdie limiet 'n positiewe getal is. Die bekende Drinfeld-Vlăduţ grens verskaf 'n algemene bogrens vir hierdie limiet.

In praktyk is asimptoties goeie torings skaars. Terwyl die eerste voorbeelde nie eksplisiet was nie, fokus ons op eksplisiete torings, dit is torings waar die vergelykings wat rekursief die uitbreidings F_{i+1}/F_i bepaal bekend is. Dit is bekend dat as die kardinaliteit van die konstante liggaam van die toring 'n volkome vierkant is, dit moontlik is om die Drinfeld-Vlăduţ bogrens vir die limiet te behaal, selfs in die eksplisiete geval. As die konstante liggaam nie 'n kwadratiese kardinaliteit het nie, is dit onbekend hoe naby die limiet van die toring aan hierdie bogrens kan kom.

In hierdie tesis sal ons die teorie ontwikkel wat benodig word om eksplisiete torings van funksieliggame te konstrueer, en hulle asimptotiese gedrag te analiseer. Verskeie torings sal aangebied word en algemene families van eksplisiete formules waarvoor die splitsingsgedrag en groei van die genus in 'n toring bereken kan word, sal bespreek word. Wanneer die nodige teorie ontwikkel is, sal ons fokus op die geval van torings oor liggame waarvan die kardinaliteit nie 'n volkome vierkant is nie, en op die oop probleem aangaande hoe goed die asimptotiese gedrag van 'n toring onder hierdie omstandighede kan wees.

Preface

The preparation of this thesis has led me to consider a much larger problem than I considered initially. Looking at explicit asymptotically good towers over a field of non-square cardinality, this led me to consider the recent history of the more general problem of constructing explicit towers over arbitrary finite fields, and to discuss the theory necessary to analyze their asymptotic behaviour. It is my hope that this dissertation will be an interesting self-contained read, while it retains the spirit of research in this field in recent years.

For the most part, I discuss the work of numerous other authors. Original work is included in Sections 5.3 and 5.4. As it stands, I believe that the approach taken in the latter section may yield further results, leaving an interesting avenue open for future research.

I would like to express my gratitude to Professor BW Green for his patience and the many fruitful discussions we had. His support and many helpful comments were essential towards the successful completion of this thesis.

The support of friends and family was also indispensable. Firstly, I wish to thank my parents for their unfaltering support and encouragement at all times. My thanks also go out to many friends, in particular fellow Huis de Villiers residents Gerhard Venter and Adriaan de Haan.

During 2002 and 2003 I was financially supported by Postgraduate Merit bursaries of the University of Stellenbosch, a GG Cillié scholarship, NRF Grantholder-linked bursaries awarded through Professor Green and an NRF/DoL Scarce Skills scholarship. The financial assistance of the National Research Foundation (NRF) towards this research is hereby gratefully acknowledged. In accordance with a condition of the NRF scholarship, I hereby declare that the opinions expressed and conclusions arrived at in this dissertation are those of myself and are not necessarily to be attributed to the National Research Foundation. During the time of study I was also partially supported by being employed as a part-time research assistant in the Department of Mathematics at the University of Stellenbosch, for which I am also very thankful.

Contents

Chapter 1

Introduction

Two of the most fundamental properties of an algebraic function field F/K are the number of places of degree one and the genus. For global function fields, these are bounded in terms of each other by the celebrated Hasse-Weil theorem. One can start making separable extensions of a field F_1, and obtain an infinite tower $F_1 \subseteq F_2 \subseteq F_3 \subseteq ...$ of them. Under certain simple conditions, we will call this a tower of function fields, denoted by $\mathcal{F}$, over K.

For the largest part of this dissertation, we will be assuming we are working with global function fields, that is function fields F/K where K is a finite field. We will, for the most part, be interested in the asymptotic behaviour of the number of places of degree one relative to the genus in a tower $\mathcal{F}$. This will lead us towards investigating the quantity

$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)}$$

where $N(F_i)$ denotes the number of places of degree one and $g(F_i)$ the genus of F_i/K. Restricting our attention to global function fields, the Hasse-Weil theorem provides an upper bound for $\lambda(\mathcal{F})$, by bounding $N(F_i)$. This upper bound was improved significantly by Drinfeld and Vlăduţ [35]. The number $\lambda(\mathcal{F})$ is bounded above by

$$A(q) = \lim_{g \to \infty} \sup \frac{N_q(g)}{g}$$

if $\mathcal{F}$ is defined over $\mathbb{F}_q$, where $N_q(g)$ denotes the maximal number of places of degree one which can be attained in a function field of genus g. It becomes an interesting problem to investigate how close $A(q)$ can come to the Drinfeld-Vlăduţ bound. Many of the constructions we will discuss have improved lower bounds for the quantity $A(q)$ for specific q, by constructing a tower $\mathcal{F}$ having an improved limit $\lambda(\mathcal{F})$, over $\mathbb{F}_q$.

The asymptotic properties of towers of algebraic function fields were put in the spotlight after Goppa [14] came up with the idea of associating an error-correcting code with a linear system on an algebraic curve over a finite field. This led to the construction of the first codes attaining the Gilbert-Varshamov bound from coding theory. This unexpected link between coding theory and algebraic geometry revived much interest in the field of counting points on curves, as is apparent from the wealth of papers produced after this landmark result. As we can translate results on non-singular algebraic curves to function fields, this explains much of the interest in towers of function fields since 1981. To be useful towards the aim of yielding asymptotically good codes, a tower $\mathcal{F}$ must be asymptotically good, that is $\lambda(\mathcal{F}) > 0$. Practical implementation of the code also requires explicit equations for each extension step in the tower.

While the applications to coding theory created much of the original motivation for the construction of asymptotically good towers, the aim of our discussions will not be to apply these constructions of towers to the construction of codes. The problem of constructing asymptotically good towers of function fields is certainly a worthy and interesting problem in its own right, as is made clear by the abundance of mathematicians working in this field. To further this point, it is interesting to note that the applications of explicit asymptotically good towers are certainly not limited to coding theory. One such example is a 1999 paper by Ballet [1] in which the bilinear complexity of multiplication in extensions of $\mathbb{F}_q$ is bounded by using an explicit asymptotically optimal tower.

Many asymptotically good non-explicit towers were constructed after the initial impetus to do so in the early 1980's. Ihara [15] constructed, over any finite field of square cardinality, a non-explicit tower of function fields which attains the Drinfeld-Vlăduţ bound by employing modular curves. Attention turned to improving results over fields of non-square cardinality, and Serre [26] proved the existence of asymptotically good towers over every finite field by providing a general, but weak, lower bound for $\lambda(\mathcal{F})$. Xing and Niederreiter used class field towers [20] and narrow ray class fields [21] to prove the existence of some asymptotically good towers with improved lower bounds for $\lambda(\mathcal{F})$. Zink [36] provided improvements in certain special cases when the cardinality of the field of constants is not a square.

It then came as a surprise in 1995, when García and Stichtenoth [9] exhibited an explicit tower of Artin-Schreier extensions over any finite field of square cardinality which met the upper bound of Drinfeld and Vlăduţ. This construction was followed by another optimal construction by them the following year in [10]. In 1997 García,

Stichtenoth and Thomas [13] exhibited explicit asymptotically good Kummer towers over every finite field, which also meet the Drinfeld-Vlăduţ bound over some finite fields.

The problem remained to improve the limit λ for towers defined over a non-square finite field. Methods to obtain lower bounds in this case were suggested by García, Stichtenoth and Thomas [13] for tamely ramified towers, and generalized by Van der Merwe [34] to be useful even in wildly ramified towers. Deolalikar [2] provided a large family of explicit towers where the extensions are made using equations involving symmetric and quasi-symmetric functions. This family of constructions allow for easy computation of the genus and number of places of degree one in the extension field. In 2001, Van der Geer and Van der Vlugt [32] constructed an explicit tower of Artin-Schreier extensions over $\mathbb{F}_8$ which is asymptotically good, and a vast improvement for the known bounds over that field.

The aim of this thesis will be to develop the theory necessary to discuss the construction of some of the above-mentioned explicit asymptotically good towers. In Chapter 2, we will introduce some of the theory leading up to the Hurwitz genus formula for function fields, based on the exposition of Stichtenoth [27]. From there on, we will assume that we are working with global function fields, and consider specific extension types of function fields. We will exhibit results on the calculation of the different exponent, and cite formulae for the genus and splitting behaviour of places in Kummer, Artin-Schreier and linearized extensions. These will be essential as they will be used extensively in the constructions of the later chapters. We will then prove the first asymptotic result, the Drinfeld-Vlăduţ bound.

Chapter 3 will introduce some preliminary properties of towers. We will discuss some of the asymptotic bounds given by non-explicit towers, in order to compare them with the explicit towers we will construct. García and Stichtenoth's asymptotically optimal tower (over fields of square cardinality) will be discussed. We will show that asymptotically good (but not necessarily optimal) towers exist over an arbitrary finite field by considering two towers of Kummer extensions of García and Stichtenoth, which were subsequently generalized by Deolalikar. As these towers are tamely ramified, we show some results which simplify the analysis of the asymptotic behaviour for tamely ramified towers, and a generalization by Van der Merwe which makes essentially the same method applicable to certain wildly ramified towers.

At this stage, most of the available explicit towers are based on explicit equations involving the trace and norm. Deolalikar's work on using extensions involving symmetric and quasi-symmetric functions is discussed in Chapter 4. Most of the known

explicit extensions are so-called trace-norm (Hermitian) constructions, but the notions of symmetry and quasi-symmetry widen the scope considerably, providing explicit equations for extensions of function fields over arbitrary finite fields where the usual trace-norm constructions can be generalized considerably. The necessary theory is also developed to make it possible to calculate the genus and number of places of degree one of the extension field precisely for the case of symmetric extensions. For quasi-symmetric extensions, we are able to split all places, but the calculation of the genus becomes difficult. For this reason, much of the emphasis of the latter part of this chapter is concerned with splitting as many places as possible in an extension, rather than minimizing the genus. This yields high $N(F_i)/[F_i : F_1]$ ratios rather than high $N(F_i)/g(F_i)$ ratios. The splitting behaviour of one such family of extensions, which could be named a trace-subtrace extension of the rational function field, is advocated by Deolalikar to be a more natural generalization of the Hermitian function field, and which need not be defined over a field of square cardinality.

In Chapter 5 we begin a discussion of Van der Geer and Van der Vlugt's tower of function fields over $\mathbb{F}_8$. This shows an asymptotically good tower, composed of explicit (Artin-Schreier) extensions which, while it does not quite meet the Drinfeld-Vlăduţ bound, comes very close. We continue to show that this wildly ramified tower can alternatively be shown to be asymptotically good (with a weaker lower bound) by using Van der Merwe's method for wildly ramified towers. We then extend the field of constants to (the non-square) $\mathbb{F}_{512}$ and show that the tower obtained in this way improves the lower bounds given by Xing and Niederreiter's non-explicit constructions over this finite field. Computer-aided results showing candidate equations for other explicit towers over small non-square fields are given by searching for such equations with good splitting behaviour, and equations are obtained for several cases in characteristic two, as well as two families of completely splitting extensions in $\mathbb{F}_{27}$. The splitting behaviour of these extensions are illustrated using splitting graphs. The latter two sections of this chapter and the computational results obtained therein are original work.

Appendix A presents some of the introductory elements of the theory of algebraic function fields. As these are rather standard results, proofs of the results stated there are mostly omitted. Appendix B contains some of the calculations done and programs written using the MAGMA computational algebra system.

Chapter 2

Preliminaries

We will briefly introduce some key notions involving differentials on algebraic function fields, canonical divisors, the Riemann-Roch Theorem, and derive the Hurwitz genus formula in order to create the machinery with which to calculate the genera of extensions of function fields. We will also look at specific families of extensions, in order to handle calculations on constructions in subsequent chapters. The exposition given here is based on that of Stichtenoth [27], and is provided as a convenience to lay the groundwork for the foundation we will require for the later chapters.

Definition 2.1. *An adele of the function field F/K is a mapping*

$$\alpha : \begin{cases} S(F/K) & \longrightarrow & F \\ P & \longmapsto & \alpha_P \end{cases}$$

such that $\alpha_P \in \mathcal{O}_P$ for almost all $P \in S(F/K)$.

The adele space of F/K is defined as

$$\mathbb{A}_F := \{\alpha : \alpha \text{ is an adele of } F/K\},$$

which can be regarded as a vector space over K. We can regard any element of the adele space as an element of the direct product $\prod_{P \in S(F/K)} F$ and hence we write $\alpha = (\alpha_P)_{P \in S(F/K)} = (\alpha_P)$.

The principal adele of an element $x \in F$ is the adele $\alpha = (x)_{P \in S(F/K)}$, thereby giving an embedding $F \hookrightarrow \mathbb{A}_F$. Valuations v_P on F/K extend naturally from F to $\mathbb{A}_F$ by setting $v_P(\alpha) := v_P(\alpha_P)$. Note that the extension of v_P to $\mathbb{A}_F$ is a natural extension as a map, but is not a valuation. We do however still denote it by v_P. By definition, $v_P(\alpha) \geq 0$ for all but finitely many $P \in S(F/K)$.

Definition 2.2. *For $A \in \mathrm{Div}(F)$ we define*

$$\mathbb{A}_F(A) := \{\alpha \in \mathbb{A}_F : v_P(\alpha) \geq -v_P(A) \text{ for all } P \in S(F/K)\},$$

which is a K-subspace of $\mathbb{A}_F$.

We also briefly recall some of the definitions concerning Weil differentials.

Definition 2.3. *A Weil differential of F/K is a K-linear map $\omega : \mathbb{A}_F \longrightarrow K$ vanishing on $(\mathbb{A}_F(A) + F)$ for some divisor $A \in \mathrm{Div}(F)$. Let*

$$\Omega_F := \{\omega : \omega \text{ is a Weil differential of } F/K\}$$

be the module of Weil differentials of F/K (which can be regarded as a K-vector space), and

$$\Omega_F(A) := \{\omega \in \Omega_F : \omega \text{ vanishes on } \mathbb{A}_F(A) + F\}$$

a subspace of Ω_F.

Ω_F is a vector space over F, when considering that for $x \in F$ and $\omega \in \Omega_F$, $(x\omega)(\alpha) := \omega(x\alpha)$ is again a Weil differential of F/K. As ω vanishes on $\mathbb{A}_F(A) + F$, it follows that $x\omega$ vanishes on $\mathbb{A}_F(A + (x)) + F$. It can be shown that Ω_F is in fact a one-dimensional vector space over F.

Definition 2.4. *The divisor (ω) of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/K so that if ω vanishes on $\mathbb{A}_F(A) + F$, then $A \leq (\omega)$. For a proof that this is indeed well-defined, consult [27, I.5.10].*

We define $v_P(\omega) := v_P((\omega))$, and identify a place $P \in S(F/K)$ as a zero (resp. pole) of ω if $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). We call ω *regular at* P if $v_P(\omega) \geq 0$, and ω is called *regular* if it is regular at every $P \in S(F/K)$. We call the divisor W a *canonical divisor* of F/K if $W = (\omega)$ for some $\omega \in \Omega_F$.

It can be shown that $(x\omega) = (x) + (\omega)$ for $0 \neq x \in F$ and $0 \neq \omega \in \Omega_F$. Moreover, if W_1 and W_2 are any two canonical divisors of F/K, then $W_1 \sim W_2$, i.e. they are equivalent as elements of the divisor class group $\mathrm{Cl}(F)$.

For an arbitrary $A \in \mathrm{Div}(F)$ and a canonical divisor $W = (\omega)$ of F/K, it can be shown that the mapping

$$\mu : \begin{cases} \mathcal{L}(W - A) & \longrightarrow & \Omega_F(A) \\ x & \longmapsto & x\omega \end{cases}$$

is an isomorphism of K-vector spaces. We have

Theorem 2.5 (Riemann-Roch). *Let W be a canonical divisor of F/K. Then, for any $A \in \mathrm{Div}(F)$, we have*

$$\dim A = \deg A + 1 - g + \dim(W - A).$$

Corollary 2.6. *For a canonical divisor W, we have*

$$\deg W = 2g - 2 \text{ and } \dim W = g.$$

Hence, by Riemann-Roch, if $\deg A \geq 2g - 1$ we must have $\deg(W - A) < 0$, implying that $\dim(W - A) = 0$, i.e. $\dim A = \deg A + 1 - g$.

A useful characterization of a canonical divisor is that

$$W \text{ is canonical} \iff \deg W = 2g - 2 \text{ and } \dim W \geq g. \tag{2.0.1}$$

2.1 The Hurwitz Formula

A common problem arising in the study of extensions of function fields, is the calculation of the genus. We will discuss the derivation of the Hurwitz genus formula, with which we can calculate the genus of finite extensions of algebraic function fields.

Let F/K be an algebraic function field, F'/F a finite separable extension, and K' the constant field of F'. It is clear that K'/K is a finite separable extension as well.

Definition 2.7. *For $P \in S(F/K)$, let $\mathcal{O}'_P$ denote the integral closure of $\mathcal{O}_P$ in F'. Then the set*

$$\mathcal{C}_P := \left\{ z \in F' : \mathrm{Tr}_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P \right\}$$

is called the complementary module over $\mathcal{O}_P$.

Note that $\mathcal{C}_P$ is trivially an $\mathcal{O}'_P$-module and $\mathcal{O}'_P \subseteq \mathcal{C}_P$ since $\mathrm{Tr}_{F'/F}(\mathcal{O}'_P) \subseteq \mathcal{O}_P$.

Proposition 2.8. *If $\{z_1, ..., z_n\}$ is an integral basis of $\mathcal{O}'_P$ over $\mathcal{O}_P$, then*

$$\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot z_i^*$$

where $\{z_1^*, ..., z_n^*\}$ is the dual basis of $\{z_1, ..., z_n\}$. (The dual basis is a basis $\{z_1^*, ..., z_n^*\} \subseteq F'$ such that $\mathrm{Tr}_{F'/F}(z_i z_j^*) = \delta_{ij}$, the Kronecker symbol.)

Proof. $(\subseteq)$: Consider $z \in \mathcal{C}_P$. As $\{z_1^*, ..., z_n^*\}$ is a basis of F'/F, there exist $x_1, ..., x_n \in F$ with $z = \sum_{i=1}^n x_i z_i^*$. Since $z \in \mathcal{C}_P$ and $z_1, ..., z_n \in \mathcal{O}'_P$, $\mathrm{Tr}_{F'/F}(zz_j) \in \mathcal{O}_P$ for $1 \leq j \leq n$. Then

$$\begin{aligned} \mathrm{Tr}_{F'/F}(zz_j) &= \mathrm{Tr}_{F'/F}\left(\sum_{i=1}^n x_i z_i^* z_j\right) \\ &= \sum_{i=1}^n x_i \cdot \mathrm{Tr}_{F'/F}(z_i^* z_j) \\ &= x_j. \end{aligned}$$

Therefore $x_j \in \mathcal{O}_P$ and $z \in \sum_{i=1}^n \mathcal{O}_P \cdot z_i^*$.

$(\supseteq)$: Let $z = \sum_{i=1}^n x_i z_i^* \in \sum_{i=1}^n \mathcal{O}_P \cdot z_i^*$, and $u = \sum_{j=1}^n y_j z_j \in \mathcal{O}'_P$. Then

$$\begin{aligned} \mathrm{Tr}_{F'/F}(zu) &= \mathrm{Tr}_{F'/F}\left(\sum_{i,j=1}^n x_i y_j z_i^* z_j\right) \\ &= \sum_{i,j=1}^n x_i y_j \mathrm{Tr}_{F'/F}(z_i^* z_j) \\ &= \sum_{i=1}^n x_i y_i \in \mathcal{O}_P, \end{aligned}$$

and hence $z \in \mathcal{C}_P$. □

Proposition 2.9. *There is an element $t \in F'$ (depending on P) such that $\mathcal{C}_P = t \cdot \mathcal{O}'_P$. Moreover $v_{P'}(t) \leq 0$ for any $P'|P$; and t is unique up to $v_{P'}(t)$ for $P'|P$.*

Proof. By Proposition 2.8 we know that $\mathcal{C}_P = \sum_{i=1}^n \mathcal{O}_P \cdot u_i$ for some $u_i \in F'$. By the Approximation Theorem we can choose $x \in F$ such that $v_P(x) \geq 0$ and $v_P(x) \geq -v_{P'}(u_i)$ for all $P'|P$ and $1 \leq i \leq n$. Then

$$v_{P'}(xu_i) = e(P'|P) \cdot v_P(x) + v_{P'}(u_i) \geq 0$$

for all $P'|P$ and $1 \leq i \leq n$, and it follows that $x\mathcal{C}_P \subseteq \mathcal{O}'_P$. $x\mathcal{C}_P$ is an ideal of $\mathcal{O}'_P$, and hence $x\mathcal{C}_P = y\mathcal{O}'_P$ for some $y \in \mathcal{O}'_P$, since $\mathcal{O}'_P$ is a principal ideal domain. Taking $t = x^{-1}y$ we have $\mathcal{C}_P = t \cdot \mathcal{O}'_P$. Since $\mathcal{O}'_P \subseteq \mathcal{C}_P$, it follows that $v_{P'}(t) \leq 0$ for all $P'|P$. Finally

$$\begin{aligned} t\mathcal{O}'_P = t'\mathcal{O}'_P &\iff t(t')^{-1} \in \mathcal{O}'_P \text{ and } t^{-1}t' \in \mathcal{O}'_P \\ &\iff v_{P'}\left(t(t')^{-1}\right) \geq 0 \text{ and } v_{P'}(t^{-1}t') \geq 0 \text{ for all } P'|P \\ &\iff v_{P'}(t) = v_{P'}(t') \text{ for all } P'|P. \end{aligned}$$

□

Proposition 2.10. *$\mathcal{C}_P = \mathcal{O}'_P$ for almost all $P \in S(F/K)$.*

Proof. Taking any basis $\{z_1, ..., z_n\}$ of F'/F, we know that both itself and its dual basis $\{z_1^*, ..., z_n^*\}$ are integral bases for almost all $P \in S(F/K)$, by [27, III.3.6]. So, the basis $\{z_1, ..., z_n\}$ and its dual basis are simultaneously integral for almost all $P \in S(F/K)$, which using Theorem 2.8 yields the desired result. □

Definition 2.11. *Consider a place $P \in S(F/K)$ and the integral closure $\mathcal{O}'_P$ of $\mathcal{O}_P$ in F'. Let $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ be the complementary module over $\mathcal{O}_P$. Then, for $P'|P$, we define the different exponent of P' over P by*

$$d(P'|P) = -v_{P'}(t).$$

By Proposition 2.9, $d(P'|P)$ is independent of the choice of t, and hence well-defined. Moreover we have that $d(P'|P) \geq 0$, and Proposition 2.10 implies that $d(P'|P) = 0$ for almost all $P \in S(F/K)$, for $\mathcal{C}_P = 1 \cdot \mathcal{O}'_P$ for almost all $P \in S(F/K)$. We can therefore define the divisor

$$\mathrm{Diff}(F'/F) := \sum_{P \in S(F/K)} \sum_{P'|P} d(P'|P)\, P',$$

which is called the *different* of F'/F. Observe that $\mathrm{Diff}(F'/F)$ is a positive divisor of F'.

A useful characterization of the complementary module $\mathcal{C}_P$ is that, for $z \in F'$ we have

$$z \in \mathcal{C}_P \iff v_{P'}(z) \geq -d(P'|P) \text{ for all } P'|P.$$

We define

$$\mathbb{A}_{F'/F} := \{\alpha \in A_{F'} : \alpha_{P'} = \alpha_{Q'} \text{ whenever } P' \cap F = Q' \cap F\}$$

which is an F'-subspace of $\mathbb{A}_{F'}$. $\mathbb{A}_{F'/F}$ consists of adeles with values at places lying above a given place $P \in S(F/K)$ being equal. We can extend the trace map $\mathrm{Tr}_{F'/F} : F' \longrightarrow F$ to an F-linear map (which we denote again by $\mathrm{Tr}_{F'/F}$) from $\mathbb{A}_{F'/F}$ to $\mathbb{A}_F$ by

$$\mathrm{Tr}_{F'/F} : \begin{cases} \mathbb{A}_{F'/F} & \longrightarrow & \mathbb{A}_F \\ \alpha = (\alpha_{P'}) & \longmapsto & \left(\mathrm{Tr}_{F'/F}(\alpha_{P'})\right) \end{cases}$$

for any place $P'|P$. The image is an adele, since $\alpha_{P'} \in \mathcal{O}_{P'}$ for almost all $P' \in S(F'/K')$ implies that $\mathrm{Tr}_{F'/F}(\alpha_{P'}) \in \mathcal{O}_P$ for almost all $P \in S(F/K)$. We want to show that given a Weil differential ω of F/K, we can lift it in a unique way to a Weil differential ω' of F'/K' such that

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right)$$

for any $\alpha \in \mathbb{A}_{F'/F}$. We call this Weil differential ω' the cotrace of ω in F'/F, and it is denoted by $\mathrm{Cotr}_{F'/F}(\omega)$. Moreover we will show that we then have that

$$(\omega') = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$$

(if $\omega \neq 0$) which gives us a way to relate the canonical divisors of the function fields F'/K' and F/K. We will do this in several steps:

Lemma 2.12. *For any $C' \in \mathrm{Div}(F')$, we have $\mathbb{A}_{F'} = \mathbb{A}_{F'/F} + \mathbb{A}_{F'}(C')$.*

Proof. Let $\alpha = (\alpha_{P'}) \in \mathbb{A}_{F'}$. By the Approximation Theorem, for all $P \in S(F/K)$, there exists $x_P \in F'$ with

$$v_{P'}(\alpha_{P'} - x_P) \geq -v_{P'}(C') \text{ for all } P'|P.$$

If we set $\beta := (\beta_{P'})$ with $\beta_{P'} = x_P$ whenever $P'|P$, then $\beta \in \mathbb{A}_{F'/F}$ and $\alpha - \beta = (\alpha_{P'} - x_P)_{P'|P, P' \in S(F'/K')} \in \mathbb{A}_{F'}(C')$. Since $\alpha = \beta + (\alpha - \beta)$, the result follows. □

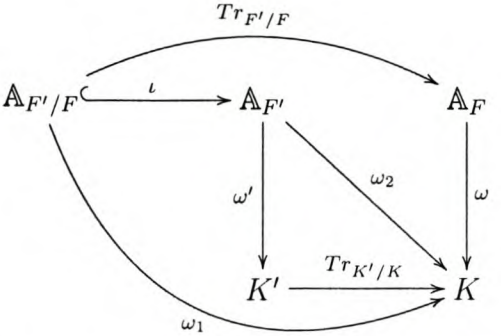
Theorem 2.13. *For every Weil differential ω of F/K there exists a unique Weil differential ω' of F'/K' such that*

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right)$$

for all $\alpha \in \mathbb{A}_{F'/F}$. If $\omega \neq 0$ then

$$(\omega') = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F).$$

We will set $W' := \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$ for use in the following lemmas and ultimate proof of the theorem. In order to clarify the need for the next three lemmas, consider the following:



The map ω is the initial Weil differential, from which we will construct ω_1, ω_2 and finally ω'. We will see in the coming lemmas that the diagram commutes, eventually giving us the desired differential ω', corresponding to the canonical divisor of the extension F'/K' of F/K.

Lemma 2.14. *The map*

$$\omega_1 : \begin{cases} \mathbb{A}_{F'/F} & \longrightarrow & K, \\ \alpha & \longmapsto & \omega \circ \mathrm{Tr}_{F'/F}(\alpha). \end{cases}$$

is

(i) K-linear,

(ii) vanishes on $\mathbb{A}_{F'/F}(W') + F'$; and

(iii) if $B' \in \mathrm{Div}(F')$ with $B' \not\leq W'$, then ω_1 does not vanish on $\mathbb{A}_{F'/F}(B')$.

Proof.

(i) The map ω_1 is K-linear since both ω and $\mathrm{Tr}_{F'/F}$ are.

(ii) ω_1 vanishes on F' since ω vanishes on F. Now let $\alpha \in \mathbb{A}_{F'/F}(W')$ and choose $x \in F$ with $v_P(x) = v_P(\omega)$. Then

$$\begin{aligned} v_{P'}(x\alpha_{P'}) &= v_{P'}(x) + v_{P'}(\alpha_{P'}) \\ &\geq e(P'|P) \cdot v_P(\omega) - v_{P'}(W') \\ &= v_{P'}\left(\mathrm{Con}_{F'/F}((\omega)) - W'\right) \\ &= -v_{P'}(\mathrm{Diff}(F'/F)) \\ &= -d(P'|P). \end{aligned}$$

Hence $x\alpha_{P'} \in \mathcal{C}_P$ (by definition), and $v_P\left(\mathrm{Tr}_{F'/F}(x\alpha_{P'})\right) \geq 0$. Since

$$\mathrm{Tr}_{F'/F}(x\alpha_{P'}) = x \cdot \mathrm{Tr}_{F'/F}(\alpha_{P'})$$

and $v_P(x) = v_P(\omega)$, we have that $v_P\left(\mathrm{Tr}_{F'/F}(\alpha_{P'})\right) \geq -v_P(\omega)$ for any $P'|P$, $P \in S(F/K)$, and hence $\alpha \in \mathbb{A}_F((\omega)) = \mathbb{A}_F(W)$, implying that $\omega_1(\alpha) = 0$.

(iii) $B' \not\leq W'$ implies that there exists $P_0 \in S(F/K)$ such that

$$v_{P^*}\left(\mathrm{Con}_{F'/F}((\omega)) - B'\right) < -d(P^*|P_0)$$

for some $P^*|P_0$. Let $\mathcal{O}'_{P_0}$ denote the integral closure of $\mathcal{O}_{P_0}$ in F', and $\mathcal{C}_{P_0}$ denote the complementary module over $\mathcal{O}_{P_0}$. Consider the set

$$J := \left\{z \in F' : v_{P^*}(z) \geq v_{P^*}\left(\mathrm{Con}_{F'/F}((\omega)) - B'\right) \text{ for all } P^*|P_0\right\}.$$

By the Approximation Theorem, there exists $u \in J$ satisfying

$$v_{P^*}(u) = v_{P^*}\left(\mathrm{Con}_{F'/F}((\omega)) - B'\right) \text{ for all } P^*|P_0.$$

Hence $J \nsubseteq \mathcal{C}_{P_0}$ by the characterization of the complementary module on page 9. Since $J \cdot \mathcal{O}'_{P_0} \subseteq J$ it follows that $\mathrm{Tr}_{F'/F}(J) \nsubseteq \mathcal{O}_{P_0}$. Choose a local parameter $t \in F$ for the place P_0, i.e. $v_{P_0}(t) = 1$. For some $r \geq 0$ we have $t^r J \subseteq \mathcal{O}'_{P_0}$, so

$$t^r \cdot \mathrm{Tr}_{F'/F}(J) = \mathrm{Tr}_{F'/F}(t^r J) \subseteq \mathcal{O}_{P_0}.$$

It is easily shown that $t^r \cdot \mathrm{Tr}_{F'/F}(J)$ is an ideal of $\mathcal{O}_{P_0}$, and consequently $t^r \cdot \mathrm{Tr}_{F'/F}(J) = t^s \mathcal{O}_{P_0}$ for some $s \geq 0$, and we obtain $\mathrm{Tr}_{F'/F}(J) = t^m \mathcal{O}_{P_0}$ for some $m \in \mathbb{Z}$. Since $\mathrm{Tr}_{F'/F}(J) \nsubseteq \mathcal{O}_{P_0}$, we have $m \leq -1$ and hence $t^{-1}\mathcal{O}_{P_0} \subseteq \mathrm{Tr}_{F'/F}(J)$.
We can find an element $x \in F$ with

$$v_{P_0}(x) = -v_{P_0}(\omega) - 1 \text{ and } \omega_{P_0}(x) \neq 0.$$

Choose $y \in F$ so that $v_{P_0}(y) = v_{P_0}(\omega)$, so $xy \in t^{-1}\mathcal{O}_{P_0}$. Since $t^{-1}\mathcal{O}_{P_0} \subseteq \mathrm{Tr}_{F'/F}(J)$ there is some $z \in J$ with $\mathrm{Tr}_{F'/F}(z) = xy$. Consider $\beta \in \mathbb{A}_{F'/F}$ given by

$$\beta_{P'} := \begin{cases} 0 & \text{if } P' \nmid P_0, \\ y^{-1}z & \text{if } P' \mid P_0. \end{cases}$$

It follows from the definition of J that for $P'|P_0$

$$\begin{aligned} v_{P'}(\beta) &= -v_{P'}(y) + v_{P'}(z) \\ &\geq -v_{P'}\left(\mathrm{Con}_{F'/F}((\omega))\right) + v_{P'}\left(\mathrm{Con}_{F'/F}((\omega)) - B'\right) \\ &= -v_{P'}(B') \end{aligned}$$

and hence $\beta \in \mathbb{A}_{F'/F}(B')$. Finally,

$$\begin{aligned} \omega_1(\beta) &= \omega\left(\mathrm{Tr}_{F'/F}(\beta)\right) = \sum_P \omega_P\left(\left(\mathrm{Tr}_{F'/F}(\beta)\right)_P\right) \\ &= \sum_P \omega_P\left(\left(\mathrm{Tr}_{F'/F}\left(\frac{z}{y}\right)\right)_P\right) = \sum_P \omega_P\left(\left(\mathrm{Tr}_{F'/F}(x)\right)_P\right) \\ &= \omega_{P_0}(x) \neq 0, \end{aligned}$$

implying that ω_1 does not vanish on $\mathbb{A}_{F'/F}(B')$, as required.

□

Lemma 2.15. *Consider the map*

$$\omega_2 : \begin{cases} \mathbb{A}_{F'} & \longrightarrow & K, \\ \alpha & \longmapsto & \omega_1(\beta). \end{cases}$$

where ω_1 is the K-linear map from the previous lemma, and $\alpha = \beta + \gamma$ with $\beta \in \mathbb{A}_{F'/F}$ and $\gamma \in \mathbb{A}_{F'}(W')$ (this representation exists by Lemma 2.12). The map ω_2 is

(i) well-defined,

(ii) vanishes on $\mathbb{A}_{F'}(W') + F'$ and

(iii) if $B' \in \mathrm{Div}(F')$ with $B' \nleq W'$, then ω_2 does not vanish on $\mathbb{A}_{F'}(B')$.

