



UNIVERSITEIT • STELLENBOSCH • UNIVERSITY

On towers of function fields over finite fields

by

Ernest Christiaan Lötter

*Dissertation presented at the University of
Stellenbosch for the degree of*



Doctor of Philosophy

Department of Mathematical Sciences
University of Stellenbosch
Private Bag X1, 7602 Matieland, South Africa

Promoter: Prof B.W. Green
Department of Mathematical Sciences
University of Stellenbosch

March 2007

Copyright © 2007 University of Stellenbosch
All rights reserved.

Declaration

I, the undersigned, hereby declare that the work contained in this dissertation 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.

Signature:

E. C. Lötter

Date:

Abstract

On towers of function fields over finite fields

E. C. Lötter

Department of Mathematical Sciences

University of Stellenbosch

Private Bag X1, 7602 Matieland, South Africa

Dissertation: PhD (Mathematics)

March 2007

Explicit towers of algebraic function fields over finite fields are studied by considering their ramification behaviour and complete splitting. While the majority of towers in the literature are recursively defined by a single defining equation in variable separated form at each step, we consider towers which may have different defining equations at each step and with arbitrary defining polynomials.

The ramification and completely splitting loci are analysed by directed graphs with irreducible polynomials as vertices. Algorithms are exhibited to construct these graphs in the case of n -step and \sim -finite towers.

These techniques are applied to find new tamely ramified n -step towers for $1 \leq n \leq 3$. Various new tame towers are found, including a family of towers of cubic extensions for which numerical evidence suggests that it is asymptotically optimal over the finite field with p^2 elements for each prime $p \geq 5$. Families of wildly ramified Artin-Schreier towers over small finite fields which are candidates to be asymptotically good are also considered using our method.

Uittreksel

On towers of function fields over finite fields

E. C. Lötter

Departement Wiskundige Wetenskappe

Universiteit van Stellenbosch

Privaatsak X1, 7602 Matieland, Suid Afrika

Proefskrif: PhD (Wiskunde)

Maart 2007

Eksplisiete torings van algebraïese funksieliggame oor eindige liggame word met behulp van hulle vertakking- en splitsinggedrag bestudeer. Terwyl die meerderheid van torings in die literatuur rekursief gedefinieer word deur 'n enkele definiërende vergelyking in veranderlike geskeide vorm by elke stap, oorweeg ons torings wat verskillende definiërende vergelykings by elke stap en arbitrêre definiërende polinome kan hê.

Die vertakking- en gehele splitsingslokusse is ondersoek deur gerigte grafieke met onherleibare polinome as nodusse. Algoritmes om hierdie grafieke te konstrueer vir n -stap en \sim -eindige torings word geïllustreer.

Hierdie tegnieke word toegepas om nuwe mak-vertakte n -stap torings te vind vir $1 \leq n \leq 3$. Verskeie nuwe mak torings word gevind, insluitend 'n familie torings van kubiese uitbreidings waarvoor numeriese berekenings voorstel dat dit asimptoties optimaal is oor die eindige liggaam met p^2 elemente vir elke priemgetal $p \geq 5$. Families van wild-vertakte Artin-Schreier torings oor klein eindige liggame wat kandidate is om asimptoties goed te wees word ook op hierdie manier bestudeer.

Acknowledgements

I would like to express my profound gratitude to my advisor, Professor Barry Green, for his support and encouragement during the course of my studies. His guidance and useful suggestions was of immense value.

From 2004 to 2006 I was financially supported by Postgraduate Merit bursaries of the University of Stellenbosch and an NRF/DoL Scarce Skills scholarship. The support of the National Research Foundation is hereby acknowledged.

I thank the Department of Mathematical Sciences at the University of Stellenbosch for the employment opportunities extended to me as research assistant and lecturer during the past few years.

These acknowledgements will not be complete without mentioning some of my family and friends whose support was indispensable. Firstly, to my parents: thank you for your patience and support during the time of writing this dissertation, as well as your encouragement throughout my student years. This would not have been possible without you.

I would like to thank the support of my friends, especially my Tassies housemates Christoph Sonntag, Gerhard Venter and Warnich Rust.

Of great value to me also is the encouragement of my grandparents, the support of my brother Frederik and sister Karin, as well as the keen interest of my parents-in-law in my work.

It is not possible to fully express my gratitude to my wife Anelda in the little space available here, but in particular I am thankful for her love and support, as well as her patience especially during the final stages of completing this manuscript.

Contents

Declaration	ii
Abstract	iii
Uittreksel	iv
Contents	vi
1 Introduction	1
2 Definitions	9
2.1 Towers and limits	9
2.1.1 Ramification	12
2.1.2 Complete splitting	15
2.2 Explicit construction	17
2.3 Transforming equations	21
3 Finite ramification	24
3.1 Identifying a finite ramification locus	28
3.2 Ramification-generating sets	34
3.3 Ramification inheritance	36
3.4 Ramification graphs	40
4 Complete splitting	51
4.1 Successor polynomials	52
4.2 Complete splitting graph	55

<i>CONTENTS</i>	vii
4.3 Splitting characteristic polynomials	64
5 Algorithms	72
5.1 Finite ramification	73
5.1.1 Predecessor polynomials	74
5.1.2 Ramification-generating polynomial sets	75
5.1.3 Ramification locus	77
5.2 Complete splitting	81
5.2.1 Successor polynomials	82
5.2.2 Computing \mathbb{F}_r	83
5.3 Tame ramified towers	88
5.3.1 n -step towers	89
5.3.2 \sim -finite towers	90
6 Applications	91
6.1 Tame towers	92
6.1.1 Towers of Fermat type	92
6.1.2 Towers of Kummer extensions	93
6.1.3 Multi-step towers	114
6.2 Wild towers	120
7 Conclusions	126
A Magma program code	129
B Supplemental graphs	140
List of Notation	146
List of Figures	147
List of Algorithms	149
Bibliography	150
Index	157

Chapter 1

Introduction

An algebraic function field in one variable over the field K is a finite algebraic extension field $F \supseteq K(x)$ where x is transcendental over K . When K is a finite field \mathbb{F}_q for some power of a prime p , we refer to such a function field as a global field.

As a one to one correspondence exists between algebraic function fields and non-singular projective curves, many geometric concepts can be transferred to the algebraic context and vice versa. Covers of algebraic curves correspond to extensions of algebraic function fields, whereas ramification in the context of curves have a natural equivalent in the function field case. The celebrated Riemann-Roch theorem has equivalent statements for curves and function fields, and in both cases implicitly define the invariant known as the genus. Similarly places of degree one in an algebraic function field over K can be counted, which can be compared with their natural counterparts in the context of algebraic curves: the set of K -rational points of the curve.

In this dissertation, we will stay in the domain of global function fields. For such an algebraic function field over \mathbb{F}_q , the Hasse-Weil bound [69] gives upper and lower bounds for the number $N(F/\mathbb{F}_q)$ of places of degree one of the function field F/\mathbb{F}_q in terms of the genus $g(F/\mathbb{F}_q)$ by

$$|N(F/\mathbb{F}_q) - (q + 1)| \leq 2 \cdot g(F/\mathbb{F}_q) \cdot q^{1/2}, \quad (1.1)$$

which was improved by Serre by replacing the right-hand side of (1.1) by $g(F/\mathbb{F}_q) \cdot \lfloor 2q^{1/2} \rfloor$. The Hasse-Weil bound makes it clear that the upper bound can only be reached if q is a square. It was independently noticed by Ihara [41] and Manin [48] (for $q = 2$) that the number of places of degree one cannot achieve the upper bound implied by (1.1) when the genus is large relative to the cardinality of the field \mathbb{F}_q , in particular that $2 \cdot g(F/\mathbb{F}_q) \leq q - q^{1/2}$. Various lower bounds and exact values of $N_q(g)$, denoting the maximum number of places of degree one which can occur in a global field of genus g , are listed in the tables of Van der Geer and Van der Vlugt [66].

If we define $A(q)$ to equal $\limsup_{g \rightarrow \infty} N_q(g) / g$, Serre's bound implies that $A(q) \leq \lfloor 2q^{1/2} \rfloor$. Ihara's work was refined to an asymptotic result by Drinfeld and Vladut [68] that $A(q) \leq q^{1/2} - 1$, known as the Drinfeld-Vladut bound.

Goppa [38] introduced the first error-correcting codes using algebraic geometry by associating an error-correcting code with a linear system on an algebraic curve over a finite field. Tsfasman, Vladut and Zink [63] then showed the existence of sequences of codes for which the transmission rate and relative distance exceed the Gilbert-Varshamov bound.

This revived interest in constructing sequences of function fields $(F_i)_{i \geq 0}$ so that each extension F_{i+1}/F_i for $i \geq 0$ is separable, each F_i has full constant field \mathbb{F}_q and that $\lim_{i \rightarrow \infty} N(F_i/\mathbb{F}_q) / g(F_i/\mathbb{F}_q)$ (which we denote by $\lambda(\mathcal{F})$ for $\mathcal{F} := \bigcup_{i=0}^{\infty} F_i$) is positive. We refer to \mathcal{F} as a tower of function fields over \mathbb{F}_q . The nonnegative real number $\lambda(\mathcal{F})$ is bounded from above by the Drinfeld-Vladut bound.