Proof. If $\alpha = \beta + \gamma = \beta_1 + \gamma_1$ with $\beta, \beta_1 \in \mathbb{A}_{F'/F}$ and $\gamma, \gamma_1 \in \mathbb{A}_{F'}(W')$ then

$$\beta_1 - \beta = \gamma - \gamma_1 \in \mathbb{A}_{F'/F} \cap \mathbb{A}_{F'}(W') = \mathbb{A}_{F'/F}(W')$$

and hence $\omega_1(\beta_1) - \omega_1(\beta) = \omega_1(\beta_1 - \beta) = 0$ by Lemma 2.14(ii), implying (i).
(ii) and (iii) follow by applying Lemma 2.14 to ω_2, and similarly ω_2 is K-linear as well. □

We have constructed the K-linear map $\omega_2 : \mathbb{A}_{F'} \to K$, but we still do not know whether it is a Weil differential of F'/K', since we could be extending the field of constants as well, i.e. we could have that $K \subsetneq K'$. We lift ω_2 to a K'-linear map in the next lemma.

Lemma 2.16. *There exists a K'-linear map $\omega' : \mathbb{A}_{F'} \longrightarrow K'$ such that*

(i) $\mathrm{Tr}_{K'/K} \circ \omega' = \omega_2$,

(ii) ω' vanishes on $\mathbb{A}_{F'}(W') + F'$ and

(iii) if $B' \in \mathrm{Div}(F')$ with $B' \nleq W'$, then ω' does not vanish on $\mathbb{A}_{F'}(B')$.

Proof.

(i) Such ω' exists uniquely by the universal property of the trace with respect to linear maps.

(ii) Since ω' is K'-linear, the image of $\mathbb{A}_{F'}(W') + F'$ under ω' is either 0 or the whole of K'. In the latter case, there exists $\alpha \in \mathbb{A}_{F'}(W') + F'$ such that $\mathrm{Tr}_{K'/K}(\omega'(\alpha)) \neq 0$, since $\mathrm{Tr}_{K'/K} : K' \longrightarrow K$ is not the zero map. Since $\omega_2 = \mathrm{Tr}_{K'/K} \circ \omega'$, $\omega_2(\alpha) \neq 0$, contradicting Lemma 2.15(ii).

(iii) By Lemma 2.15(iii) there exists $\beta \in \mathbb{A}_{F'}(B')$ with $\omega_2(\beta) \neq 0$, implying that $\mathrm{Tr}_{K'/K}(\omega'(\beta)) \neq 0$ and the result follows.

□

Proof (Theorem 2.13). *Existence*: For $\omega = 0$ let $\omega' := 0$. We therefore assume from here onwards that $\omega \neq 0$. The construction and ω_1, ω_2 and ω' in Lemmata 2.14, 2.15 and 2.16 readily show that, for $\alpha \in \mathbb{A}_{F'/F}$,

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega_2(\alpha) = \omega_1(\alpha) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right)$$

with $\omega' : \mathbb{A}_{F'} \longrightarrow K'$ a K'-linear map, and we have that

$$(\omega') = W' = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F),$$

as required.
Uniqueness: Suppose ω^* is another Weil differential of F'/K' satisfying

$$\mathrm{Tr}_{K'/K}(\omega^*(\alpha)) = \omega\left(\mathrm{Tr}_{F'/F}(\alpha)\right) = \mathrm{Tr}_{K'/K}(\omega'(\alpha))$$

for all $\alpha \in \mathbb{A}_{F'/F}$. If we set $\eta := \omega^* - \omega'$, we obtain

$$\mathrm{Tr}_{K'/K}(\eta(\alpha)) = 0 \text{ for all } \alpha \in \mathbb{A}_{F'/F}.$$

Since η is a Weil differential on F'/K', η vanishes on $\mathbb{A}_{F'}(C')$ for some $C' \in \mathrm{Div}(F')$. By Lemma 2.12 it follows that $\mathrm{Tr}_{K'/K}(\eta(\alpha)) = 0$ for all $\alpha \in \mathbb{A}_{F'}$, implying $\eta = 0$ and $\omega' = \omega^*$. □

Proposition 2.17 ([27, III.4.10]). *The cotrace mapping*

$$\mathrm{Cotr}_{F'/F} : \begin{cases} \Omega_F & \longrightarrow & \Omega_{F'} \\ \omega & \longmapsto & \mathrm{Cotr}_{F'/F}(\omega) \end{cases}$$

is F'-linear and for a tower $F \subseteq F' \subseteq F''$ of finite separable extensions we have

$$\mathrm{Cotr}_{F''/F} = \mathrm{Cotr}_{F''/F'} \circ \mathrm{Cotr}_{F'/F}.$$

Corollary 2.18. *In a tower $F \subseteq F' \subseteq F''$ of finite separable extensions we have*

$$\mathrm{Diff}(F''/F) = \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F').$$

Proof. Choose $0 \neq \omega \in \Omega_F$. By Theorem 2.13 we have

$$\left(\mathrm{Cotr}_{F''/F}(\omega)\right) = \mathrm{Con}_{F''/F}((\omega)) + \mathrm{Diff}(F''/F).$$

On the other hand, the properties of the cotrace and the conorm (A.18) implies that

$$\begin{aligned}\left(\mathrm{Cotr}_{F''/F}(\omega)\right) &= \left(\mathrm{Cotr}_{F''/F'}\left(\mathrm{Cotr}_{F'/F}(\omega)\right)\right)\\ &= \mathrm{Con}_{F''/F'}\left(\left(\mathrm{Cotr}_{F'/F}(\omega)\right)\right) + \mathrm{Diff}(F''/F')\\ &= \mathrm{Con}_{F''/F'}\left(\mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)\right) + \mathrm{Diff}(F''/F')\\ &= \mathrm{Con}_{F''/F}((\omega)) + \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F')\end{aligned}$$

and hence that

$$\mathrm{Diff}(F''/F) = \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F').$$

□

It is a trivial consequence of Corollary 2.18 that if P, P' and P'' are places lying above each other in respectively F, F' and F'' as above, then

$$d(P''|P) = e(P''|P') \cdot d(P'|P) + d(P''|P'). \tag{2.1.1}$$

Theorem 2.19 (Hurwitz Genus Formula). *Let F/K and F'/K' be algebraic function fields with F'/F a finite separable extension and respective genera g and g'. Then*

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

Proof. Choose $0 \neq \omega \in \Omega_F$. By Theorem 2.13

$$\left(\mathrm{Cotr}_{F'/F}(\omega)\right) = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F).$$

Recalling that the degree of a canonical divisor is $2g - 2$, we have

$$\begin{aligned}2g' - 2 &= \deg \mathrm{Cotr}_{F'/F}(\omega)\\ &= \deg \mathrm{Con}_{F'/F}((\omega)) + \deg \mathrm{Diff}(F'/F)\\ &= \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathrm{Diff}(F'/F).\end{aligned}$$

□

We may sometimes find it useful to write the genus formula in the form

$$g' = \frac{[F' : F]}{[K' : K]}(g - 1) + 1 + \frac{1}{2}\deg \mathrm{Diff}(F'/F).$$

It is clear that the problem of calculating the genus of a finite separable extension of a function field has been reduced to calculating the degree of the different. We will briefly remark on some known methods of doing so and derive expressions for the genus for some well-known extension types. We will assume throughout that F/K and F'/K' are algebraic function fields with F'/F finite separable and P, P' are places of these function fields respectively with $P'|P$.

Definition 2.20. *Suppose* $e(P'|P) > 1$. *We say*

$$P'|P \text{ is } \begin{cases} \text{tamely ramified} & \text{if } \operatorname{char} K \nmid e(P'|P), \\ \text{wildly ramified} & \text{if } \operatorname{char} K \mid e(P'|P). \end{cases}$$

A useful result due to Dedekind is the Dedekind Different Theorem, which states that, in the notation of the previous definition, if $P'|P$ in F', then

$$d(P'|P) \geq e(P'|P) - 1$$

with equality if and only if $P'|P$ is tamely ramified in F'. Looking at this from the viewpoint of divisors, this means that

$$e(P'|P) > 1 \iff P' \leq \operatorname{Diff}(F'/F),$$

which emphasizes the interplay between the different divisor and ramification in an extension. Another way to visualize the situation is by using ramification groups:

Definition 2.21. *If* F'/F *is a Galois extension of function fields and* P' *a place of* F', *then the ith ramification group of* $G = \operatorname{Gal}(F'/F)$ *relative to* P' *is*

$$G_i := \{\sigma \in G : v_{P'}(\sigma(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_{P'}\},$$

for $i \geq -1$.

Using the above definition, G_{-1} is the decomposition group, G_0 the inertia group and $G_{-1}/G_0 \cong \operatorname{Gal}(F'_{P'}/F_P)$. This means that the sequence

$$0 \longrightarrow G_0 \longrightarrow G_{-1} \longrightarrow G_{-1}/G_0 \cong \operatorname{Gal}(F'_{P'}/F_P) \longrightarrow 0$$

is exact, where we have that $|\operatorname{Gal}(F'_{P'}/F_P)| = f(P'|P)$ by definition, and it can be shown that $|G_0| = e(P'|P)$ and $|G_{-1}| = e(P'|P) \cdot f(P'|P)$ (see [23, 9.6] for an exposition).

Moreover, G_i is a normal subgroup of both G_{-1} and G_{i-1} for $i \geq 0$. If F is of characteristic $p > 0$, then G_1 is a p-group and G_0/G_1 is a cyclic group of order coprime to p. A tool which is often used to study these ramification groups is the indicator function i_G defined by

$$i_G(s) = v_{P'}(s(x) - x) \tag{2.1.2}$$

for $s \in G$ and x a generator for $\mathcal{O}_{P'}$ over $\mathcal{O}_P$. The value is independent of the choice of x, and it follows from Definition 2.21 that, for $s \neq 1$, $i_G(s)$ is a non-negative

integer while $i_G(1) = \infty$. A property that follows directly from the definition is the characterization

$$i_G(s) \geq i+1 \iff s \in G_i.$$

The groups G_i for $i \geq 0$ are almost all trivial, which makes the sum in the following result well-defined:

Theorem 2.22 (Hilbert's different formula). *Let F'/F be a Galois extension of function fields. For places P and P', respectively of F and F', with $P' \mid P$, we have that*

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

For constant field extensions of F/K, i.e. function fields $F'/K' := FK'/K'$ with $K \subseteq K'$, the genus is preserved ([27, III.6.3]), i.e. $g(F'/K') = g(F/K)$, if K is a perfect[1] field.

2.2 Extensions

We will regularly encounter Artin-Schreier and Kummer extensions of function fields in the coming chapters. They are used in the constructions of Garcia and Stichtenoth [9], [10], Van der Geer and Van der Vlugt [32] and Deolalikar [2], [3] and we briefly mention the theory needed to calculate the effect on the genus of such an extension here. We will assume the case of a finite constant field $\mathbb{F}_q$ of characteristic $p > 0$ throughout.

Definition 2.23. *Let $n > 1$ be an integer. We call $f \in F/\mathbb{F}_q$*

(i) nth Kummer degenerate if there exists $u \in F$ and $d|n$, $d > 1$ such that $f = u^d$, and

(ii) nth Kummer nondegenerate otherwise.

Observe that if $(v_P(f), n) = 1$ for some $P \in S(F/K)$, then $f \in F$ is nth Kummer nondegenerate. Indeed, $f = u^d$ implies that $v_P(f) = d \cdot v_P(u)$, so if $(v_P(f), n) > 1$, f cannot be nth Kummer nondegenerate.

[1] A field is perfect if all its algebraic extensions are separable.

Definition 2.24 (Kummer extension). *Given a function field $F/\mathbb{F}_q$, an integer $n > 1$ with $n \mid q-1$, an nth Kummer nondegenerate element $f \in F$ and y a root of $T^n - f = 0$. Then $F' := F(y)$ is called a Kummer extension.*

Proposition 2.25. *Assuming notation as in Definition 2.24, one has for the extension F'/F and places $P'|P$ that*

(i) F'/F is a cyclic extension of degree n,

(ii) $\mathbb{F}_q$ is the full constant field of F', and

(iii) $e(P'|P) = \frac{n}{(v_P(f),n)}$.

Note that since $n|q-1$ implies that $\mathrm{char}(K) = p \nmid n$, and hence $\mathrm{char}(K) \nmid e(P'|P)$, and so $P'|P$ is tamely ramified in F'. By Dedekind's Different Theorem it follows that $d(P'|P) = \frac{n}{(v_P(f),n)} - 1$. The genus of $F'/\mathbb{F}_q$ can then be calculated as

$$\begin{aligned} g(F') &= \frac{[F':F]}{[\mathbb{F}_q:\mathbb{F}_q]}(g(F)-1) + 1 + \tfrac{1}{2}\deg \mathrm{Diff}(F'/F) \\ &= \frac{n}{1}(g(F)-1) + 1 + \tfrac{1}{2}\sum_{P\in S(F/K)}\sum_{P'|P} d(P'|P)\cdot \deg P' \\ &= \frac{n}{1}(g(F)-1) + 1 + \tfrac{1}{2}\sum_{P\in S(F/K)} (v_P(f),n)\left(\frac{n}{(v_P(f),n)} - 1\right)\cdot \deg P \\ &= 1 + n(g(F)-1) + \tfrac{1}{2}\sum_{P\in S(F/K)} (n - (v_P(f),n))\cdot \deg P. \end{aligned}$$

Definition 2.26. *We call $f \in F/\mathbb{F}_q$ with char $\mathbb{F}_q = p$*

- *Artin-Schreier degenerate* if there exists $u \in F$ such that $u^p - u = f$, and
- *Artin-Schreier nondegenerate* otherwise.

An often useful result in this case is that if, for some $P \in S(F/\mathbb{F}_q)$ we have that $(v_P(f-(z^p-z)),p) = 1$, $v_P(f-(z^p-z)) < 0$ and $z \in F$, then $f \in F$ is Artin-Schreier nondegenerate.

Definition 2.27. *Given a function field $F/\mathbb{F}_q$, an Artin-Schreier nondegenerate element $f \in F$ and y a root of $T^p - T - f = 0$. Then $F' := F(y)$ is called an Artin-Schreier extension.*

It can be shown that, for $z \in F$, the integer $v_P(f-(z^p-z))$ is uniquely determined, and hence the definition

$$m_P := \begin{cases} -v_P(f-(z^p-z)) & \text{if } p \nmid v_P(f-(z^p-z)) < 0 \text{ for some } z \in F, \\ -1 & \text{if } v_P(f-(z^p-z)) \geq 0 \text{ for some } z \in F \end{cases}$$

makes sense. It turns out that the extension has the properties mentioned in the following proposition:

Proposition 2.28. *Assuming the extension as given in Definition 2.27, and places $P'|P$ in F' and F respectively, we have the following properties:*

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

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

(ii) P is unramified in $F'/F \iff m_P = -1$.

(iii) P is totally ramified in $F'/F \iff m_P > 0$. In this case there is a unique place P' lying above P, and we have

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

(iv) If there is at least one $Q \in S(F/\mathbb{F}_q)$ such that $m_Q > 0$, then $\mathbb{F}_q$ is the full constant field of F'.

A proof of Proposition 2.28 can be found in [27].

If $\mathbb{F}_q$ is the full constant field of the Artin-Schreier extension F' of F, we can apply the Hurwitz formula and obtain

$$\begin{aligned} g(F') &= \frac{[F':F]}{[\mathbb{F}_q:\mathbb{F}_q]}(g(F)-1)+1+\frac{1}{2}\deg \mathrm{Diff}(F'/F) \\ &= \frac{p}{1}(g(F)-1)+1+\frac{1}{2}\deg \sum_{P\in S(F/K)}\sum_{P'|P} d(P'|P)\cdot P' \\ &= p(g(F)-1)+1+\frac{1}{2}\sum_{P\in S(F/K)}(p-1)(m_P+1)\deg P \\ &= p(g(F)-1)+1+\frac{p-1}{2}\sum_{P\in S(F/K)}(m_P+1)\deg P. \end{aligned}$$

In fact, the situation as described above for a Artin-Schreier extension holds more generally for linearised polynomials (also frequently referred to as extensions of *modified Artin-Schreier type*):

Definition 2.29. *A linearized polynomial $R(x) \in \mathbb{F}_q[X]$ is a polynomial of the form*

$$R(X) = a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + ... + a_1 X^p + a_0 X$$

where p is the characteristic of $\mathbb{F}_q$.

These linearized polynomials have the special property that $R(u+v) = R(u) + R(v)$ for any $u, v \in F$. It can be seen immediately that the Artin-Schreier extension above is defined by means of such a polynomial, and in fact the result for these Artin-Schreier extensions can be easily generalised to the following result for extensions having linearized polynomials as defining equations:

Proposition 2.30. *Consider an algebraic function field F/K with K of characteristic $p > 0$ and a separable linearized polynomial $R(X) \in K[X]$ of degree p^n with all its roots in K. Let $u \in F$ and suppose that there exists a place $P \in S(F/K)$ such that $v_P(u) = -m_P$, $m_P > 0$ and $p \nmid m_P$. Then the polynomial*

$$R(T) - u = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + ... + a_1 T^p + a_0 T - u$$

is absolutely irreducible. If we let $F' := F(y)$ where y satisfies $R(y) = u$, then the following hold:

(i) F'/F is a Galois extension with $[F' : F] = p^n$,

$$\mathrm{Gal}(F'/F) = \{\sigma_\beta : y \longmapsto y + \beta\}_{R(\beta)=0},$$

$\mathrm{Gal}(F'/F)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ and K is the full constant field of F'.

(ii) The place P is totally ramified in F'/F. If P' is the unique place lying above P in F'/F, then $d(P'|P) = (p^n - 1)(m_P + 1)$.

(iii) Any $R \in S(F/K)$ with $v_R(u) \geq 0$ is unramified in F'/F.

(iv) If $g(F')$ and $g(F)$ respectively denote the genera of F'/K and F/K, then the Hurwitz genus formula implies that

$$g(F') = p^n \cdot (g(F) - 1) + 1 + \frac{p^n - 1}{2} \sum_{P \in S(F/K)} (m_P + 1) \cdot \deg P.$$

(v) If $a_n = a_{n-1} = ... = a_0 = 1$ and $Q \in S(F/K)$ is a zero of the function $u - \gamma$ for $\gamma \in \mathbb{F}_q$, then Q splits completely in F'/F.

A proof of Proposition 2.30 can be found in [27] and [29]. Because the existence of a place P where the hypotheses are satisfied cannot be guaranteed, a criterion for determining the irreducibility of the defining equation of the extension is needed. Deolalikar [2] provides this in the following general form:

Theorem 2.31. *Let V be a finite subgroup of the additive group of $\overline{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$). Then V is an $\mathbb{F}_p$-vector space. Define $L_V(T) = \prod_{v \in V}(T - v)$. Then $L_V(T)$ is a separable $\mathbb{F}_p$-linear polynomial of degree the cardinality of V. For $f(x) \in \overline{\mathbb{F}}_p[X]$, the polynomial*

$$h(T, x) := L_V(T) - f(x)$$

is reducible over $\overline{\mathbb{F}}_p[T, X]$ if and only if there exists a polynomial $g(x) \in \overline{\mathbb{F}}_p[X]$ and a proper additive subgroup W of V such that $f(x) = L_{W'}(g(x))$, where $W' = L_W(V)$.

Proof. As the proof is rather technical and not central to the theory we are developing, it is omitted. It is available in [2, 1.3.8]. □

For $f(x) \in \overline{\mathbb{F}}_p[X]$, a term of f is said to be coprime if it has a nonzero coefficient and its degree is coprime to p. The coprime degree of f is the degree of the coprime term of f having largest degree. Theorem 2.31 leads to the following condition for irreducibility:

Condition 2.32. *Let $f(x) \in \overline{\mathbb{F}}_p[X]$. If there exists a coprime term in $f(x)$ of degree d, such that there are no terms of degree dp^i for $i > 0$ in $f(x)$, then $L_V(T) - f(x)$ is irreducible for any subgroup $V \subset \overline{\mathbb{F}}_p$.*

Proof. Suppose $f(x)$ is the image of a linear polynomial $\sum a_n x^{p^n}$. Then the coprime term can occur only in the image of the term $a_0 x$, since all others will necessarily be of degree a multiple of p. But then the images of the coprime term (of degree d, say) under $a_n x^{p^n}$ for $n > 0$ will have degrees dp^i for some $i > 0$, a contradiction. □

As an example, the equation

$$y^{q^2} + y^q + y = x^{q^2+q} + x^{q^2+1} + x^{q+1}$$

is absolutely irreducible over $\overline{\mathbb{F}}_p$, since the coprime degree of the right-hand side is $q^2 + 1$, and there are no terms of degree $(q^2 + 1)\,p^i$ for $i > 0$.

The coprime degree of a polynomial arises in another important context. For a (general) Artin-Schreier extension, it is possible to transform the separating element to obtain simpler defining formulae. In particular, we have the following lemma:

Lemma 2.33. *Let $F = \mathbb{F}_{q^n}(x)$ where $q = p^m$. Consider the (general) Artin-Schreier extension $E = F(y)$ of F where $y^p + ay = f(x)$, for some $f(x) \in \mathbb{F}_p[X]$ and $a \in \mathbb{F}_{q^n}^\times$. Then there exist $Y \in E$ and $f^*(x) \in \mathbb{F}_{q^n}[X]$ such that $E = F(Y)$ with $Y^p + aY = f^*(x)$ such that each term of $f^*(x)$ has degree coprime to p.*

Proof. We can write the polynomial $f(x)$ uniquely in the form

$$f(x) = f_A(x) + f_B(x)$$

where $f_A(x)$ consists of those terms of $f(x)$ where $(e, p) = 1$, and $f_B(x)$ of those terms of $f(x)$ of degree e where $(e, p) > 1$. Then the coprime degree of $f(x)$ is the degree of $f_A(x)$. We now start an inductive reduction procedure for the defining equation of E over F.
Let sx^{pk} be the term of maximal degree in $f_B(x)$, for some $s \in \mathbb{F}_p$. Note that by performing the transformation $y' := y - x^k$, we obtain

$$\begin{aligned} y'^p + ay' &= \left(y - x^k\right)^p + a\left(y - x^k\right) \\ &= y^p - x^{pk} + ay - ax^k \\ &= f(x) - x^{pk} - ax^k \\ &= f_A(x) + f_B(x) - x^{pk} - ax^k. \end{aligned}$$

Because a single x^{pk} is subtracted in the final line of the previous equation, it is clear that now the term of maximal degree in $f_B(x) - x^{pk}$ is $(s-1)x^{pk}$. Because $s \in \mathbb{F}_p$, applying this transformation s times will ensure that the term of maximal non-coprime degree of the right-hand side is reduced. Also, $y - x^k \in E$ implies that $y \in E$, and therefore each transformation of the variable preserves the extension. The procedure can be repeated on the next term of maximal degree in the newly obtained $f'_B(x)$ (say) of lower degree than $f_B(x)$, and the process terminates when only terms of degree coprime to p remain in the expression, proving the lemma. □

Corollary 2.34. *Consider the hypotheses of Lemma 2.33 and the additional condition that the coprime degree of $f(x)$ is greater than $\frac{1}{p}\deg f(x)$. Then there exist $Y \in E$ and $f^*(x) \in \mathbb{F}_{q^n}[X]$ with the properties as described earlier, as well as that the coprime degree of $f(x)$ equals $\deg f^*(x)$.*

Proof. The degree of a term is reduced by a factor of p when the iterative procedure described in the proof of Lemma 2.33 is applied to it. Therefore every term obtained in this way has degree smaller than the coprime degree of $f(x)$, implying the result. □

The previous result shows that we can often reduce the defining equation of an Artin-Schreier extension to an equivalent equation where the degree of the polynomial on the right-hand side has all its terms coprime to p. If the extra condition of Corollary 2.34 is satisfied, the coprime degree of $f(x)$ is preserved after the transformation.

2.3 Bounds on the number of places of degree one

Denote by $N(F)$ the number of places of degree one of the function field $F/\mathbb{F}_q$ of genus g. The celebrated Hasse-Weil bound states that

$$|N(F) - (q+1)| \leq 2gq^{1/2}. \tag{2.3.1}$$

However, for numerous combinations of constant field cardinality q and genus g, equality cannot be obtained in (2.3.1), which leaves room for improvement of the bound in those cases. If q is non-square, the right-hand side of 2.3.1 is nonintegral, and we have the trivial improvement

$$|N(F) - (q+1)| \leq \left\lfloor 2gq^{1/2} \right\rfloor. \tag{2.3.2}$$

This was improved significantly by Serre, giving

Theorem 2.35 (Serre Bound). *For a function field $F/\mathbb{F}_q$ of genus g,*

$$|N(F) - (q+1)| \leq g \left\lfloor 2q^{1/2} \right\rfloor. \tag{2.3.3}$$

Another result due to Serre which improves the Serre Bound under some circumstances is that if $F/\mathbb{F}_q$ is a function field of genus 3 or more and $N(F)$ does not attain the upper bound of (2.3.3), then

$$N(F/\mathbb{F}_q) \leq q - 1 + g \left\lfloor 2q^{1/2} \right\rfloor. \tag{2.3.4}$$

We are interested in function fields with many places of degree one. We define

$$N_q(g) = \max\{N(F) : F/\mathbb{F}_q \text{ is a function field of genus } g\}.$$

Obviously $N(F) \leq N_q(g) \leq q + 1 + 2gq^{1/2}$ for any function field $F/\mathbb{F}_q$, with equality holding when some genus g function field $F/\mathbb{F}_q$ attains the Hasse-Weil bound. By our previous remarks it follows that $N_q(g)$ can attain (2.3.1) only if q is square.

We call the function field $F/\mathbb{F}_q$ of genus g *maximal* if $N(F) = q + 1 + 2gq^{1/2}$, and we call it *optimal* if $N(F) = N_q(g)$. Obviously every maximal function field is

optimal. Van der Geer and van der Vlugt [33] maintain a regularly updated list of the known values of $N_q(g)$ for $2 \leq g \leq 50$ and q being a small power of 2 or 3.

Maximal curves can only occur over fields $\mathbb{F}_{q^2}$, i.e. fields of square cardinality. Many results about the possible genera a maximal curve can have under these circumstances are available in the literature. Amongst others, it was partly conjectured by Stichtenoth and Xing, and later proved in [8] and [16] by Fuhrmann, Korchmáros and Torres that either

$$g = \frac{1}{2}q(q-1),\ g = \left\lfloor \frac{1}{4}(q-1)^2 \right\rfloor \text{ or } g \leq \left\lfloor \frac{1}{6}\left(q^2 - q + 4\right) \right\rfloor.$$

By employing the explicit formula method after Serre [26], we can find real numbers a and b such that

$$N(F) \leq ag + b. \tag{2.3.5}$$

For large g this will improve the Hasse-Weil bound significantly. More precisely we have the following :

Proposition 2.36. *Suppose $F/\mathbb{F}_q$ is a function field of genus g and $c_1, ..., c_m$ are nonnegative real numbers, not all zero and*

$$f_m(t) \geq 0 \text{ for all } t \in \mathbb{C} \text{ with } |t| = 1$$

where

$$\lambda_m(t) = \sum_{r=1}^{m} c_r t^r \text{ and } f_m(t) = 1 + \lambda_m(t) + \lambda_m\left(t^{-1}\right).$$

Then

$$N(F) \leq \frac{g}{\lambda_m\left(q^{-1/2}\right)} + \frac{\lambda_m\left(q^{1/2}\right)}{\lambda_m\left(q^{-1/2}\right)} + 1.$$

Proof. Let $N_r := N(F_r)$, where $F_r = F\mathbb{F}_{q^r}$ is the constant field extension of F of degree r, and $N := N(F)$. Write

$$\omega_i := \alpha_i q^{-1/2}$$

where α_i, $1 \leq i \leq 2g$ are the reciprocals of the roots the L-polynomial $L_F(t)$ of F. Then by the Hasse-Weil theorem $|\omega_i| = 1$, and we can reorder the ω_i without loss of generality so that $\omega_{g+i} = \overline{\omega_i} = \omega_i^{-1}$ for $1 \leq i \leq g$. Since

$$N_r = q^r + 1 - q^{r/2} \sum_{i=1}^{g} \left(\omega_i^r + \omega_i^{-r}\right),$$

it follows that

$$q^{-r/2} \cdot N_r = q^{r/2} + q^{-r/2} - \sum_{i=1}^{g} \left(\omega_i^r + \omega_i^{-r}\right)$$

and after multiplying through by c_r that

$$Nc_r q^{-r/2} = c_r q^{r/2} + c_r q^{-r/2} - \sum_{i=1}^{g} c_r \left(\omega_i^r + \omega_i^{-r}\right) - (N_r - N)\, c_r q^{-r/2}. \tag{2.3.6}$$

Summing over $r = 1, ..., m$ and using the facts that $N \leq N_r$ and $f_m(t) \geq 0$ we obtain

$$\begin{aligned} \lambda_m\left(q^{-1/2}\right) N &= \lambda_m\left(q^{1/2}\right) + \lambda_m\left(q^{-1/2}\right) + g - \sum_{i=1}^{g} f_m(\omega_i) - \sum_{r=1}^{m} (N_r - N)\, c_r q^{-r/2} \\ &\leq \lambda_m\left(q^{1/2}\right) + \lambda_m\left(q^{-1/2}\right) + g \end{aligned}$$

and hence

$$\begin{aligned} N &\leq \frac{\lambda_m\left(q^{1/2}\right) + \lambda_m\left(q^{-1/2}\right) + g}{\lambda_m\left(q^{-1/2}\right)} \\ &= \frac{g}{\lambda_m\left(q^{-1/2}\right)} + \frac{\lambda_m\left(q^{1/2}\right)}{\lambda_m\left(q^{-1/2}\right)} + 1 \\ &= \left(\frac{1}{\lambda_m\left(q^{-1/2}\right)}\right) g + \left(\frac{\lambda_m\left(q^{1/2}\right)}{\lambda_m\left(q^{-1/2}\right)} + 1\right). \end{aligned}$$

□

From the previous proposition, it seems that a good choice for the function f (i.e. for the parameters $c_1, ..., c_m$) may improve the bound obtained. Finding optimal values for such f is a linear programming problem which was solved by Oesterlé [24], resulting in the so-called Oesterlé bounds.

The previous result, combined with the Hasse-Weil bound may lead one to believe that the bound for the number of places of degree one (for fixed q) grows with order $O(g)$. In fact, if we define

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g}, \tag{2.3.7}$$

the Serre Bound (Theorem 2.35) implies that $A(q) \leq \lfloor 2q^{1/2} \rfloor$. This was improved significantly by Drinfeld and Vlăduţ [35] by applying Serre's method in [26]:

Theorem 2.37 (Drinfeld-Vlăduţ Bound). $A(q) \leq q^{1/2} - 1$.

Proof. Fix $m \geq 1$, and let $c_r := 1 - \frac{r}{m}$ for $r = 1, ..., m$. In the notation of Theorem 2.36 we have

$$\lambda_m(t) = \sum_{r=1}^{m} \left(1 - \frac{r}{m}\right) t^r = \frac{t}{(1-t)^2}\left(\frac{t^m - 1}{m} + 1 - t\right)$$

and

$$f_m(t) = 1 + \lambda_m(t) + \lambda_m\left(t^{-1}\right) = \frac{2 - \left(t^m - t^{-m}\right)}{m(t-1)\left(t^{-1} - 1\right)}.$$

Since $|t| = 1 \Longrightarrow t^{-1} = \bar{t}$ for $t \in \mathbb{C}$, we have $f_m(t) \geq 0$ for such t. Applying Theorem 2.36 yields

$$\frac{N(F)}{g} \leq \frac{1}{\lambda_m\left(q^{-1/2}\right)} + \frac{1}{g}\left(1 + \frac{\lambda_m\left(q^{1/2}\right)}{\lambda_m\left(q^{-1/2}\right)}\right).$$

If we let $m \to \infty$ we have

$$\lambda_m\left(q^{-1/2}\right) \longrightarrow \frac{q^{-1/2}}{\left(1 - q^{-1/2}\right)^2}\left(1 - q^{-1/2}\right) = \frac{1}{q^{1/2} - 1},$$

and hence for any $\varepsilon > 0$ there exists m_0 such that

$$\lambda_{m_0}\left(q^{-1/2}\right)^{-1} < q^{1/2} - 1 + \tfrac{\varepsilon}{2}$$

and hence we can choose g_0 such that

$$\frac{1}{g_0}\left(1 + \frac{\lambda_{m_0}\left(q^{1/2}\right)}{\lambda_{m_0}\left(q^{-1/2}\right)}\right) < \tfrac{\varepsilon}{2}.$$

Then, $g > g_0$ implies

$$\frac{N(F)}{g} < q^{1/2} - 1 + \varepsilon,$$

and hence $A(q) \leq q^{1/2} - 1$. □

Chapter 3

Towers

3.1 Towers of Function Fields

We will begin by stating the basic definitions concerning towers of function fields. In order to apply these to the specific examples we will discuss, we will work with the case of an arbitrary *finite* field of constants $\mathbb{F}_q$, where q is a power of a prime p.

Definition 3.1. *A tower of function fields over $\mathbb{F}_q$ is a sequence*

$$\mathcal{F} = (F_1, F_2, F_3, ...)$$

of function fields $F_i/\mathbb{F}_q$ such that

(a) $F_1 \subsetneqq F_2 \subsetneqq F_3 \subsetneqq ...$,

(b) The extension F_{i+1}/F_i is separable for each $i = 1, 2, ...$,

(c) $g(F_j) > 1$ for some $j \geq 1$ and

(d) $\mathbb{F}_q$ is the full constant field of each F_i.

The proper inclusions of the sequence of fields and the fact that there exists some $j \geq 1$ such that $g(F_j) > 1$ implies that, by Theorem 2.19, $\lim_{i\to\infty} g(F_i) = \infty$. We will call a tower *tame* if each extension F_{i+1}/F_i is tamely ramified.

The most prominent measure of a tower of function fields $\mathcal{F}$ turns out to be the asymptotic behaviour of the sequence $(N(F_i)/g(F_i))_{i\geq 1}$. To show that this sequence is indeed convergent, we follow [11]:

Lemma 3.2. *Let E/F be a finite extension of function fields over $\mathbb{F}_q$, and assume that $g(F) > 1$. Then*

$$\frac{N(E)}{g(E)-1} \leq \frac{N(F)}{g(F)-1}.$$

Proof. We can find[1] an intermediate field $F \subseteq F' \subseteq E$ such that F'/F is separable and E/F' purely inseparable of degree p^v with $v \geq 0$. Then $F' = E^{p^v}$ is isomorphic to E (see [27, Prop. III.9.2]), so $N(F') = N(E)$ and $g(F') = g(E)$. The Hurwitz genus formula (Theorem 2.19) applied to the (separable) extension F'/F gives

$$\begin{aligned} 2g(F') - 2 &= [F' : F] \cdot (2g(F) - 2) + \deg \operatorname{Diff}(F'/F) \\ &\geq [F' : F] \cdot (2g(F) - 2) \end{aligned}$$

which implies that $g(F') - 1 \geq [F' : F](g(F) - 1)$. Since any place $P \in S(F/\mathbb{F}_q)$ of degree one can have at most $[F' : F]$ extensions $P' \in S(F'/\mathbb{F}_q)$ of degree one lying above it, $N(F') \leq [F' : F] \cdot N(F)$. It follows that

$$\frac{N(E)}{g(E)-1} = \frac{N(F')}{g(F')-1} \leq \frac{[F' : F] \cdot N(F)}{[F' : F] \cdot (g(F) - 1)} = \frac{N(F)}{g(F)-1}.$$

□

It can be seen that the preceding lemma is much stronger than is necessary for our definition of a tower of function fields. In fact, assumption (b) from Definition 3.1 can be weakened to allow extensions which are just not purely inseparable. We will however keep Definition 3.1 as it stands.

Corollary 3.3. *For any tower $\mathcal{F} = (F_1, F_2, \ldots)$ of function fields over $\mathbb{F}_q$, the sequence $(N(F_i)/g(F_i))_{i \geq 1}$ converges.*

Proof. We can assume that $g(F_i) > 1$ by considering Definition 3.1(c). Lemma 3.2 implies that the sequence $(N(F_i)/(g(F_i) - 1))_{i \geq 1}$ is monotonously decreasing, and hence convergent, since the terms of the sequence are clearly non-negative. Hence the sequence $(N(F_i)/g(F_i))_{i \geq 1}$ is also convergent, and since $\lim_{i \to \infty} g(F_i) = \infty$, its limit equals that of $(N(F_i)/(g(F_i) - 1))_{i \geq 1}$. □

We can therefore associate to any tower $\mathcal{F} = (F_1, F_2, \ldots)$ the function

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)}$$

[1] Set $F' := F^{\text{sep}} \cap E$ where F^{sep} is the separable closure of F (See Lang [18, p. 243])

which we may also refer to as the *limit* of the tower $\mathcal{F}$. Clearly the Drinfeld-Vlăduţ bound (Theorem 2.37) and the above comments imply that for any tower $\mathcal{F}$ of function fields over $\mathbb{F}_q$,

$$0 \leq \lambda(\mathcal{F}) \leq A(q).$$

Definition 3.4. *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$. We call $\mathcal{F}$ asymptotically*

$$\begin{array}{ll} \textit{bad} & \textit{if } \lambda(\mathcal{F}) = 0, \\ \textit{good} & \textit{if } \lambda(\mathcal{F}) > 0, \\ \textit{optimal} & \textit{if } \lambda(\mathcal{F}) = A(q). \end{array}$$

Definition 3.5. *Let $\mathcal{E} = (E_1, E_2, ...)$ and $\mathcal{F} = (F_1, F_2, ...)$ be towers of function fields over $\mathbb{F}_q$. We call $\mathcal{E}$ a subtower of $\mathcal{F}$ (written $\mathcal{E} \prec \mathcal{F}$) if there exists an embedding*

$$\iota : \bigcup_{i \geq 1} E_i \hookrightarrow \bigcup_{i \geq 1} F_i$$

over $\mathbb{F}_q$, i.e. for every $i \geq 1$ there exists $m_i \geq 1$ such that $\iota(E_i) \subseteq F_{m_i}$.

This definition and Lemma 3.2 enables us to obtain the following result:

Corollary 3.6. *Let $\mathcal{F}$ be a tower of function fields over $\mathbb{F}_q$, and let $\mathcal{E}$ be a subtower of $\mathcal{F}$. Then*

(i) $\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$,

(ii) if $\mathcal{E}$ is asymptotically bad, then $\mathcal{F}$ is asymptotically bad, and

(iii) if $\mathcal{F}$ is asymptotically optimal, then $\mathcal{E}$ is asymptotically optimal.

In the light of the applications to coding theory of these towers when they are explicitly defined, constructing good geometric Goppa codes with parameters attaining or exceeding the Gilbert-Varshamov bound requires us to construct asymptotically good towers of curves. This is however equivalent to constructing asymptotically good towers of function fields $\mathcal{F} = (F_1, F_2, ...)$, where each step F_{i+1}/F_i must be a separable extension with a known irreducible polynomial $f_i = 0$. In the coming sections we will remark on some known bounds for $A(q)$ using both explicit and non-explicit methods, and look at some explicit constructions of towers of function fields.

3.2 Bounds on $A(q)$

We have discussed the construction and some introductory properties of towers $\mathcal{F}$ of function fields. For the sake of obtaining good codes, there should be asymptotically many places of degree one compared to the genus. This reinforces the notion of the quantity $\lambda(\mathcal{F})$ as a measure of how good a geometric Goppa code constructed from such a tower would be in terms of its transmission rate and percentage of errors corrected. Good geometric codes can be constructed from $\mathcal{F} = (F_1, F_2, ...)$ when $\lim_{i\to\infty} N(F_i)/g(F_i) > 0$, and this requires that $\lambda(\mathcal{F}) > 0$, i.e. that the tower is asymptotically good.

Since $\lambda(\mathcal{F})$ is bounded above by $A(q)$, we will look at some known bounds for $A(q)$. The Drinfeld-Vlăduţ bound (Theorem 2.37) provides us with the upper bound $A(q) \leq q^{1/2} - 1$. Serre [26] showed, using Hilbert class field towers, that we have the lower bound

$$A(q) > \frac{\log_2 q}{96}, \tag{3.2.1}$$

thereby proving that there exist asymptotically good towers of function fields over any finite field. So, we know that asymptotically good constructions exist over every finite field. The problem, however, is to construct them explicitly. In a later construction of towers of Kummer extensions in this chapter (Theorems 3.18 and 3.19) we will see that there do indeed exist asymptotically good towers of function fields over an arbitrary constant field $\mathbb{F}_q$, in particular with $A(q) \geq \frac{2}{q-2}$. Although these are certainly positive lower bounds, they can be seen to be rather weak lower bounds for $A(q)$, and we will look at situations in which they can be improved.

For square q, there exist towers $\mathcal{F}$ of function fields attaining the Drinfeld-Vlăduţ bound, as was first shown by Ihara [15]. This means that

$$A(q) = q^{1/2} - 1 \text{ if } q \text{ is a square.} \tag{3.2.2}$$

His construction was done using Shimura curves, but this was not explicit. The surprising construction in 1995 of an explicit tower of function fields attaining the Drinfeld-Vlăduţ bound by García and Stichtenoth [9] for square q will be discussed in more detail in the next section, thereby also providing proof of the above equation.

For non-square q, results are much more sketchy. The value of $A(q)$ is unknown, but some improvements of (3.2.1) do exist. Zink [36] showed, using degenerations of Shimura surfaces that for any prime p we have

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}. \tag{3.2.3}$$

A more general result due to Xing and Niederreiter [20] shows using class field towers that for $m \geq 3$,

$$A(q^m) \geq \begin{cases} \frac{2q}{\lceil 2(2q+1)^{1/2} \rceil + 1} & \text{if } q \text{ is odd,} \\ \frac{q+1}{\lceil 2(2q+2)^{1/2} \rceil + 2} & \text{if } q \geq 4 \text{ is even.} \end{cases} \tag{3.2.4}$$

Let q $(= p^n)$ be called *special* if either $p \mid \lfloor 2q^{1/2} \rfloor$, or q is representable as $k^2 + 1$, $k^2 + k + 1$ or $k^2 + k + 2$ for some $k \in \mathbb{Z}$. Then, using narrow ray class fields, Xing and Niederreiter [21] showed that, if $q \geq 11$ is odd, non-special and $\lfloor 2q^{1/2} \rfloor$ is even, then

$$A(q^3) \geq \frac{2q + 4\lfloor 2q^{1/2} \rfloor}{5 + \left\lceil 2\left(2q + 4\lfloor 2q^{1/2} \rfloor + 1\right)^{1/2} \right\rceil}. \tag{3.2.5}$$

There are also bounds available for cases where q is even or special. In general, these constructions based on narrow ray class fields are slightly better than those using the class field towers of [20].

In order to compare the above-mentioned bounds for some small (non-prime, non-square) finite fields, consider the following table of bounds for $A(q)$ for varying q:

q	Serre	Kummer	Class field	Narrow ray	Zink	DV
$8 = 2^3$	0.0313	0.3333	0.6923		1.5000	1.8284
$27 = 3^3$	0.0495	2.0000	0.8571	1.2868	3.2000	4.1961
$32 = 2^5$	0.0521	0.0667	1.7368			4.6569
$125 = 5^3$	0.0726	0.6667	1.2500	1.6250	6.8571	10.180
$128 = 2^7$	0.0729	0.0158	0.6667			10.314
$243 = 3^5$	0.0826	2.0000	0.8571			14.588
$343 = 7^3$	0.0877	0.4000	1.5556	1.6923	10.6667	17.520

All the bounds indicated are lower bounds, except for DV which is the Drinfeld-Vlăduţ upper bound. The Kummer column mentions the best result obtainable by either using Theorem 3.18 or 3.19, which will be discussed in more detail later.

While the constructions using class field towers and narrow ray class fields by Xing and Niederreiter and those based on Shimura surfaces by Zink generally deliver stronger lower bounds for $A(q)$ than the Kummer towers, the former constructions are not explicit at all.

3.3 García and Stichtenoth's tower

We look at the surprising discovery of an explicit asymptotically optimal tower of function fields by García and Stichtenoth [9]. It has the novelty of avoiding the use

of modular curves and class field towers, and using only (modified) Artin-Schreier extensions. The ramification behaviour of Artin-Schreier extensions and use of the Hurwitz formula will be essential to obtain the result.

We choose an arbitrary finite field of square cardinality which we denote by $\mathbb{F}_{q^2}$ where q is an arbitrary power of a prime p.

Definition 3.7. *Let $F_1 := \mathbb{F}_{q^2}(x_1)$ be the rational function field over $\mathbb{F}_{q^2}$. For $n \geq 1$, we recursively define*

$$F_{n+1} := F_n(z_{n+1})$$

where

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \tag{3.3.1}$$

with

$$x_n := z_n / x_{n-1} \text{ for } n \geq 2.$$

We denote this recursive tower by

$$\mathcal{F} = (F_1, F_2, \ldots).$$

It is noted that $F_2 = F_1(z_2)$ with $z_2^q + z_2 = x_1^{q+1}$, i.e. the Hermitian function field, which is the unique function field of genus $g = q(q-1)/2$ over $\mathbb{F}_{q^2}$ attaining the Hasse-Weil bound. We define the (modified) Artin-Schreier operator $\wp$ as $\wp(u) := u^q + u$.

Proposition 3.8. *Suppose that F/K is an algebraic function field over K (where $K = \mathbb{F}_{q^2}$ is algebraically closed in F). Let $w \in F$ and assume that there exists a place $P \in S(F/K)$ such that $v_P(w) = -m$, $m > 0$ and $(m, q) = 1$. The polynomial $T^q + T - w \in F[T]$ is absolutely irreducible, and define the extension field E of F by $E = F(z)$ with $z^q + z = w$. Then*

(i) *E/F is a Galois extension with $[E : F] = q$ with group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\log_p q}$ and K the full constant field of E.*

(ii) *If $Q \in S(F/K)$ with $v_Q(\wp(u) - w) \geq 0$ for some $u \in F$, then Q is unramified in E/F. In particular, this occurs when $v_Q(w) \geq 0$.*

(iii) *The place P is totally ramified in E, i.e. there exists a unique place $P' \in S(E/K)$ lying above P, and $e(P'|P) = q$. Moreover, $\deg P' = \deg P$ and $d(P'|P) = (q-1)(m+1)$.*

(iv) Suppose $Q \in S(F/K)$ is a zero of $w - \gamma$ with $\gamma \in \mathbb{F}_q$. The equation $\wp(\alpha) = \gamma$ has q distinct roots $\alpha \in K$, and for each such root α there exists a unique place $Q_\alpha \in S(E/K)$ such that $Q_\alpha | Q$ and Q_α is a zero of $z - \alpha$; in particular, the place Q splits completely in E.

Proof. These statements follow directly from Proposition 2.30. □

Lemma 3.9. *Suppose $x_n \in F_n$ and $P \in S(F_n/\mathbb{F}_{q^2})$ is a simple pole of x_n in F_n. Then P is totally ramified in F_{n+1}/F_n. The (unique) place $P' \in S(F_{n+1}/\mathbb{F}_{q^2})$ extending P to F' is a simple pole of x_{n+1}.*

Proof. Since $v_P(x_n) = -1$, $v_P(x_n^{q+1}) = -(q+1)$. We have $[F_{n+1} : F_n] = q$. From the recursive definition (Equation 3.3.1) and the theory of Artin-Schreier extensions of function fields in Chapter 2, it follows that P is totally ramified in F_{n+1}/F_n. Denoting by P' the unique place lying above P, we have

$$v_{P'}\left(z_{n+1}^q + z_{n+1}\right) = v_{P'}\left(x_n^{q+1}\right) = -q(q+1),$$

so $v_{P'}(z_{n+1}) = -(q+1)$ and

$$v_{P'}(x_{n+1}) = v_{P'}(z_{n+1}/x_n) = v_{P'}(z_{n+1}) - v_{P'}(x_n) = -(q+1) - (-q) = -1,$$

proving that P' is a simple pole of x_{n+1}, as required. □

Since $\mathbb{F}_{q^2}$ is algebraically closed in $F_1 = \mathbb{F}_{q^2}(x_1)$ and x_1 has a simple pole in $S(F_1/\mathbb{F}_{q^2})$ we obtain inductively that $\mathbb{F}_{q^2}$ is algebraically closed in each F_n for $n \geq 1$, i.e. $\mathbb{F}_{q^2}$ is the full constant field of each F_n, and $[F_n : F_1] = q^{n-1}$.

Lemma 3.10. *For all $n \geq 1$ there exists a unique place $Q_n \in S(F_n/\mathbb{F}_{q^2})$ which is a common zero of the functions $x_1, z_2, z_3, ..., z_n$. The place Q_n has degree 1, and for $1 \leq k \leq n$, the place Q_n is also a zero of x_k, and we have $v_{Q_n}(x_k) = q^{k-1}$. In the extension F_{n+1}/F_n the place Q_n splits into q places of F_{n+1} of degree 1 (one of them being Q_{n+1}).*

Proof. This follows by induction on n using the ramification behaviour as described in Proposition 3.8. □

The broad strategy will now be to determine precisely all places of F_n which ramify in F_{n+1}/F_n. We will denote the restriction of a place $P \in S(F_n/\mathbb{F}_{q^2})$ to F_k with $1 \leq k \leq n$ by $P_k := P \cap F_k$. To study the ramification behaviour in extensions, we define the following sets:

1. For $n \geq 2$, let

$$S_0^{(n)} := \{P \in S(F_n/\mathbb{F}_{q^2}) : P_{n-1} = Q_{n-1} \text{ and } P \neq Q_n\}$$

and for $1 \leq i \leq \lfloor \frac{n-3}{2} \rfloor$, let

$$S_i^{(n)} := \left\{P \in S(F_n/\mathbb{F}_{q^2}) : P_{n-1} \in S_{i-1}^{(n-1)}\right\}.$$

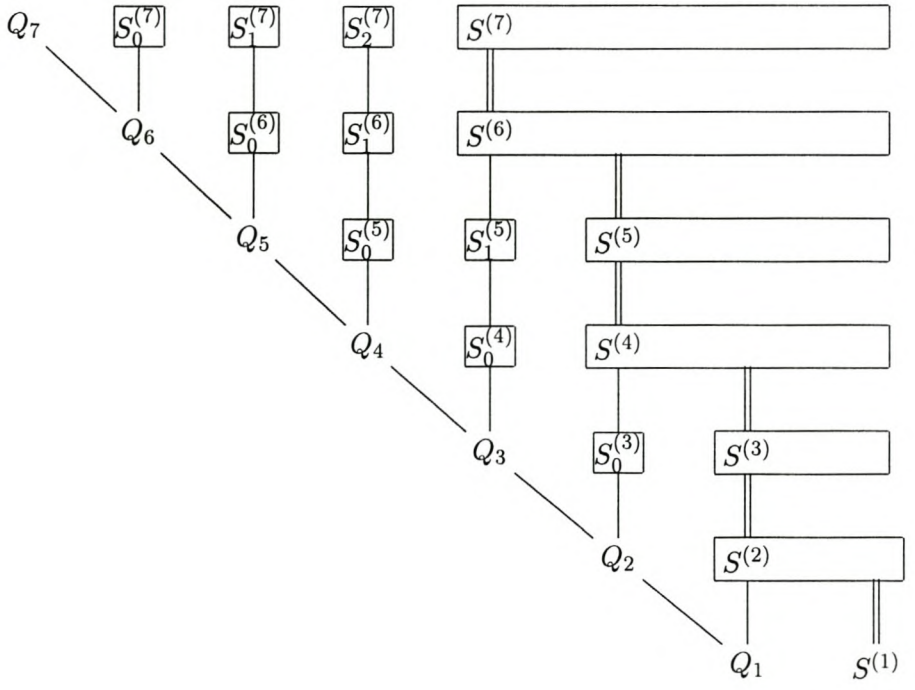
2. Let P_∞ denote the pole of x_1 in F_1. Then let

$$S^{(1)} := \{P_\infty\} \text{ and}$$
$$S^{(2)} := \left\{P \in S(F_2/\mathbb{F}_{q^2}) : P \in S_0^{(2)} \text{ or } P_1 \in S^{(1)}\right\};$$

i.e. $S^{(2)}$ contains all places of F_2 which are either a pole of x_1 or a common zero of x_1 and $z_2 - \alpha$ where $\alpha \in \mathbb{F}_{q^2}$ is a root of $\wp(\alpha) = 0$. For $n \geq 3$ we define

$$S^{(n)} := \begin{cases} \left\{P \in S(F_n/\mathbb{F}_{q^2}) : P_{n-1} \in S^{(n-1)}\right\} & \text{if } n \equiv 1 \bmod 2, \\ \left\{P \in S(F_n/\mathbb{F}_{q^2}) : P_{n-1} \in S^{(n-1)} \cup S_{\frac{n-4}{2}}^{(n-1)}\right\} & \text{if } n \equiv 0 \bmod 2. \end{cases}$$

The inclusions of these sets in the tower can be visualized in the following way, as done in [9]:



where the rows represent partitions of $S(F_n/\mathbb{F}_{q^2})$ for $n = 1, 2, ...$ from the bottom up, vertical lines represent places lying above each other, and double lines indicate places lying above each other which will turn out to be totally ramified. To show this, the ramification behaviour of this tower of extensions will have to be studied. It turns out that the critical step in calculating the genus $g(F_n)$ will be to prove the following proposition:

Proposition 3.11. *Let $0 \leq i \leq \left\lfloor \frac{n-3}{2} \right\rfloor$ and $P \in S_i^{(n)} \subset S(F_n/\mathbb{F}_{q^2})$. Then the place P is unramified in the extension F_{n+1}/F_n.*

In order to prove this, we require two lemmas. We will write $x = y + O(z)$ at a place P if $v_P(x-y) \geq v_P(z)$, i.e. $x = y + tz$ with $v_P(t) \geq 0$. In particular, $x = y + O(1)$ at P means that $v_P(x-y) \geq 0$.

Lemma 3.12. *Let $2 \leq k \leq n$ and $P \in S(F_n/\mathbb{F}_{q^2})$ be a place above Q_k (i.e. P is a common zero of $x_1, z_2, ..., z_k$). Then*

$$x_k = x_{k-1}^q \left(1 - x_{k-1}^{(q+1)(q-1)} + O\left(x_{k-1}^{(q+1)\left(q^2-1\right)}\right)\right)$$

and

$$x_k^{-(q+1)} = \wp\left(x_{k-1}^{-(q+1)}\right) + O(1).$$

Proof. From the defining equations we have

$$\begin{aligned} x_k &= z_k / x_{k-1} \\ &= \left(x_{k-1}^{q+1} - z_k^q\right) / x_{k-1} \\ &= \left(x_{k-1}^{q+1} - \left(x_{k-1}^{q+1} - z_k^q\right)^q\right) / x_{k-1} \\ &= x_{k-1}^q \left(1 - x_{k-1}^{(q+1)(q-1)} + O\left(x_{k-1}^{(q+1)\left(q^2-1\right)}\right)\right), \end{aligned}$$

giving us the first equality. For the second, let $y := x_{k-1}^{q+1}$ and note that

$$\begin{aligned} x_k^{-1} &= x_{k-1} z_k^{-1} \\ &= x_{k-1}^{-q} \left(1 - y^{q-1} + O\left(y^q\right)\right)^{-1} \\ &= x_{k-1}^{-q} \left(1 + y^{q-1} + O\left(y^q\right)\right), \end{aligned}$$

and hence

$$\begin{aligned} x_k^{-(q+1)} &= y^{-q} \left(1 + y^{q-1} + O\left(y^q\right)\right)^{q+1} \\ &= y^{-q} \left(1 + y^{q-1} + O\left(y^q\right)\right) \\ &= \wp\left(y^{-1}\right) + O(1), \end{aligned}$$

as required. □

Lemma 3.13. *Suppose* $0 \leq i \leq \left\lfloor \frac{n-2}{2} \right\rfloor$ *and* $P \in S_i^{(n)}$. *Then* $x_n^{q+1} = \gamma \cdot x_{n-2i-1}^{-(q+1)} + O(1)$ *at* P *for some* $\gamma \in \mathbb{F}_q^\times$.

Proof. The proof is by induction on i. If $i = 0$, a place $P \in S_0^{(n)}$ is the common zero of $x_1, z_2, ..., z_{n-1}$ and $z_n - \alpha$ with $\alpha \in \mathbb{F}_{q^2}^\times$ satisfying $\wp(\alpha) = \alpha^q + \alpha = 0$. We have $(z_n - \alpha)^q + (z_n - \alpha) = x_{n-1}^{q+1}$ and hence

$$z_n - \alpha = x_{n-1}^{q+1} + O\left(x_{n-1}^{q(q+1)}\right).$$

Then

$$\begin{aligned} x_n^{q+1} \cdot x_{n-1}^{q+1} &= z_n^{q+1} \\ &= ((z_n - \alpha) + \alpha)^{q+1} \\ &= \alpha^{q+1} + \alpha^q \left(x_{n-1}^{q+1} + O\left(x_{n-1}^{q(q+1)}\right)\right) + O\left(x_{n-1}^{q(q+1)}\right) \\ &= \alpha^{q+1} + \alpha^q x_{n-1}^{q+1} + O\left(x_{n-1}^{q(q+1)}\right). \end{aligned}$$

Setting $\gamma := \alpha^{q+1}$ we obtain $x_n^{q+1} = \gamma \cdot x_{n-1}^{-(q+1)} + O(1)$. (Note that $\gamma \in \mathbb{F}_q$ since $\alpha \in \mathbb{F}_{q^2}$.)
Suppose now that $i \geq 1$. Then the place P lies above Q_{n-1-i} and $P_{n-1} \in S_{i-1}^{(n-1)}$. By the induction hypothesis we have

$$x_{n-1}^{q+1} = \gamma \cdot x_{n-2i}^{-(q+1)} + O(1) \tag{3.3.2}$$

with $\gamma \in \mathbb{F}_q^\times$. Lemma 3.12 gives

$$x_{n-2i}^{-(q+1)} = \wp\left(x_{n-2i-1}^{-(q+1)}\right) + O(1),$$

and since $\gamma \in \mathbb{F}_q$ this yields

$$x_{n-1}^{q+1} = \wp\left(\gamma x_{n-2i-1}^{-(q+1)}\right) + O(1).$$

Since $z_n^q + z_n = x_{n-1}^{q+1}$ we have

$$\wp\left(z_n - \gamma x_{n-2i-1}^{-(q+1)}\right) = O(1)$$

and hence

$$z_n = \gamma x_{n-2i-1}^{-(q+1)} + O(1). \tag{3.3.3}$$

Since $x_n = z_n / x_{n-1}$ we can set

$$x_n^{q+1} = \frac{(z_n x_{n-2i})^{q+1}}{(x_{n-1} x_{n-2i})^{q+1}} = A^{q+1} \cdot B^{-1}$$

where $A := z_n x_{n-2i}$ and $B := x_{n-1}^{q+1} x_{n-2i}^{q+1}$.
Now, $v_P(x_{n-2i}) > 0$ (since $n - 2i \leq n - 1 - i$) and $x_{n-2i} = O(x_{n-2i-1})$ by Lemma 3.12 (the assumption that $i \leq \lfloor \frac{n-2}{2} \rfloor$ implies that $n - 2i \geq 2$). We obtain from (3.3.2) that $B = \gamma + O\left(x_{n-2i}^{q+1}\right)$, hence

$$B^{-1} = \gamma^{-1} + O\left(x_{n-2i}^{q+1}\right) = \gamma^{-1} + O\left(x_{n-2i-1}^{q+1}\right).$$

Applying Lemma 3.12 to (3.3.3) with $k = n - 2i$ we obtain

$$\begin{aligned} A &= z_n x_{n-2i} \\ &= \left(\gamma x_{n-2i-1}^{-(q+1)} + O(1)\right) \cdot x_{n-2i-1}^{q} \left(1 + O\left(x_{n-2i-1}^{q^2-1}\right)\right) \\ &= \gamma x_{n-2i-1}^{-1} + O\left(x_{n-2i-1}^{q}\right). \end{aligned}$$

It follows that

$$A^{q+1} = \gamma^{q+1} x_{n-2i-1}^{-(q+1)} + O(1) = \gamma^2 x_{n-2i-1}^{-(q+1)} + O(1).$$

We substitute these expressions for A^{q+1} and B^{-1} back and obtain

$$\begin{aligned} x_n^q &= A^{q+1} B^{-1} \\ &= \left(\gamma^2 x_{n-2i-1}^{-(q+1)} + O(1)\right)\left(\gamma^{-1} + O\left(x_{n-2i-1}^{q+1}\right)\right) \\ &= \gamma x_{n-2i-1}^{-(q+1)} + O(1), \end{aligned}$$

as required. □

Putting these lemmas together, we prove Proposition 3.11:

Proof (Proposition 3.11). Consider a place $P \in S_i^{(n)}$, where $0 \leq i \leq \lfloor \frac{n-3}{2} \rfloor$. We have that $x_n^{q+1} = \gamma x_{n-2i-1}^{-(q+1)} + O(1)$ at P by Lemma 3.13 with $0 \neq \gamma \in \mathbb{F}_q$ and $n - 2i - 1 \geq 2$. Lemma 3.12 yields that $x_{n-2i-1}^{-(q+1)} = \wp\left(x_{n-2i-2}^{-(q+1)}\right) + O(1)$ and therefore

$$x_n^{q+1} = \wp\left(\gamma x_{n-2i-2}^{-(q+1)}\right) + O(1),$$

in other words, $v_P\left(x_n^{q+1} - \wp\left(\gamma x_{n-2i-2}^{-(q+1)}\right)\right) \geq 0$. Since $F_{n+1} = F_n(z_{n+1})$ and $z_{n+1}^q + z_{n+1} = x_n^{q+1}$, Proposition 3.8(ii) implies that P is unramified in F_{n+1}. □

We now continue to to describe the valuations on the functions x_n at places in $S_i^{(n)}$ and $S^{(n)}$ in order to be able to apply Proposition 3.8 to the current situation.

Lemma 3.14. *Let $P \in S_i^{(n)}$ with $0 \leq i \leq \lfloor \frac{n-3}{2} \rfloor$. Then, $v_P(x_n) = -q^{n-2i-2}$.*

Proof. By Lemma 3.13, $x_n^{q+1} = \gamma \cdot x_{n-2i-1}^{-(q+1)} + O(1)$ for some $\gamma \in \mathbb{F}_q^\times$. In terms of the valuation, this means that

$$v_P\left(x_n^{q+1} - \gamma \cdot x_{n-2i-1}^{-(q+1)}\right) \geq 0. \tag{3.3.4}$$

Also, Lemma 3.10 implies that $v_P(x_{n-2i-1}) = q^{n-2i-2}$, and therefore

$$(q+1)\, v_P(x_n) = v_P\left(x_n^{q+1}\right) \geq v_P\left(\gamma x_{n-2i-1}^{-(q+1)}\right) = v_P\left(x_{n-2i-1}^{-(q+1)}\right) = -(q+1)\, v_P(x_{n-2i-1})$$

which implies that $v_P(x_n) \geq -v_P(x_{n-2i-1}) = -q^{n-2i-2}$. The triangle inequality of the valuation v_P implies that

$$\begin{aligned} v_P\left(x_n^{q+1} - \gamma \cdot x_{n-2i-1}^{-(q+1)}\right) &\geq \min\left\{v_P\left(x_n^{q+1}\right), v_P\left(\gamma \cdot x_{n-2i-1}^{-(q+1)}\right)\right\} \\ &= \min\left\{v_P\left(x_n^{q+1}\right), v_P\left(x_{n-2i-1}^{-(q+1)}\right)\right\} \\ &= (q+1)\min\left\{v_P(x_n), -v_P(x_{n-2i-1})\right\} \\ &= (q+1)\min\left\{v_P(x_n), -q^{n-2i-2}\right\}. \end{aligned}$$

Note that the second argument of the minimum is negative. Since the whole right-hand side of the inequality cannot be negative by (3.3.4), the ultrametric property must apply in this case with the valuations of the two arguments of the minimum being equal. Therefore $v_P(x_n) = -q^{n-2i-2}$. □

Lemma 3.15. *Let $P \in S^{(n)}$. Then $v_P(x_n) = -1$.*

Proof. The proof is by induction. The assertion is clear for $n \leq 2$ and we suppose $n \geq 3$. If n is odd, then $P_{n-1} = P \cap F_{n-1} \in S^{(n-1)}$ and from the induction hypothesis, P_{n-1} is a simple pole of x_n. It follows from Lemma 3.9 that the place P is a simple pole of x_n.

If n is even and $P_{n-1} = P \cap F_{n-1} \in S^{(n-1)}$, the same argument applies. It remains to check the case when n is even, $n \geq 4$ and $P_{n-1} \in S^{(n-1)}_{\frac{n-4}{2}}$. From Lemma 3.14 we know that $v_{P_{n-1}}(x_{n-1}) = -q$. Since $z_n^q + z_n = x_{n-1}^{q+1}$ and $P \mid P_{n-1}$ is unramified (Proposition 3.11), we have that

$$q \cdot v_P(z_n) = (q+1)\, v_P(x_{n-1}) = -q(q+1)$$

and hence $v_P(z_n) = -(q+1)$. It follows that

$$\begin{aligned} v_P(x_n) &= v_P(z_n/x_{n-1}) \\ &= v_P(z_n) - v_P(x_{n-1}) \\ &= -(q+1) - (-q) \\ &= -1. \end{aligned}$$

□

Lemma 3.16. *If we denote by*

$$R_n := \sum_{P \in S\left(F_n/\mathbb{F}_{q^2}\right)} v_P\left(x_n\right) P$$

the principal divisor of x_n in the function field $F_n/\mathbb{F}_{q^2}$, then

$$R_n = q^{n-1} Q_n - \sum_{i=0}^{\left\lfloor \frac{n-3}{2} \right\rfloor} q^{n-2i-2} D_i^{(n)} - D^{(n)},$$

where

$$D_i^{(n)} := \sum_{P \in S_i^{(n)}} P \text{ and } D^{(n)} := \sum_{P \in S^{(n)}} P.$$

Moreover, $\deg D_i^{(n)} = q^i\left(q-1\right)$ *and* $\deg D^{(n)} = q^{\left\lfloor \frac{n}{2} \right\rfloor}$.

Proof. This follows by induction on n, using Lemmas 3.14 and 3.15 and the defining equations $z_{n+1}^q + z_{n+1} = x_n^{q+1}$ and $x_{n+1} = z_{n+1}/x_n$. □

At this stage we have enough information to derive the recurrence needed to calculate the genus of any function field in the tower. Together Lemma 3.16 and Propositions 3.8 and 3.11 imply that the ramified places of the function field $F_n/\mathbb{F}_{q^2}$ are exactly those $P \in S^{(n)}$, and they are totally ramified. The different exponent of a place $P' \in S\left(F_{n+1}/\mathbb{F}_{q^2}\right)$ with $P' \mid P$ is $d\left(P'\right) = \left(q-1\right)\left(q+2\right)$. Hence, if we denote the respective genera of $F_n/\mathbb{F}_{q^2}$ and $F_{n+1}/\mathbb{F}_{q^2}$ by g_n and g_{n+1}, the Hurwitz genus formula (Theorem 2.19) yields

$$2g_{n+1} - 2 = q\left(2g_n - 2\right) + q^{\left\lfloor \frac{n}{2} \right\rfloor}\left(q-1\right)\left(q+2\right).$$

This recurrence enables us to establish (by induction) that the following explicit formula for the genus holds:

Theorem 3.17. *The genus $g_n = g\left(F_n\right)$ is given by*

$$g_n = \begin{cases} q^n + q^{n-1} - \frac{1}{2}q^{\frac{n}{2}+1} - \frac{3}{2}q^{\frac{n}{2}} - q^{\frac{n}{2}-1} + 1 & \text{if } n \equiv 0 \bmod 2, \\ q^n + q^{n-1} - q^{\frac{n+1}{2}} - 2q^{\frac{n-1}{2}} + 1 & \text{if } n \equiv 1 \bmod 2. \end{cases} \tag{3.3.5}$$

It remains to be shown that there are enough places of degree one in the constituent fields of the tower to ensure that the tower does meet the Drinfeld-Vlăduţ bound. Consider the subset of places of degree one of $F_n/\mathbb{F}_{q^2}$ of the following type: Let $P \in S\left(F_1/\mathbb{F}_{q^2}\right)$ be a zero of $x_1 - \alpha$ with $0 \neq \alpha \in \mathbb{F}_{q^2}$. The place P splits completely

in F_n/F_1 into q^{n-1} places in $F_n/\mathbb{F}_{q^2}$. Since there are q^2-1 possible choices of α, there are $(q^2-1)\,q^{n-1}$ places of degree one of this type in F_n. From this we have that

$$N\left(F_n/\mathbb{F}_{q^2}\right) \geq \left(q^2-1\right) q^{n-1}. \tag{3.3.6}$$

Note that only a lower bound for the number of places of degree one has been established. García and Stichtenoth show in [9] how to refine the computation in order to obtain an exact number, but this is not necessary for showing that the given tower is asymptotically optimal, as we set out to do.

The formulae for the number of places of degree one and the genus in the tower imply that $g_n \leq q^n + q^{n-1}$ and $N_n \geq (q^2-1)\,q^{n-1}$. This implies that

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} \frac{N\left(F_n/\mathbb{F}_{q^2}\right)}{g\left(F_n/\mathbb{F}_{q^2}\right)} \geq \lim_{n\to\infty} \frac{(q^2-1)\,q^{n-1}}{q^n+q^{n-1}} \geq q-1.$$

Since $q-1 \leq \lambda(\mathcal{F}) \leq A(q^2) \leq q-1$ by the Drinfeld-Vlăduţ bound (Theorem 2.37) we have that $\lambda(\mathcal{F}) = q-1$, i.e. the tower is asymptotically optimal. Noting that the construction is valid for any $q = p^n$ with p prime and $n > 1$, it also follows that $A(q^2) = q-1$, as was stated without proof earlier.