While various methods exist for obtaining lower bounds for $A(q)$ for various q , many of these were non-explicit in the sense that the sequence $(F_i)_{i \geq 0}$ could not be characterised by a sequence of explicit polynomial equations characterizing each extension F_{i+1}/F_i . Ihara [40] showed in 1979 that $A(q^2) = q - 1$ for each prime power q using a sequence of modular curves, implying that the Drinfeld-Vladut bound can be met for towers over fields of square cardinality. Serre [56] showed that $A(q)$ is positive for each q by exhibiting a general, but weak lower bound. Xing

and Niederreiter [50], [51] improved these lower bounds using class field towers and narrow ray class fields for various q . Zink [72] showed that $A(p^3) \geq 2(p^2 - 1) / (p + 2)$ when p is a prime.

In 1995, García and Stichtenoth [29] showed that $A(q^2) = q - 1$ for each prime power q by exhibiting an explicit sequence of defining polynomials which give rise to a tower meeting the Drinfeld-Vladut bound. This motivated the study of explicit towers of function fields, leading to a subtower with simpler equations by García and Stichtenoth [31]. García, Stichtenoth and Thomas [37] exhibited asymptotically good towers of Kummer extensions over every nonprime finite field, meeting the Drinfeld-Vladut bound over some small finite fields. Elkies [21] showed that many of these towers are modular, and conjectured that in fact all asymptotically maximal towers are modular.

The first explicit tower over a field of nonsquare cardinality coming close to the Drinfeld-Vladut bound was the construction of Van der Geer and Van der Vlugt [64] of a tower over \mathbb{F}_8 which meets Zink's bound [72]. This was generalized by Bezerra, Garcia and Stichtenoth [12] to an explicit sequence of non-Galois extensions (for $q > 2$) over \mathbb{F}_{q^3} attaining a generalization of Zink's bound, $A(q^3) \geq 2(q^2 - 1) / (q + 2)$, for any prime power q .

Most of the constructions mentioned so far involved wildly ramified towers, in many cases making the computation of the limit $\lambda(\mathcal{F})$ difficult. Asymptotically good wildly ramified towers have been constructed over fields of square and cubic cardinality, it is however unknown whether any with good limit is possible over fields of quintic or higher prime degree over the prime subfield.

García, Stichtenoth and Rück [36] returned to the case of tamely ramified towers of quadratic extensions in odd characteristic. They studied various towers, amongst those an interesting asymptotically optimal tower with splitting behaviour related to Deuring's polynomial.

In this thesis, we consider arbitrary towers where different defining equations can be utilized at each step. This is a more general context than

the usual case (e.g. in the constructions above) where the same defining polynomial is used in each step of the tower. Although in many cases the steps of such a one-step tower can be refined into smaller steps (for example the Bezerra-García-Stichtenoth tower [12]), our method assumes explicitly known equations for the (distinct) substeps.

We construct directed graphs which are more convenient for explicit calculations than those in [5] in order to study the ramification structure and complete splitting of the tower. As a result, we exhibit algorithms which can, given the explicit equations for each step of a multi-step tower, find a ramification locus and completely splitting locus for such a tower.

These algorithms were implemented in the Magma computer algebra system [13] in order to allow us to perform numerical experiments by finding ramification and complete splitting loci for various candidate equations defining steps in towers. As computer aided studies of one-step towers of quadratic extensions have been performed for various small, odd characteristic by Li, Maharaj, Stichtenoth and Elkies [45] as well as Maharaj and Wulftange [47] using the KASH computer algebra system, we focus on the computationally more difficult family of towers consisting of cubic or higher degree extensions of constituent function fields.

Various new tamely ramified towers are exhibited, and graphs are used to describe their ramification and complete splitting structure. As our method is also applicable to wildly ramified towers, we use a classification theorem of Beelen, García and Stichtenoth [10] to compute families of defining polynomials for Artin-Schreier towers of small degree.

We now give a survey of the remaining chapters:

In **Chapter 2**, definitions and an overview of the basic properties of towers of algebraic function fields are given, focusing on the case of explicit towers where the defining equation at each step is known. We introduce equivalence relations on the indeterminates of these equations which can be extended to the defining equations themselves, which are useful when constructing graphs in Chapters 3 and 4. We conclude the chapter by considering transformations of defining polynomials of towers.

Chapter 3 considers the problem of determining whether a tower has a finite ramification locus. We note that a place of the function field F_0 is ramified in a tower \mathcal{F} if there exists some step F_i of the tower so that the place is ramified in F_i/F_0 . Determining a (finite) ramification locus can now be seen as determining the possibilities for ramification occurring in the extension F_i/F_{i-1} for each $i \geq 1$, which allows us to consider only the residue classes at each step of the (algebraic closure of) the tower where the defining polynomial of the extension yields repeated roots.

This process is started with the introduction of reciprocal polynomials in Definition 3.3, handling the case of a repeated root of an equation $f(x, y) = 0$ where either $x = \infty$ or $y = \infty$ (or both).

The idea of finding a finite subset of $\overline{\mathbb{F}} \cup \{\infty\}$ which captures ramification in the sense of Definition 3.5 for a single-step tower is not new, but here the process is generalized for an arbitrary explicit tower. In some cases, the splitting of the place at infinity of the rational function field must be carefully considered, as some repeated roots may actually be completely splitting places (for example, the infinite place splitting completely in Example 2.20).

In Proposition 3.6 it is then formally shown that a bounded ramification-capturing sequence, even if it contains elements corresponding to unramified places, results in a finite ramification locus. Identifying these superfluous elements helps to improve the lower bounds on $\lambda(\mathcal{F})$ which we obtain.

In Definition 3.9 we replace sequences of subsets of $\overline{\mathbb{F}} \cup \{\infty\}$ by directed graphs in monic irreducible polynomials in x_i (and the function $\frac{1}{x_i}$) for each $i \geq 0$, where i corresponds to the relevant step in the tower. In this way we obtain the \mathbb{F}_l -splitting graph Γ for an explicit tower, using the defining polynomial at each step. While the graphs in [5] consider the case of one-step towers and having vertex set $\overline{\mathbb{F}} \cup \{\infty\}$, our approach is more general as it allows arbitrary towers with different defining polynomials at each step generalising the one-step case, and uses polynomials in x_i (and $\frac{1}{x_i}$) as vertices in step i of the tower. This allows efficient calculations using Theorem 3.10 showing that we can employ a Gröbner basis approach in

most cases using the notion of retrospective *predecessor polynomials*. These relate the possible residue classes of places in the function field F_i at step i of a tower if we know the possible residue classes of places of the function field F_{i+1} at step $i + 1$. When the set of such possibilities is finite for the initial (rational) function field F_0 , Theorem 3.19 implies that the tower has a finite ramification locus.

The predecessor polynomials recursively computed in this way using polynomials with repeated roots as generators naturally lead to the \mathbb{F}_l -ramification graph Γ_B , a subgraph of Γ which corresponds to those places which are ramified in the tower. As an analogue to Theorem 3.19, the graph Γ_B enables us to deduce that the tower has a finite ramification locus by considering whether the vertices in x_0 of Γ_B is a finite set.

The chapter is concluded with an example of a representation of a ramification graph for a two-step tower of Kummer extensions

In **Chapter 4** we study the existence of places of degree one which split completely in the tower. The *successor polynomials*, a prospective analogue of predecessor polynomials, are introduced. As we define successor polynomials in terms of predecessors, they have the same convenient computational properties using Gröbner bases.

We note that if we consider the subgraph of Γ which does not contain any vertices of Γ_B , each place corresponding to an element of this subgraph must correspond to a place which is completely splitting. However, we do not restrict this to places of degree one, and rather choose to extend the field of definition of the function field to a convenient field to ensure that the necessary places are of degree one to ensure complete splitting. We refer to this subgraph of Γ as Γ_T , the complete \mathbb{F}_l -splitting graph of the tower \mathcal{F} . At this point in our analysis, we have partitioned the graph Γ into subgraphs Γ_B and Γ_T , where all ramification is guaranteed to occur inside Γ_B .

Proposition 4.5 and Theorem 4.6 underlines the importance of finding at least one connected component Γ_T^* of Γ_T with degree boundedness, a property described by considering whether the sets $\mathcal{A}(\Gamma_T^*, i)$ is finite for at least one (and hence all) $i \geq 0$. When this occurs, the degree of all

polynomials occurring as vertices in Γ_T^* is bounded, ensuring that there exists a finite extension of \mathbb{F}_l so that the tower will be completely splitting over the relevant field.

In Section 4.3 it is shown that if we can find a polynomial which is “self-successive”, even when computing its successor polynomial more than once in a recursive manner for an n -step tower, one can show that the tower splits completely, with splitting locus corresponding to the zeros of that polynomial. Many known examples, e.g. the Van der Geer/Van der Vlugt tower [65] falls into this category and their complete splitting can be described in terms of a single self-successive polynomial. In Corollary 4.13 this result is shown to hold even if more than one connected component of Γ_T has the degree boundedness property.

Chapter 5 serves as a description of pseudocode algorithms derived from the results in Chapters 3 and 4. These include the calculation of predecessor and successor polynomials, constructing ramification-generating sets of functions. Finally, algorithms are given to determine (if they exist) a finite ramification locus and complete splitting locus of a one-step tower, an n -step tower and a \sim -finite tower.

In **Chapter 6** we use an implementation of the algorithms of Chapter 5 in the Magma computer algebra system to enable us to perform computations on a large scale. We focus on the case of tamely ramified towers of one-step towers. As an extensive computational study of equations for towers of extensions of degree two and odd characteristic has been made in [45] and [47], we focus on obtaining explicit equations for higher degree.

Amongst others, we find an asymptotically optimal family of explicit towers of cubic extensions over \mathbb{F}_{p^2} (for $p \geq 5$) where the places which split completely are described using a polynomial with the Franel numbers as coefficients. This is interesting to compare with the optimal tower of García, Stichtenoth and Rück in [36] where the places which split completely are described by a polynomial with the coefficients of Deuring’s polynomial as coefficients.