Although outside the scope of this dissertation, it is interesting to point out a connection with Drinfeld modular curves. Elkies [4] shows that the tower of García and Stichtenoth described in this section is modular, and that we can hence find explicit equations for these towers of modular curves. He also conjectures that all asymptotically optimal towers of function fields are modular.

3.4 Two towers of Kummer extensions

In [10], García and Stichtenoth introduced two towers of Kummer extensions which were subsequently generalized by Deolalikar in [2]. As these constructions yield asymptotically good towers, even in the case where the cardinality of the field of constants is non-square, it presents us with a positive lower bound for $A(q)$ for arbitrary q. We present these generalizations of Deolalikar:

Theorem 3.18. *Let $q = p^n$ and $m|n$ where $m \neq n$. Let $k = \frac{p^n-1}{p^m-1}$. Consider the tower $\mathcal{T} = (T_1, T_2, \ldots)$ of function fields over $\mathbb{F}_q$ where $T_1 = \mathbb{F}_q(x_1)$ and for $i \geq 1$, $T_{i+1} = T_i(x_{i+1})$ where*

$$x_{i+1}^k + z_i^k = b_i^k,$$

$$z_i = a_i x_i^{r_i} + b_i,$$

where $a_i, b_i \in \mathbb{F}_{p^m}^{\times}$ for $i \geq 1$ and each r_i is a power of p. Then

(i) P_∞ *splits completely throughout the tower.*

(ii) Every ramified place in the tower lies above a rational place in T_1.

(iii) $\lambda(T) \geq \frac{2}{q-2}$.

Proof. First, note that if $P \in S(T_2/\mathbb{F}_q)$ is a zero of x_1 in T_2, then we obtain a zero of x_2 of order not divisible by k. Hence the right-hand side is not a kth power of an element of T_1. This argument similarly holds for a place dividing x_i in T_{i+1} for $i \geq 2$. Therefore each equation is irreducible, and the tower is well-defined.

(i) Considering a typical step in the tower, we have

$$\begin{aligned} x_{i+1}^k &= b_i^k - (a_i x_i^{r_i} + b_i)^k \\ &= x_i^{r_i k}\left(\frac{b_i}{x_i^{r_i k}} - \left(a_i + \frac{b_i}{x^{r_i}}\right)^k\right) \\ &= a_i^k x_i^{r_i k}\left(\frac{b_i}{a_i^k x_i^{r_i k}} - \left(1 + \frac{b_i}{a_i x_i^{r_i}}\right)^k\right). \end{aligned}$$

The extension $T_{i+1} = T_i(x_{i+1})$ is then clearly equal to the extension $T_{i+1} = T_i(X_{i+1})$ where $X_{i+1} = \frac{x_{i+1}}{a_i x_i^{r_i}}$, since $\frac{1}{a_i x_i^{r_i}} \in T_i$. Hence the defining equation of T_{i+1}/T_i is equivalent to

$$X_{i+1}^k = \frac{b_i}{a_i^k x_i^{r_i k}} - \left(1 + \frac{b_i}{a_i x_i^{r_i}}\right)^k \tag{3.4.1}$$

and we set α equal to the right-hand side of (3.4.1). Then, working at $P_\infty = (x)_\infty$, we have $v_{P_\infty}(\alpha) = 0$ and in the residue field $\overline{\alpha} = -\overline{1} \in \mathcal{O}_{P_\infty}/P_\infty$. Hence, by [6, p.130 (2.28)], P_∞ splits into k distinct places in the extension T_{i+1}/T_i.

(ii) Working with the residue classes, note that for ramification to take place in T_{i+1}/T_i, we must have that the norm of $\overline{z_i}$ must be an element of $\mathbb{F}_{p^m}$. Thus $\overline{z_i} \in \mathbb{F}_q$. Since $\overline{z_i}$ is obtained by a linear transformation with $\mathbb{F}_q$ coefficients of a characteristic power of $\overline{x_i}$, $\overline{x_i} \in \mathbb{F}_q$. But then, since $\overline{x_i}^k + \overline{z_{i-1}}^k = \overline{b_i}^k$, $\overline{z_{i-1}} \in \mathbb{F}_q$, and therefore $\overline{x_{i-1}} \in \mathbb{F}_q$. Continuing in this way to the first step of the tower, we obtain $\overline{x_1} \in \mathbb{F}_q$. Therefore every ramified place in T_i lies above a (finite) rational place in T_1.

(iii) Firstly, it is easy to see that $N(T_j) > k^{j-1}$ for $j \geq 2$ by (i). We proceed to find an upper bound for the degree of the different. For the jth stage of the

tower, the degree of the different is always less than it would have been if all q finite rational places ramified from the second stage of the tower onwards. This yields, using the transitivity of the different

$$\begin{aligned}\deg \mathrm{Diff}\left(T_j/T_1\right) &< q\left((k-1)\,k^{j-2}+(k-1)\,k^{j-3}+\ldots+(k-1)\,k+(k-1)\right)\\ &= q\,(k-1)\left[1+k+k^2+\ldots+k^{j-2}\right]\\ &< q\left(k^{j-1}-1\right).\end{aligned}$$

Using the Hurwitz genus formula, we obtain

$$g\left(T_j\right) < \frac{1}{2}\,(q-2)\left(k^{j-1}-1\right).$$

Hence

$$\lambda\left(\mathcal{T}\right) = \lim_{j\to\infty}\frac{N\left(T_j\right)}{g\left(T_j\right)} \geq \lim_{j\to\infty}\frac{2k^{j-1}}{(q-2)\left(k^{j-1}-1\right)} = \frac{2}{q-2}.$$

□

In its original form, this tower first appeared in [10] with $m = r_i = a_i = b_i = 1$. Over $\mathbb{F}_4$, this tower meets the Drinfeld-Vlăduţ bound.

The above theorem proves that there exists explicit towers of function fields over any finite field which are asymptotically good, although the bound $A\left(q\right) \geq \frac{2}{q-2}$ is of course rather weak when working over large finite fields $\mathbb{F}_q$. A stronger lower bound can be obtained using the next tower, which also first appeared in less general form in [10]:

Theorem 3.19. *Let $q = p^n > 4$, and let $l = p^m - 1$ so that $m|n$ and $l > 1$. Consider the tower $\mathcal{U} = (U_1, U_2, \ldots)$ of function fields over $\mathbb{F}_q$ where $U_1 = \mathbb{F}_q\left(x_1\right)$ and for $i \geq 1$, $U_{i+1} = U_i\left(x_{i+1}\right)$, where*

$$x_{i+1}^l + z_i^l = 1,$$

$$z_i = a_i x_i^{s_i} + b_i,$$

where $a_i, b_i \in \mathbb{F}_{p^m}^{\times}$ for $i \geq 1$ and each s_i is a power of p. Then

(i) P_∞ splits completely throughout the tower,

(ii) Every ramified place in the tower lies above a rational place in U_1 of the form P_γ, with $\gamma \in \mathbb{F}_{p^m}$ and

(iii) $\lambda\left(\mathcal{U}\right) \geq \frac{2}{p^m-2}$.

Proof. Again, it is first verified that $\mathcal{U}$ is indeed a tower of function fields. This follows, as in the proof of Theorem 3.18, because $b_i^l = b_i^{p^m-1} = 1$. The proof of (i) follows similarly to that of Theorem 3.18(i). For (ii), note that to have ramification at the ith stage of the tower, we must have that $\overline{z_i}^l = 1$, i.e. $\overline{z_i} \in \mathbb{F}_{p^m}^\times$. Similarly to the proof of Theorem 3.18, we inductively find that each $\overline{z_j}$ and $\overline{x_j}$ for $j \leq i$ is in $\mathbb{F}_{p^m}^\times$, and hence $\overline{x_1} \in \mathbb{F}_{p^m}^\times$, implying that the ramified place lies above a rational place of the form P_γ, with $\gamma \in \mathbb{F}_{p^m}$. By again bounding the different divisor as before, we also obtain (iii). □

The tower $\mathcal{U}$ as described above can yield better lower bounds for $A(q)$, considering that Theorem 3.19 implies that whenever we have an extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ we can (for odd p) explicitly construct a tower $\mathcal{U}$ of Kummer extensions over $\mathbb{F}_{p^n}$ with $\lambda(\mathcal{U}) \geq \frac{2}{p^m-2}$ instead of the much weaker $\lambda(\mathcal{T}) \geq \frac{2}{p^n-2}$ implied by Theorem 3.18.

3.5 Towers of finite ramification type

In [13] García, Stichtenoth and Thomas consider the value of $\lambda(\mathcal{F})$ for tame towers $\mathcal{F}$ over a constant field of not necessarily square cardinality. We follow notation from [12] and make the following definition:

Definition 3.20. *Let $\mathcal{F} = (F_1, F_2, ...)$ be a tower of function fields over $\mathbb{F}_q$. Let*

$$V(\mathcal{F}) := \{P \in S(F_1/\mathbb{F}_q) : P \text{ is ramified in } F_n/F_1 \text{ for some } n \geq 2\}$$

be the ramification locus of $\mathcal{F}$. We will say $\mathcal{F}$ is of finite ramification type if $V(\mathcal{F})$ is finite.

We also make the following definition in order to analyze the splitting behaviour:

Definition 3.21. *Let $\mathcal{F} = (F_1, F_2, ...)$ be a tower of function fields over $\mathbb{F}_q$. We say that $\mathcal{F}$ is completely splitting if the set*

$$T(\mathcal{F}) := \{P \in S(F_1/\mathbb{F}_q) : \deg P = 1 \text{ and } P \text{ splits completely in all } F_n/F_1\}$$

is non-empty.

García, Stichtenoth and Thomas gave a lower bound for the case where the tower is tamely ramified. This was subsequently generalized by Van der Merwe in [34], giving the following theorem which is applicable even in the case of towers which are not tamely ramified:

Theorem 3.22. *Let $\mathcal{F} = (F_1, F_2, ...)$ be a tower of function fields over $\mathbb{F}_q$ where the following three conditions hold:*

(i) $\mathcal{F}$ is of finite ramification type.

(ii) $\mathcal{F}$ is completely splitting.

(iii) Suppose for each $Q \in S(F_n/\mathbb{F}_q)$ we let a_Q be a non-negative constant such that $d(Q|P) \leq a_Q \cdot e(Q|P)$ where $P = Q \cap F_1$, and the set $\{a_Q : Q \in S(F_n/\mathbb{F}_q)\}$ is bounded.

Then

$$\lambda(\mathcal{F}) \geq \frac{2 \cdot |T(\mathcal{F})|}{2g(F_1) - 2 + \sum_{P' \in V(\mathcal{F})} a_{P'} \cdot \deg P'} > 0 \tag{3.5.1}$$

where the $a_{P'}$ are constants such that $a_Q \leq a_{P'}$ if $Q|P'$ for $Q \in S(F_n/\mathbb{F}_q)$.

Proof. Note that (i) implies that $V(\mathcal{F})$ is finite. Let $S = \{P_1, P_2, ..., P_m\}$ be some finite subset of $S(F_1/\mathbb{F}_q)$ which contains $V(\mathcal{F})$. We may of course have that $S = V(\mathcal{F})$, but relaxing this condition will not weaken the obtained lower bound. Since the different divisor involves only those places lying over ramified places,

$$\begin{aligned}
\deg \ \mathrm{Diff}(F_n/F_1) &= \sum_{j=1}^{m} \sum_{Q|P_j, Q \in S(F_n/\mathbb{F}_q)} d(Q|P_j) \deg Q \\
&\leq \sum_{j=1}^{m} \sum_{Q|P_j, Q \in S(F_n/\mathbb{F}_q)} a_{P_j} \cdot e(Q|P_j) \cdot \deg Q \\
&= [F_n : F_1] \sum_{j=1}^{m} a_{P_j} \cdot \deg P_j.
\end{aligned}$$

The Hurwitz genus formula (Theorem 2.19) yields

$$\begin{aligned}
2g(F_n) - 2 &= [F_n : F_1](2g(F_1) - 2) + \deg \ \mathrm{Diff}(F_n/F_1) \\
&\leq [F_n : F_1](2g(F_1) - 2) + [F_n : F_1] \sum_{j=1}^{m} a_{P_i} \deg P_i \\
&= [F_n : F_1] \left(2g(F_1) - 2 + \sum_{i=1}^{m} a_{P_j} \deg P_j \right)
\end{aligned}$$

and hence

$$\begin{aligned}\frac{N(F_n)}{g(F_n)-1} &\geq \frac{2N(F_n)}{[F_n:F_1]\left(2g(F_1)-2+\sum_{j=1}^{m} a_{P_j}\deg P_j\right)} \\ &\geq \frac{2\cdot|T(\mathcal{F})|\cdot[F_n:F_1]}{[F_n:F_1]\left(2g(F_1)-2+\sum_{j=1}^{m} a_{P_j}\deg P_j\right)} \\ &= \frac{2\cdot|T(\mathcal{F})|}{2g(F_1)-2+\sum_{j=1}^{m} a_{P_j}\deg P_j}\end{aligned}$$

which implies that

$$\begin{aligned}\lambda(\mathcal{F}) &\geq \frac{2\cdot|T(\mathcal{F})|}{2g(F_1)-2+\sum_{j=1}^{m} a_{P_j}\deg P_j} \\ &= \frac{2\cdot|T(\mathcal{F})|}{2g(F_1)-2+\sum_{P'\in V(\mathcal{F})} a_{P'}\deg P'}\end{aligned}$$

since we can choose $a_P = 0$ for $a_P \in S \setminus V(\mathcal{F})$, since the different exponents of such P are zero. □

As an immediate corollary we have

Corollary 3.23.

(i) If $\mathcal{F}$ has no ramification, then $\lambda(\mathcal{F}) \geq \frac{|T(\mathcal{F})|}{g(F_1)-1}$.

(ii) If $\mathcal{F}$ is tame, then $\lambda(\mathcal{F}) \geq \frac{2\cdot|T(\mathcal{F})|}{2g(F_1)-2+\sum_{P'\in V(\mathcal{F})}\deg P'}$.

Proof. In case (i) $V(\mathcal{F}) = \varnothing$, and we can choose all the a_{P_i} to be zero. In case (ii) the Dedekind Different Theorem becomes an equality, and $d(Q|P_i) = e(Q|P_i) - 1$, and hence we can choose all $a_{P_j} = 1$, since $d(Q|P_i) \leq 1\cdot(e(Q|P_i)-1)$. □

Corollary 3.23 can be used as an alternative way to prove that the tower $\mathcal{T}$ from Theorem 3.18 has $\lambda(\mathcal{T}) \geq \frac{2}{q-2}$. Indeed, in the notation of Theorem 3.18, the extensions are certainly tame since $(l,p) = 1$, the infinite place splits completely in all extensions giving $|T(\mathcal{F})| \geq 1$ by Theorem 3.18(i), and $V(\mathcal{F}) \subseteq S$ where S consists of all the finite places of degree one in T_1 by Theorem 3.18(ii). Corollary 3.23(ii) applies, proving Theorem 3.18(iii).

As a way of finding better values of a_P for $P \in V(\mathcal{F})$ for use in Theorem 3.22, the following proposition is useful:

Proposition 3.24. *Let $\mathcal{F} = (F_1, F_2, \ldots)$ be a tower of function fields over $\mathbb{F}_q$. For $P \in S(F_1/\mathbb{F}_q)$, let a_P be a non-negative constant such that $a_P \cdot (e(Q_{i+1}|Q_i) - 1) \geq$*

$d(Q_{i+1}|Q_i)$ for all $i \geq 1$ where $Q_i \in S(F_i/\mathbb{F}_q)$, $Q_{i+1} \in S(F_{i+1}/\mathbb{F}_q)$ and $P \subseteq Q_i \subseteq Q_{i+1}$. Then

$$a_P \cdot e(Q|P) \geq d(Q|P) \text{ for all } Q \in P(F_n/\mathbb{F}_q) \text{ with } Q|P.$$

Proof. Let $F_1' \subseteq F_2' \subseteq F_3'$ be finite separable extensions of function fields and $P_1 \subseteq P_2 \subseteq P_3$ respective places of them lying over each other. If a_P is a non-negative constant such that $a_P(e(P_{i+1}|P_i) - 1) \geq d(P_{i+1}|P_i)$ for $i = 1, 2$ then

$$\begin{aligned} d(P_3|P_1) &= e(P_3|P_2) \cdot d(P_2|P_1) + d(P_3|P_2) \\ &\leq e(P_3|P_2)\, a_P(e(P_2|P_1) - 1) + a_P(e(P_3|P_2) - 1) \\ &= a_P(e(P_3|P_1) - 1), \end{aligned}$$

and the result follows by transitivity. □

Theorem 3.22 provides a way to obtain lower bounds for $\lambda(\mathcal{F})$ for even the cases of $\mathcal{F}$ having wild ramification or being defined over a field of constants of non-square cardinality. We will apply this theorem to a wildly ramified tower over a non-square, non-prime finite field in Chapter 5.

In [11], García and Stichtenoth introduce a new asymptotically optimal tower of function fields over $\mathbb{F}_{q^2}$ by letting $\mathcal{E} = (E_1, E_2, ...)$ where $E_1 = \mathbb{F}_{q^2}(x_1)$ and $E_{i+1} = E_i(x_{i+1})$ with

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1} \text{ for } i = 1, 2, ... \tag{3.5.2}$$

This was proved independently first in [11] (by recursively bounding the degree of the different divisor) and later by Van der Merwe [34] (by using Corollary 3.23). García and Stichtenoth, in [11], after proving that this tower is optimal, mention that the tower $\mathcal{E}$ is in fact a subtower of their previous tower $\mathcal{F}$ described in Definition 3.7 from [9]. This can be seen by noting that

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} = \frac{z_n^{q+1}}{x_{n-1}^{q+1}} = \frac{z_n^{q+1}}{z_n^q + z_n} = \frac{z_n^q}{z_n^{q-1} + 1} \text{ for } n = 2, 3, ...,$$

and hence $E_n \subseteq \mathbb{F}_{q^2}(x_1, z_2, z_3, ..., z_n) = F_n$ for $n \geq 2$, and $\mathcal{E} \prec \mathcal{F}$. Since $\mathcal{F}$ was shown to be asymptotically optimal, it follows by Corollary 3.6, that $\mathcal{E}$ is asymptotically optimal as well. García and Stichtenoth proved this fact for $\mathcal{E}$ in [11] in a completely different way, however.

Writing the right-hand side of (3.5.2) as $\frac{x_i^{q+1}}{x_i^q + x_i}$, we note that this expression is in terms of the trace (denominator) and norm (numerator). This motivates the study of extensions using these and generalizations of these functions in the next chapter.

Chapter 4

Symmetry

Heuristically, a tower of function fields $\mathcal{F} = (F_1, F_2, ...)$ over K which is asymptotically good, should in some way have constituent field extensions which split as many as possible rational places in each step, while keeping the degree of the different divisor low, thereby minimizing the growth of the genus. This is illustrated well by for example considering Theorem 3.22 over an algebraically closed (infinite) field. In that situation, almost all places are split completely in each step of the extension, and the places which are ramified lie over a finite subset of $S(F_1/K)$. The observation may also be made that while constituent field extensions which are optimal with respect to the number of places of degree one may be preferable, this aim is secondary to ensuring that as many places as possible split completely in each step of the tower, and not just those early in the tower. The reason for this is that while in the short term optimal function fields are good to get a high $N(F_i)$ for the first steps in the tower, it is essential to keep this as high as possible asymptotically. Optimal choices early in the tower may create difficulties later on, making an asymptotically good construction impossible.

The secondary problem with which we are faced is to describe these extensions explicitly, i.e. derive explicit rational functions f_i and g_i with $f_i(x_{i+1}) = g_i(x_i)$ which define the extensions $F_{i+1} := F_i(x_{i+1})$ recursively. Doing so, we would hope that the rational functions arising in this way would in some way be natural, leading to possible generalizations. In the examples we will consider, f_i will often be a polynomial defining a Kummer, Artin-Schreier or linearized extension, and g_i a rational function constructed in terms of symmetric or quasi-symmetric functions.

In this chapter we will give an overview of the calculation of the genus in many situations. The emphasis will however not primarily be on improving the $N(F_i)/g(F_i)$ ratio in $\mathcal{F}$ as $i \to \infty$, but rather the ratio $N(F_i)/[F_i : F_1]$. This will give us free rein

to focus on the problem of splitting as many places as possible in each extension of the tower relative the the degree of the extension, i.e. splitting almost all places of degree one, while possibly at the cost of a large genus.

Deolalikar looks at the situation as described above in his Ph.D. thesis [2], and considers the effect of splitting almost all rational places in extensions of function fields. Particularly, he describes families where all rational places, or all rational places except one are split completely. This splitting is achieved by using the symmetric and quasi-symmetric functions mentioned earlier, and gives a natural form for the explicit constructions in terms of these functions. This also leads to a natural generalization of the Hermitian function field, which in some cases yields some of the best values for $N_q(g)$ as listed in Van der Geer and Van der Vlugt's tables [33].

Some properties of towers of these forms are discussed, and we exhibit an example by Deolalikar implying that splitting all places of degree one except one is better than splitting all places of degree one to limit the growth of the genus in extensions of function fields, although the number of places of degree one in the extension field is less. This emphasizes the fact that asymptotically good towers are rare, and that a "greedy" approach, for example attempting maximal splitting of all places of degree one in each step of a tower will most likely result in asymptotically bad towers. What follows is a discussion of this work of Deolalikar.

4.1 Symmetric extensions

Let R be an integral domain and let K be the field of fractions of R. Consider the polynomial ring in n variables over R, given by $R[X] := R[x_1, x_2, ..., x_n]$. The symmetric group S_n in n variables acts naturally on $R[X]$, permuting the variables. A polynomial $f(X) \in R[X]$ which is fixed under the action of S_n, is called a *symmetric polynomial*. If S_n is allowed to act on the quotient field $K(X)$ in the natural way, its fixed elements will be called *symmetric rational functions*, or simply *symmetric functions*. These form a subfield $K(X)_s$ of $K(X)$. The theory of symmetric functions forms a rich branch of the study of polynomials in several indeterminates. Amongst others, we have the fundamental theorem on symmetric functions, which states that

$$K(X)_s = K(s_{n,1}(X), s_{n,2}(X), ..., s_{n,n}(X))$$

where the n elementary symmetric polynomials in n variables are

$$\begin{aligned} s_{n,1}(X) &= \sum_{1\leq i\leq n} x_i, \\ s_{n,2}(X) &= \sum_{1\leq i<j\leq n} x_i x_j, \\ \vdots &= \vdots \\ s_{n,n}(X) &= x_1 x_2 ... x_n \end{aligned}$$

i.e. that any symmetric rational function can be written as a rational function in the elementary symmetric polynomials.

We now consider an arbitrary finite field $\mathbb{F}_q$, and an arbitrary extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of degree n of it. From Galois theory, we know that this is a Galois extension, it is cyclic, and that the group is generated by the Frobenius automorphism $\phi : \alpha \longmapsto \alpha^q$ of the extension. For this extension, we will evaluate the elementary symmetric polynomials (resp. symmetric functions) in $\mathbb{F}_{q^n}(t)$ at $(t, \phi(t), \phi^2(t), ..., \phi^{n-1}(t))$ where t is some indeterminate. We will call these the (n,q)-elementary symmetric polynomials (resp. (n,q)-symmetric functions) and writing them as functions of t, we have

$$\begin{aligned} s_{n,1}(t) &= \sum_{0\leq i\leq n-1} t^{q^i}, \\ s_{n,2}(t) &= \sum_{0\leq i<j\leq n-1} t^{q^i} t^{q^j}, \\ \vdots &= \vdots \\ s_{n,n}(t) &= t^{1+q+q^2+...+q^{n-1}}. \end{aligned}$$

There are n (n,q)-elementary symmetric polynomials, of which $s_{n,1}(t)$ and $s_{n,n}(t)$ are the familiar trace and norm, respectively. If $n \geq 3$, there are more possibilities, and Deolalikar strongly suggests that these are more useful towards the aim of constructing function fields with many rational places than the trace and norm. We note that these polynomials are, by construction, invariant under the action of Frobenius. As is known for the trace and norm, we also have more generally the following lemma:

Lemma 4.1. *Let $f(t)$ be an (n,q)-symmetric function with coefficients from $\mathbb{F}_q$ and let $\gamma \in \mathbb{F}_{q^n}$. Then, we have that $f(\gamma) \in \mathbb{F}_q \cup \infty$.*

Proof. We can write $f(t)$ as a rational function in $\{s_{n,i}(t)\}_{1\leq i\leq n}$ with coefficients in $\mathbb{F}_q$. Note that each (n,q)-symmetric polynomial is invariant under the operation

of raising to the qth power, modulo $\left(t^{q^n} - t\right)$, by definition. Hence, each (n, q)-elementary symmetric polynomial, restricted to $\mathbb{F}_{q^n}$, is invariant under this operation, as are the coefficients, since they are from $\mathbb{F}_q$. The only other possibility is γ being a pole of f, which yields the possibility ∞. □

It can be checked [2, Lemma 1.2.6-1.2.12] that $s_{n,1}(t)$ is a permutation polynomial over $\mathbb{F}_{q^m}$ (i.e., induces a bijection over $\mathbb{F}_{q^m}$) if $\gcd(m, n) = 1$ and $p \nmid n$, where p is the characteristic of $\mathbb{F}_q$.

We will denote the field of (n, q)-symmetric functions with coefficients in $\mathbb{F}_{q^n}$ by

$$F_s := \mathbb{F}_{q^n}\left(s_{n,1}(x), s_{n,2}(x), ..., s_{n,n}(x)\right) \subset \mathbb{F}_{q^n}(x)$$

and the field of (n, q)-symmetric functions with coefficients in $\mathbb{F}_q$ by

$$F_s^{\phi} := \mathbb{F}_q\left(s_{n,1}(x), s_{n,2}(x), ..., s_{n,n}(x)\right) \subset \mathbb{F}_{q^n}(x).$$

The superscript ϕ indicates that the values of these functions are fixed by ϕ on $\mathbb{F}_{q^n}$, and hence lie in $\mathbb{F}_q$, by Lemma 4.1.

Let $F/\mathbb{F}_{q^n}$ be a function field, and E a finite separable extension of F generated by y, where $\varphi(y) = 0$ for φ an irreducible polynomial over F. The aim will now be to describe families of extensions of F whose generators satisfy explicit equations in terms of only (n, q)-symmetric functions. Let y satisfy $g(y) = f(x)$ where $f, g \in F_s^{\phi}$. By Lemma 4.1 and the subsequent comments, it is clear that f and g will only assume values in $\mathbb{F}_q \cup \infty$, rather than other values in $\mathbb{F}_{q^n} \cup \infty$. It is this property of these functions which tends to increase the number of solution pairs (x, y) of the equation. The case of f being an (n, q)-elementary symmetric polynomial will be considered in the rest of the chapter, but the same methods can be used to handle cases where we do not make this assumption, and choose arbitrary $f \in F_s^{\phi}$.

In order to describe a family of modified Artin-Schreier extensions based on the elementary symmetric polynomials, we prove the following lemma:

Lemma 4.2. *Let $F = \mathbb{F}_{q^n}(x)$, $q = p^m$ and $r = m(n-1)$. Moreover, let $E := F(y)$ where y satisfies*

$$y^{q^{n-1}} + y^{q^{n-2}} + ... + y = f(x)$$

and $f(x)$ is not the image of any element in F under a linear polynomial. Then the following hold:

(i) The extension E/F is Galois of degree $[E : F] = q^{n-1}$. Elements of $\mathrm{Gal}(E/F) = \{\sigma_\beta : y \longmapsto y + \beta\}_{s_{n,1}(\beta)=0}$ can be identified with the set of elements in $\mathbb{F}_{q^n}$ whose

trace $(s_{n,1})$ *is zero. This gives* $\mathrm{Gal}(E/F)$ *the structure of a* r*-dimensional* $\mathbb{F}_p$ *vector space.*

(ii) There exists a tower of subextensions

$$F = E^0 \subset E^1 \subset ... \subset E^r = E$$

such that for $i = 0, 1, ..., r-1$, $[E^{i+1} : E^i]$ *is Galois of degree* p.

(iii) Let $\{b_i\}_{1 \leq i \leq r}$ *be a* $\mathbb{F}_p$*-basis for* $\mathrm{Gal}(E/F)$. *The tower of subextensions of (ii) can then be constructed in the following manner. For* $j = 0, 1, ..., r-1$, *let* E^j *be the fixed field of the subgroup of* $\mathrm{Gal}(E/F)$ *generated by* $\{b_1, b_2, ..., b_{r-j}\}$. *The generators of* E^j *are then* $\{y_1, y_2, ..., y_j\}$ *where* $y_1, y_2, ..., y_r = y$ *satisfy*

$$\begin{aligned} y^p - B_r^{p-1} y &= y_{r-1}, \\ y_{r-1}^p - B_{r-1}^{p-1} y_{r-1} &= y_{r-2}, \\ \vdots &= \vdots \\ y_1^p - B_1^{p-1} y_1 &= f(x), \end{aligned}$$

where

$$\begin{aligned} \beta_{r,j} &= b_{r-j+1}, \\ \beta_{r-1,j} &= \beta_{r,j}^p - B_r^{p-1} \beta_{r,j}, \\ \vdots &= \vdots \\ \beta_{1,j} &= \beta_{2,j}^p - B_2^{p-1} \beta_{2,j} \end{aligned}$$

and

$$B_i = \beta_{i,i}.$$

Proof.

(i) We note that since

$$s_{n,1}(y) = y^{q^{n-1}} + y^{q^{n-2}} + ... + y$$

is additive, its roots (being $\beta \in \mathbb{F}_{q^n}$ with $s_{n,1}(\beta) = 0$) form a finite abelian subgroup $V \subseteq \mathbb{F}_{q^n}$ (considered as an additive group). Using Theorem 2.31, one finds that $s_{n,1}(y) - f(x)$ is absolutely irreducible, and hence by Proposition 2.30 is a Galois extension where the Galois group is isomorphic to the kernel of $s_{n,1}$.

(ii) Examining the description for $\mathrm{Gal}(E/F)$ given in (i), we observe that it is a product of p-cycles and hence has exponent p. Indeed, if $\beta_1, \beta_2 \in \mathbb{F}_{q^n}$ with $s_{n,1}(\beta_1) = 0 = s_{n,1}(\beta_2)$, then $\langle \sigma_{\beta_1} \rangle$ and $\langle \sigma_{\beta_2} \rangle$ are both p-cycles, and hence $\langle \sigma_{\beta_1}, \sigma_{\beta_2} \rangle$ is an abelian group of order p^2, therefore a product of p-cycles. Hence we can always find a normal series

$$\mathrm{Gal}(E/\mathbb{F}_{q^n}) = G^0 \rhd G^1 \rhd \ldots \rhd G^r = 1$$

such that $[G^{i+1} : G^i] = p$. The fundamental theorem of Galois theory then implies the existence of the desired tower by setting E^i to be the fixed field of G^i.

(iii) Note that (ii) already provided a proof of the existence of a tower with the desired properties. We show that the successive extensions will satisfy the given recursive equations. Let G^{r-1} be the $\mathbb{F}_p$-span of b_1, and E^{r-1} its fixed field.The automorphisms of E^r/E^{r-1} are then given by $y \longmapsto y + ab_1$ with $a \in \mathbb{F}_p$. Therefore

$$\prod_{a \in \mathbb{F}_p} (y - ab_1) = \prod_{a \in \mathbb{F}_p} b_1 \left(\frac{y}{b_1} - a \right) = b_1^p \prod_{a \in \mathbb{F}_p} \left(\frac{y}{b_1} - a \right) = y^p - b_1^{p-1} y = y_{r-1}$$

Now this procedure is iterated by letting G^{r-2} be the $\mathbb{F}_p$-span of $\{b_1, b_2\}$ and considering the extension E^{r-1}/E^{r-2}, and noting that the automorphism of E/F given by $y \longmapsto y + b_2$, when restricted to an automorphism of E^{r-1}/E^{r-2} is given by $y_{r-1} \longmapsto y_{r-1} + b_2^p - b_1^{p-1} b_2$. By continuing setting G^{r-j}, $j \geq 2$ to be the $\mathbb{F}_p$-span of $\{b_1, b_2, \ldots, b_j\}$ and restricting the automorphisms of E/F to E^{r-j+1}/E^{r-j}, we get the defining equations stated above in terms of the basis elements.

□

In the notation of Lemma 4.2, it is clear that every subextension E^1 of E which has degree p over F is of the form $F(z)$, where z satisfies $z^p - Az = f(x)$, for some $A \in \mathbb{F}_{q^n}$. We now focus on the case where $f(x)$ is an elementary symmetric polynomial, and derive a result analogous to Proposition 2.30 in the form of the following theorem

Theorem 4.3 ([2, 1.3.14]). *Let $F = \mathbb{F}_{q^n}(x)$, $q = p^m$ and $r = m(n-1)$. For each $i = 2, 3, \ldots, n$, let*

$$E_i := F(y)$$

where y satisfies

$$y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y = s_{n,i}(x).$$

Then the following hold for each extension E_i/F:

(i) E_i/F is Galois of degree $[E_i : F] = q^{n-1}$ and

$$\mathrm{Gal}(E_i/F) = \{\sigma_\beta : y \to y + \beta\}_{s_{n,1}(\beta)=0}.$$

(ii) The only place of $F/\mathbb{F}_{q^n}$ that is ramified in E_i is the unique pole P_∞ of x. Moreover, this pole P_∞ is totally ramified in E_i. We denote the unique place lying above P_∞ in E_i/F by P'_∞.

(iii) Let m_i denote the coprime degree of $s_{n,i}(x)$. Then

$$m_i = q^{n-1} + q^{n-2} + \ldots + q^{n-i+1} + 1.$$

The ramification groups of $P'_\infty|P_\infty$ are $G_0 = G_1 = \ldots = G_{m_i+1} = \mathrm{Gal}(E_i/F)$ and $G_{m_i+2} = \{0\}$.

(iv) The different exponent $d(P'_\infty|P_\infty) = (q^{n-1} - 1)(m_i + 1)$.

(v) The genus $g(E_i) = \frac{1}{2}(q^{n-1} - 1)(m_i - 1)$.

(vi) All other rational places of $F/\mathbb{F}_{q^n}$ split completely in E_i/F, giving $N(E_i) = q^{2n-1} + 1$, a number independent of the choice of (n, q)-elementary symmetric polynomial $s_{n,i}(x)$.

Proof.

(i) Note that p times the coprime degree of $s_{n,i}(x)$ is larger than the degree of $s_{n,i}(x)$. This follows because the term of $s_{n,i}(x)$ determining the coprime degree of the polynomial must be $x^{q^{n-1}+q^{n-2}+\ldots+q^{n-i+1}+1}$ by maximality, and the nondivisibility by p of the exponent of x. Therefore the hypotheses of Condition 2.32 are met, ensuring that the defining equation of E_i/F is absolutely irreducible. Then the proof is completed by applying Lemma 4.2(i).

(ii) By Proposition 2.30 and in particular part (v) (with the hypotheses satisfied by P_∞), only the infinite place P_∞ is ramified in this extension, and it is totally ramified.

(iii) Let $G = \mathrm{Gal}(E_i/F)$. In order to study the sequence of ramification groups

$$G = G_{-1} \geq G_0 \geq G_1 \geq G_2 \geq ...,$$

we use the indicator function i_G as defined on page 16. For each subgroup $H \leq G$, define $(G/H)_k$ to be the kth ramification group of the fixed field of H, relative to P'_∞. We then analogously use the indicator function $i_{G/H}$ on G/H which has the characterization

$$i_{G/H}(\overline{s}) \geq k+1 :\Longleftrightarrow \overline{s} \in (G/H)_k$$

where $\overline{s} = s + H$.

Claim 1: If $[G : H] = p$, we have that

$$i_{G/H}(\overline{s}) = \begin{cases} \infty & \text{if } \overline{s} = 0, \\ m_i + 2 & \text{otherwise.} \end{cases}$$

Proof: The case for $\overline{s} = 0$ follows immediately, since $v_{P'_\infty}(0) = \infty$. The subgroup H of G of index p corresponds to a subextension E_i^1 of degree p over F. By the remarks following Lemma 4.2, this extension has the form $E_i^1 = F(z)$ where $z^p - Az = s_{n,i}(x)$ for some $A \in \mathbb{F}_{q^n}$. By the comments on the coprime degree in the proof of (i), Corollary 2.34 applies, and hence it is possible to find a polynomial $s^*_{n,i}(x) \in \mathbb{F}_{q^n}[X]$ such that $E_i^1 = F(Z)$ where

$$Z^p - AZ = s^*_{n,i}(x) \text{ with } \deg s^*_{n,i}(x) = m_i. \tag{4.1.1}$$

Suppose P^*_∞ is the unique place lying above P_∞ in E_i^1. We have that $\widehat{\mathcal{O}}_{P_\infty} = \mathbb{F}_{q^n}[\![x^{-1}]\!]$, and wish to find $w \in E_i^1$ such that $\widehat{\mathcal{O}}_{P^*_\infty} = \mathbb{F}_{q^n}[\![w]\!]$, in order to be able to evaluate the indicator function at $\overline{s}$. From (4.1.1), noting that $e(P^*_\infty | P_\infty) = p$ by (ii), and as $v_{P_\infty}\left(s^*_{n,i}(x)\right) < 0$, it follows that $p \cdot v_{P_\infty}(Z) = m_i \cdot v_{P_\infty}(x)$ and therefore $v_{P_\infty}(Z^{-1}) = \frac{m_i}{p}$, i.e. $v_{P^*_\infty}(Z^{-1}) = m_i$. Therefore

$$Z^{-1} = w^{m_i} \cdot u$$

where $u = a_0 + a_1 w + a_2 w^2 + ...$ is a unit ($a_0 \neq 0$) in $\widehat{\mathcal{O}}_{P^*_\infty}$, and hence

$$Z^{-1/m_i} = w \cdot u^{1/m_i}.$$

Therefore we have $\widehat{\mathcal{O}}_{P^*_\infty} = \mathbb{F}_{q^n}[\![Z^{-1/m_i}]\!]$ and equation (2.1.2) from page 16 applies. Since $\overline{s}(Z) = Z + \beta$ (say), we have

$$\overline{s}\left(Z^{-1}\right) = \frac{1}{Z+\beta} = \frac{1}{Z\left(1+\frac{\beta}{Z}\right)}$$

which yields

$$\begin{aligned}
i_{G/H}(\overline{s}) &= v_{P_\infty^*}\left(\overline{s}\left(Z^{-1/m_i}\right) - Z^{-1/m_i}\right) \\
&= v_{P_\infty^*}\left(Z^{-1/m_i}\cdot\left(1+\frac{\beta}{Z}\right)^{-1/m_i} - Z^{-1/m_i}\right) \\
&= v_{P_\infty^*}\left(Z^{-1/m_i}\right) + v_{P_\infty^*}\left(\left(1+\frac{\beta}{Z}\right)^{-1/m_i} - 1\right) \\
&= 1 + v_{P_\infty^*}\left(\left(1+\left(-\frac{1}{m_i}\right)\frac{\beta}{Z} + \left(-\frac{1}{m_i}\right)\left(-\frac{1}{m_i}-1\right)\frac{\beta^2}{Z^2}+\ldots\right) - 1\right) \\
&= 1 + v_{P_\infty^*}\left(\left(-\frac{1}{m_i}\right)\frac{\beta}{Z} + \left(-\frac{1}{m_i}\right)\left(-\frac{1}{m_i}-1\right)\frac{\beta^2}{Z^2}+\ldots\right) \\
&= 1 + v_{P_\infty^*}\left(\left(-\frac{1}{m_i}\right)\frac{\beta}{Z}\right) \\
&= 1 + v_{P_\infty^*}\left(\left(-\frac{1}{m_i}\right)\beta w^{m_i}\right) \\
&= 1 + m_i,
\end{aligned}$$

which completes the proof of the first claim, since $\overline{s} \in (G/H)_{-1} = \mathrm{Gal}\left(E_i^1/F\right)$ as well.

Claim 2: For any proper subgroup $K \subsetneqq G$, the average value of $i_{G/K}$ over the nonzero elements of G/K is $m_i + 2$.

Proof: Fix some proper subgroup $K \subsetneqq G$ and suppose $[G:K] = p^l$. We consider all the intermediate subgroups $K \subset H \subset G$ such that $[G:H] = p$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & G & \longrightarrow & G/K & \longrightarrow & 0 \\
 & & & & {\scriptstyle p}\downarrow & & {\scriptstyle p}\downarrow & & \\
0 & \longrightarrow & K & \longrightarrow & H & \longrightarrow & H/K & \longrightarrow & 0 \\
 & & & & {\scriptstyle p^{l-1}}\downarrow & & & & \\
 & & & & K & & & &
\end{array}$$

These intermediate subgroups H are in one to one correspondence with the subgroups of G/K of index p, of which there are $\frac{p^l-1}{p-1}$. Any particular $0 \neq s \in G/K$ is contained in exactly $\frac{p^{l-1}-1}{p-1}$ of these subgroups of G/K, denoted by H/K. From [25, IV Proposition 3] we get the formula

$$i_{G/H}(\overline{s}) = \frac{1}{p^{l-1}}\sum_{s\to\overline{s}} i_{G/K}(s). \tag{4.1.2}$$

Varying H, each $0 \neq s \in G/K$ is nonzero in exactly p^{l-1} of the G/H, since

$[H : K] = p^{l-1}$. Then we have

$$\sum_{K \subset H \subset G, [G:H]=p} \sum_{0 \neq \overline{s} \in G/H} i_{G/H}(\overline{s}) = \sum_{K \subset H \subset G, [G:H]=p} \frac{1}{p^{l-1}} \sum_{s \to \overline{s}} i_{G/K}(s) \text{ (by (4.1.2))}$$
$$= \sum_{0 \neq s \in G/K} \frac{1}{p^{l-1}} \cdot p^{l-1} \cdot i_{G/K}(s) = \sum_{0 \neq s \in G/K} i_{G/K}(s).$$

We note that the expression on the left-hand side has exactly $\frac{p^l-1}{p-1}(p-1) = p^l - 1$ terms, and the final expression on the right-hand side has exactly $p^l - 1$ terms as well. Therefore the average value of the terms summed over on the left must be equal to the average of the terms on the right, and it follows that, since $i_{G/H}(\overline{s}) = m_i + 2$ for $\overline{s} \neq 0$, the average of the items on the right-hand side is $m_i + 2$ as well, proving the second claim.

Now, suppose that there exists $0 \neq s \in G$ so that $i_G(s) \neq m_i + 2$. Because of Claim 1 above, we can assume without loss of generality that $i_G(s) > m_i + 2$. Since i_G is constant on cyclic subgroups, G cannot be cyclic. But then the average of i_G on $G/\langle s \rangle$ will be less than $m_i + 2$, a contradiction. It follows that $i_G(s) = m_i + 2$ for nonzero $s \in G$, and therefore implies that

$$\text{Gal}(E_i/F) = G_0 = G_1 = \ldots = G_{m_i+1} \text{ and } G_{m_i+2} = 0.$$

(iv) By Hilbert's Different Theorem,

$$d(P'_\infty | P_\infty) = \sum_{i=0}^{\infty} (|G_i| - 1) = \left(q^{n-1} - 1\right)(m_i + 1).$$

(v) Since $g(F) = 0$, the Hurwitz genus formula implies that

$$g(E_i) = 1 + q^{n-1}(-1) + \frac{1}{2}\left(q^{n-1} - 1\right)(m_i + 1)$$
$$= \frac{1}{2}\left(q^{n-1} - 1\right)(m_i - 1)$$

since $\text{Diff}(E_i/F) = (q^{n-1} - 1)(m_i + 1) \cdot P'_\infty$.

(vi) The complete splitting of the other rational places follows directly from Proposition 2.30. The number of places of degree one in E_i is then given by the places lying above finite places of F (there are $q^n \cdot q^{n-1}$ of them) and the unique place P'_∞ lying above P_∞ adding up to $q^{2n-1} + 1$ places of degree one.

□

It may now be noted that the example shown on page 21 can be studied in the light of Theorem 4.3. In particular, we can now consider the extension E_2/F determined by the equation

$$y^{q^2} + y^q + y = s_{3,2}(x)$$

where $F = \mathbb{F}_{q^3}(x)$. From the preceding theorem it immediately follows that all rational places of F, except for the pole P_∞, splits completely in E_2/F. Then the function field E_2/F has $q^5 + 1$ rational places and $g(E_2) = \frac{1}{2}q^2(q^2 - 1)$, since the coprime degree of $s_{3,2}(x)$ in this context is $m_2 = q^2 + 1$.

It is interesting to note that the above example, when $q = 2$, yields the defining equation

$$y^4 + y^2 + y = x^6 + x^5 + x^3$$

for an extension of the rational function field over $\mathbb{F}_8$ which has $2^5 + 1 = 33$ places of degree one and genus $\frac{1}{2}2^2(2^2 - 1) = 6$. From Van der Geer and Van der Vlugt's tables [33] for $N_q(g)$, we find this function field attains the best known value for $N_8(6)$. It is unknown whether there exist function fields over $\mathbb{F}_8$ of genus 6 which has more than 33 places of degree one. Similarly, the analogous equation for $q = 3$ yields a function field of genus 36 having 244 places of degree one, also attaining the best known value for $N_{27}(36)$ on the tables.

It has been long known that the "trace-norm" extensions of the form E/F, $E = F(y)$ with

$$s_{n,1}(y) = s_{n,n}(x)$$

split all rational places of degree one, except for the pole, which is totally ramified. It is now clear, however, that this is only one special case of a more general family of symmetric extensions sharing many of the same properties. For the case $n = 2$, this yields the known maximal Hermitian function field, where the trace and norm are taken down to $\mathbb{F}_q$. However, if $q \neq p$, it may be possible to take the trace and norm down to a smaller subfield of $\mathbb{F}_q$. When doing so, the degree of the extension, the number of rational places and the genus will increase. The maxima for these three properties of the extension are reached when the trace and norm is taken down to $\mathbb{F}_p$.

We can therefore continue and consider for a function field over $\mathbb{F}_{q^n}$, trace-norm extensions with the trace and norm going down to any subfield $\mathbb{F}_{q^{n/m}} \subseteq \mathbb{F}_{q^n}$, where $m|n$. Considering these in terms of $(n/m, q^m)$-elementary symmetric polynomials, these generalized trace-norm constructions are of the form

$$s_{\frac{n}{m},1}(y) = s_{\frac{n}{m},\frac{n}{m}}(x).$$

While both the number of places of degree one and the genus increases with increasing m, we would like to see the behaviour of their ratio N/g as m increases. This is done in the following lemma:

Lemma 4.4. *Let $F = \mathbb{F}_{q^n}(x)$, and for $m \neq n$ with $m|n$, $r = \frac{n}{m}$, let $E = F(y)$ where y satisfies*

$$y^{q^{m(r-1)}} + y^{q^{m(r-2)}} + \ldots + y = x^{q^{m(r-1)}+q^{m(r-2)}+\ldots+1},$$

i.e. where the norm and trace are being taken down to $\mathbb{F}_{q^m}$. Then, the ratio N/g, of the number of rational places to the genus, increases with increasing m.

Proof. In this situation, we have $N(E) = q^{2n-m} + 1$, because q^{n-m} places of E lie above each of the q^n places in F which split completely (giving $q^n \cdot q^{n-m} = q^{2n-m}$ places), and the unique place lying above P_∞. Also, the coprime degree of $x^{q^{m(r-1)}+q^{m(r-2)}+\ldots+1}$ is just

$$m = q^{m(r-1)} + q^{m(r-2)} + \ldots + 1 = \frac{1-q^{mr}}{1-q^m} = \frac{q^n-1}{q^m-1},$$

from which we obtain

$$d(P'_\infty|P_\infty) = \frac{q^m(q^{n-m}-1)^2}{(q^m-1)}$$

and hence $g(E) = \frac{q^m(q^{n-m}-1)^2}{2(q^m-1)}$. Then

$$\frac{N(E)}{g(E)} = \frac{2(q^m-1)(q^m+q^{2n})}{(q^n-q^m)^2}.$$

From this it is clear that the numerator increases with increasing m, and the denominator decreases with increasing m. Hence $N(E)/g(E)$ increases with increasing m. □

Clearly, if n is even, the optimal (in the context of increasing N/g) choice of m is $m := \frac{n}{2}$. This gives rise to the Hermitian function field. When n is not even, the best we can do is to let p_0 be the smallest prime factor of n, and consider $m := \frac{n}{p_0}$, $r = p_0$ in Lemma 4.4.

However, Theorem 4.3 gives us another way to improve the ratio. For a specific value of n, it describes $n-1$ symmetric extensions $E_2, E_3, \ldots, E_n$ of the rational function field $F = \mathbb{F}_{q^n}(x)$. While each of these symmetric extensions of F have the same number $N(E) = q^{2n-1} + 1$ of rational places, the different exponent of the infinite place of each is determined by the coprime degree of the associated elementary symmetric polynomial $s_{n,i}(x)$. Considering the proof of Theorem 4.3(i), it is clear that

the coprime degree m_i of $s_{n,i}(x)$ increases as i increases. Because of the expression for the genus in Theorem 4.3(v), we have

$$g(E_2) < g(E_3) < \ldots < g(E_n).$$

It follows that if $n > 2$, for the purposes of improving the N/g ratio for a symmetric extension, E_2/F is the best choice, and E_n/F the worst. Since E_n/F is the trace-norm extension, it turns out that the trace-norm is the worst of the symmetric extensions, while the extension using the second (n,q)-symmetric polynomial is the best, with respect to lowering the genus. This leads Deolalikar [2] to investigate E_2 as a possibly more natural generalization of the Hermitian function field than E_n for $n \geq 3$. To motivate this, consider the following:

The Hermitian function field has genus $\frac{1}{2}q(q-1)$ and is the unique maximal function field over $\mathbb{F}_{q^2}$ of genus $g \geq \frac{1}{2}q(q-1)$, see for example [16]. The Hermitian function field has an extremely large automorphism group. If we denote by $N_m(E)$ the number of places of degree m of E, then $N_2 = 0$ for the Hermitian function field, i.e. there are no new rational places over $\mathbb{F}_{q^4}$ which were not already present over $\mathbb{F}_{q^2}$.

The symmetric extension E_2 shares many of these properties. We have seen that it has minimal genus in the family of symmetric extensions described by Theorem 4.3. For each α and β in $\mathbb{F}_{q^2}$ satisfying $\beta^q + \beta = \alpha^{q+1}$, an automorphism σ of the Hermitian function field is given by

$$\sigma : (x,y) \longmapsto (x+\beta, y + x\beta^q + \alpha).$$

For the symmetric extension E_2 a description of the automorphisms are given by the following proposition, of which a proof can be found in [2, 1.5.2] :

Proposition 4.5. *Let $F = \mathbb{F}_{q^n}(x)$ and $E = F(y)$ where y satisfies*

$$y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y = s_{n,2}(x)$$

and this defining equation is satisfied by some $(\alpha,\beta) = (x,y) \in \mathbb{F}_{q^n}^2$. Then there exists an automorphism σ of E given by

$$\sigma : (x,y) \longmapsto \left(x+\beta, y + x\beta^q + x\beta^{q^2} + \ldots + x\beta^{q^{n-1}} + \alpha\right).$$

These automorphisms keep F fixed and form a subgroup of order q^{2n-1} of the full automorphism group of the function field $E/\mathbb{F}_{q^n}$. Moreover, $N_2(E_2) = 0$ if $n \notin \{3,4,6\}$.

4.2 Quasi-symmetric extensions

The symmetric polynomials described in the previous section enabled us to construct extensions of the rational function field where all places except one were split completely. We will follow Deolalikar's [2], [3] development of the theory of these extensions when we generalize symmetric functions to the larger class of quasi-symmetric functions. This will enable us to again split almost all rational places, and even in some cases split *all* rational places. As before, the methods described here will provide the tools with which we can construct extensions of the rational function field of arbitrarily high genus and number of places of degree one.

To begin, we introduce the notion of quasi-symmetry. As before, R is an integral domain and K its field of fractions:

Definition 4.6. *A polynomial $f(X) \in R[X]$ is called quasi-symmetric if it is fixed by the cycle $\gamma = (1\,2\,...\,n) \in S_n$, where S_n is the symmetric group on n variables. The fixed elements of the action of γ on $K(X)$ will be called quasi-symmetric rational functions, or simply quasi-symmetric functions. We denote this set of quasi-symmetric functions by $K(X)_{qs}$, which forms a subfield of $K(X)$.*

In order to see that there are quasi-symmetric functions which are not symmetric, consider for example (for $n = 3$)

$$f(x_1, x_2, x_3) = x_1x_2^2 + x_2x_3^2 + x_3x_1^2.$$

This example can be generalized in the obvious way for larger n.

On page 49 the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of finite fields was considered, and symmetric polynomials were evaluated at $(X) = \left(t, t^q, ..., t^{q^{n-1}}\right)$. Analogously we will evaluate quasi-symmetric polynomials (resp. quasi-symmetric functions) in $\mathbb{F}_{q^n}(X)$ also at $(X) = \left(t, t^q, ..., t^{q^{n-1}}\right)$. As functions of t, we will call these (n, q)-quasi-symmetric polynomials (resp. (n, q)-quasi-symmetric functions). In this format, the above example of a $(3, q)$-quasi-symmetric polynomial would appear as

$$f(t) = t^{1+2q} + t^{q+2q^2} + t^{q^2+2}.$$

Lemma 4.7. *Let $f(t) \in R[t]$ be (n, q)-quasi-symmetric. Then*

$$f(t^q) = f(t) \bmod \left(t^{q^n} - t\right).$$

Proof. Considering $f(t)$ as a polynomial in $R[X]$ evaluated at $\left(t, t^q, ..., t^{q^{n-1}}\right)$, we have that since $f\left(\gamma\left(t, t^q, ..., t^{q^{n-1}}\right)\right) = f\left(t^q, t^{q^2}, ..., t^{q^{n-1}}, t\right)$, it follows that

$$f\left(t^q, t^{q^2}, ..., t^{q^{n-1}}, t\right) = f(t^q) \bmod \left(t^{q^n} - t\right). \tag{4.2.1}$$

But, quasi-symmetry of $f(t)$ implies that the LHS of (4.2.1) equals $f(t)$, implying the result. □

Deolalikar shows that the converse of the above result holds if $f(t)$ has degree less than q^n, i.e. if $\deg f(t) < q^n$, then $f(t)$ is (n,q)-quasi-symmetric if and only if $f(t^q) = f(t) \bmod \left(t^{q^n} - t\right)$. It follows that quasi-symmetry is characterized by its action on the elements of $\mathbb{F}_{q^n}$, as the following corollary states :

Corollary 4.8. *A polynomial $f(t) \in \mathbb{F}_{q^n}[t]$ is (n,q)-quasi-symmetric if and only if $f(z^q) = f(z)$ for all $z \in \mathbb{F}_{q^n}$.*

Analogously to the symmetric functions generalizing the norm and the trace in the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ mapping elements of $\mathbb{F}_{q^n}$ down to $\mathbb{F}_q$, we have the following result for quasi-symmetric polynomials with coefficients in $\mathbb{F}_q$:

Lemma 4.9. *Let $f(X) \in \mathbb{F}_q[X]$ be (n,q)-quasi-symmetric. Then $f(z) \in \mathbb{F}_q$ for all $z \in \mathbb{F}_{q^n}$.*

Proof. It suffices to show that $(f(z))^q = f(z)$. But, this follows immediately from Corollary 4.8 and the fact that the coefficients of f are in $\mathbb{F}_q$. □

Due to the following result, the notions of (n,q)-quasi-symmetric function and (n,q)-quasi-symmetric polynomial can be used interchangably:

Lemma 4.10. *Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a function satisfying $f(z^q) = f(z)$ for each $z \in \mathbb{F}_{q^n}$. Then there exists an (n,q)-quasi-symmetric polynomial $g(t) \in \mathbb{F}_{q^n}[t]$ such that $f(z) = g(z)$ for all $z \in \mathbb{F}_{q^n}$.*

Proof. By Lagrange interpolation a polynomial $g(t) \in \mathbb{F}_{q^n}[t]$ can be found which agrees with f on $\mathbb{F}_{q^n}$. To be precise, Lagrange interpolation yields the polynomial

$$g(t) = \sum_{j=1}^{q^n} \left(\frac{\prod_{1 \le i \le q^n,\, i \neq j} (t - z_i)}{\prod_{1 \le i \le q^n,\, i \neq j} (z_j - z_i)} \cdot f(z_j) \right)$$

where $\mathbb{F}_{q^n} = \{z_1, z_2, ..., z_{q^n}\}$, i.e. some enumeration of the elements of $\mathbb{F}_{q^n}$. Since $z_j - z_i \neq 0$ in each factor, this is well-defined over the finite field $\mathbb{F}_{q^n}$. Thus $g(z^q) = g(z)$ for each $z \in \mathbb{F}_{q^n}$, and hence by Corollary 4.8, $g(t)$ is (n,q)-quasi-symmetric. □

It is worth noting that the polynomial representation g for the function f as obtained in the previous lemma is not unique, although Lagrange interpolation yields one possibility.

We now define

$$U_{qs} := \{f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \ : \ f \text{ is a } (n,q)\text{-quasi-symmetric function}\}, \text{ and}$$
$$V_{qs} := \{f \in U_{qs} : \exists g(t) \in \mathbb{F}_q[t] \text{ such that } \forall z \in \mathbb{F}_{q^n} : f(z) = g(z)\}.$$

The set U_{qs} can be considered a $\mathbb{F}_{q^n}$-vector space and $V_{qs} \subseteq U_{qs}$ the $\mathbb{F}_q$-subspace of functions representable by polynomials with coefficients in $\mathbb{F}_q$.

Lemma 4.11. *Any $\mathbb{F}_q$-linearly independent subset $\{f_i(t)\}_{1 \leq i \leq r}$ in V_{qs} is $\mathbb{F}_{q^n}$-linearly independent in V_{qs}.*

Proof. Suppose

$$\sum_{i=1}^{r} u_i f_i(t) = 0$$

with $u_i \in \mathbb{F}_{q^n}$, and $\{w_1, w_2, ..., w_n\}$ a $\mathbb{F}_q$-basis for $\mathbb{F}_{q^n}$. Then each $u_i = \sum_{j=1}^{n} a_{ij} w_j$ for $a_{ij} \in \mathbb{F}_q$ and hence

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{r} a_{ij} f_i(t) \right) w_j = 0,$$

and since $f_i(z) \in \mathbb{F}_q$ for $z \in \mathbb{F}_{q^n}$, each $\sum_{i=1}^{r} a_{ij} f_i(t) = 0$, and hence $a_{ij} = 0$ for $i = 1, 2, ..., r$ and $j = 1, 2, ..., n$. □

We now define $\mathcal{G}$ to denote the set of orbits of Galois for the action of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ on $\mathbb{F}_{q^n}$. Then U_{qs} can be seen to be functions $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ which are constant on each orbit in G, and V_{qs} contains functions $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ that are constant on these orbits. While we could only prove the existence of a polynomial representation of an element of U_{qs} in Lemma 4.10, we now show the essential uniqueness of such a representation if we restrict ourselves to V_{qs}:

Proposition 4.12. *For each $f \in V_{qs}$ there exists a unique polynomial representation $g(t) \in \mathbb{F}_q[t]$ of degree less than q^n, such that $f(z) = g(z)$ for all $z \in \mathbb{F}_{q^n}$.*

Proof. Choose a polynomial representation $g(t)$ of f of degree less than q^n. Recalling that $\phi(z) = z^q$, define $\phi(g(t))_q$ to be the unique polynomial of degree less than q^n which is congruent to $\phi(g(t)) \bmod (t^{q^n} - t)$. Since $f \in V_{qs}$, $g(t)$ and $\phi(g(t))_q$ must agree on $\mathbb{F}_{q^n}$. Hence they must be equal, since if not, the polynomial $g(t) - \phi(g(t))_q$ would have q^n zeros and degree at most $q^n - 1$, a contradiction. Hence the coefficients of $g(t)$ are fixed by $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, and therefore $g(t) \in \mathbb{F}_q[t]$. Similarly as above, if there exist polynomials $g(t), g^*(t) \in \mathbb{F}_q[t]$ both being representatives of f of degree less than q^n, then their difference $g(t) - g^*(t)$ would be a polynomial with more zeros than its degree. Therefore the obtained $g(t)$ is unique, as required. □

Deolalikar moreover shows that the dimension of U_{qs} (resp. V_{qs}) as a $\mathbb{F}_{q^n}$-vector space (resp. $\mathbb{F}_q$-vector space) is $|\mathcal{G}|$. This can be seen by constructing a linearly independent set of functions $\{f_i\}_{1 \leq i \leq |\mathcal{G}|}$, for example one where $f_i = 1$ on the ith orbit of Galois and $f_i = 0$ otherwise.

Lemma 4.13. *There exist (n, q)-quasi-symmetric functions that have no zeros in $\mathbb{F}_{q^n}$.*

Proof. Considering the linearly independent subset mentioned above, we are free to assign any value in $\mathbb{F}_q$ for a (n, q)-quasi-symmetric function on an orbit of Galois. In particular we can choose nonzero values, and this presents us with $(q-1)^{|\mathcal{G}|}$ such functions which are nonzero on orbits of Galois, and no zeros in $\mathbb{F}_{q^n}$. □

Lemma 4.13 guarantees the existence of many (n, q)-quasi-symmetric functions having no zeros in $\mathbb{F}_{q^n}$. One way to explicitly construct these are by composing quasi-symmetric functions with irreducible polynomials:

Lemma 4.14. *Let $i(t) \in \mathbb{F}_q[t]$ be an irreducible polynomial, and $s(t) \in V_{qs}$ be a (n, q)-quasi-symmetric polynomial. Then $(i \circ s)(t)$ is (n, q)-quasi-symmetric, maps $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, and has no zeros in $\mathbb{F}_{q^n}$.*

Proof. Since $s(t)$ maps $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and $i(t) \in \mathbb{F}_q[t]$, $i(s(t))$ is (n, q)-quasi-symmetric and maps $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Concerning the zeros, suppose $i(s(t))$ has a zero $\alpha \in \mathbb{F}_{q^n}$, i.e. $i(s(\alpha)) = 0$. Then $s(\alpha) \in \mathbb{F}_q$ is a zero of $i(t)$, which is impossible since $i(t)$ is irreducible over $\mathbb{F}_q$. □

In the next constructions, we will often use $i(t) = t^m - \beta$ (where β is not an mth power in $\mathbb{F}_q$) as the irreducible polynomial in Lemma 4.14.

Analogously to the symmetric extensions of the rational function field as described in an earlier section, we now look at quasi-symmetric extensions. As before, we will look at extensions of the rational function field $F := \mathbb{F}_{q^n}(x)$. Given this rational function field, we will often use F_{qs} to denote the field of (n, q)-quasi-symmetric functions in F, and F_{qs}^{ϕ} to denote those functions in F_{qs} whose coefficients are from $\mathbb{F}_q$ (i.e. are fixed by ϕ).

The general quasi-symmetric extension we will consider is of the form

$$g(y) = f(x)$$

where $f, g \in F_{qs}^{\phi}$. Working over $K = \mathbb{F}_{q^n}$, the remarks made in the previous section imply that, in the residue field of some $P \in S(F/K)$, the functions $f(x)$ and $g(y)$ will take values in $\mathbb{F}_q \cup \infty$, rather than the larger $\mathbb{F}_{q^n} \cup \infty$. We will again look at the case where the left-hand side is a linearized symmetric polynomial, hence quasi-symmetric.

Theorem 4.15. *Let $F = K(x)$ where $K = \mathbb{F}_{q^n}$. Let $E = F(y)$, where y satisfies*

$$y^{q^{n-1}} + y^{q^{n-2}} + ... + y = \frac{h(x)}{g(x)}$$

where $h(x)$, $g(x) \in F_{qs}^{\phi}$, and $\frac{h(x)}{g(x)}$ is not the image of a rational function in F under a linear polynomial. Then

(i) E/F is Galois with $[E : F] = q^{n-1}$ and $\mathrm{Gal}(E/F) = \{\sigma_\beta : y \longmapsto y + \beta\}_{s_{n,1}(\beta)=0}$.

(ii) Let $P \in S(F/K)$ with $v_P\left(\frac{h(x)}{g(x)}\right) = -m$, $m > 0$ and $(m, q) = 1$. Then P is totally ramified in E, with $d(P'|P) = (q^{n-1} - 1)(m + 1)$ where P' is the unique place lying above P.

(iii) Let $Q \in S(F/K)$ with $v_Q\left(\frac{h(x)}{g(x)}\right) \geq 0$. Then Q splits completely in E.

Proof. Irreducibility of the defining equation follows by Theorem 2.31, thereby implying (i), since Theorem 2.31 can be extended to apply to rational functions as well. Noting that $h(x), g(x) \in F_{qs}^{\phi}$ it follows that the residue class of $\frac{h(x)}{g(x)}$ at any rational place is in $\mathbb{F}_q$. Therefore Proposition 2.30 applies, implying (ii) and (iii). □

In order to split all rational places, quasi-symmetric functions with no zeros in K are used. These can be obtained by the construction described in Lemma 4.14.

Theorem 4.16. *Consider the extension as described in Theorem 4.15 with the additional hypotheses that $\deg g(x) > \deg h(x)$ and $g(x)$ has no zeros in $\mathbb{F}_{q^n}$. Then all the rational places of F split completely in E, and $N(E) = q^{n-1}(q^n + 1)$.*

Proof. For all $z \in \mathbb{F}_{q^n}$, $h(z)/g(z) \in \mathbb{F}_q$, and this ensures that all places of the form P_z split completely. Since $\deg g(x) > \deg h(x)$, the RHS of the defining equation has a zero at P_∞, implying that P_∞ also splits completely in E, considering Proposition 2.30(v). □

In the situation as described in Theorem 4.16, the ratio $N(E)/[E : F]$ attains its maximal possible value, namely $q^n + 1$.

4.3 Towers where all places split completely

For the coming results, we will assume that we are working with a tower $\mathcal{F} = (F_1, F_2, ...)$ of function fields over $\mathbb{F}_{q^n}$. We will denote the subfield of F_i consisting of (n, q)-quasi-symmetric functions of x_j by $F_{j,qs} \subseteq F_i$ and the subfield of F_i of

(n,q)-quasi-symmetric functions of x_j with $\mathbb{F}_q$ coefficients by $F^{\phi}_{j,qs}$. First we will look at the case where all rational places split completely:

Theorem 4.17. *Consider the tower $\mathcal{F} = (F_1, F_2, ...)$ of function fields where $F_1 = \mathbb{F}_{q^n}(x_1)$ and for $i \geq 1$ $F_{i+1} = F_i(x_{i+1})$ where*

$$x_{i+1}^{q^{n-1}} + x_{i+1}^{q^{n-2}} + ... + x_{i+1} = \frac{g(x_i)}{h(x_i)},$$

$g(x_i), h(x_i) \in F^{\phi}_{i,qs}$, $\frac{g(x_i)}{h(x_i)}$ is not the image of a rational function under a linear polynomial, and $h(x)$ has no zeros in $\mathbb{F}_{q^n}$. Also, $\deg g(x_i) \leq \deg h(x_i)$. Then

(i) All rational places of F_1 split completely in all steps of the tower.

(ii) For every place P in F_i that is ramified in F_{i+1}, a place P' in F_{i+1} lying above P is unramified in F_{i+2}.

Proof.

(i) The place P_∞ splits completely because of the condition on the degrees of g and h. Also, for any rational place P, the right-hand side of the defining equation is in the valuation ring since $\deg g \leq \deg h$. The class of the right-hand side in the residue class field is in $\mathbb{F}_q$ at each of these places, since itself is in $F^{\phi}_{i,qs}$. Then Proposition 2.30(v) implies that every rational place in F_i splits completely in F_{i+1}.

(ii) Suppose $P \in S(F_i/\mathbb{F}_{q^n})$ is ramified in F_{i+1}/F_i, and P' is a place lying above it in $S(F_{i+1}/\mathbb{F}_{q^n})$. Then the right-hand side of

$$x_{i+2}^{q^{n-1}} + x_{i+2}^{q^{n-2}} + ... + x_{i+2} = \frac{g(x_{i+1})}{h(x_{i+1})}$$

has a zero at P' because of the condition on the degrees of g and h. Therefore P' is unramified in F_{i+2}.

□

A more specific result is obtained if we select g and h to be irreducibles of a certain type. In particular, we can choose them as we had after Lemma 4.14 as being of the form $x^m - \beta$ where β is not an mth power. We will restrict ourselves further, and look at the simpler case for $m = 2$, which describes a typical tower of the type described above.

Theorem 4.18. *Consider the tower $\mathcal{F} = (F_1, F_2, ...)$ of function fields over $\mathbb{F}_{q^n}$ (not of characteristic 2) where $F_1 = \mathbb{F}_{q^n}(x_1)$, and for $i \geq 1$, $F_{i+1} = F_i(x_{i+1})$ where*

$$x_{i+1}^{q^{n-1}} + x_{i+1}^{q^{n-2}} + ... + x_{i+1} = \frac{1}{\left(x_i^{q^{n-1}} + x_i^{q^{n-2}} + ... + x_i\right)^2 - \alpha}, \tag{4.3.1}$$

and $\alpha \in \mathbb{F}_q$ is not a square. Then

(i) F_{i+1}/F_1 is abelian for each $i \geq 2$.

(ii) All rational places split completely throughout the tower.