Various other examples of tame one-step towers of small degree are given with their corresponding representations of subgraphs of interest of

Γ_B and Γ_T . While no examples of more than one disconnected component of Γ_T yielding completely splitting places over a finite extension of \mathbb{F}_l could be found using computer search, examples of Γ_B being disconnected do appear in concrete examples. The case for Γ_T is related to a question posed in [36] considering whether one place which splits completely in the set Ω (see page 59) has each element in Ω as successor.

We further consider simple examples of two-step and three-step towers where some cycle of defining polynomials are used to define the tower. Their ramification and complete splitting structure are analysed using the algorithms from Chapter 5, and described using ramification graphs.

A classification theorem by Beelen, García and Stichtenoth gives a set form for defining polynomials of one-step Artin-Schreier towers over a given finite field. In particular, over the finite field with two elements this gives rise to four wildly ramified towers of function fields, of which three are known to be asymptotically good. We show that if the fourth is asymptotically good, it must be defined over a finite field of cardinality exceeding 2^{25} .

Appendix A lists some of our Magma program code with which many of the numerical experiments and tower analysis was done, while **Appendix B** lists some graphs which were too unwieldy for the main text.

Chapter 2

Definitions

2.1 Towers and limits

In this section, some definitions and properties of towers are stated, after the exposition given in [36].

Definition 2.1 (Tower of function fields) *A tower of function fields over \mathbb{F}_q is an extension field $\mathcal{F} \supseteq \mathbb{F}_q$ such that (i) \mathcal{F}/\mathbb{F}_q has transcendence degree one, (ii) \mathbb{F}_q is algebraically closed in \mathcal{F} and (iii) \mathcal{F}/\mathbb{F}_q is not finitely generated.*

We usually denote such a tower by calligraphic capital letters, i.e. \mathcal{F} over \mathbb{F}_q , \mathcal{F}/\mathbb{F}_q or, if the context is clear, just \mathcal{F} .

By $F < \mathcal{F}$ we mean that $\mathbb{F}_q \subseteq F \subseteq \mathcal{F}$, where F is a finitely generated field extension of \mathbb{F}_q of transcendence degree one, contained in \mathcal{F} . We call a tower *separable* if, for some $F < \mathcal{F}$, the (infinite) extension \mathcal{F}/F is separable.

Definition 2.2 (Representation of tower) *Let \mathcal{F} be a tower. The infinite sequence $(F_i)_{i \geq 0}$ of function fields $F_i < \mathcal{F}$ is a representation of \mathcal{F} if the function fields form an ascending chain $(F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots)$ and $\bigcup_{i=0}^{\infty} F_i = \mathcal{F}$.*

As \mathbb{F}_q is algebraically closed in \mathcal{F} , it is algebraically closed inside each of the F_i , for any representation $(F_i)_{i \geq 0}$ of \mathcal{F} .

Remark 2.3 Using the characterization of separable towers from [36, Lemma 2.3], one finds that every separable tower \mathcal{F}/\mathbb{F}_q can be represented by a sequence $(F_i)_{i \geq 0}$ of algebraic function fields such that

- (i) each F_i has full constant field \mathbb{F}_q ,
- (ii) each extension F_{i+1}/F_i for $i \geq 0$ is a separable extension and
- (iii) $\lim_{i \rightarrow \infty} g(F_i/\mathbb{F}_q) = \infty$.

In fact, it is easily seen that any sequence $(F_i)_{i \geq 0}$ with the properties noted in Remark 2.3 generates a separable tower $\mathcal{F} := \bigcup_{i \geq 0} F_i$. Because of this, we refer to the sequence $(F_i)_{i \geq 0}$ with the above properties itself as a (separable) tower as well, when convenient.

In the following definitions we describe the first asymptotic properties of towers:

Definition 2.4 Let \mathcal{F} be a tower, and F some function field with $F < \mathcal{F}$. Let $(F_i)_{i \geq 0}$ be a representation of \mathcal{F} with $F_0 = F$. The F -splitting rate of \mathcal{F} is

$$\nu_F(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{N(F_i/\mathbb{F}_q)}{[F_i : F]} \quad (2.1)$$

where $N(F_i/\mathbb{F}_q)$ is the number of places of degree one (rational places) of F_i/\mathbb{F}_q , and the F -genus rate of \mathcal{F} is

$$\gamma_F(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{g(F_i/\mathbb{F}_q)}{[F_i : F]} \quad (2.2)$$

where $g(F_i/\mathbb{F}_q)$ is the genus of F_i/\mathbb{F}_q .

The F -splitting rate and F -genus rate of a tower \mathcal{F} exists, and is independent of the choice of representation $(F_i)_{i \geq 0}$, by [36, Proposition 2.4 and Proposition 2.16].

Definition 2.5 (Limit of a separable tower) *The limit of the separable tower \mathcal{F} is defined to be the real number*

$$\lambda(\mathcal{F}) := \frac{\nu_F(\mathcal{F})}{\gamma_F(\mathcal{F})}, \quad (2.3)$$

which is independent of the choice of function field $F < \mathcal{F}$.

It follows that for a separable tower \mathcal{F} , $\lambda(\mathcal{F})$ can be found by choosing any representation $(F_i)_{i \geq 0}$ of \mathcal{F} , and then computing

$$\lambda(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{N(F_i/\mathbb{F}_q)}{g(F_i/\mathbb{F}_q)}.$$

Theorem 2.6 *Suppose \mathcal{F} is a separable tower over \mathbb{F}_q . Then*

$$0 \leq \lambda(\mathcal{F}) \leq q^{1/2} - 1. \quad (2.4)$$

Proof. The left-hand inequality is obvious, the right-hand one is the Drinfeld-Vladut bound, see [68]. ■

Definition 2.7 (Asymptotically good and bad towers) *The tower \mathcal{F} is called asymptotically good if $\lambda(\mathcal{F}) > 0$, otherwise it is asymptotically bad.*

It is clear from (2.3) that a tower is asymptotically good if and only if $\nu_F(\mathcal{F}) > 0$ and $\gamma_F(\mathcal{F}) < \infty$. It is possible to define the quantity

$$A(q) := \sup_{\mathcal{F}/\mathbb{F}_q} \lim_{i \rightarrow \infty} \frac{N(F_i/\mathbb{F}_q)}{g(F_i/\mathbb{F}_q)}$$

which denotes the maximal possible limit that a tower over a fixed finite field \mathbb{F}_q can achieve. As an trivial consequence of this definition we can rewrite (2.4) as

$$0 \leq \lambda(\mathcal{F}) \leq A(q) \leq q^{1/2} - 1. \quad (2.5)$$

Due to this, we can make two additions to Definition 2.7 in the form of the following definition:

Definition 2.8 (Asymptotically optimal and maximal towers) *The tower \mathcal{F} is called asymptotically optimal if $\lambda(\mathcal{F}) = A(q)$. The tower \mathcal{F} is asymptotically maximal if it is asymptotically optimal and $A(q) = q^{1/2} - 1$.*

It was shown by Serre [57] that $A(q) > 0$ for every prime power q . Ihara [40] showed that if q is a square, the Drinfeld-Vladut bound is attained, i.e. $A(q) = q^{1/2} - 1$, although a tower attaining this may not be explicit. García and Stichtenoth [29] later constructed an explicit¹ tower over every finite field of square cardinality for which this holds. In other words, there exist explicit asymptotically maximal towers over every finite field of square cardinality.

The value of $A(q)$ is therefore known in the case of square q . Various lower bounds have been calculated for other possible values of q , in particular $A(p^3) \geq \frac{2(p^2-1)}{p+2}$ for a prime p by Zink [72], later generalized to $A(q^3) \geq \frac{2(q^2-1)}{q+2}$ for any power of a prime p by Bezerra, García and Stichtenoth [12]. Serre [56] showed that $96 \cdot A(q) > \log_2 q$ for all prime powers q using Hilbert class field towers. For prime fields, it is known that $A(2) \geq \frac{97}{376}$ due to Xing and Yeo [71], and $A(3) \geq \frac{8}{17}$, $A(5) \geq \frac{8}{11}$ due to Anglès and Maire [2] and Temkine [61]. A summary of known lower bounds for general $A(q)$ can be found in [52].

From this point onward, we assume that all towers are separable, unless stated otherwise.

Definition 2.9 *Suppose \mathcal{E} and \mathcal{F} are towers over \mathbb{F}_q , and $\mathcal{E} \subseteq \mathcal{F}$. Then we call \mathcal{E} a subtower of \mathcal{F} .*

It is shown in [31] that if \mathcal{E} is a subtower of \mathcal{F} , then $\gamma_{\mathcal{F}}(\mathcal{E}) \leq \gamma_{\mathcal{F}}(\mathcal{F})$, and as a result $\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$.

2.1.1 Ramification

Definition 2.10 (Ramified tower) *Let \mathcal{F} be a tower over \mathbb{F}_q .*

¹See Section 2.2.

1. \mathcal{F} is called *totally ramified*, if for some $F < \mathcal{F}$ there exists $P \in S(F/\mathbb{F}_q)$ which is totally ramified in each E/F with $F \subset E < \mathcal{F}$.
2. \mathcal{F} is called *tamely ramified*, if for some $F < \mathcal{F}$ all extensions E/F with $F \subset E < \mathcal{F}$ are tamely ramified (all ramification degrees are relatively prime to q).
3. Otherwise, the tower is called *wildly ramified*².