(iii) When a (non-rational) place $P \in S(F_i/\mathbb{F}_{q^n})$ is ramified in F_{i+1}, it behaves like a rational place for splitting thereafter, i.e. splits completely from there on throughout the tower.

Proof. It is first shown that the defining equations are irreducible. We claim that if $P \in S(F_i/\mathbb{F}_{q^n})$ is a zero of

$$\left(x_i^{q^{n-1}} + x_i^{q^{n-2}} + ... + x_i\right)^2 - \alpha,$$

(i.e. a pole of the right-hand side of the defining equation (4.3.1)) then the zero can have degree at most two. This follows, because if $\sqrt{\alpha}$ is one of the square roots of α, then

$$\begin{aligned} x_i^{q^{n-1}} + x_i^{q^{n-2}} + ... + x_i - \sqrt{\alpha} &= \frac{1}{\left(x_{i-1}^{q^{n-1}} + x_{i-1}^{q^{n-2}} + ... + x_{i-1}\right)^2 - \alpha} - \sqrt{\alpha} \\ &= \frac{1 - \sqrt{\alpha}\left(\left(x_{i-1}^{q^{n-1}} + x_{i-1}^{q^{n-2}} + ... + x_{i-1}\right)^2 - \alpha\right)}{\left(x_{i-1}^{q^{n-1}} + x_{i-1}^{q^{n-2}} + ... + x_{i-1}\right)^2 - \alpha}. \end{aligned}$$

We note that the second derivative of the numerator of the obtained final expression with respect to x_{i-1} is constant, while the denominator is a unit. Therefore the zeros of the right-hand side can occur with multiplicity at most two. The same argument holds for each $i \geq 2$, and hence the valuation of this expression at P must be a power of two, which is relatively prime to the characteristic of $\mathbb{F}_{q^n}$, which was assumed to be not equal to two. Irreducibility is then ensured by Proposition 2.30 and each extension F_{i+1}/F_i is Galois.

(i) Our claim is that F_i/F_1 is (Galois) abelian for each $i \geq 2$. We proceed by induction. The extension F_i/F_1 is certainly Galois for $i = 2$ by the preceding comments, and abelian by Theorem 4.15.

Now, suppose F_i/F_1 is (Galois) abelian for some $i \geq 2$. We know that F_{i+1}/F_i is Galois. In order to show that F_{i+1}/F_1 is Galois, it suffices to show that it is normal, since separability is ensured by the defining equation. Observe that if σ is an endomorphism of F_j/F_{j-1} into $\overline{F}_{j-1}$ (the algebraic closure of F_{j-1}) then

$$\sigma\left(x_j^{q^{n-1}} + x_j^{q^{n-2}} + ... + x_j\right) = x_j^{q^{n-1}} + x_j^{q^{n-2}} + ... + x_j \tag{4.3.2}$$

since this expression is already in F_{j-1} by (4.3.1). Consequently, if σ is an endomorphism of F_{i+1}/F_1 into $\overline{F}_1$, we can examine the restrictions $\sigma|_{F_1}$, $\sigma|_{F_2}$, ..., $\sigma|_{F_i}$ of σ to the subfields of F_{i+1} in the tower and see that (4.3.2) holds in this context for each $j = 1, 2, ..., i+1$. Hence $\sigma(x_{i+1})$ is a root of (4.3.1) which defined the extension F_{i+1}/F_i. Since F_{i+1}/F_i is Galois (hence normal), $\sigma(x_{i+1}) \in F_{i+1}$, and hence F_{i+1}/F_1 is normal, hence Galois (we have separability). The extension is certainly abelian as well, as can be seen by noting that the action of the Galois group is additive, adding a root β of the p-linear equation

$$X_j^{q^{n-1}} + X_j^{q^{n-2}} + ... + X_j = 0,$$

by looking at Theorem 4.15(i). The result follows by induction.

(ii)-(iii) Note that the class of the right-hand side in the residue field at any rational place is in $\mathbb{F}_q$ at any stage of the tower (the denominator is (n, q)-quasi-symmetric with no zeros in $\mathbb{F}_{q^n}$), which implies that the defining equation splits into linear factors. By Proposition 2.30(v) this place splits completely. Similarly, a place $P \in S(F_i/\mathbb{F}_{q^n})$ which is ramified (i.e a non-rational place) in F_{i+1}/F_i will behave the same and split completely in all subsequent stages of the tower as well.

□

The previous theorem implies that it is possible to construct abelian extensions of the rational function field of arbitrary degree over non-prime fields in which all rational places split completely in all steps of the tower. Even the splitting behaviour of places of degree greater than one is very good, with them behaving like rational places in places above ramified places.

Considering the situation as described in Theorem 4.17, but instead with the condition on the degrees turned around, we have the following theorem:

Theorem 4.19. *Consider the tower* $\mathcal{F} = (F_1, F_2, ...)$ *of function fields where* $F_1 = \mathbb{F}_{q^n}(x_1)$ *and for* $i \geq 1$ *we let* $F_{i+1} = F_i(x_{i+1})$ *where*

$$x_{i+1}^{q^{n-1}} + x_{i+1}^{q^{n-2}} + ... + x_{i+1} = \frac{g(x_i)}{h(x_i)},$$

$g(x_i), h(x_i) \in F_{i,qs}^{\phi}$, $\frac{g(x_i)}{h(x_i)}$ *is not the image of a rational function under a linear polynomial, and* $h(x)$ *has no zeros in* $\mathbb{F}_{q^n}$. *Also,* $\deg g(x_i) > \deg h(x_i)$. *Then all rational places of* F_1, *except for the infinite place* P_∞, *split completely in all steps of the tower. If we more specifically have that* $\deg g(x_i) = \deg h(x_i) + 1$, *then the pole order of* x_i *in the unique place lying above* $P_\infty \in S(F_i/\mathbb{F}_q)$ *remains one for all* $i \geq 1$.

Proof. The proof of the splitting behaviour of the finite rational places follows as in Theorem 4.17. Because of the constraint on the degrees, P_∞ does not split completely in any stage of the tower, and in particular for the case where $\deg g(x_i) = \deg h(x_i) + 1$, $v_{P_\infty}(x_i) = -1$ for $i \geq 1$. □

We can put Theorems 4.17 and 4.19 together in one unified result for linearized extensions defined by a rational quasi-symmetric function:

Corollary 4.20. *Consider the tower* $\mathcal{F} = (F_1, F_2, ...)$ *of function fields where* $F_1 = \mathbb{F}_{q^n}(x_1)$ *and for* $i \geq 1$ *we let* $F_{i+1} = F_i(x_{i+1})$ *where*

$$x_{i+1}^{q^{n-1}} + x_{i+1}^{q^{n-2}} + ... + x_{i+1} = \frac{g(x_i)}{h(x_i)},$$

$g(x_i), h(x_i) \in F_{i,qs}^{\phi}$, $\frac{g(x_i)}{h(x_i)}$ *is not the image of a rational function under a linear polynomial and* $h(x)$ *has no zeros in* $\mathbb{F}_{q^n}$. *Then, all finite rational places of* F_1 *split completely in each step of the tower, and the infinite rational place* $P_\infty \in S(F_1/\mathbb{F}_{q^n})$ *splits completely as well in each step of the tower if* $\deg g(x_i) \leq \deg h(x_i)$.

Therefore, using quasi-symmetric polynomials $g(x), h(x) \in \mathbb{F}_q[X]$, we can construct, using Corollary 4.20, towers of function fields which either split all, or all except one rational place of the rational function field $F_1 = \mathbb{F}_{q^n}(x_1)$. This provides us with a standard way of constructing towers of which the splitting behaviour is known, and is near-optimal. While this will keep the number of places of degree one very close to optimal, the genus of function fields in each stage of the tower may still grow due to ramification occurring in places of degree greater than one. We exhibit the following example to show that the effect on the different divisor when all places of degree one split completely is particularly bad when compared to a case where all except one place of degree one are split completely, which is due to Deolalikar [2] :

Let $F = \mathbb{F}_{q^2}(x)$ be the rational function field over $\mathbb{F}_{q^2}$. Let $E = F(y)$ where

$$y^q + y = \frac{x^{q+1}}{(x^q + x)^2 - \alpha}$$

where α is not a square in $\mathbb{F}_q$, and $E' = F(z)$ where

$$z^q + z = x^{q+1},$$

i.e. the Hermitian function field. We consider the special case where $q = 5$ and $\alpha = 2$. We know that all rational places split in E/F, and that all except one split in E'/F. A primitive element for $\mathbb{F}_{25}$ over $\mathbb{F}_5$ is given by a root t of $T^2 - 3 = 0$, which yields the factorization

$$(x^5 + x)^2 - 2 = (x^5 + x + 2t)(x^5 + x + 3t).$$

Using Theorem 4.15 one can show that $\deg \mathrm{Diff}(E/F) = 80$, with the contribution to the different exponents given by places of degree greater than one. Similarly, the situation for the Hermitian function field is well-known and can also be described in terms of Theorem 4.3, giving $\deg \mathrm{Diff}(E'/F) = 28$, with the contribution to the different exponents given by the single ramified place P_∞.

Looking at this from the viewpoint of splitting places, this means that by splitting the remaining ramified place in the Hermitian extension E'/F by using the quasi-symmetric extension E/F instead, the degree of the different is almost tripled, causing excessive growth of the genus. Deolalikar points out that this example is typical in this respect, and that splitting all places of degree one in each stage of a tower will result in asymptotically bad behaviour.

Consequently, we would want to focus on towers where not necessarily all places of degree one are split completely. When ramification occurs above non-rational places, we would want to be able to limit their effect, possibly by ensuring that the defining equations of the tower enforce a finite ramification locus.

In the next chapter we will look at a particular case due to Van der Geer and Van der Vlugt where the effect of the ramification in these places of higher degree can be determined exactly. This tower will turn out to split all places of degree one except for two completely in all stages of the tower. This suggests that it may be worthwhile to study explicit defining equations which force two or more rational places not to split, possibly using symmetric or quasi-symmetric functions.

Chapter 5

Constructions over non-square finite fields

As seen earlier in this dissertation, there are various towers of function fields which meet the Drinfeld-Vlăduţ bound over $\mathbb{F}_q$ if q is square. Moreover, there exist explicit towers with this property over any square field $\mathbb{F}_q$. When q is not square results are a lot weaker and most of the constructions with good asymptotic properties are non-explicit. In particular, we recall from Chapter 3 that Zink [36] constructed, in a non-explicit fashion, asymptotically good towers of function fields over $\mathbb{F}_{p^3}$, p a prime. He provided the best-known lower bounds for $A\left(p^3\right)$ for any prime p. It then came as a surprise when Van der Geer and Van der Vlugt [32] successfully constructed an explicit asymptotically good tower of curves for the case where $p = 2$, which meets the bound $A\left(p^3\right) \geq \frac{2\left(p^2-1\right)}{p+2}$ of Zink.

The choice of $\mathbb{F}_8$ as field of constants is minimal with respect to choosing a non-prime field with lowest non-square cardinality, and therefore exhibits a minimal example showing that good explicit constructions are possible over some non-square fields.

While the construction of Van der Geer and Van der Vlugt [32] was originally given in a geometric context, we will present the results in the context of algebraic function fields.

5.1 Van der Geer and Van der Vlugt's tower

We begin by defining the tower:

Definition 5.1. *Let $F_0 = \mathbb{F}_8\left(x_0\right)$ be the rational function field over $\mathbb{F}_8$. For $n \geq 0$,*

we recursively define

$$F_{n+1} = F_n\left(x_{n+1}\right)$$

where

$$x_{n+1}^2 + x_{n+1} = \frac{x_n^2 + x_n + 1}{x_n}. \tag{5.1.1}$$

We denote this recursive tower by

$$\mathcal{F} = \left(F_0, F_1, F_2, ...\right).$$

As can be seen immediately, this is a tower of Artin-Schreier extensions (see Proposition 2.28) over $\mathbb{F}_8$. Considering only the first step of the tower, it can be shown that the function field $F_1/\mathbb{F}_8 = F_0\left(x_1\right)/\mathbb{F}_8$, where

$$x_1^2 + x_1 = \frac{x_0^2 + x_0 + 1}{x_0} = x_0 + 1 + \frac{1}{x_0}, \tag{5.1.2}$$

is a function field of genus 1, and that it attains the Serre bound with $N\left(F_1/\mathbb{F}_8\right) = 14$. For a computational exposition, see Proposition B.1 in Appendix B.

It can also be shown that, for every $a_0 \in \mathbb{F}_8 \setminus \mathbb{F}_2$, there exists exactly two values $a_1 \in \mathbb{F}_8 \setminus \mathbb{F}_2$ satisfying (5.1.2). This is shown using MAGMA in Proposition B.2. This implies that for any $x_0 \in \mathbb{F}_8 \setminus \mathbb{F}_2$, there exist sequences of solutions $(x_0, x_1, x_2, ...)$ satisfying (5.1.1) for $n \geq 0$.

We will first focus our attention on the calculation of the genus of the function fields $F_i/\mathbb{F}_8$. We can perform a constant field extension of each function field in the tower to the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}_8$, and we denote the obtained tower by $\overline{\mathcal{F}}$. Since the genus is invariant under extensions of the field of constants, studying the genus of function fields in $\overline{\mathcal{F}}$ over $\overline{\mathbb{F}}$ is the same as studying those in $\mathcal{F}$ over $\mathbb{F}_8$. Working over the algebraic closure, we use the sequences of solutions as mentioned in the previous paragraph to give a representation of the places in successive function fields in $\mathcal{F}$. In particular, we can represent the elements of $S\left(F_n/\overline{\mathbb{F}}\right)$ by elements of the set D_n defined by

$$D_n = \left\{ (a_0, a_1, ..., a_n) \in \prod_{i=0}^{n} \left(\overline{\mathbb{F}} \cup \{\infty\}\right) : a_{i+1}^2 + a_{i+1} = a_i + 1 + \frac{1}{a_i} \text{ for } 0 \leq i \leq n-1 \right\}$$

via the map

$$\eta : \begin{cases} S\left(F_n/\overline{\mathbb{F}}\right) & \longrightarrow & D_n \\ P & \longmapsto & (a_0, a_1, ..., a_n) \end{cases}$$

where $a_i = x_i\left(P\right)$ (the residue class map) for each $0 \leq i \leq n$, and the possibility of $a_i = \infty$ is included to consider solutions of (5.1.1) where we employ the usual

arithmetic rules involving ∞. The map is well-defined, due to the defining equations (5.1.1) on places lying above each other. So, in the sequel, we will often rather identify a place $P \in S\left(F_n/\overline{\mathbb{F}}\right)$ with its image in D_n, the so-called *index sequence* $P\left(a_0, a_1, ..., a_n\right)$, or just $\left(a_0, a_1, ..., a_n\right)$.

We note that if we have places $P_i \in S\left(F_i/\overline{\mathbb{F}}\right)$ and $P_{i+j} \in S\left(F_{i+j}/\overline{\mathbb{F}}\right)$ with P_{i+j} lying above P_i, then the index sequence of P_{i+j} has its first $i+1$ coordinates matching those of the index sequence of P_i. In this context, we may write $P_{i+j} = P_i\left(a_{i+1}, a_{i+2}, ..., a_{i+j}\right)$ where the index sequence of P_{i+j} is $\left(a_0, a_1, a_2, ..., a_{i+j}\right)$. Moreover, we will write $P\left(\infty, \infty, ..., \infty\right)$ where there are j ∞'s as $P\left(\infty^j\right)$ for brevity.

In order to discover exactly where in the tower ramification can occur, consider the following lemma, in which we work with the tower $\overline{\mathcal{F}}$. Since we are working with Artin-Schreier extensions, we are able to restrict our attention to poles of the function $f_i = \frac{x_i^2 + x_i + 1}{x_i}$ (see Proposition 2.28).

Lemma 5.2. *(i) The zeros of x_i on $F_i/\overline{\mathbb{F}}$ are places $P \in S\left(F_i/\overline{\mathbb{F}}\right)$ of the form*

$$P\left(a_0, a_1, ..., a_i\right)$$

where $a_i = 0$, $a_{i-j} \in \mathbb{F}_4 \setminus \mathbb{F}_2$ if $j \geq 1$ is odd and $a_{i-j} = 1$ if $j \geq 2$ is even.

(ii) The poles of x_i on $F_i/\overline{\mathbb{F}}$ are places $P \in S\left(F_i/\overline{\mathbb{F}}\right)$ of the form

$$P\left(\underbrace{a_0,\ a_1,\ a_2,\ ...,\ a_j}_{\text{index seq. of a zero of } x_j}\ ,\ \underbrace{\infty,\ \infty,\ ...,\ \infty}_{(i-j)\ \infty\text{'s}}\right)$$

where $P\left(a_0, a_1, ..., a_j\right)$ is a zero of x_j on $F_j/\overline{\mathbb{F}}$, or of the form

$$P\left(\underbrace{\infty, \infty, ..., \infty}_{(i+1)\ \infty\text{'s}}\right).$$

Proof. Note that the notion of an index sequence consisting of elements of $P\left(\mathbb{F}_4\right)$ is well-defined, since $\mathbb{F}_4$ and $\mathbb{F}_8$ has the same algebraic closure, namely $\overline{\mathbb{F}}$. The proof is by induction on i. It is obviously true for $i = 0$. From the equation

$$x_i^2 + x_i = \frac{x_{i-1}^2 + x_{i-1} + 1}{x_{i-1}} =: f_{i-1}$$

it follows by taking divisors that

$$\left(f_{i-1}\right) = \left(x_i\right) + \left(x_i + 1\right) = \left(x_i\right)_0 + \left(x_i\right)_1 - 2\left(x_i\right)_\infty .$$

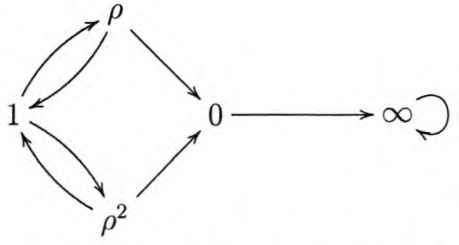
So, poles of x_i lie above poles of f_{i-1}, and places $P \in S\left(F_i/\overline{\mathbb{F}}\right)$ with $x_i(P) \in \mathbb{F}_2$ lie above zeroes of f_{i-1}. If ρ is a primitive element for $\mathbb{F}_4$ over $\mathbb{F}_2$, we have

$$\begin{aligned}(f_{i-1}) &= (x_{i-1}+\rho) + \left(x_{i-1}+\rho^2\right) - (x_{i-1}) \\ &= (x_{i-1})_\rho + (x_{i-1})_{\rho^2} - (x_{i-1})_0 - (x_{i-1})_\infty ,\end{aligned}$$

which implies that poles of f_{i-1} are zeros and poles of x_{i-1}, and that the zeros of f_{i-1} are $P' \in S\left(F_{i-1}/\overline{\mathbb{F}}\right)$ so that $x_{i-1}(P') \in \mathbb{F}_4 \setminus \mathbb{F}_2 = \{\rho, \rho^2\}$.
Putting the above comments together, we derive that the index sequence for a zero of x_i is obtained by adding a zero to an index sequence which ends on an element of $\{\rho, \rho^2\}$ and which alternates between 1 and elements of $\{\rho, \rho^2\}$. The index sequence for a pole of x_i is obtained by adding a ∞ to a zero or pole of x_{i-1}. From these constructions for zeros and poles, the statement of the lemma follows. □

From the above lemma, where we worked over the algebraic closure, it becomes evident that ramification in the tower $\overline{\mathcal{F}}$ can only occur at places for which the corresponding index sequence representation has coordinates in $\mathbb{F}_4 \cup \{\infty\}$. This is a very important property of this specific tower of function fields, since it restricts the occurrence of ramification in the tower very much, implying that the tower has a finite ramification locus. We will touch upon this again in Lemma 5.12.

Notice that solving equation (5.1.1) over $\mathbb{F}_4 \cup \{\infty\}$, we find that the index sequence $P(a_0, a_1, ..., a_n)$ of a place $P \in S\left(F_n/\overline{\mathbb{F}}\right)$ which is possibly ramified in F_{n+1}/F_n can be found by starting at any vertex of the following directed graph, traversing it and setting the coordinates of the index sequence to equal the vertex labels (in order) as they are met:



The graph contains edges $a_{i-1} \longrightarrow a_i$ for $1 \leq i \leq n$ for index sequences of these potentially ramified places in $\overline{\mathbb{F}}$. In terms of the graph, such an index sequence corresponds to a zero (resp. a pole) when the graph traversal terminates at 0 (resp. at ∞). If the length (the number of edges crossed) of such a path is n, it corresponds to a place in $S\left(F_n/\overline{\mathbb{F}}\right)$. The graph therefore gives us a representation for the possible index sequences a ramified place may possess.

In order to determine which of the places belonging to this restricted set of index sequences are in fact ramified in their respective extensions, we will write elements

of $F_i/\overline{\mathbb{F}}$ as a power series in a local parameter at a given place $P \in S\left(F_i/\overline{\mathbb{F}}\right)$. The contribution to the ramification will be determined by the valuation $v_P\left(f_i^*\right)$ at poles P on $F_i/\overline{\mathbb{F}}$ of the Artin-Schreier reduction f_i^* of the function $f_i = x_i + 1 + \frac{1}{x_i}$. This reduction will be obtained by the same method as that used in Lemma 2.33. As before, with García and Stichtenoth's tower of (modified) Artin-Schreier extensions [9] as discussed in Section 3.3, we will often only be interested in the principal part, and reduce elements by writing $f = g + O(1)$ at P if $v_P(f - g) \geq 0$.

Working in the function field $F_i/\overline{\mathbb{F}}$, we now consider a sequence $(P_j)_{0 \leq j \leq i}$ of places where

(i) $P_j \in S\left(F_j/\overline{\mathbb{F}}\right)$ for $0 \leq j \leq i$,

(ii) $P_{j+1}|P_j$ for each $0 \leq j \leq i-1$ and

(iii) the index sequence $P(a_0, a_1, ..., a_i)$ of P_i consists of coordinates alternating between 1 and elements of $\{\rho, \rho^2\}$.

In the discussion that follows we will assume that $a_0 = 1$ for these places, similar results hold when $a_0 \in \{\rho, \rho^2\}$. Choosing a local parameter $t = x_0 + 1$ at P_0 in $F_0/\overline{\mathbb{F}}$, this function will remain a local parameter at P_j in $F_j/\overline{\mathbb{F}}$ for $1 \leq j \leq i$.

For each of these places P_j, the completion $\widehat{\mathcal{O}}_{P_j}$ of the associated local ring $\mathcal{O}_{P_j}$ is isomorphic to the power series ring $\overline{\mathbb{F}}[\![t]\!]$, which is a standard result discussed in for example [25, II 4, Theorem 2]. Since $x_j(P_j) = a_j$, we can therefore write the function x_j in the form

$$x_j = a_j + m_j(t)$$

where $m_j(t) \in \overline{\mathbb{F}}[\![t]\!]$ with zero constant term. In order to investigate the principal part of $\frac{1}{m_j(t)}$, the following lemma is useful:

Lemma 5.3. *In the quotient field $\mathbb{F}(\!(t)\!)$ of the formal power series ring $\overline{\mathbb{F}}[\![t]\!] \cong \widehat{\mathcal{O}}_{P_j}$, the function $m_j(t)$ satisfies*

$$\frac{1}{m_j} = \begin{cases} \frac{a_{j-1}}{m_{j-1}} + O(1) \text{ at } P_j & \text{if } j \geq 2 \text{ is even,} \\ \frac{1}{m_{j-1}^2} + \frac{1}{m_{j-1}} + O(1) \text{ at } P_j & \text{if } j \geq 1 \text{ is odd,} \end{cases}$$

for $0 \leq j \leq i$.

Proof. The proof is by induction, and we start with $m_0(t) = x_0 + 1 = t$, since we assumed $a_0 = 1$. Then, for even $j \geq 2$ we have that $a_j = 1$ and $a_{j-1} \in \{\rho, \rho^2\}$. From the defining equation

$$x_j^2 + x_j = x_{j-1} + 1 + \frac{1}{x_{j-1}}$$

we obtain

$$\begin{aligned} m_j^2 + m_j &= (a_j + m_j)^2 + (a_j + m_j) \\ &= (a_{j-1} + m_{j-1}) + 1 + \frac{1}{a_{j-1} + m_{j-1}} \\ &= (a_{j-1} + m_{j-1}) + 1 + \frac{1}{a_{j-1}} \frac{1}{1 + \frac{m_{j-1}}{a_{j-1}}} \\ &= a_{j-1} + m_{j-1} + 1 + \frac{1}{a_{j-1}} \sum_{n=0}^{\infty} \left(\frac{m_{j-1}}{a_{j-1}} \right)^n \\ &= a_{j-1}^2 m_{j-1} + m_{j-1}^2 + \text{ higher powers of } m_{j-1}. \end{aligned}$$

Hence $m_j = a_{j-1}^2 m_{j-1} \cdot (1 + r)$ where $r \in (m_{j-1})$, i.e. $u = 1 + r$ is a 1-unit in m_{j-1}. This implies that

$$\frac{1}{m_j} = \frac{a_{j-1}}{m_{j-1}} \cdot u = \frac{a_{j-1}}{m_{j-1}} + O(1) \text{ at } P_j.$$

For j odd, $a_j \in \{\rho, \rho^2\}$, and $a_{j-1} = 1$. Then, again using the defining equation we obtain

$$\begin{aligned} a_j^2 + m_j^2 + a_j + m_j &= (1 + m_{j-1}) + 1 + \frac{1}{1 + m_{j-1}} \\ &= 1 + \sum_{n=2}^{\infty} m_{j-1}^n \end{aligned}$$

and hence, since $a_j^2 + a_j = 0$ for $a_j \in \{\rho, \rho^2\}$,

$$m_j^2 + m_j = \sum_{n=2}^{\infty} m_{j-1}^n$$

and therefore

$$m_j = m_{j-1}^2 + m_{j-1}^3 + \text{ higher powers of } m_{j-1}.$$

Then

$$\begin{aligned} \frac{1}{m_j} &= \frac{1}{m_{j-1}^2} + \frac{1}{m_{j-1}} + \text{ higher powers of } m_{j-1} \\ &= \frac{1}{m_{j-1}^2} + \frac{1}{m_{j-1}} + O(1) \text{ at } P_j. \end{aligned}$$

□

From here on, only the principal part F_j of $\frac{1}{m_j}$ is considered, thereby absorbing the regularity notation $O(1)$. It is an immediate corollary of Lemma 5.3 that this principal part F_j satisfies

$$F_j = \begin{cases} a_{j-1} \cdot F_{j-1} & \text{if } j \geq 2 \text{ is even,} \\ F_{j-1}^2 + F_{j-1} & \text{if } j \geq 1 \text{ is odd,} \end{cases}$$

and it can be proved inductively that F_j is a 2-linearized polynomial in $\frac{1}{t}$ of the form

$$F_j = \frac{b_0}{t} + \frac{b_1}{t^2} + ... + \frac{b_{k-1}}{t^{2^{k-1}}} + \frac{b_k}{t^{2^k}}$$

where $k = \left\lfloor \frac{j+1}{2} \right\rfloor$, $b_k \neq 0$ and $b_i \in \mathbb{F}_4$ for $0 \leq i \leq k$ by taking $F_0 = \frac{1}{t}$ and $F_1 = \frac{1}{t^2} + \frac{1}{t}$ as the base step. As mentioned before, we have a similar result for the principal part if we assume $a_0 \in \{\rho, \rho^2\}$ rather than $a_0 = 1$.

5.2 The ramification behaviour and genus

We again assume $a_0 = 1$, and investigate the ramification behaviour in the tower at a place $P_i \in S\left(F_i/\overline{\mathbb{F}}\right)$ which is a zero of x_i in $F_i/\overline{\mathbb{F}}$. In terms of an index sequence, we therefore know that P_i is representable in the form

$$P\left(a_0 = 1, a_1, ..., a_{i-1}, a_i = 0\right)$$

where i is even and $a_j \in \{\rho, \rho^2\}$ if j is odd, and $a_j = 1$ if $j < i$ is even. If $a_0 \in \{\rho, \rho^2\}$, the ramification behaviour is similar.

We recall the (2-linear) Artin-Schreier operator $\wp(f) = f^2 + f$ as introduced on page 32, and show the following lemma which will be useful in order to perform Artin-Schreier reductions on the equations we will obtain.

Lemma 5.4. *A linear combination* $\sum_{j=2,\ even}^{i-2} B_{j,i}F_j$ *of principal parts where* $B_{j,i} \in \mathbb{F}_4$ *can be expressed in the form*

$$\sum_{j=2,\ even}^{i} B_{j,i}F_j = \wp\left(\sum_{j=0,\ even}^{i-2} B_{j,i-2}F_j\right) + B_i^*F_0$$

with

$$B_i^* = \wp\left(\sum_{j=2,\ even}^{i} B_{j,i}a_{j-1}\right)$$

and

$$B_{j,i-2} = \left(B_i^* + \wp\left(\sum_{k=2,\ even}^{j} B_{k,i}a_{k-1}\right)\right) \cdot a_{j+1}^2 + \wp\left(B_{j+2,i}\right).$$

Proof. Using the recursive expression for the principal part, we have for even $j \geq 2$ that

$$\begin{aligned} B_{j,i}F_j &= B_{j,i} \cdot a_{j-1} \cdot F_{j-1} \\ &= B_{j,i} \cdot a_{j-1} \cdot \wp\left(F_{j-2}\right) \\ &= \wp\left(B_{j,i}^2 a_{j-1}^2 F_{j-2}\right) + \wp\left(B_{j,i}a_{j-1}\right) \cdot F_{j-2}. \end{aligned}$$

By applying this transformation to its own second term, we obtain

$$\begin{aligned} B_{j,i}F_j &= \wp\left(B_{j,i}^2 a_{j-1}^2 F_{j-2}\right) + \wp\left(B_{j,i}a_{j-1}\right)\cdot F_{j-2} \\ &= \wp\left(B_{j,i}^2 a_{j-1}^2 F_{j-2}\right) + \wp\left(\wp\left(B_{j,i}a_{j-1}\right) a_{j-3}^2 F_{j-4}\right) + \wp\left(B_{j,i}a_{j-1}\right)\cdot F_{j-4}, \end{aligned}$$

using the fact that $\wp(a_k) = 1$ for k odd. Repeated application of this transformation leads to an expression of the form

$$B_{j,i}F_j = \wp\left(\text{linear combination of } F_0, F_2, ..., F_{j-2}\right) + \wp\left(B_{j,i}a_{j-1}\right) F_0.$$

Adding these expressions for all terms in $\sum_{j=2,\text{ even}}^{i-2} B_{j,i}F_j$ leads to the desired form with the coefficients satisfying the stated conditions. □

Note that all the coefficients in the above expansion are in $\mathbb{F}_4$, and that $B_i^* \in \mathbb{F}_2$ since $\wp$ is 2-linear and for each term $B_{j,i}a_{j-1}$ with j even, both $B_{j,i}$ and a_{j-1} are in $\mathbb{F}_4$, hence their product are, and hence $\wp\left(B_{j,i}a_{j-1}\right) \in \mathbb{F}_2$.

We now look at the extension F_{i+1}/F_i above the place $P_i \in S\left(F_i/\overline{\mathbb{F}}\right)$ which is a zero of x_i. Viewing P_i as an index sequence $(1, a_1, ..., a_{i-1}, 0)$, we have the relation

$$x_{i+1}^2 + x_{i+1} = x_i + 1 + \frac{1}{x_i} = F_i + O(1) \text{ at } P_i, \tag{5.2.1}$$

and therefore the principal part of $x_{i+1}^2 + x_{i+1}$ at P_i is F_i. Lemma 5.4 implies that we can write F_i in the form

$$F_i = \wp\left(\sum_{j=0,\text{ even}}^{i-2} B_{j,i-2}F_j\right) + B_i^* F_0$$

where $B_i^* = a_{i-1}^2 + a_{i-1} = 1$ and $B_{j,i-2} = a_{j+1}^2$ for even $j \leq i-2$. By transforming the variable x_{i+1} via

$$X_{i+1} := \sum_{j=0,\text{ even}}^{i-2} B_{j,i-2}F_j + x_{i+1}, \tag{5.2.2}$$

we can reduce (5.2.1) to

$$\begin{aligned} X_{i+1}^2 + X_{i+1} &= B_i^* F_0 + O(1) \text{ at } P_i \\ &= F_0 + O(1) \text{ at } P_i, \end{aligned} \tag{5.2.3}$$

where $F_0 = \frac{1}{t}$. Because of this, we immediately have

Corollary 5.5. *The place $P_i = P(1, a_1, a_2, ..., a_{i-1}, 0) \in S\left(F_i/\overline{\mathbb{F}}\right)$ is totally ramified in F_{i+1}/F_i, i.e. for the unique pole P_{i+1} lying above P_i, $e(P_{i+1}|P_i) = 2$ and $v_{P_{i+1}}(x_{i+1}) = -2^{\left\lfloor \frac{i+1}{2} \right\rfloor}$.*

So, at this stage we have that the zero $P_i = P(1, a_1, a_2, ..., a_{i-1}, 0)$ of x_i is totally ramified in F_{i+1}/F_i. We will now go one stage up the tower and look at the situation for $P_{i+1} = P_i(\infty)$ lying above P_i in the extension F_{i+2}/F_{i+1}. The place P_{i+1} is a pole of the function $f_{i+1} = x_{i+1} + 1 + \frac{1}{x_{i+1}}$ in F_{i+2}/F_{i+1}. The defining equation yields

$$\begin{aligned}
x_{i+2}^2 + x_{i+2} &= x_{i+1} + 1 + \frac{1}{x_{i+1}} \\
&= x_{i+1} + O(1) \text{ at } P_{i+1} \\
&= \sum_{j=0,\text{ even}}^{i-2} B_{j,i-2}F_j + X_{i+1} + O(1) \text{ at } P_{i+1} \text{ (applying (5.2.2))} \\
&= \wp\left(\sum_{j=0,\text{ even}}^{i-4} B_{j,i-4}F_j\right) + B_{i-2}^*F_0 + B_{0,i-2}F_0 + X_{i+1} + O(1) \text{ at } P_{i+1} \\
&= \wp\left(\sum_{j=0,\text{ even}}^{i-4} B_{j,i-4}F_j\right) + \wp\left(B_{i-2}^*X_{i+1}\right) + \wp\left(B_{0,i-2}^2X_{i+1}\right) \\
&\quad + \left(B_{0,i-2}^2 + B_{0,i-2} + 1\right)X_{i+1} + O(1) \text{ at } P_{i+1} \text{ (applying (5.2.3))} \\
&= \wp\left(\sum_{j=0,\text{ even}}^{i-4} B_{j,i-4}F_j\right) + \wp\left(\left(B_{i-2}^* + B_{0,i-2}^2\right)X_{i+1}\right) + O(1) \text{ at } P_{i+1},
\end{aligned}$$

since $B_{0,i-2}^2 + B_{0,i-2} + 1 = a_1^2 + a_1 + 1 = 0$. Therefore the equation of F_{i+2}/F_{i+1} is

$$x_{i+2}^2 + x_{i+2} = \wp\left(\sum_{j=0,\text{ even}}^{i-4} B_{j,i-4}F_j\right) + \wp\left(\left(B_{i-2}^* + B_{0,i-2}^2\right)X_{i+1}\right) + \mathcal{O}(1) \text{ at } P_{i+1}.$$

Making the transformation

$$X_{i+2} := \wp\left(\sum_{j=0,\text{ even}}^{i-4} B_{j,i-4}F_j\right) + \wp\left(\left(B_{i-2}^* + B_{0,i-2}^2\right)X_{i+1}\right) + x_{i+2}, \tag{5.2.4}$$

this implies that

$$X_{i+2}^2 + X_{i+2} = O(1) \text{ at } P_{i+1}. \tag{5.2.5}$$

We immediately have the following corollary:

Corollary 5.6. *The place $P_{i+1} = P_i(\infty) \in S\left(F_{i+1}/\overline{\mathbb{F}}\right)$ is unramified in F_{i+2}/F_{i+1}, i.e. for the place P_{i+2} lying above P_{i+1}, we have $e(P_{i+2}|P_{i+1}) = 1$, and $v_{P_{i+2}}(x_{i+2}) = -2^{\left\lfloor \frac{i+1}{2} \right\rfloor - 1}$.*

Again we continue another step up the tower, and look at the ramification behaviour of the place $P_{i+2} = P_i(\infty^2)$ lying above P_{i+1}, in the extension F_{i+3}/F_{i+2}. We

start with the defining equation. Then

$$\begin{aligned} x_{i+3}^2 + x_{i+3} &= x_{i+2} + O(1) \text{ at } P_{i+2} \\ &= \wp\left(\sum_{j=0,\text{ even}}^{i-4} B_{j,i-4}F_j\right) + \left(B_{i-2}^* + B_{0,i-2}^2\right) X_{i+1} + O(1) \text{ at } P_{i+2} \\ &= \wp\left(\sum_{j=0,\text{ even}}^{i-6} B_{j,i-6}F_j\right) + \wp\left(\left(B_{i-4}^* + B_{0,i-4}^2\right) X_{i+1}\right) \\ &\quad + \left(\wp(B_{0,i-4}) + B_{i-2}^* + B_{0,i-2}^2\right) X_{i+1} + O(1) \text{ at } P_{i+2} \end{aligned}$$

by Lemma 5.4 and (5.2.3).