Definition 2.11 (F -ramification locus) Let \mathcal{F} be a tower over \mathbb{F}_q . We define the F -ramification locus of \mathcal{F} as

$$V_F(\mathcal{F}) := \{P \in S(F/\mathbb{F}_q) \mid P \text{ is ramified in } E/F \text{ for some } E < \mathcal{F}\}$$

where we denote by $S(F/\mathbb{F}_q)$ the set of places of the function field F/\mathbb{F}_q .

We say a tower \mathcal{F} is of *finite ramification type* if there exists a function field $F < \mathcal{F}$ such that $V_F(\mathcal{F})$ is a finite set. If \mathcal{F}/E and \mathcal{F}/F are both separable, then $V_E(\mathcal{F})$ is a finite set if and only if $V_F(\mathcal{F})$ is a finite set (see [36, Lemma 2.13]).

We recall the notation $d(Q|P)$ for the different exponent of the place Q lying above the place P . For an exposition, we refer to [59, III.4]. The following result gives an effective bound on the F -genus rate of \mathcal{F} given some conditions on the tower, and was shown by Van der Merwe [67].

Theorem 2.12 Let \mathcal{F} be a tower over \mathbb{F}_q of finite ramification type, and choose some $F < \mathcal{F}$. Suppose further that for each $P \in S(F/\mathbb{F}_q)$, there exists a non-negative real constant a_P such that for all E/F , each $Q \in S(E/\mathbb{F}_q)$ with $Q|P$, we have that $a_P \geq \frac{d(Q|P)}{e(Q|P)}$. Then the F -genus rate of \mathcal{F} is finite, with

$$\gamma_F(\mathcal{F}) \leq g(F) - 1 + \frac{1}{2} \sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P.$$

²The unramified case is impossible, as the definition of a tower requires some ramification to occur.

Proof. Suppose E is some extension of F , contained in \mathcal{F} . As $V_F(\mathcal{F})$ is finite, and the different divisor involves only places lying over ramified places, the following equations involve only finite sums:

$$\begin{aligned} \deg \text{Diff}(E/F) &= \sum_{P \in V_F(\mathcal{F})} \left(\sum_{Q|P, Q \in S(E/\mathbb{F}_q)} d(Q|P) \cdot \deg Q \right) \\ &\leq \sum_{P \in V_F(\mathcal{F})} \left(\sum_{Q|P, Q \in S(E/\mathbb{F}_q)} a_P \cdot e(Q|P) \cdot \deg Q \right) \\ &= [E : F] \cdot \sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P, \end{aligned}$$

by the transitivity of the ramification indices. The Hurwitz genus formula [59, III.4] then yields

$$\begin{aligned} 2g(E) - 2 &= [E : F] (2g(F) - 2) + \deg \text{Diff}(E/F) \\ &\leq [E : F] (2g(F) - 2) + [E : F] \sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P \\ &= [E : F] \left(2g(F) - 2 + \sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P \right). \end{aligned}$$

Dividing each side by $2[E : F]$, we find

$$\frac{g(E) - 1}{[E : F]} \leq g(F) - 1 + \frac{1}{2} \sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P.$$

Considering Equation 2.2, and any representation $(F_i)_{i \geq 0}$ of \mathcal{F} with $F_0 = F$, we see that

$$\gamma_F(\mathcal{F}) \leq g(F) - 1 + \frac{1}{2} \sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P.$$

■

Corollary 2.13 *Let \mathcal{F} be a tamely ramified tower over \mathbb{F}_q of finite ramification*

type, and choose some $F < \mathcal{F}$. Then the F -genus rate of \mathcal{F} is finite, with

$$\gamma_F(\mathcal{F}) \leq g(F) - 1 + \frac{1}{2} \sum_{P \in V_F(\mathcal{F})} \deg P.$$

Proof. The Dedekind Different theorem [59, Theorem III.5.1] implies that in the tamely ramified case, $d(Q|P) = e(Q|P) - 1$. As $a_P \geq \frac{d(Q|P)}{e(Q|P)} = \frac{e(Q|P)-1}{e(Q|P)}$ and $\frac{e(Q|P)-1}{e(Q|P)} \rightarrow 1$ as $e(Q|P) \rightarrow \infty$, $a_P = 1$ is a suitable choice for a_P , for all $P \in S(F/\mathbb{F}_q)$. The result now follows, using Theorem 2.12. ■

Theorem 2.12 and Corollary 2.13 show that in the case of a tamely ramified tower, a finite ramification locus suffices to show that the tower has finite F -genus rate, where in the case of a wildly ramified tower, we have to bound the degree of the different as well.

2.1.2 Complete splitting

Definition 2.14 (Completely splitting tower) A tower \mathcal{F} over \mathbb{F}_q is called completely splitting if there exist $F < \mathcal{F}$ and an \mathbb{F}_q -rational place of F which splits completely in E/F , for any $E < \mathcal{F}$.

Definition 2.15 (F -completely splitting locus) Let \mathcal{F} be a tower over \mathbb{F}_q . The F -completely splitting locus is defined as

$$T_F(\mathcal{F}) := \{P \in S(F/\mathbb{F}_q) \mid \deg P = 1 \text{ and } P \text{ splits completely in } E/F, \text{ for all } E\}.$$

We note that $\#T_F(\mathcal{F}) > 0$ if and only if \mathcal{F} is a completely splitting tower. Also, $\nu_F(\mathcal{F}) \geq \#T_F(\mathcal{F})$, by [36, Lemma 2.20]. For one-step explicit towers (which we will define in the next section), it is conjectured [9] that $\nu_F(\mathcal{F}) = \#T_F(\mathcal{F})$, and proved for the case where the number of places lying above the elements of the ramification locus of the tower over the degree of the extension tends to 0.

We are interested in the situation of towers \mathcal{F} with positive limit, that is, $\lambda(\mathcal{F}) \geq 0$. The next theorem (see [67]) gives sufficient conditions for a tower to have positive limit, and a way to compute this limit.

Theorem 2.16 *Let \mathcal{F} be a completely splitting tower over \mathbb{F}_q , which has a finite F -ramification locus for some $F < \mathcal{F}$. Suppose further that for each $P \in S(F/\mathbb{F}_q)$, there exists a non-negative real constant a_P such that for all E/F , each $Q \in S(E/\mathbb{F}_q)$ with $Q|P$, we have that $a_P \geq \frac{d(Q|P)}{e(Q|P)}$. Then*

$$\lambda(\mathcal{F}) \geq \frac{\#T_F(\mathcal{F})}{g(F) - 1 + \frac{1}{2}\sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P'}$$

Proof. In the discussion above, we noted that $\nu_F(\mathcal{F}) \geq \#T_F(\mathcal{F})$. From Theorem 2.12, we know that $\gamma_F(\mathcal{F}) \leq g(F) - 1 + \frac{1}{2}\sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P$. Then

$$\lambda(\mathcal{F}) = \frac{\nu_F(\mathcal{F})}{\gamma_F(\mathcal{F})} \geq \frac{\#T_F(\mathcal{F})}{g(F) - 1 + \frac{1}{2}\sum_{P \in V_F(\mathcal{F})} a_P \cdot \deg P'}$$

which is positive, as required. ■

The boundedness condition applied here to $\frac{d(Q|P)}{e(Q|P)}$ for fixed P is equivalent to the notion of B -boundedness (see [35]).

Finding adequate choices for the a_P may be difficult in practise when studying wildly ramified towers. The following proposition gives a way to find good values of a_P for application in Theorems 2.12 and 2.16:

Proposition 2.17 *Let \mathcal{F} be a tower over \mathbb{F}_q , and $(F_i)_{i \geq 0}$ a representation of \mathcal{F} . For each $P \in V_{F_0}(\mathcal{F})$, let a_P be a non-negative constant such that*

$$a_P \geq \frac{d(P_{i+1}|P_i)}{e(P_{i+1}|P_i) - 1}$$

for all places P_i and P_{i+1} such that $P \subseteq P_i \subseteq P_{i+1}$, $P \in S(F_0/\mathbb{F}_q)$, $P_i \in S(F_i/\mathbb{F}_q)$ and $P_{i+1} \in S(F_{i+1}/\mathbb{F}_q)$ for all $i \geq 1$. Then

$$a_P \geq \frac{d(P'|P)}{e(P'|P)}$$

for all $P'|P$ with $P' \in S(F_n/\mathbb{F}_q)$, for any $n \geq 1$.

Proof. For a proof, see [46, Proposition 3.24]. ■

Theorem 2.16 simplifies considerably when we know that \mathcal{F} is a tamely ramified tower:

Corollary 2.18 *Let \mathcal{F} be a tamely ramified completely splitting tower over \mathbb{F}_q , which has a finite F -ramification locus for some $F < \mathcal{F}$. Then*

$$\lambda(\mathcal{F}) \geq \frac{\#T_F(\mathcal{F})}{g(F) - 1 + \frac{1}{2}\sum_{P \in V_F(\mathcal{F})} \deg P}.$$

Proof. This is a trivial consequence of Theorem 2.16 and Corollary 2.13. ■

2.2 Explicit construction

Definition 2.19 (Explicit tower) *A (separable) tower \mathcal{F}/\mathbb{F}_q is called explicit if it has a representation $(F_i)_{i \geq 0}$ such that (i) $F_0 = \mathbb{F}_q(x_0)$, the rational function field, and (ii) there exists a sequence $(f_i)_{i \geq 1}$ of polynomials in $\mathbb{F}_q[x_{i-1}, x_i]$ (for $i \geq 1$) such that each (separable) extension F_{i+1}/F_i can be described by $F_{i+1} = F_i(x_{i+1})$ where $f_{i+1}(x_i, x_{i+1}) = 0$ for some explicit separable polynomial $f_{i+1} \in \mathbb{F}_q[x_i, x_{i+1}]$.*

We refer to the sequence $(f_i)_{i \geq 1}$ of polynomials (with respectively each $f_{i+1}(x_i, x_{i+1}) \in \mathbb{F}_q[x_i, x_{i+1}]$) as the *defining polynomials* of the recursive tower \mathcal{F} .

In many cases in the literature (see [8]), a tower is described as a sequence of equations rather than bivariate polynomials. For example, in the case that the defining polynomial $f_{i+1}(x_i, x_{i+1})$ has the form

$$f_{i+1}(x_i, x_{i+1}) = h_1(x_{i+1})g_2(x_i) - h_2(x_{i+1})g_1(x_i) = 0,$$

(for $h_1, h_2 \in \mathbb{F}_q[x_{i+1}]$ and $g_1, g_2 \in \mathbb{F}_q[x_i]$) we can express this relation in variable separated form

$$h(x_{i+1}) = g(x_i)$$

where $h(x_{i+1}) = \frac{h_1(x_{i+1})}{h_2(x_{i+1})}$ and $g(x_i) = \frac{g_1(x_i)}{g_2(x_i)}$.

Note that this does not imply that any sequence of defining polynomials $(f_i)_{i \geq 1}$ will necessarily generate a tower \mathcal{F} by performing successive extensions, starting at the rational function field $F_0 = \mathbb{F}_q(x_0)$. One has to ensure that the constant field \mathbb{F}_q is algebraically closed in each extension, that the extensions are all separable extensions (with each $f_{i+1}(x_i, Y) \in F_i[Y]$ an irreducible polynomial over $F_i = \mathbb{F}_q(x_0, x_1, \dots, x_i)$), and that $g(F_i) \rightarrow \infty$ as $i \rightarrow \infty$ (the three properties mentioned in Remark 2.3). A situation that makes the last condition much easier to establish is when there exists a place in $S(F_0/\mathbb{F}_q)$ which is totally ramified in \mathcal{F} .

A further necessary condition for the tower \mathcal{F} to be asymptotically good, is that the generating polynomials f_i should have balanced degree, i.e. for all $i \geq 1$,

$$\deg_{x_i} f_{i+1}(x_i, x_{i+1}) = [F_{i+1} : F_i] = \deg_{x_{i+1}} f_{i+1}(x_i, x_{i+1}),$$

see [33]. When the context makes it clear that we are working with polynomials of balanced degree, we will abbreviate the notation to $\deg f \equiv \deg_{x_i} f = \deg_{x_{i+1}} f$. This will be the case throughout when considering the sequence of defining polynomials for an explicit tower of function fields.

Example 2.20 Consider the sequence $(f_i)_{i \geq 1}$ given by $f_{i+1} := x_{i+1}^3 - (x_i + 1)^3 + 1$ generating an explicit tower over \mathbb{F}_4 , i.e. with $F_0 = \mathbb{F}_4(x_0)$, and the representation $(F_i)_{i \geq 0}$ recursively defined by $F_{i+1} = F_i(x_{i+1})$. The more general case for $\deg f = m \geq 3$ was considered in [37]. To verify that this is indeed a tower, we note firstly that each f_{i+1} does indeed define a separable extension. Secondly, writing $f_{i+1} = 0$ as an equation in variable separated form

$$x_{i+1}^3 = (x_i + 1)^3 - 1$$

we note that the place $x_i = 0$ is a simple zero of the right-hand side, and hence ramifies totally in the extension F_{i+1}/F_i . We denote this place by P , and Q is the unique place lying above it. Hence $v_P((x_i + 1)^3 - 1) = 1$ and $e(Q|P) = 3$.

Then

$$v_Q(x_{i+1}) = \frac{1}{3}v_Q(x_{i+1}^3) = \frac{1}{3}e(Q|P) \cdot v_P(x_{i+1}^3) \quad (2.6)$$

$$= \frac{1}{3} \cdot 3 \cdot v_P((x_i + 1)^3 - 1) = 1 \quad (2.7)$$

and hence the unique place Q above P is a simple zero of x_{i+1} . Therefore we inductively see that the place of F_0 corresponding to $x_0 = 0$ is totally ramified in F_n for all $n \geq 1$, implying (i) that \mathbb{F}_4 is algebraically closed in each element of $(F_i)_{i \geq 0}$ and (ii) that as $d(Q|P) = 1$ by the Dedekind Different theorem, it follows that $\lim_{i \rightarrow \infty} g(F_i/\mathbb{F}_q) = \infty$ by the Hurwitz genus formula.

An explicit tower over \mathbb{F}_q for which $(f_i)_{i \geq 1}$ is a generating set of polynomials will also be referred to as a $(f_i)_{i \geq 1}$ -tower over \mathbb{F}_q . A frequent special case we will encounter is when the sequence $(f_i)_{i \geq 1}$ is constant, i.e. where each $f_i = f$ for some $f \in \mathbb{F}_q[x, y]$. In this case, we will simply refer to such a tower as an f -tower, or a *one-step tower*.

In the case of an f -tower, we refer to

$$F = \mathbb{F}_q(x, y) / \langle f_1(x, y) \rangle \cong F_1 = \mathbb{F}_q(x_0, x_1) / \langle f_1(x_0, x_1) \rangle$$

as the *basic function field* of the tower \mathcal{F} . When both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Galois, the f -tower \mathcal{F} is called a Galois tower.

More generally, one may have n -step towers for $n > 1$, of which the simplest example is the two-step tower. In this case, one may have two separable polynomials f and g in two variables, both of (possibly different) balanced degree. When the sequence $(h_i)_{i \geq 1}$ with

$$h_{i+1} = \begin{cases} f & \text{if } i \equiv 0 \pmod{2} \\ g & \text{if } i \equiv 1 \pmod{2} \end{cases}$$

defines a tower, we refer to such a tower as an *alternating two-step tower*, or just a *two-step tower*.

To study the general n -step tower we first make some general definitions. Suppose \sim is an arbitrary equivalence relation on the set of indeter-

minates $\{x_i : i \geq 0\}$. Let the residue classes be

$$\{\tilde{x}_j : j \in \Lambda\} := \{x_i : i \geq 0\} / \sim \quad (2.8)$$

where Λ is some index set.

The equivalence relation \sim on the set $\{x_i : i \geq 0\}$ induces an equivalence relation on the set of defining polynomials $\{f_{i+1}(x_i, x_{i+1}) : i \geq 0\}$ (which we, by abuse of notation, also denote by \sim) by defining (noting that $f_{i+1} \in \mathbb{F}_q[x_i, x_{i+1}]$ and $f_{j+1} \in \mathbb{F}_q[x_j, x_{j+1}]$)

$$f_{i+1} \sim f_{j+1} : \iff (x_{i+1} \sim x_{j+1}) \wedge (x_i \sim x_j) \wedge (f_{i+1} = \lambda f_{j+1}) \quad (2.9)$$

for some $\lambda \neq 0$.

We can then define the set of residue classes of $\{f_{i+1}(x_i, x_{i+1}) : i \geq 0\}$ modulo \sim as

$$\{\tilde{f}_k : k \in \Lambda'\} := \{f_{i+1}(x_i, x_{i+1}) : i \geq 0\} / \sim \quad (2.10)$$

where Λ' is some index set. When Λ' in (2.10) is finite, we refer to the tower induced by $(f_i)_{i \geq 1}$ over \mathbb{F}_q as a \sim -finite tower. If the index set Λ from (2.8) is finite, then Λ' is finite as well, since $\#\Lambda' \leq (\#\Lambda)^2$.

Definition 2.21 (*n*-step tower) Let $n \in \mathbb{N}$ and define the equivalence relation \sim_n on the set $\{x_i : i \geq 0\}$ as

$$x_i \sim_n x_j : \iff i \equiv j \pmod{n}.$$

If the set of defining polynomials $\{f_{i+1}(x_i, x_{i+1}) : i \geq 0\}$ of an explicit tower \mathcal{F} satisfy the induced equivalence relation \sim_n on the f_i (again using the same notation), in other words if $f_{i+1}(x_i, x_{i+1}) = f_{j+1}(x_j, x_{j+1})$ for all $i, j \geq 0$ and all the indices considered modulo n , then \mathcal{F} is an n -step tower.

Clearly an n -step tower \mathcal{F} is a \sim_n -finite tower. In this case $\#\Lambda = \#\Lambda' = n$, and suitable defining polynomials can be chosen by prescribing the residue classes of $\{f_{i+1}(x_i, x_{i+1}) : i \geq 0\} / \sim_n$, i.e. by choosing

n balanced-degree bivariate polynomials $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$ and then defining the sequence of defining polynomials of \mathcal{F} to be

$$(f_{i+1}(x_i, x_{i+1}))_{i \geq 1} \text{ where } f_i := \tilde{f}_j \text{ if and only if } i \equiv j \pmod{n}.$$

This ensures that $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\} = \{f_{i+1}(x_i, x_{i+1}) : i \geq 0\} / \sim_n$, satisfying (2.10). The main distinction between n -step towers and \sim -finite towers are therefore that while both have essentially a finite set of distinct polynomials defining the subsequent steps in the tower, the (cyclic) ordering is fixed in an n -step tower, while it is arbitrary in the more general case of a \sim -finite tower.

We will consider ramification and completely splitting graphs, respectively in Chapters 3 and 4, modulo \sim_n for the well-known (one-step) $n = 1$ case, as well as the (two-step) $n = 2$ case. In Chapter 5 we will consider algorithms for working with \sim_n for arbitrary n , as well as equivalence relations \sim where we do not assume that \sim induces an n -step tower for some $n \geq 1$, but make the weaker assumption that \sim induces a \sim -finite tower.