Note that the expression for $B_{j,i-2}$ of Lemma 5.4 implies that the coefficient of X_{i+1} in the above expression can be written as

$$\wp(B_{0,i-4}) + B_{i-2}^* + B_{0,i-2}^2 = B_{i-2}^* + B_{i-2}^* + B_{0,i-2}^2 = B_{0,i-2}^2 = a_1^2 \neq 0,$$

and therefore

$$x_{i+3}^2 + x_{i+3} = \wp\left(\sum_{j=0,\text{ even}}^{i-6} B_{j,i-6}F_j\right) + \wp\left(\left(B_{i-4}^* + B_{0,i-4}^2\right) X_{i+1}\right) + B_{0,i-2}^2 X_{i+1} + O(1)$$

at P_{i+2}. Applying the transformation

$$X_{i+3} = \sum_{j=0,\text{ even}}^{i-6} B_{j,i-6}F_j + \left(B_{i-4}^* + B_{0,i-4}^2\right) X_{i+1} + x_{i+3}$$

the equation for F_{i+3}/F_{i+2} becomes

$$X_{i+3}^2 + X_{i+3} = B_{0,i-2}^2 X_{i+1} + O(1) \text{ at } P_{i+2}.$$

and we have the immediate corollary

Corollary 5.7. *The place $P_{i+2} = P_i(\infty^2) \in S\left(F_{i+2}/\overline{\mathbb{F}}\right)$ is totally ramified in F_{i+3}/F_{i+2}, i.e. for the place P_{i+3} lying above P_{i+2}, we have $e(P_{i+3}|P_{i+2}) = 2$, and $v_{P_{i+2}}(x_{i+2}) = -2^{\lfloor \frac{i+1}{2} \rfloor - 1}$.*

We have shown only the first three steps (Corollaries 5.5, 5.6 and 5.7) of an iterative analysis of the ramification behaviour above the zero $P_i \in S\left(F_i/\overline{\mathbb{F}}\right)$ of x_i. If this is continued in the same manner, it can be shown inductively that we have the following formula for F_{i+t}/F_{i+t-1} at $P_{i+t-1} = P_i(\infty^{t-1})$ for $2 \leq t \leq i$:

$$x_{i+t}^2 + x_{i+t} = \begin{cases} \wp(A_{i,t}) + O(1) \text{ at } P_{i+t-1} & \text{if } t \text{ is even,} \\ \wp(A_{i,t}) + B_{t-3,i-2}^2 X_{i+t-2} + O(1) \text{ at } P_{i+t-1} & \text{if } t \text{ is odd.} \end{cases} \tag{5.2.6}$$

where

$$A_{i,t} = \sum_{j=0,\ \text{even}}^{i-2t} B_{j,i-2t} F_j + \left(B^*_{i-2t+2} + B^2_{0,i-2t+2}\right) X_{i+1} + \sum_{k=1}^{\left\lfloor \frac{t-2}{2} \right\rfloor} \left(B_{2k-2,i-2t+4k} B^2_{2k-2,i-2}\right) X_{i+2k+1}.$$

By applying the usual transformation $X_{i+t} = A_{i,t} + x_{i+t}$ to (5.2.6) we obtain

$$X^2_{i+t} + X_{i+t} = \begin{cases} O(1) \text{ at } P_{i+t-1} & \text{if } t \text{ is even,} \\ B^2_{t-3,i-2} X_{i+t-2} + O(1) \text{ at } P_{i+t-1} & \text{if } t \text{ is odd.} \end{cases} \tag{5.2.7}$$

This implies that for $2 \leq t \leq i$ we have alternate ramification and non-ramification in the tower in F_{i+t}/F_{i+t-1} above the zero P_i of x_i. This pattern cannot continue beyond $t = i$. Indeed, since ramification occurs in $\left\lfloor \frac{t+1}{2} \right\rfloor$ of the t stages of the tower from F_i up to F_{i+t} over P_i, we have

$$v_{P_{i+t}}(x_{i+t}) = -2^{\left\lfloor \frac{(i+2)-(t+1)}{2} \right\rfloor},$$

implying that $v_{P_{2i}}(x_{2i}) = -1$, and all extensions lying above P_{2i} onwards are totally ramified.

The results coming from the recursive formulae mentioned above and the discussion thereafter can be summarized in the following theorem:

Theorem 5.8. *A pole $P_{i+j} = P(a_0, a_1, ..., a_{i-1}, 0, \infty^j) \in S\left(F_{i+j}/\overline{\mathbb{F}}\right)$ of $x_{i+j} \in F_{i+j}/\overline{\mathbb{F}}$ for $j \geq 1$ or a zero $P_i = P(a_0, a_1, ..., a_{i-1}, 0) \in S\left(F_i/\overline{\mathbb{F}}\right)$ with $a_0 = 1$ is*

(i) totally ramified in F_{i+j+1}/F_{i+j} for $j = 0, 2, 4, ..., i-2$ or $j \geq i$, with ramification index 2,

(ii) unramified in F_{i+j+1}/F_{i+j} for $j = 1, 3, 5, ..., i-1$.

The case $a_0 \in \{\rho, \rho^2\}$ can be handled similarly, and leads to the following theorem:

Theorem 5.9. *A pole $P_{i+j} = P(a_0, a_1, ..., a_{i-1}, 0, \infty^j) \in S\left(F_{i+j}/\overline{\mathbb{F}}\right)$ of $x_{i+j} \in F_{i+j}/\overline{\mathbb{F}}$ for $j \geq 1$ or a zero $P_i = P(a_0, a_1, ..., a_{i-1}, 0) \in S\left(F_i/\overline{\mathbb{F}}\right)$ with $a_0 \in \{\rho, \rho^2\}$ is*

(i) totally ramified in F_{i+j+1}/F_{i+j} for $j = 0, 2, 4, ..., i-3$ or $j \geq i-1$, with ramification index 2,

(ii) unramified in F_{i+j+1}/F_{i+j} for $j = 1, 3, 5, ..., i-2$.

Theorems 5.8 and 5.9 imply that when, for some $i > 0$, we have that a sequence

$$P_0 \subseteq P_1 \subseteq P_2 \subseteq ... \subseteq P_{i-1} \subseteq P_i \subseteq P_{i+1} \subseteq ... \subseteq P_{2i-1} \subseteq P_{2i} \subseteq P_{2i+1} \subseteq ...$$

of places lying above each other with $P_k \in S\left(F_k/\overline{\mathbb{F}}\right)$ for each $k \geq 0$, P_i is a zero of x_i and the index sequence consists of elements of $\mathbb{F}_4 \cup \{\infty\}$, then the ramification of these places over each other occurs as follows:

$$\underbrace{P_0 \subseteq P_1 \subseteq ... \subseteq P_{i-1} \subseteq}_{\text{no ramification}} P_i \underbrace{\subseteq P_{i+1} \subseteq ... \subseteq P_{2i-1} \subseteq}_{\text{alternating ramification}} P_{2i} \underbrace{\subseteq P_{2i+1} \subseteq ...}_{\text{total ramification}} \tag{5.2.8}$$

Considering our previous comments, it is clear that ramified places must have an index sequence which is a traversal of the directed graph on page 73, starting at an arbitrary vertex. Theorems 5.8 and 5.9 handle the cases for $a_0 \in \{\rho, \rho^2, 1\}$. The only remaining cases to mention are the totally ramified places with index sequences $(0, \infty, \infty, ..., \infty)$ and $(\infty, \infty, ..., \infty)$, thereby also finishing the cases where $a_0 \in \{0, \infty\}$.

This characterizes all ramified places in the tower. In particular, it can be shown inductively using the above facts that if we define

$$n_i := \left|\left\{P \in S\left(F_i/\overline{\mathbb{F}}\right) : P \text{ is totally ramified in } F_{i+1}/F_i\right\}\right|,$$

then one can derive, by noting that for $i \geq 1$, there exists $j \leq i$ such that $x_j(P) = 0$ and then considering the cases of even or odd i, and whether $i < 2j$ or $i \geq 2j$ (i.e. whether j is in the finite tower of alternating ramification of (5.2.8)) that

$$n_i = \begin{cases} \left(\left\lfloor \frac{i+2}{4} \right\rfloor + 2\right) \cdot 2^{\frac{i}{2}} & \text{if } \ i \text{ is even,} \\ \left(\left\lfloor \frac{i}{4} \right\rfloor + 2\right) \cdot 2^{\frac{i+1}{2}} & \text{if } \ i \text{ is odd.} \end{cases} \tag{5.2.9}$$

We further note that for any place $P \in S\left(F_i/\overline{\mathbb{F}}\right)$ ramified in F_{i+1}/F_i with $P'|P$, the properties of the different exponents of Artin-Schreier extensions described in Proposition 2.28 imply that

$$\begin{aligned} d(P'|P) &= (p-1)(m_P+1) \\ &= (2-1)(1+1) \\ &= 2 \end{aligned}$$

because we have for m_P that

$$\begin{aligned} v_P(f_i) &= v_P\left(x_i + 1 + \frac{1}{x_i}\right) \\ &= v_P\left(\frac{x_i^2 + x_i + 1}{x_i}\right) \\ &= -1, \end{aligned}$$

for both the zero $P = P(a_0, a_1, ..., a_{i-1}, 0)$ and pole $P = P(a_0, a_1, ..., a_{j-1}, 0, \infty^{i-j})$ of x_i.

Therefore we have that

$$\deg \mathrm{Diff}(F_{i+1}/F_i) = 2n_i,$$

(noting that all places are of degree one since we are working in $\overline{\mathbb{F}}$) and by the Hurwitz genus formula (Theorem 2.19) it follows that we have the recursive equation

$$\begin{aligned} 2g(F_{i+1}) - 2 &= 2[2g(F_i) - 2] + \deg \mathrm{Diff}(F_{i+1}/F_i) \\ &= 2[2g(F_i) - 2] + 2n_i. \end{aligned} \tag{5.2.10}$$

for the genus. As mentioned earlier, $g(F_1) = 1$, and this forms the basis of an inductive proof (using (5.2.10)) showing that

$$g(F_i) = 1 + \sum_{j=1}^{i-1} 2^{i-j-1} n_j \tag{5.2.11}$$

for $i \geq 2$.

Substituting (5.2.9) into (5.2.11), we obtain the following explicit formula for the genus:

$$g(F_i) = 2^{i+2} + 1 - \begin{cases} (i+10) \cdot 2^{\frac{i}{2}-1} & \text{if } i \text{ is even,} \\ \left(i + 2\left\lfloor \frac{i}{4} \right\rfloor + 15\right) \cdot 2^{\frac{i-3}{2}} & \text{if } i \text{ is odd.} \end{cases} \tag{5.2.12}$$

5.3 The asymptotic behaviour

In order to compute the number of places of degree one, we return to the original tower $\mathcal{F}$ over $\mathbb{F}_8$. Counting the number of places of degree one of $F_i/\mathbb{F}_8$ turns out to be easy, as the splitting behaviour over $\mathbb{F}_8$ is very good. We have the following theorem, which gives a simple expression for the number of places of degree one in any stage of $\mathcal{F}$:

Theorem 5.10. *The number of places of degree one of* $F_i/\mathbb{F}_8$ *is* $6 \cdot 2^i + 2$ *for* $i \geq 1$.

Proof. Let α be a primitive element of $\mathbb{F}_8$ satisfying $\alpha^3 + \alpha + 1 = 0$. If we let $f(x) = x + 1 + \frac{1}{x}$ and $g(y) = y^2 + y$ it can be shown by direct computation that

$$\{f(x) : x \in \mathbb{F}_8 \setminus \mathbb{F}_2\} = \{\alpha, \alpha^2, \alpha^4\}$$

and

$$\{g(y) : y \in \mathbb{F}_8 \setminus \mathbb{F}_2\} = \{\alpha, \alpha^2, \alpha^4\}.$$

Therefore the 6 rational places in $F_0/\mathbb{F}_8$ corresponding to the elements of $\mathbb{F}_8 \setminus \mathbb{F}_2$ split completely throughout the tower, yielding $6 \cdot 2^i$ places of degree one in $F_i/\mathbb{F}_8$. Other than these, we also have the two totally ramified places $P(0, \infty, \infty, ..., \infty)$ and $P(\infty, \infty, ..., \infty)$ of degree one which are defined over $\mathbb{F}_2$. Putting this together, we obtain $N(F_i/\mathbb{F}_8) = 6 \cdot 2^i + 2$. □

It is now easy to show that the tower $\mathcal{F}$ is indeed asymptotically good:

Theorem 5.11. $\lambda(\mathcal{F}) = \frac{3}{2} > 0$.

Proof. We note from (5.2.12) that

$$g(F_i) = 2^{i+2} + \text{ lower order terms}$$

and from Theorem 5.10 that

$$N(F_i/\mathbb{F}_8) = 6 \cdot 2^i + \text{ lower order terms.}$$

Therefore

$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{N(F_i/\mathbb{F}_8)}{g(F_i)} = \lim_{i \to \infty} \frac{6 \cdot 2^i}{2^{i+2}} = \frac{3}{2} > 0.$$

□

It is interesting to note that this tower meets the limit of Zink's non-explicit tower in [36], while it has no immediate interpretation in terms of Shimura surfaces.

We briefly divert from the current discussion, and prove a lower bound for the limit $\lambda(\mathcal{F})$ of $\mathcal{F}$. Strictly speaking, this is not necessary since we have already determined it exactly. It does however show that a relatively good lower bound can be obtained with a much smaller amount of work, and using a method (Theorem 3.22) which may be applicable to many other towers over non-square finite fields as well when they have a finite ramification locus. The bound obtained in this way already improves those obtained from many non-explicit constructions, for example those from [20] and [21].

Theorem 5.12. $\lambda(\mathcal{F}) \geq 1$.

Proof. We note that the tower $\mathcal{F}$ is of finite ramification type since it was shown in Lemma 5.2 that ramification can only occur at places with index sequences defined over $\mathbb{F}_4 \cup \{\infty\}$. We have seen that ramification occurs in the tower above places in $S(F_0/\mathbb{F}_8)$ corresponding to the elements of $\mathbb{F}_4 \cup \{\infty\}$. Therefore, for ρ a primitive element of $\mathbb{F}_4$, we write the places of $S(F_0/\mathbb{F}_8)$ corresponding to the divisors (x), $(x-1)$, $(x-\rho)$, $(x-\rho^2)$ and $\left(\frac{1}{x}\right)$ respectively as Q_0, Q_1, Q_ρ, Q_{ρ^2} and Q_∞, and have that for the ramification locus of $\mathcal{F}$

$$V(\mathcal{F}) = \{Q_0, Q_1, Q_\rho, Q_{\rho^2}, Q_\infty\} \subseteq S(F_0/\mathbb{F}_8).$$

The proof of Theorem 5.10 implies that $\mathcal{F}$ is completely splitting (see Definition 3.21) with $|T(\mathcal{F})| = 6$. Furthermore we note that

$$\deg Q_0 = \deg Q_1 = \deg Q_\infty = 1 \text{ and } \deg Q_\rho = \deg Q_{\rho^2} = 2.$$

To apply Theorem 3.22, we have to find non-negative constants a_P (for each $P \in V(\mathcal{F})$) satisfying condition (iii) of the theorem. From earlier comments, we know that if P, P' are places lying in F_i and F_{i+1} respectively with $P'|P$, then $e(P'|P) \in \{1,2\}$ and $d(P'|P) \in \{0,2\}$. Proposition 3.24 implies that we can choose $a_P = 2$ for each $P \in V(\mathcal{F})$, since $2 \cdot (e(Q'|Q) - 1) \geq d(Q'|Q)$ for any places $Q'|Q$ in some extension F_{i+1}/F_i. We further note that the genus of the rational function field $F_0/\mathbb{F}_8$ is 0. Then Theorem 3.22 implies that

$$\begin{aligned}
\lambda(\mathcal{F}) &\geq \frac{2 \cdot |T(\mathcal{F})|}{2g(F_0) - 2 + \sum_{P \in V(\mathcal{F})} a_P \cdot \deg P} \\
&= \frac{2 \cdot 6}{-2 + (2 \cdot 1 + 2 \cdot 1 + 2 \cdot 2 + 2 \cdot 2 + 2 \cdot 1)} \\
&= 1.
\end{aligned}$$

□

From García and Stichtenoth's tower which was described in Section 3.3, we know that there exist towers over every finite field of square cardinality which meet the Drinfeld-Vlăduţ bound. We will therefore restrict our attention to possible constructions in fields of non-square cardinality. We have the following canonical method of extending explicit towers over a finite field to an explicit tower over an extension field:

Lemma 5.13. *Given an explicit tower $\mathcal{F} = (F_1, F_2, \ldots)$ of function fields over $\mathbb{F}_{p^m}$ with $\lambda(\mathcal{F}) = l$, there exists, for any integer $r \geq 1$, an explicit tower*

$$\mathcal{F}^{(r)} = \left(F_1^{(r)}, F_2^{(r)}, \ldots\right)$$

of function fields over $\mathbb{F}_{p^n} = \mathbb{F}_{p^{rm}}$ *with* $\lambda\left(\mathcal{F}^{(r)}\right) \geq l$, *using the same explicit equations.*

Proof. For each $i \geq 1$, let $F_i^{(r)}/\mathbb{F}_{p^n} := F_i/\left(\mathbb{F}_{p^m} \cdot \mathbb{F}_{p^n}\right)$, i.e. $F_i^{(r)}$ is just F_i with the field of constants extended from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^n} = \mathbb{F}_{p^{mr}}$. Obviously the same explicit defining equation will still hold in each extension $F_{i+1}^{(r)}/F_i^{(r)}$ as it did for F_{i+1}/F_i, for $i \geq 1$. Since the genus is preserved under constant field extensions, $g\left(F_i^{(r)}\right) = g\left(F_i\right)$ for $i \geq 1$. We also have that $N\left(F_i^{(r)}\right) \geq N\left(F_i\right)$ since $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Therefore

$$\lambda\left(\mathcal{F}^{(r)}\right) = \lim_{i\to\infty} \frac{N\left(F_i^{(r)}\right)}{g\left(F_i^{(r)}\right)} \geq \lim_{i\to\infty} \frac{N\left(F_i\right)}{g\left(F_i\right)} = \lambda\left(\mathcal{F}\right) = l.$$

□

5.4 Observations

As we are interested in the non-square finite field case, Lemma 5.13 may only be helpful towards improving lower bounds for $A\left(p^{mr}\right)$ when r is chosen to be odd, and the tower $\mathcal{F}$ defined over $\mathbb{F}_{p^m}$ where m is odd as well. The explicit tower $\mathcal{F}$ of Van der Geer and Van der Vlugt can be extended using Lemma 5.13 in this way by choosing $r = 3$, and thereby obtaining an explicit tower $\mathcal{F}^{(3)}$ of function fields over $\mathbb{F}_{2^9} = \mathbb{F}_{512}$ which has $\lambda\left(\mathcal{F}^{(3)}\right) \geq \frac{3}{2}$.

In Section 3.2 a brief survey of some bounds on $A\left(q\right)$ was given. In particular, Xing and Niederreiter [21] showed analogously to equation (3.2.5), using narrow ray class fields, that if q is even and $\left\lfloor 2q^{1/2} \right\rfloor$ is odd, then

$$A\left(q^3\right) \geq \frac{q + \left\lfloor 2q^{\frac{1}{2}} \right\rfloor}{3 + \left\lceil 2\left(2q + 2\left\lfloor 2q^{\frac{1}{2}} \right\rfloor - 2\right)^{\frac{1}{2}} \right\rceil}.$$

In our case, $q = 2^3$ and hence $\left\lfloor 2q^{1/2} \right\rfloor = 5$, and the conditions are satisfied. Therefore their narrow ray class field construction yields the bound

$$A\left(2^9\right) \geq \frac{2^3 + \left\lfloor 2 \cdot (2^3)^{\frac{1}{2}} \right\rfloor}{3 + \left\lceil 2\left(2 \cdot 2^3 + 2\left\lfloor 2 \times (2^3)^{\frac{1}{2}} \right\rfloor - 2\right)^{\frac{1}{2}} \right\rceil} = 1. \tag{5.4.1}$$

Similarly, using their bound using class field towers in equation (3.2.4), we have

$$A\left(2^9\right) \geq \frac{2^3 + 1}{\left\lceil 2 \times (2 \cdot 2^3 + 2)^{\frac{1}{2}} \right\rceil + 2} = \frac{9}{11} \approx 0.8181. \tag{5.4.2}$$

We note that both these bounds given by (5.4.1) and (5.4.2) are weaker than the bound $A(2^9) \geq \frac{3}{2}$ implied by the tower $\mathcal{F}^{(3)}$, i.e. the lifting of Van der Geer and Van der Vlugt's tower $\mathcal{F}$ over $\mathbb{F}_8$ to $\mathcal{F}^{(3)}$ over $\mathbb{F}_{512}$ improves Xing and Niederreiter's lower bounds for $A(512)$ given by class field towers in [20] and those given by narrow ray class fields in [21].

We can continue this process, and extend Van der Geer and Van der Vlugt's tower $\mathcal{F}$ by $r = 5$ to $\mathcal{F}^{(5)}$. This gives us a tower $\mathcal{F}^{(5)}$ over $\mathbb{F}_{2^{15}}$ with $\lambda(\mathcal{F}) \geq \frac{3}{2}$. However, the class field and narrow ray class field constructions of Xing and Niederreiter respectively yield $A(2^{15}) \geq \frac{33}{19} \approx 1.7368$ and $A(2^{15}) \geq \frac{43}{22} \approx 1.9545$. Therefore only the "lifting" $\mathcal{F}^{(3)}$ of Van der Geer and Van der Vlugt's tower $\mathcal{F}$ improves the existing bounds for $A(512)$. The liftings $\mathcal{F}^{(r)}$ for $r \geq 5$ are still explicit though, a property not shared by the other above-mentioned constructions by Xing and Niederreiter.

The question now arises whether we may be able to find other explicit formulae which may lead to the construction of towers over other non-prime fields of non-square cardinality which have asymptotically good behaviour. We will look at possible Artin-Schreier extensions over fields $\mathbb{F}_{p^n}$ (with odd $n \geq 3$) of the form

$$y^p - y = f(x) = \frac{a(x)}{b(x)} \tag{5.4.3}$$

where $a(x), b(x) \in \mathbb{F}_p[x]$. Using an equation of this type one can, as before, recursively construct a tower $\mathcal{F}$ by letting $F_0 := \mathbb{F}_{p^n}(x_0)$ and then letting $F_i := F_{i-1}(x_i)$ where $x_{i+1}^p - x_{i+1} = f(x_i)$ for $i \geq 1$. We note immediately that the tower of Van der Geer and Van der Vlugt described in before Proposition 5.1 is of this form with $p^n = 2^3$, $a(x) = x^2 + x + 1$ and $b(x) = x$.

The MAGMA procedure `Split` described in Appendix B has been written to search for polynomial pairs $(a(x), b(x))$ which yields Artin-Schreier extensions (of the type in equation (5.4.3)) with properties which may yield asymptotically good towers if they are recursively applied, over a given finite field $\mathbb{F}_{p^n}$. It starts by performing a brute-force search by exhaustively considering all possible polynomials $a(x)$, $b(x) \in \mathbb{F}_p[x]$ of degree at most 10, but only analyzing them when the equation of the form of (5.4.3) is irreducible. Moreover, the brute-force search starts with $a(x)$ and $b(x)$ of low degree and gradually works its way up. In this way, we will find minimal degree defining equations faster.

We can also specify an interval of allowable values for $v_\infty(f) = \deg b(x) - \deg a(x)$ in order to possibly minimize the associated m_P as described in Definition 2.28. Doing so will minimize the different exponent at the infinite place, and hopefully (this

requires further analysis of the particular family of extensions) the other different exponents as well. We will show many $(a(x), b(x))$ pairs which are reducible by the procedure of Lemma 2.33. The rationale behind not reducing them is that we would like to force the infinite place to be totally ramified in towers using the particular equation, and reduction by the mentioned lemma may cause v_∞ to become nonnegative (noting that reduction by Lemma 2.33 makes a difference to the valuation at the infinite place since the degree of $a(x)$ is reduced). This occurs when $v_\infty(f)$ is not prime to p. We will focus on the case where $v_\infty(f) < 0$ for this reason. The value $v_\infty(f) = -1$ is the best possibility under these restrictions (which is also the value for Van der Geer and Van der Vlugt's tower).

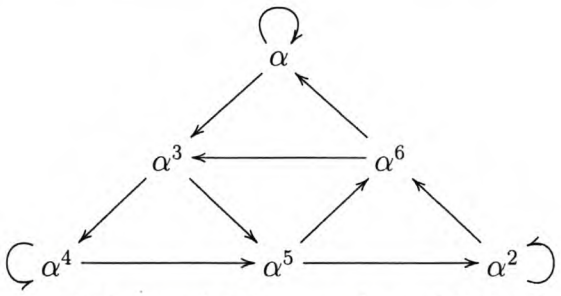
When this valuation is in the allowable range, the splitting behaviour of the extension will be analyzed, to see whether there exists a set of rational places which split completely in all extensions of the tower. This is done in the same way as the single stage description of Proposition B.2 where is it shown that a single extension of the type described there preserves the elements of $\mathbb{F}_8 \setminus \mathbb{F}_2$, and therefore they will split completely thereafter, since we use the same equation for each stage of the tower. If $T(\mathcal{F}) \neq \varnothing$, its cardinality is shown as a measure of how good the splitting behaviour is.

If the above-mentioned properties all hold, `Split` computes the genus of the extension, and outputs the found explicit equation only if the genus is minimal with respect to the extensions found so far. By minimizing the genus of these candidate extensions, it is hoped that the asymptotic growth of the genus will be kept low as well.

It is worth noting that the equations obtained by running `Split` does not guarantee that they yield asymptotically good towers. In order to be able to apply Theorem 3.22 for example, we will still need to show that the ramification locus $V(\mathcal{F})$ is finite, and that we can find constants a_P satisfying the requirements. To do so, may require proving analogues of Lemma 5.2 for these specific cases. Calculation of the different exponents $d(P'|P)$ should not provide a major obstacle, since we are looking at standard Artin-Schreier extensions.

Also, the test for splitting requires that the preservation of all elements of $\mathbb{F}_{p^n}$ which are preserved occur in a single extension. This is a sufficient but not necessary condition for complete splitting of a tower with the given equation. It is foreseeable that a MAGMA program can be written to consider these more subtle cases as well, but it may require much more processing time, since it would require showing that there exists a connected subgraph $\mathcal{H}$ of the directed graph $\mathcal{G}$ where the vertex set

$V(\mathcal{G}) = \mathbb{F}_{p^n}$ and edge set $E(\mathcal{G}) = \left\{(x \longrightarrow y) : y^p - y = \frac{a(x)}{b(x)}\right\}$, such that each vertex of $\mathcal{H}$ has out-degree p (corresponding to each of these places splitting). The elements of $T(\mathcal{F})$ for a tower $\mathcal{F}$ based upon this equation correspond to the vertices of $\mathcal{H}$. `Split` performs this test only for the (much simpler) case where the vertices of $\mathcal{H}$ consists of all those vertices of $\mathcal{G}$ having out-degree p, i.e. all $x \in \mathbb{F}_{p^n}$ such that there exists p distinct $y \in \mathbb{F}_{q^n}$ satisfying the defining equation, and may therefore miss some equations with more subtle splitting behaviour. As an example, the subgraph $\mathcal{H}$ induced by the vertices $\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ in Van der Geer and Van der Vlugt's tower has the above-mentioned properties, and gives a pleasing graphical representation for the good splitting properties of the elements of $\mathbb{F}_8 \setminus \mathbb{F}_2$ in that particular tower :



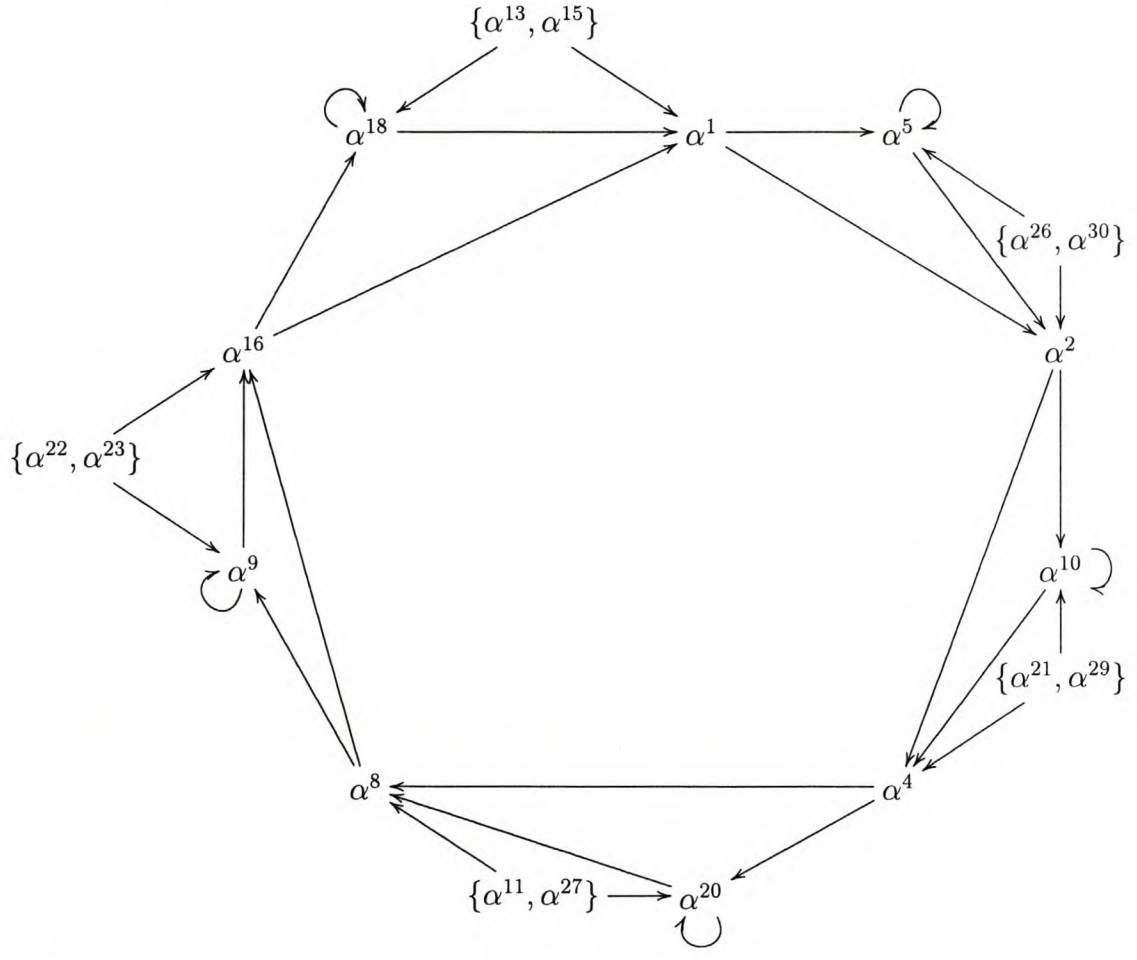
We now present some of the candidate equations obtained using `Split`. We omit non-minimal degree pairs $(a(x), b(x))$ which match the best genus, $v_\infty(a/b)$ and $|T(\mathcal{F})| > 0$ values over a given field $\mathbb{F}_{p^n}$. The symbol $\mathcal{F}$ corresponds to a hypothetical tower of function fields constructed by recursively extending the rational function field by using the candidate equation over $\mathbb{F}_{p^n}$. In some cases, many distinct $(a(x), b(x))$ pairs yield the same splitting properties - in those cases only one is listed.

Explicit equations in characteristic 2:

Field	**Equation**	$\lvert T(\mathcal{F})\rvert$	**Genus**	$v_\infty\left(\frac{a(x)}{b(x)}\right)$
$\mathbb{F}_{2^3}$	$y^2 - y = \frac{x^2+x+1}{x} = x + 1 + \frac{1}{x}$	6	1	-1
$\mathbb{F}_{2^5}$	$y^2 - y = \frac{x^8+x^7+x^3+x}{x^4+x^2+1}$	12	1	-4
$\mathbb{F}_{2^5}$	$y^2 - y = \frac{x^8+x^7+x^5+x^2+1}{x^6}$	15	1	-2
$\mathbb{F}_{2^5}$	$y^2 - y = \frac{x^4+x^2+1}{x^2+x}$	20	1	-2
$\mathbb{F}_{2^5}$	$y^2 - y = \frac{x^6+x^3+1}{x^5+x}$	20	1	-1
$\mathbb{F}_{2^5}$	$y^2 - y = \frac{x^5+x}{x^2+x+1}$	22	3	-3
$\mathbb{F}_{2^5}$	$y^2 - y = \frac{x^6+x^2+1}{x^3+x}$	25	2	-3
$\mathbb{F}_{2^7}$	$y^2 - y = \frac{x^4+x+1}{x^2+x+1}$	70	1	-2
$\mathbb{F}_{2^9}$	$y^2 - y = \frac{x^4+x+1}{x^2+x+1}$	258	1	-2

We note that the tower of Van der Geer and Van der Vlugt's defining equation

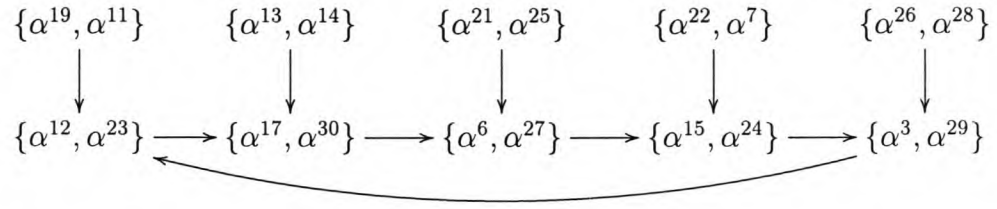
is the first one `Split` finds. It is interesting to note that the splitting graph for the extension given by $y^2-y=\frac{x^6+x^3+1}{x^5+x}$ over $\mathbb{F}_{2^5}$ also has a very symmetrical representation as that of the Van der Geer and Van der Vlugt tower, and indicates that there may exist a general family of towers of function fields containing a subset of places splitting completely in all subsequent stages of the tower in characteristic two. It is interesting to note that this particular example is not of the type described using quasi-symmetric extensions in Chapter 4, since the denominator of the right-hand side certainly has a zero in $\mathbb{F}_{2^5}$. In the following representation of the splitting graph, α is a primitive element for $\mathbb{F}_{2^5}$:



The notation $\{\alpha^i,\alpha^j\}\longrightarrow\alpha^k$ is shorthand for indicating that both $\alpha^i\longrightarrow\alpha^k$ and $\alpha^j\longrightarrow\alpha^k$.

It is interesting to note that the associated splitting graph for those elements of $\mathbb{F}_{32}$ which split completely if we rather use the equation $y^2-y=\frac{x^4+x^2+1}{x^2+x}$, has a somewhat simpler form, although it has the same number of vertices. While the previous graph had cycles of each length greater or equal to 5, the graph for this equation has only

cycles of length multiples of 5. It can be represented as follows:



In this diagram, by considering the earlier notation, each arrow refers to four underlying arrows.

Explicit equations in characteristic 3:

Field	Equation	$\lvert T(\mathcal{F})\rvert$	Genus	$v_\infty\left(\frac{a(x)}{b(x)}\right)$
$\mathbb{F}_{3^3}$	$y^3 - y = \frac{x^4-x^2}{x^2+1}$	3	5	-2
$\mathbb{F}_{3^3}$	$y^3 - y = \frac{x^5+x^3+2x^2+2x+1}{2x^4+x^3+2x+1}$	13	5	-1

The splitting graph of the extension with equation $y^3 - y = \frac{x^5+x^3+2x^2+2x+1}{2x^4+x^3+2x+1}$ over $\mathbb{F}_{3^3}$ is also very symmetrical. If β is a primitive element for $\mathbb{F}_{27}$ then the graph consists of the edges generated by

$$\begin{aligned}
\{0, \beta^4, \beta^{10}, \beta^{12}\} &\longrightarrow \{\beta^{14}, \beta^{16}, \beta^{22}\}, \\
\{\beta^2, \beta^{11}, \beta^{22}\} &\longrightarrow \{\beta^4, \beta^7, \beta^{18}\}, \\
\{\beta^6, \beta^7, \beta^{14}\} &\longrightarrow \{\beta^2, \beta^{12}, \beta^{21}\}, \\
\{\beta^{16}, \beta^{18}, \beta^{21}\} &\longrightarrow \{\beta^6, \beta^{10}, \beta^{11}\}
\end{aligned}$$

which has the necessary properties for complete splitting since each element occuring in the right-hand side also occurs in the left-hand side, implying that $|T(\mathcal{F})| = 3 \times 4 + 1 = 13$ as shown by `Split`.

Partial trial runs of `Split` over $\mathbb{F}_{5^3}$, $\mathbb{F}_{7^3}$ and $\mathbb{F}_{11^3}$ have been done, with no candidate equations obtained so far. From this it can be concluded that if completely splitting explicit extensions exist over these fields, they are of the more subtle type commented on before, and are therefore missed by `Split`, or have significantly higher degree defining polynomials.

A secondary, more general possibility is towers of function fields where the same explicit equation is not necessarily used in each step of the tower, as was used in almost all explicit extensions in this dissertation. It may be possible to perform a similar heuristic analysis of these possibilities by using a modified `Split` and stages of a tower alternating between the equations $y^p - y = a_1(x)/b_1(x)$ and $y^p - y = a_2(x)/b_2(x)$, where $a_1, a_2, b_1, b_2 \in \mathbb{F}_p[x]$, over $\mathbb{F}_{p^n}$.

Appendix A

Algebraic Function Fields

A concise overview of the theory of algebraic function fields of one variable is given, after [27].

A.1 Definitions and elementary properties

Definition A.1. *Given fields F and K such that $K \subset F$ and F is a finite algebraic extension of $K(x)$ for some $x \in F$ which is transcendental over K, we call F/K an algebraic function field of one variable over K.*

For brevity we will refer to F/K simply as a *function field.*

$$\widetilde{K} := \{z \in F : z \text{ is algebraic over } K\}$$

is a subfield of F, and is called the *field of constants* of F/K. It is easily verified that $F/\widetilde{K}$ is a function field over $\widetilde{K}$. We call K the *full constant field* of F if $K = \widetilde{K}$.

We will, unless noted otherwise, assume that from here onwards K is algebraically closed in F, i.e. that K is the full constant field of F.

Definition A.2. *A discrete valuation ring of the function field F/K is a ring $\mathcal{O}$ with $K \subsetneq \mathcal{O} \subsetneq F$ such that for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

For a valuation ring $\mathcal{O}$ of the function field F/K with full constant field K we have

1. $\mathcal{O}$ is a local ring, i.e. $\mathcal{O}$ has a unique maximal ideal $\mathfrak{m} = \mathcal{O} \setminus \mathcal{O}^\times$ where $\mathcal{O}^\times = \{z \in \mathcal{O} : \exists y \in \mathcal{O} \text{ such that } yz = 1\}$.

2. For $0 \neq x \in F$, $x \in \mathfrak{m} \iff x^{-1} \notin \mathcal{O}$.

3. $K \subseteq \mathcal{O}$ and $K \cap \mathfrak{m} = \{0\}$.

Moreover, we have that $\mathfrak{m}$ is a principal ideal. If $\mathfrak{m} = t\mathcal{O}$, then any nonzero $z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$, $u \in \mathcal{O}^\times$. The integer n is independent of the choice of t.

Definition A.3. *A place P of the function field F/K is the unique maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Any element $t \in P$ such that $P = t\mathcal{O}$ is called a local parameter for P. We let*

$$S(F/K) := \{P : P \text{ is a place of } F/K\}.$$

An equivalent way of defining a discrete valuation ring of F/K is by defining a function $v : F \to \mathbb{Z} \cup \{\infty\}$ which we call a valuation when, for $x, y \in F$,

1. $v(x) = \infty \iff x = 0$.
2. $v(xy) = v(x) + v(y)$.
3. There exists a $z \in F$ with $v(z) = 1$.
4. $0 \neq a \in K \implies v(a) = 0$.
5. $v(x + y) \geq \min\{v(x), v(y)\}$.

The last inequality is known as the Triangle Inequality. A stronger result, which can be derived from the axioms, holds : if $v(x) \neq v(y)$, then we have equality, i.e. $v(x + y) = \min\{v(x), v(y)\}$.

Definition A.4. *To each place $P \in S(F/K)$ we associate a function*

$$v_P : \begin{cases} F & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ z & \longmapsto & n \end{cases}$$

by choosing a local parameter t of P, and for $0 \neq z \in F$,letting n be the (unique) exponent of t such that $z = t^n u$, $n \in \mathbb{Z}$ and $u \in \mathcal{O}_P^\times$, and hence $v_P(z) := n$. If $z = 0$, we set $v_P(0) = \infty$. The definition depends only on the choice of P, and not on the choice of t. Moreover, it turns out that for each $P \in S(F/K)$, v_P is a discrete valuation of F/K.

We can now express the valuation rings and corresponding maximal ideals in terms of these valuations. Given a discrete valuation v of F/K, we have that $\mathcal{O}_v, \mathcal{O}_v^\times$ and P_v defined by

$$\begin{aligned}\mathcal{O}_v &= \{z \in F : v(z) \geq 0\},\\ \mathcal{O}_v^\times &= \{z \in F : v(z) = 0\},\\ P_v &= \{z \in F : v(z) > 0\},\end{aligned}$$

are respectively a valuation ring, group of units of the valuation ring and the unique maximal ideal of the valuation ring. In the case where $v = v_P$ (i.e. when the valuation comes from a given place $P \in S(F/K)$) we denote these by $\mathcal{O}_P, \mathcal{O}_P^\times$ and P, respectively. An element $x \in F$ is a local parameter for $P \in S(F/K)$ if and only if $v_P(x) = 1$.

For $P \in S(F/K)$ and its valuation ring $\mathcal{O}_P$, we have that P is a maximal ideal of $\mathcal{O}_P$, and hence the residue class ring $F_P := \mathcal{O}_P/P$ is in fact a field. We define

$$x(P) := \begin{cases} \text{residue class of } x \text{ modulo } P & \text{if } \ x \in \mathcal{O}_P,\\ \infty & \text{if } \ x \in F \setminus \mathcal{O}_P. \end{cases}$$

We know that $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$, and hence the residue class map $\mathcal{O}_P \longrightarrow \mathcal{O}_P/P$ induces a canonical embedding of K into $\mathcal{O}_P/P$. We can therefore consider K as a subfield of $\mathcal{O}_P/P$ via this embedding.

Definition A.5. *For $P \in S(F/K)$, we define $F_P := \mathcal{O}_P/P$ as the residue class field of P. The map $x \longmapsto x(P)$ is called the residue class map w.r.t. P. Moreover, $\deg P := [F_P : K]$ is the degree of P, which turns out to be finite.*

Remark A.6. *When $\deg P = 1$ we have $F_P = K$, and the residue class map maps F to $K \cup \{\infty\}$, and hence for $x \in F$*

$$x : \begin{cases} S(F/K) & \longrightarrow & K \cup \{\infty\},\\ P & \longmapsto & x(P), \end{cases}$$

thereby motivating the name function field for F/K. The elements of K can be interpreted as constant functions, and hence called the constant field of F.

Definition A.7. *Given $x \in F$ and $P \in S(F/K)$, we say that*

$$\begin{aligned} P \text{ is a zero of } x &:\Longleftrightarrow v_P(x) > 0,\\ P \text{ is a pole of } x &:\Longleftrightarrow v_P(x) < 0. \end{aligned}$$

If $v_P(x) > 0$ we say P is a zero of order $v_P(x)$, if $v_P(x) < 0$ we say P is a pole of order $-v_P(x)$.

Theorem A.8 (Approximation Theorem). *Let F/K be a function field and $P_1, ..., P_n \in S(F/K)$ distinct places of F/K. For any $x_1, ...x_n \in F$ and $r_1, ..., r_n \in \mathbb{Z}$ there exists $x \in F$ such that*

$$v_{P_i}(x - x_i) = r_i \text{ for } i = 1, ..., n.$$

Theorem A.9 (Chevalley). *Let F/K be a function field and R a subring of F with $K \subseteq R \subseteq F$. If $\{0\} \subsetneq I \subsetneq R$ is a proper ideal of R, then there exists a place $P \in S(F/K)$ such that $I \subseteq P$ and $R \subseteq \mathcal{O}_P$.*

Chevalley's Theorem implies that $S(F/K) \neq \varnothing$, which is rather crucial to the theory remarked on so far. Also, each $z \in F \setminus K$ has at least one zero and one pole, by applying Chevalley's Theorem to the ring $R = K[z]$ and ideal $I = zK[z]$. It can moreover be shown that any $0 \neq z \in F$ has only finitely many zeros and poles.

We form the free abelian group on $S(F/K)$ and denote it by $\mathrm{Div}(F)$, called the *divisor group* of F/K. Elements of $\mathrm{Div}(F)$ are called *divisors* of F/K, and can be written as a formal sum

$$D = \sum_{P \in S(F/K)} n_P P$$

with $n_P \in \mathbb{Z}$ and almost all $n_P = 0$. We define the *support* of $D \in \mathrm{Div}(F)$ by

$$\mathrm{supp}\ D := \{P \in S(F/K) : n_P \neq 0\}.$$

A divisor of the form $D = P \in S(F/K)$ is called a *prime divisor*. Divisors are added componentwise, i.e.

$$\sum_{P \in S(F/K)} n_P P + \sum_{P \in S(F/K)} n'_P P = \sum_{P \in S(F/K)} (n_P + n'_P) P$$

and the zero element is the formal sum where each $n_P = 0$. We apply a valuation to $D = \sum n_P P \in \mathrm{Div}(F)$ at $Q \in S(F/K)$ by defining $v_Q(D) := n_Q$. We use this to define a partial ordering on $\mathrm{Div}(F)$ by

$$D_1 \leq D_1 :\Longleftrightarrow v_P(D_1) \leq v_P(D_2) \text{ for each } P \in S(F/K).$$

We call a divisor $D \geq 0$ positive, and define

$$\deg D := \sum_{P \in S(F/K)} v_P(D) \cdot \deg P = \sum_{P \in S(F/K)} v_P(D) \cdot [F_P : K].$$

Definition A.10. *For $0 \neq x \in F$, let $Z := \{P \in S(F/K) : v_P(x) > 0\}$, the set of zeros of x, and $N := \{P \in S(F/K) : v_P(x) < 0\}$, the set of poles of x. Then*

$$(x)_0 := \sum_{P \in Z} v_P(x) P \quad \text{, the zero divisor of } x,$$

$$(x)_\infty := \sum_{P \in N} (-v_P(x)) P \quad \text{, the pole divisor of } x,$$

$$(x) := (x)_0 - (x)_\infty = \sum_{P \in S(F/K)} v_P(x) P \quad \text{, the principal divisor of } x.$$

The nonzero constant elements of F are characterized by

$$x \in K \Longleftrightarrow (x) = 0.$$

We define $\mathrm{Prin}(F) := \{(x) : 0 \neq x \in F\}$, the *group of principal divisors*. $\mathrm{Prin}(F)$ is a subgroup of $\mathrm{Div}(F)$. The factor group $\mathrm{Cl}(F) := \mathrm{Div}(F) / \mathrm{Prin}(F)$ is known as the *divisor class group* or just the *class group* of F/K. We call elements $D_1, D_2 \in \mathrm{Div}(F)$ equivalent (written $D_1 \sim D_2$) if they belong to the same coset in $\mathrm{Cl}(F)$, i.e.

$$D_1 \sim D_2 \Longleftrightarrow D_1 = D_2 + (x), \, 0 \neq x \in F.$$

Definition A.11. *For a divisor $A \in \mathrm{Div}(F)$, set*

$$\mathcal{L}(A) := \{x \in F : (x) \geq -A\} \cup \{0\}$$

which is readily seen to be a finite-dimensional vector space over K and hence define

$$\dim A := \dim \mathcal{L}(A).$$

For $A_1, A_2 \in \mathrm{Div}(F)$, $A_1 \sim A_2$ implies that $\mathcal{L}(A_1) \cong \mathcal{L}(A_2)$ (as vector spaces). Also $\mathcal{L}(0) = K$, and $\mathcal{L}(A) = 0$ for $A < 0$. Moreover, if $A_1 \leq A_2$ then $\mathcal{L}(A_1) \subseteq \mathcal{L}(A_2)$ and $\dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \leq \deg A_2 - \deg A_1$.

If $A = A_+ - A_-$ with $A_+, A_- \geq 0$, then $\dim A \leq \deg A_+ + 1$. If $\deg A = 0$, then A is principal if and only if $\dim A = 1$. It can be derived that $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$ for $x \in F \setminus K$, and hence

$$\deg(x) = \deg((x)_0 - (x)_\infty) = \deg(x)_0 - \deg(x)_\infty = 0,$$

i.e. every principal ideal has degree 0, and it must have dimension 1.

Definition A.12. *The genus g of the function field F/K is defined by*

$$g := \max\{\deg A - \dim A + 1 : A \in \mathrm{Div}(F)\}.$$

Theorem A.13 (Riemann). *There is an integer c, depending on F/K, such that $\dim A = \deg A + 1 - g$ whenever $\deg A \geq c$.*

Definition A.14. *For $A \in \mathrm{Div}(F)$, let*

$$i(A) := \dim A - \deg A + g - 1$$

be the index of speciality of A.

The number $i(A)$ is a non-negative integer, and $i(A) = 0$ if $\deg A$ is sufficiently large, by Riemann's Theorem.

A.2 Extensions

Suppose F/K and F'/K' are algebraic function fields. We call F'/K' an algebraic extension of F/K if F'/F is an algebraic extension, and $K \subseteq K'$. The function field F'/K' is a constant field extension of F/K if $F' = FK'$. F'/K' is a finite extension of F/K if F'/F is a finite extension.

If $P \in S(F/K)$ and $P' \in S(F'/K')$, we say that P' lies over P (P' divides P, P' is an extension of P) if $P \subseteq P'$, and we denote this by $P'|P$.

Definition A.15 (Ramification index). *We call $e(P'|P)$ the ramification index of P' over P and it satisfies $e(P'|P) = e$ where $v_{P'}(x) = e \cdot v_P(x)$ for any $x \in F$. We call $P'|P$*

$$\begin{aligned} &\textit{ramified} && \textit{if} \quad e(P'|P) > 1, \\ &\textit{unramified} && \textit{if} \quad e(P'|P) = 1. \end{aligned}$$

Definition A.16 (Residue degree). *We call $f(P'|P)$ the residue degree or relative degree of P' over P and it satisfies*

$$f(P'|P) = [F'_{P'} : F_P] = \frac{[F'_{P'} : K'] \cdot [K' : K]}{[F_P : K]} = [K' : K] \frac{\deg P'}{\deg P}.$$

Theorem A.17. *Suppose F'/K' is a finite extension of F/K and $P \in S(F/K)$ a fixed place of F/K. If $P_1, ..., P_m$ are all the distinct places of F' lying over P, then*

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

Proof. A proof can be found in most standard texts, for example [27, III.1.11] or [25, I Par. 3 Prop. 10]. □

Definition A.18. *Let F'/K' be an algebraic extension of F/K. For a place $P \in S(F/K)$ we define its conorm (w.r.t. F'/F) by*

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P'.$$

We can extend this map in a natural way to a map

$$\mathrm{Con}_{F'/F} : \begin{cases} \mathrm{Div}(F) & \longrightarrow & \mathrm{Div}(F'), \\ \sum n_P \cdot P & \longmapsto & \sum n_P \cdot \mathrm{Con}_{F'/F}(P). \end{cases}$$

A property of the conorm which we will readily apply is its good behaviour in towers of function fields. For $F \subseteq F' \subseteq F''$ we have

$$\mathrm{Con}_{F''/F} = \mathrm{Con}_{F''/F'} \circ \mathrm{Con}_{F'/F},$$

which is essentially due to the transitivity of the ramification exponent $e(P'|P)$ in towers of function fields.

Theorem A.19. *Let F/K and F'/K' be algebraic function fields with F'/F a finite extension. Then for $A \in \mathrm{Div}(F)$,*

$$\deg \mathrm{Con}_{F'/F}(A) = \frac{[F' : F]}{[K' : K]} \cdot \deg A.$$

Proof. By linearity, it is sufficient to consider a prime divisor $A = P \in S(F/K)$. Then

$$\begin{aligned}
\deg \mathrm{Con}_{F'/F}(P) &= \deg \left(\sum\nolimits_{P'|P} e(P'|P) \cdot P' \right) \\
&= \sum\nolimits_{P'|P} e(P'|P) \cdot [F'_{P'} : K'] \\
&= \sum\nolimits_{P'|P} e(P'|P) \cdot \tfrac{[F'_{P'} : K]}{[K' : K]} \\
&= \tfrac{1}{[K' : K]} \sum\nolimits_{P'|P} e(P'|P) [F'_{P'} : F_P] [F_P : K] \\
&= \tfrac{1}{[K' : K]} \sum\nolimits_{P'|P} e(P'|P) f(P'|P) \deg P \\
&= \tfrac{[F' : F]}{[K' : K]} \cdot \deg P
\end{aligned}$$

by Theorem A.17. □

Appendix B

MAGMA computations

In this Appendix we will summarize the computations done using the MAGMA computational algebra package, version 2.10-14. For the computations done here, extensive use of MAGMA's algebraic geometry and algebraic function field packages was made.

B.1 Single extensions

In the next two propositions, a is a primitive element for $\mathbb{F}_8$.

Proposition B.1. *The function field given by the first step of the tower of Definition 5.1 has genus one and attains the Serre Bound.*

Proof.

```
>GF8<a>:= GF(8);
>F0<x0>:= RationalFunctionField(GF8);
>P0<x1>:= PolynomialRing(F0);
>F1<x1>:= FunctionField(x1^2+x1+x0+1+1/x0);
>#Places(F1,1);
14
>SerreBound(F1);
14
```

□

Proposition B.2. *Considering a single extension in the tower of Definition 5.1 over* $\mathbb{F}_8$, *each* $a_0 \in \mathbb{F}_8 \setminus \mathbb{F}_2$ *corresponds with exactly two possible choices of* $a_1 \in \mathbb{F}_8 \setminus \mathbb{F}_2$, *preserving these elements and implying that the places corresponding to them split completely in all extensions of the tower.*

Proof.

```
>A<x,y>:= AffineSpace(GF8,2);
>C := Curve(A, x*(y^2+y)+x^2+x+1);
>Points(C);
{@ (a, a), (a^6, a), (a^2, a^2), (a^5, a^2), (a, a^3), (a^6, a^3),
(a^3, a^4), (a^4, a^4), (a^3, a^5), (a^4, a^5), (a^2, a^6), (a^5, a^6)
@}
```

□

B.2 Completely splitting extensions

We now present a MAGMA function written to search for Artin-Schreier extensions over $\mathbb{F}_{p^n}$ which have good splitting behaviour, in the sense that a tower $\mathcal{F}$ constructed by means of such extensions will have $|T(\mathcal{F})| > 0$. The procedure `Split` takes p and n as parameters, and runs through a family of Artin-Schreier extensions over $\mathbb{F}_{p^n}$, listing those with good splitting behaviour and low genus. A more in-depth discussion of the approach taken is given in Section 5.4.

```
procedure Split(p,n);
  Fq<a> := GF(p^n);
  Fp := GF(p);
  PP<x,y> := PolynomialRing(Fp,2);
  P<x> := PolynomialRing(Fp);
  q := p^n;
  MaxDegree := 10;
  MaxValInf := -1;
  MinValInf := -10;
  LowestGenus := 1000;
  G := LowestGenus;
  A<x,y> := AffineSpace(Fq, 2);
  a1 := 0; a2 := 0; a3 := 0; a4 := 0; a5 := 0; a6 := 0; a7 := 0;
  a8 := 0; a9 := 0; a10 := 0; b1 := 0; b2 := 0; b3 := 0; b4 := 0;
  b5 := 0; b6 := 0; b7 := 0; b8 := 0; b9 := 0; b10 := 0;
  for
    a10 in [0..p-1], b10 in [0..p-1],
    a9 in [0..p-1],  b9 in [0..p-1],
    a8 in [0..p-1],  b8 in [0..p-1],
```

```
a7 in [0..p-1],  b7 in [0..p-1],
a6 in [0..p-1],  b6 in [0..p-1],
a5 in [0..p-1],  b5 in [0..p-1],
a4 in [0..p-1],  b4 in [0..p-1],
a3 in [0..p-1],  b3 in [0..p-1],
a2 in [0..p-1],  b2 in [0..p-1],
a1 in [0..p-1],  b1 in [0..p-1],
a0 in [0..p-1],  b0 in [0..p-1]
do
if ((b1 ne 0) or (b2 ne 0) or (b3 ne 0) or (b4 ne 0) or
    (b5 ne 0) or (b6 ne 0) or (b7 ne 0) or (b8 ne 0) or
    (b9 ne 0) or (b10 ne 0))
  then
  a<x> := a0+a1*x+a2*x^2+a3*x^3+a4*x^4+a5*x^5+a6*x^6+a7*x^7+
          a8*x^8+a9*x^9+a10*x^10;
  b<x> := b0+b1*x+b2*x^2+b3*x^3+b4*x^4+b5*x^5+b6*x^6+b7*x^7+
          b8*x^8+b9*x^9+b10*x^10;
  v := Degree(b,x)-Degree(a,x);
  if ((v le MaxValInf) and (v ge MinValInf) and
      (Degree(a,x) le MaxDegree) and
      (Degree(b,x) le MaxDegree))
    then
    C<x,y> := Curve(A, b*(y^p-y)-a);
    X := P[1] : P in Points(C);
    Y := P[2] : P in Points(C);
    XY := X meet Y;
    if (IsIrreducible(C)) then
      if (#Y ge 1) then
        if (Y subset X) then
          G := Genus(C);
          if ((G le LowestGenus) and (G ge 1)) then
            LowestGenus := G;
            ''Equation: y'',p,'' - y = a(x)/b(x) with '';
            ''a(x) = '',a;
            ''b(x) = '',b;
            Splitter := {<x,#{y : y in Fq [x, y] in C}> : x in X};
```

```
                ''Splitting of X : '', Splitter;
                ''Points : '',Points(C);
                ''v_inf(a/b)='',v,'', T ='',#(X),'',N(C)>='',
                  #Points(C),'',g(F)='',G;
                '' '';
              end if;
            end if;
          end if;
        end if;
      end if;
    end if;
  end for;
end procedure;
```

Note that some aspects of the search as done by `Split` can be customized. For example the allowable values at the infinite place of the rational function $f(x) = a(x)/b(x)$ can be set by changing `MinValInf` and `MaxValInf`, of which the default settings are to only allow $v_\infty(f) = -1$, thereby minimizing the different exponents in the Artin-Schreier extension.

An interesting case is running procedure `Split` with parameters $p = 2$ and $n = 3$ (i.e. over $\mathbb{F}_8$). This yields many possible extensions, of which the first one is

```
Equation: y^2 - y = a(x)/b(x) with
a(x) = x^2 + x + 1
b(x) = x
Splitting of X : { <a, 2>, <a^3, 2>, <a^5, 2>, <a^6, 2>, <a^4, 2>,
<a^2, 2> }
Points : {@ (a, a), (a^6, a), (a^2, a^2), (a^5, a^2), (a, a^3),
(a^6, a^3), (a^3, a^4), (a^4, a^4), (a^3, a^5), (a^4, a^5),
(a^2, a^6), (a^5, a^6) @}
v_inf(a/b)= -1 , T = 6 , N(F) >= 12 , g(F) = 1
```

This corresponds exactly to a typical extension of the tower $\mathcal{F}$ of Definition 5.1 and yields the splitting behaviour as shown in Proposition B.2. This example shows that `Split` can indeed find candidates for defining equations which may yield asymptotically good towers of function fields, and in particular finds the defining equation of the tower of Van der Geer and Van der Vlugt very quickly. Trial runs and results over fields other than $\mathbb{F}_8$ are discussed in Section 5.4.

List of Notation

$\mathbb{N}$ natural numbers

$\mathbb{Z}$ integers

$\mathbb{Q}$ rational numbers

$\mathbb{R}$ real numbers

$\mathbb{C}$ complex numbers

$\mathbb{F}_q$ finite field with $q = p^n$ elements, p prime

S_n symmetric group on n elements

$\lfloor a \rfloor$ integer part of the real number a

F/K algebraic function field of one variable

$\mathcal{O}$ valuation ring of F/K

$\mathcal{O}^\times$ group of units of $\mathcal{O}$

P place of F/K

$S(F/K)$ set of places of F/K

$\mathcal{O}_P$ valuation ring corresponding to the place P

v_P discrete valuation corresponding to the place P

F_P residue class ring $\mathcal{O}_P/P$ corresponding to P

$x(P)$ residue class of $x \in \mathcal{O}_P$ in F_P

$\mathrm{Div}(F)$ divisor group of F/K

$\mathrm{Prin}(F)$	group of principal divisors of F/K
$\mathrm{Cl}(F)$	divisor class group of F/K
$\mathcal{L}(A)$	space of functions associated with $A \in \mathrm{Div}(F)$
$\mathbb{A}_F$	adele space of F/K
$\mathbb{A}_F(A)$	adele space of F/K associated with $A \in \mathrm{Div}(F)$
Ω_F	module of Weil differentials of F/K
$\Omega_F(A)$	module of Weil differentials of F/K associated with $A \in \mathrm{Div}(F)$
(ω)	divisor of a nonzero Weil differential
W	canonical divisor
$P'\|P$	the place P' lies over the place P
$e(P'\|P)$	ramification index of P' over P
$f(P'\|P)$	residue degree of P' over P
$\mathcal{C}_P$	complementary module over $\mathcal{O}_P$
$d(P'\|P)$	different exponent of P' over P
$\mathrm{Diff}(F'/F)$	different divisor of F'/F
$\mathrm{Tr}_{F'/F}$	trace map from F' to F
$\mathrm{N}_{F'/F}$	norm map from F' to F
$\mathrm{Cotr}_{F'/F}$	cotrace of a Weil differential $\omega \in \Omega_F$
$\mathrm{Con}_{F'/F}$	conorm of a place or divisor in F'/F
$N(F)$	$\#\{P \in S(F/K) : \deg P = 1\}$
$N_q(g)$	$\max\{N(F) : F/K$ is a function field over $\mathbb{F}_q$, $g(F/K) = g\}$
$A(q)$	$\limsup_{g\to\infty} N_q(g)/g$
$V(\mathcal{F})$	the ramification locus of the tower $\mathcal{F}$
$T(\mathcal{F})$	the places of degree one in F_1 in $\mathcal{F} = (F_1, F_2, ...)$ which are completely splitting

References

[1] S. Ballet. Curves with many points and multiplication complexity in any extension of $\mathbf{F}_q$. *Finite Fields Appl.*, 5(4):364–377, 1999.

[2] V. Deolalikar. *On splitting places of degree one in extensions of algebraic function fields, towers of function fields meeting asymptotic bounds, and basis constructions for algebraic-geometric codes.* PhD thesis, University of Southern California, Los Angeles, May 1999.

[3] V. Deolalikar. Extensions of algebraic function fields with complete splitting of all rational places. *Comm. Algebra*, 30(6):2687–2698, 2002.

[4] N. D. Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 189–198. Birkhäuser, Basel, 2001.

[5] O. Endler. *Valuation theory.* Springer-Verlag, New York, 1972.

[6] A. Frölich and M. Taylor. *Algebraic Number Theory.* Cambridge 27, 1991.

[7] R. Fuhrmann, A. García, and F. Torres. On maximal curves. *J. Number Theory*, 67(1):29–51, 1997.

[8] R. Fuhrmann and F. Torres. The genus of curves over finite fields with many rational points. *Manuscripta Math.*, 89(1):103–106, 1996.

[9] A. García and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Invent. Math.*, 121(1):211–222, 1995.

[10] A. García and H. Stichtenoth. Asymptotically good towers of function fields over finite fields. *C. R. Acad. Sci. Paris Sér. I Math.*, 322(11):1067–1070, 1996.

[11] A. García and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996.

[12] A. García, H. Stichtenoth, and H-G. Rück. On tame towers over finite fields. *J. Reine Angew. Math.*, 557:53–80, 2003.

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

[14] V.D. Goppa. Codes on algebraic curves. *Sov. Math. Dokl.*, 24:170–172, 1981.

[15] Y. Ihara. Congruence relations and Shimura curves. *J. Fac. Sci. Univ. Tokyo*, 25:301–361, 1979.

[16] G. Korchmáros and F. Torres. On the genus of a maximal curve. *Math. Ann.*, 323(3):589–608, 2002.

[17] S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970.

[18] S. Lang. *Algebra.* Springer-Verlag, New York, 2002.

[19] P.J. McCarthy. *Algebraic Extensions of Fields.* Dover Publications, 1991.

[20] H. Niederreiter and C. Xing. Towers of global function fields with asymptotically many rational places and an improvement of the Gilbert-Varshamov bound. *Math. Nachr.*, 195:171–186, 1998.

[21] H. Niederreiter and C. Xing. Curve sequences with asymptotically many rational points. In *Applications of curves over finite fields (Seattle, WA, 1997)*, volume 245 of *Contemp. Math.*, pages 3–14. Amer. Math. Soc., Providence, RI, 1999.

[22] H. Niederreiter and C. Xing. *Rational Points on Curves over Finite Fields, Theory and Applications.* Cambridge University Press, 2001.

[23] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

[24] R. Schoof. Algebraic curves and coding theory. *Lecture Notes*, 1990.

[25] J.P. Serre. *Local Fields.* Springer-Verlag, 1979.

[26] J.P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur in corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.

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

[28] H. Stichtenoth. Explicit constructions of towers of function fields with many rational places. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 219–224. Birkhäuser, Basel, 2001.

[29] F. J. Sullivan. p-torsion in the class group of curves with too many automorphisms. *Arch. Math.*, 26:253–261, 1975.

[30] M.A. Tsfasman, S.G. Vlăduţ, and Th. Zink. On Goppa codes which are better than the Varshamov-Gilbert bound. *Math. Nachrichten*, 109:21–28, 1982.

[31] G. van der Geer. Curves over finite fields and codes. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 225–238. Birkhäuser, Basel, 2001.

[32] G. van der Geer and M. van der Vlugt. An asymptotically good tower of curves over the field with eight elements. *Bull. London Math. Soc.*, 34(3):291–300, 2002.

[33] G. van der Geer and M. van der Vlugt. Tables of curves with many points, August 2003. Available at `http://www.science.uva.nl/~geer/`.

[34] A. B. van der Merwe. Towers of global function fields with asymptotically many rational places. 2003. Preprint.

[35] S.G. Vlăduţ and V.G. Drinfeld. Number of points of an algebraic curve. *Funct. Anal.*, 17:68–69, 1983.

[36] T. Zink. Degeneration of Shimura surfaces and a problem in coding theory. *Fundamentals of Computation Theory*, 199:503–511, 1985.