In general, we may define any equivalence relation \sim on the set of indeterminates $\{x_i : i \geq 0\}$. The aim here is not to change the structure of the tower, but to discern some structure to the sequence of defining polynomials $(f_i)_{i \geq 1}$, as in practise there is often many repeated terms in this sequence. This structure will be more easily discerned when looking at the splitting graphs defined in Chapters 3 and 4 for arbitrary (not even \sim -finite) towers.

2.3 Transforming equations

Let \mathcal{F} be an explicit tower over \mathbb{F}_q with representation (F_0, F_1, F_2, \dots) generated by the sequence $(f_i(x_{i-1}, x_i))_{i \geq 1}$ of balanced-degree separable polynomials, and let A be an arbitrary element of the general linear group

$GL(\mathbb{F}_q, 2)$. Following [10], we define a group action

$$GL(\mathbb{F}_q, 2) \times F_i \rightarrow F_i \quad (2.11)$$

for each $i \geq 0$ by

$$A \cdot x_i := \frac{a_{11}x_i + a_{12}}{a_{21}x_i + a_{22}} \quad (2.12)$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in GL(\mathbb{F}_q, 2)$$

for $F_{i+1} = F_i(x_{i+1})$ with $f_{i+1}(x_i, x_{i+1}) = 0$. As A is invertible, this is well-defined for each $i \geq 0$. This group action is also sometimes referred to as a *linear fractional transformation* or the *Möbius transformation*.

The group action described by (2.12) induces a group action on the set of sequences of defining polynomials $(f_{i+1}(x_i, x_{i+1}))_{i \geq 0}$ by

$$\left(A, (f_{i+1}(x_i, x_{i+1}))_{i \geq 0} \right) \mapsto \left(f_{i+1}^A(x_i, x_{i+1}) \right)_{i \geq 0}$$

where

$$f_{i+1}^A(x_i, x_{i+1}) = (a_{21}x_i + a_{22})^{\deg f_{i+1}} (a_{21}x_{i+1} + a_{22})^{\deg f_{i+1}} f_i(A \cdot x_i, A \cdot x_{i+1})$$

for each $i \geq 0$. Because of the irreducibility of f_{i+1} , f_{i+1}^A is irreducible and $\deg f_{i+1} = \deg f_{i+1}^A$.

By varying $A \in GL(\mathbb{F}_q, 2)$, we obtain different sequences of defining polynomials, which all yield the tower \mathcal{F} with same representation (F_0, F_1, F_2, \dots) . The action of $GL(\mathbb{F}_q, 2)$ on these sets of sequences defines an equivalence relation on these sequences, and we can define the $GL(\mathbb{F}_q, 2)$ -orbit of a given sequence $(f_{i+1})_{i \geq 0} = (f_{i+1}(x_i, x_{i+1}))_{i \geq 0}$ by

$$(f_{i+1})_{i \geq 0}^A := \left\{ \left(f_{i+1}^A(x_i, x_{i+1}) \right)_{i \geq 0} : A \in GL(\mathbb{F}_q, 2) \right\}.$$

We can consider $GL(\mathbb{F}_q, 2)$ modulo the kernel of the linear fractional transformation and replace $GL(\mathbb{F}_q, 2)$ by $PGL(\mathbb{F}_q, 2)$ when convenient. In the

computations of Chapter 6 we utilize the orbits of $GL(\mathbb{F}_q, 2)$ (alternatively, $PGL(\mathbb{F}_q, 2)$) to reduce the number of candidate sequences of defining polynomials which needs to be considered. As $\#PGL(\mathbb{F}_q, 2) = (q + 1)q(q - 1)$, such an orbit has cardinality at most $(q + 1)q(q - 1)$ and compares favourably with the cardinality of $GL(\mathbb{F}_q, 2)$. When convenient, we will consider orbits over a subfield $\mathbb{F}_l \subseteq \mathbb{F}_q$, for which we use the subgroup $PGL(\mathbb{F}_l, 2)$.

Chapter 3

Finite ramification

In this chapter, we will analyse the ramification locus of explicit towers. In the light of Theorem 2.16, identifying a finite ramification locus is both computationally useful and necessary. We will therefore develop methods by which one can (a) test whether a tower has a finite ramification locus, (b) identify it, and (c) if it is not possible or feasible to precisely identify it, find a finite set of places containing the ramification locus.

This will be done by introducing ramification graphs, which generalizes the graph-theoretical approach of Beelen et al [5], [9] by essentially restricting computations to using sets of functions in the indeterminates x_i for $i \geq 0$ instead of $\mathbb{F}_q \cup \{\infty\}$ as vertex sets for the relevant graphs.

Where we previously only considered towers of function fields over finite fields, we will now extend the field of constants to an algebraic closure of the (finite) constant field. This will enable us to perform an analysis of the defining equations of the tower over the residue field.

Definition 3.1 (Algebraic closure of a tower) *Let \mathcal{F} be a tower over K . The algebraic closure of the tower \mathcal{F} , denoted by $\tilde{\mathcal{F}}$, is the compositum of the field \mathcal{F} with an algebraic closure \bar{K} of K , in other words $\tilde{\mathcal{F}} := \mathcal{F} \cdot \bar{K}$. This is a tower with constant field \bar{K} .*

One can readily see from Definition 2.1 that $\tilde{\mathcal{F}}$ over \bar{K} is indeed a tower. In what follows, we will denote the algebraic closure of \mathbb{F}_q by $\bar{\mathbb{F}}$.

Proposition 3.2 *Suppose \mathcal{F} is an explicit tower over \mathbb{F}_q generated by the sequence $(f_i)_{i \geq 1}$ of polynomials. Let $\tilde{\mathcal{F}}$ over $\bar{\mathbb{F}}$ be the algebraic closure of the tower \mathcal{F} over \mathbb{F}_q . Fix $n \in \mathbb{N}$ and suppose $P_n \in S(F_n/\bar{\mathbb{F}})$ and $P_{n-1} := P_n \cap F_{n-1} \in S(F_{n-1}/\bar{\mathbb{F}})$. Suppose*

$$x_n(P_n) = a_n \in \bar{\mathbb{F}} \text{ and } x_{n-1}(P_{n-1}) = a_{n-1} \in \bar{\mathbb{F}}.$$

Then $f_n(a_{n-1}, a_n) = 0$ and if we further have that $e(P_n|P_{n-1}) > 1$, then $0 = f_n(a_{n-1}, Y) \in \bar{\mathbb{F}}[Y]$ has a repeated root in $\bar{\mathbb{F}}$.

Proof. As the function field F_{n-1} has $\bar{\mathbb{F}}$ as its field of constants, $\deg P_{n-1} = 1$. Similarly $\deg P_n = 1$. Then

$$v_{P_n}(x_n - a_n) > 0 \text{ and } v_{P_n}(x_{n-1} - a_{n-1}) \geq v_{P_{n-1}}(x_{n-1} - a_{n-1}) > 0.$$

Then $f_n(x_{n-1}, x_n) = 0$ implies that

$$\begin{aligned} 0 &= 0(P_n) \\ &= f_n(x_{n-1}, x_n)(P_n) \\ &= f_n((x_{n-1} - a_{n-1}) + a_{n-1}, (x_n - a_n) + a_n)(P_n) \\ &= f_n(a_{n-1}, a_n). \end{aligned}$$

Let Q_1, Q_2, \dots, Q_r be all the places lying above P_{n-1} in F_n . If $e(P_n|P_{n-1}) > 1$, then $r < [F_n : F_{n-1}] = \deg_Y f_n(a_{n-1}, Y)$. As $Y = x_n(Q_1), x_n(Q_2), \dots, x_n(Q_r)$ are the solutions of $f_n(a_{n-1}, Y) = 0$, this equation must have a repeated root by the Fundamental Theorem of Algebra. ■

Definition 3.3 (Reciprocal polynomials) *Let $f(x, y) \in \mathbb{F}_q[x, y]$ be an irreducible polynomial of balanced degree d , in other words $\deg_x f(x, y) = d = \deg_y f(x, y)$. Then we define its associated reciprocal polynomials with respect to*

x, y , or x and y as

$$f^{(x)}(x, y) = f^{(x, \cdot)}(x, y) := x^d \cdot f\left(\frac{1}{x}, y\right), \quad (3.1)$$

$$f^{(y)}(x, y) = f^{(\cdot, y)}(x, y) := y^d \cdot f\left(x, \frac{1}{y}\right) \text{ and} \quad (3.2)$$

$$f^{(x, y)}(x, y) := x^d \cdot y^d \cdot f\left(\frac{1}{x}, \frac{1}{y}\right). \quad (3.3)$$

Then the polynomials $f^{(x, \cdot)}$, $f^{(\cdot, y)}$ and $f^{(x, y)}$ are also irreducible and of balanced degree d .

Proof. We prove the validity of the properties of the reciprocal polynomial $f^{(x, \cdot)}$ only, the others follow similarly. Consider

$$f(x, y) = f_d(y) x^d + f_{d-1}(y) x^{d-1} + \dots + f_1(y) x + f_0(y) \in \mathbb{F}_q[y][x]$$

where the $f_i(y)$ are elements of $\mathbb{F}_q[y]$, for $0 \leq i \leq d$. Then

$$f^{(x, \cdot)}(x, y) = f_0(y) x^d + f_1(y) x^{d-1} + \dots + f_{d-1}(y) x + f_d(y) \in \mathbb{F}_q[y][x],$$

and as f is irreducible, $f_0(y) \neq 0$ and hence $\deg_x f^{(x, \cdot)} = d$. The fact that $\deg_y f^{(\cdot, y)} = d$ follows similarly by considering $f \in \mathbb{F}_q[x][y]$ and transitivity. Irreducibility of $f^{(x)}$ follows by examining (3.1) and the fact that x does not divide $f^{(x, \cdot)}(x, y)$. ■

Proposition 3.4 Suppose \mathcal{F} is an explicit tower over \mathbb{F}_q generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $\mathbb{F}_q[x, y]$. Let $\tilde{\mathcal{F}}$ over $\bar{\mathbb{F}}$ be the algebraic closure of \mathcal{F} over \mathbb{F}_q . Fix $n \in \mathbb{N}$ and suppose $P_n \in S(F_n/\bar{\mathbb{F}})$ and $P_{n-1} := P_n \cap F_{n-1}$. Suppose that f_n is of balanced degree d_n . If $e(P_n|P_{n-1}) > 1$, then

- (i) $x_{n-1}(P_{n-1}) \in \bar{\mathbb{F}}, x_n(P_n) \in \bar{\mathbb{F}} \Rightarrow f_n(a_{n-1}, Y) = 0$ has a repeated root,
- (ii) $x_{n-1}(P_{n-1}) \in \bar{\mathbb{F}}, x_n(P_n) = \infty \Rightarrow f_n^{(\cdot, x_n)}(a_{n-1}, Y) = 0$ has $Y = 0$ as a repeated root,
- (iii) $x_{n-1}(P_{n-1}) = \infty, x_n(P_n) \in \bar{\mathbb{F}} \Rightarrow f_n^{(x_{n-1}, \cdot)}(0, Y) = 0$ has a repeated root, and

(iv) $x_{n-1}(P_{n-1}) = \infty, x_n(P_n) = \infty \Rightarrow f_n^{(x_{n-1}, x_n)}(0, Y) = 0$ has $Y = 0$ as a repeated root.

Proof. As we are working over the algebraic closure, it follows that $x_n(P_n) \in \overline{\mathbb{F}} \cup \{\infty\}$ and $x_{n-1}(P_{n-1}) \in \overline{\mathbb{F}} \cup \{\infty\}$. We then have the following four cases:

- (i) For $x_{n-1}(P_{n-1}) = a_{n-1} \in \overline{\mathbb{F}}, x_n(P_n) = a_n \in \overline{\mathbb{F}}$, this follows by direct application of Proposition 3.2.
- (ii) For $x_{n-1}(P_{n-1}) = a_{n-1} \in \overline{\mathbb{F}}, x_n(P_n) = \infty$, we have to rewrite f_n first to be able to apply Proposition 3.2. As $x_n(P_n) = \infty$, we have that $\left(\frac{1}{x_n}\right)(P_n) = 0$. By using the definition of reciprocal polynomials (Definition 3.3), we obtain

$$\frac{f_n(x_{n-1}, x_n)}{x_n^{d_n}} = f_n^{(\cdot, x_n)}\left(x_{n-1}, \frac{1}{x_n}\right).$$

Then, working modulo P_n , we obtain

$$0 = \frac{f_n(x_{n-1}, x_n)}{x_n^{d_n}}(P_n) = f_n^{(\cdot, x_n)}\left(x_{n-1}, \frac{1}{x_n}\right)(P_n) = f_n^{(\cdot, x_n)}(a_{n-1}, 0).$$

We can now apply Proposition 3.2 to the polynomial $f_n^{(x_n)}(a_{n-1}, a_n)$ (since in this case $a_n = 0 \in \overline{\mathbb{F}}$) from which it follows that the polynomial $f_n^{(x_n)}(a_{n-1}, Y) \in \overline{\mathbb{F}}[Y]$ has $Y = 0$ as a repeated root.

- (iii) For $x_{n-1}(P_{n-1}) = \infty, x_n(P_n) = a_n \in \overline{\mathbb{F}}$ the derivation is similar to case (ii).
- (iv) For $x_{n-1}(P_{n-1}) = \infty, x_n(P_n) = \infty$, we again have to rewrite f_n to be able to apply Proposition 3.2. As both $x_{n-1}(P_n) = \infty$ and $x_n(P_n) = \infty$, Definition 3.3 implies that

$$\frac{f_n(x_{n-1}, x_n)}{x_{n-1}^{d_n} x_n^{d_n}} := f_n^{(x_{n-1}, x_n)}\left(\frac{1}{x_{n-1}}, \frac{1}{x_n}\right).$$

Then

$$0 = \frac{f_n(x_{n-1}, x_n)}{x_{n-1}^{d_n} x_n^{d_n}} (P_n) = f_n^{(x_{n-1}, x_n)} \left(\frac{1}{x_{n-1}}, \frac{1}{x_n} \right) (P_n) = f_n^{(x_{n-1}, x_n)}(0, 0).$$

As in case (ii), we can now apply Proposition 3.2 to the polynomial $f_n^{(\cdot, x_n)}(a_{n-1}, a_n)$ with $a_{n-1} = 0$ and $a_n = 0$. Hence $f_n^{(x_{n-1}, x_n)}(0, Y)$ has $Y = 0$ as a repeated root.

■

3.1 Identifying a finite ramification locus

We now outline a construction which will aid the identification of a finite ramification locus for a given explicit tower of function fields. Let \mathcal{F} be an explicit tower over \mathbb{F}_q (and subsequently, its algebraic closure $\tilde{\mathcal{F}}$ over $\overline{\mathbb{F}}$) defined by the sequence $(f_i)_{i \geq 1}$ of polynomials in $\mathbb{F}_q[x, y]$, and let $(F_i)_{i \geq 0}$ be the induced sequence of function fields obtained as representative of \mathcal{F} by the polynomials in the sequence $(f_i)_{i \geq 1}$.

Definition 3.5 (Ramification-capturing sequence) *Given an explicit tower \mathcal{F} over \mathbb{F}_q , let $\tilde{\mathcal{F}}$ over $\overline{\mathbb{F}}$ be its algebraic closure. Suppose \mathcal{F} has the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$ as representation which generates the sequence $(F_i)_{i \geq 0}$ of function fields over \mathbb{F}_q . Then any sequence $(U_i)_{i \geq 0}$ of subsets of $\overline{\mathbb{F}} \cup \{\infty\}$ for which the following properties hold:*

- (i) *if $e(P_{j+1}|P_j) > 1$ for some $j \geq 0$, $P_{j+1} \in S(F_{j+1}/\mathbb{F}_q)$ and $P_j = P_{j+1} \cap F_j$, then $x_j(P_j) \in U_j$*
- (ii) *if $u_{j+1} \in U_{j+1} \setminus \{\infty\}$ for some $j \geq 0$, then*
 - (a) *$f_{j+1}(u, u_{j+1}) = 0$ for some $u \in \overline{\mathbb{F}}$ implies that $u \in U_j$, and*
 - (b) *$f_{j+1}^{(x_j, \cdot)}(0, u_{j+1}) = 0$ implies that $\infty \in U_j$.*
- (iii) *if $\infty \in U_{j+1}$ for some $j \geq 0$, then*

- (a) $f_{j+1}^{(\cdot, x_{j+1})}(u, 0) = 0$ for some $u \in \overline{\mathbb{F}}$ implies that $u \in U_j$, and
 (b) $f_{j+1}^{(x_j, x_{j+1})}(0, 0) = 0$ implies that $\infty \in U_j$.

is called a ramification-capturing sequence for the explicit tower \mathcal{F} over \mathbb{F}_q defined by the sequence $(f_i)_{i \geq 1}$ of polynomials.

Property (i) of a ramification-capturing sequence introduces “new” elements to the constituent elements of the sequence $(U_i)_{i \geq 0}$ corresponding to ramification happening in the j th step of the tower. In contrast, properties (ii) and (iii) describes the effect of those elements introduced through property (i) to the lower steps 1 to $j - 1$ of the tower.

Property (ii) handles the case where the ramification is inherited from the case $x_{j+1}(P_{j+1}) \in \overline{\mathbb{F}}$ (with the cases $x_j(P_j) \in \overline{\mathbb{F}}$ and $x_j(P_j) = \infty$).

Property (iii) handles the case where the ramification is inherited from the case $x_{j+1}(P_{j+1}) = \infty$ (with the cases $x_j(P_j) \in \overline{\mathbb{F}}$ and $x_j(P_j) = \infty$).

Proposition 3.6 *Suppose $(U_i)_{i \geq 0}$ is some ramification-capturing sequence for the tower \mathcal{F} over \mathbb{F}_q generated by the polynomial sequence $(f_i)_{i \geq 1}$. Then, for any $j \geq 0$, the F_j -ramification locus*

$$V_{F_j}(\mathcal{F}) \subseteq \{P \in S(F_j/\mathbb{F}_q) : x_j(P) \in U_j\}.$$

Proof. Suppose $P_j \in V_{F_j}(\mathcal{F})$. Then $P_j \in S(F_j/\mathbb{F}_q)$ and let $k \in \mathbb{N}$ be the smallest natural number for which $P_{j+k} \in S(F_{j+k}/\mathbb{F}_q)$ with $P_{j+k}|P_j$ we have that $e(P_{j+k}|P_j) > 1$.

Then, in the extension F_{j+k}/F_{j+k-1} with $F_{j+k} = F_{j+k-1}(x_{j+k})$, we have that $e(P_{j+k}|P_{j+k-1}) > 1$. This extension is defined by the (separable) equation $f_{j+k}(x_{j+k-1}, x_{j+k}) = 0$. By Definition 3.5 property (i), it follows that $x_{j+k-1}(P_{j+k-1}) \in U_{j+k-1}$. By repeatedly applying property (ii), it follows that $x_j(P_j) \in U_j$, as required. ■

Corollary 3.7 *Suppose $(U_i)_{i \geq 0}$ is a ramification-capturing sequence for the explicit tower \mathcal{F} over \mathbb{F} generated by the polynomial sequence $(f_i)_{i \geq 1}$. Then \mathcal{F} is of finite ramification type if any of the U_j (for $j \geq 0$) are finite.*

Proof. For \mathcal{F} to be of finite ramification type, its F_j -ramification locus $V_{F_j}(\mathcal{F})$ should be finite for some $j \geq 0$. If none of the $V_{F_j}(\mathcal{F})$ are finite, the same holds for all the U_j because of Proposition 3.6. ■

If we are able to calculate a ramification-capturing sequence $(U_i)_{i \geq 0}$ for a tower \mathcal{F} over \mathbb{F}_q , and we find that some U_j is finite, then \mathcal{F} is of finite ramification type. However, it is easily seen (by checking the two properties from Definition 3.5) that every tower has a trivial ramification-capturing sequence given by $(\overline{\mathbb{F}} \cup \{\infty\})_{i \geq 0}$, which is clearly infinite. For a specific choice of tower, one may find many infinite ramification-capturing sequences, so to identify a finite ramification locus by means of Corollary 3.7, one should be careful not to introduce too many superfluous elements into the respective U_j , especially considering point (c) mentioned in the first paragraph of page 24. Clearly, given ramification-capturing sequences $(U_i)_{i \geq 0}$ and $(U'_i)_{i \geq 0}$ for a tower \mathcal{F} , their intersection $(U_i \cap U'_i)_{i \geq 0}$ is also a ramification-capturing sequence for \mathcal{F} .

At this stage, using properties (i) and (ii) of Definition 3.5 to explicitly calculate ramification-capturing sequences is possible, but the formulation can be changed to better detail the ramification structure involved. In the next definitions and sections, we will change our terminology by translating the description of the ramification structure of a tower from a sequence of subsets of $\overline{\mathbb{F}} \cup \{\infty\}$ to a sequence of subsets of irreducible polynomials in x_i , and possibly the element $\frac{1}{x_i}$, for each $i \geq 0$.

To make this more precise, we introduce some notation in the following definition, for \mathbb{F}_l some subfield of \mathbb{F}_q :

Definition 3.8 (Set of monic irreducible functions) For a finite field \mathbb{F}_l , we denote by $MI_{\mathbb{F}_l}(T)$ the set of monic \mathbb{F}_l -irreducible polynomials in the variable T , together with the element $\frac{1}{T}$. Hence

$$MI_{\mathbb{F}_l}(T) = \{p(T) \in \mathbb{F}_l[T] : p(T) \text{ is monic and irreducible over } \mathbb{F}_l\} \cup \left\{ \frac{1}{T} \right\},$$

which we from here on refer to as the set of monic irreducible functions over \mathbb{F}_l .

Note that the set of monic irreducible functions $MI_{\mathbb{F}_l}(T)$ is different to the rational functions $\mathbb{F}_l(T)$, as we are only allowing a denominator of 1

or T , and in the latter case only a numerator of 1.

Definition 3.9 (\mathbb{F}_l -Ramification-capturing function sequence) *Let \mathcal{F} over \mathbb{F}_q be an explicit tower of function fields, generated by the polynomial sequence $(f_i(x_{i-1}, x_i))_{i \geq 1}$. Suppose \mathbb{F}_l is a subfield of \mathbb{F}_q . Let $(M_i)_{i \geq 0}$ be a sequence of subsets of $MI_{\mathbb{F}_l}(x_i)$ (for each respective $i \geq 0$) chosen in such a way that the sequence*

$$U_i := \{r \in \overline{\mathbb{F}} \cup \{\infty\} : p_i(r) = 0 \text{ for some } p_i(x_i) \in M_i\} \quad (3.4)$$

is a ramification-capturing sequence, where we assume that $\frac{1}{\infty} = 0$. We call such a sequence $(M_i)_{i \geq 0}$ an \mathbb{F}_l -ramification-capturing function sequence.

We note that this definition makes sense, and is just a translation of Definition 3.5 (which describes the residue classes of ramification elements as subsets of $\overline{\mathbb{F}} \cup \{\infty\}$) to a description of these points as being the zeros of rational functions in $\mathbb{F}_l(T_i)$. This is also a natural construction, by considering Definitions 3.5 and 3.9 as the two sides of the so-called algebra-geometry dictionary by the ideal-variety correspondence (for an exposition, see [16]).

A critical point which may influence calculations is the choice of subfield \mathbb{F}_l . In many practical computations we will not even fix the field \mathbb{F}_q beforehand (however stay in characteristic p), but will be able to choose a minimal \mathbb{F}_l by specifying it to be the prime subfield \mathbb{F}_p . While this minimal case has computational advantages, it may imply that while the U_i 's obtained in (3.4) do indeed yield a ramification-capturing sequence, it may not be minimal. In this case, superfluous elements are included in the associated ramification-capturing sequence which, in our further analysis, may cause a tower of finite ramification type not to be classified as such.

In many of the examples we will consider in this and the subsequent chapters, we will use $\mathbb{F}_l = \mathbb{F}_p$.

Theorem 3.10 *Suppose $(M_i)_{i \geq 0}$ is an \mathbb{F}_l -ramification-capturing function sequence for some subfield \mathbb{F}_l of \mathbb{F}_q , in the explicit tower \mathcal{F} over \mathbb{F}_q , generated by*

$(f_i)_{i \geq 1}$, where $f_i(T_{i-1}, T_i) \in \mathbb{F}_q[T_{i-1}, T_i]$ for each $i \geq 1$. For some fixed $i = k$, consider the places $P_{k+1} \in S(F_{k+1}/\mathbb{F}_q)$ and $P_k := P_{k+1} \cap F_k \in S(F_k/\mathbb{F}_q)$. Let $a_k := T_k(P_k)$ and $a_{k+1} := T_{k+1}(P_{k+1})$ so that both $a_k, a_{k+1} \in \overline{\mathbb{F}} \cup \{\infty\}$. Then the following hold:

- (i) If $p_{k+1}(a_{k+1}) = 0$ for some $p_{k+1}(T_{k+1}) \in M_{k+1} \setminus \left\{ \frac{1}{T_{k+1}} \right\}$ and $a_k \in \overline{\mathbb{F}}$, then every monic \mathbb{F}_l -irreducible factor $p_k(T_k)$ of the univariate generator polynomial of the elimination ideal $\langle f_{k+1}(T_k, T_{k+1}), p_{k+1}(T_{k+1}) \rangle \cap \mathbb{F}_l[T_k]$ is an element of M_k .
- (ii) If $p_{k+1}(a_{k+1}) = 0$ for $p_{k+1}(T_{k+1}) = \frac{1}{T_{k+1}}$ and $a_k \in \overline{\mathbb{F}}$, then every monic \mathbb{F}_l -irreducible factor $p_k(T_k)$ of $f_{k+1}^{(\cdot, T_{k+1})}(T_k, 0)$ is an element of M_k .
- (iii) If $p_{k+1}(a_{k+1}) = 0$ for some $p_{k+1}(T_{k+1}) \in M_{k+1} \setminus \left\{ \frac{1}{T_{k+1}} \right\}$ and $a_k = \infty$, then $p_k(T_k) := \frac{1}{T_k} \in M_k$ if $f_{k+1}^{(T_k, \cdot)}(0, a_{k+1}) = 0$.
- (iv) If $p_{k+1}(a_{k+1}) = 0$ for $p_{k+1}(T_{k+1}) = \frac{1}{T_{k+1}}$ and $a_k = \infty$, then $p_k(T_k) := \frac{1}{T_k} \in M_k$ if $f_{k+1}^{(T_k, T_{k+1})}(0, 0) = 0$.

Proof. All four cases are an application of Definition 3.5, rewritten in the language of ramification-capturing function sequences. Case (i) deserves special attention: in this case both a_k and a_{k+1} are in $\overline{\mathbb{F}}$, and $p_{k+1}(T_{k+1})$ is a polynomial of which we know a_{k+1} is a zero. Suppose

$$p_k(T_k) \in \langle f_{k+1}(T_k, T_{k+1}), p_{k+1}(T_{k+1}) \rangle \cap \mathbb{F}_l[T_k].$$

Then $p_k(T_k) = \alpha f_{k+1}(T_k, T_{k+1}) + \beta p_{k+1}(T_{k+1})$ for some $\alpha, \beta \in \mathbb{F}_l[T_k, T_{k+1}]$. Substituting $T_k = a_k$ and $T_{k+1} = a_{k+1}$, we obtain

$$\begin{aligned} p_k(a_k) &= \alpha f_{k+1}(a_k, a_{k+1}) + \beta p_{k+1}(a_{k+1}) \\ &= 0 + 0 = 0. \end{aligned}$$

As a_k is a root of $p_k(T_k)$, $p_k \in M_k$ and the result follows. ■

A recurring problem in the next sections will be to, given $(f_i)_{i \geq 1}$ and a partial ramification-capturing function sequence $(M_i)_{i \geq k}$ for some $k \geq 0$,

calculate the possible $p_k \in M_k$ given some $p_{k+1} \in M_{k+1}$. In the next definition, we will refer to such p_k as predecessors of the respective p_{k+1} .

In case (i) of Theorem 3.10, this calculation can be done using a Gröbner basis (see [16]), where we choose some monomial ordering on $\overline{\mathbb{F}}[T_k, T_{k+1}]$ with $T_{k+1} > T_k$ in order to ensure the elimination of the indeterminate T_{k+1} in favour of the indeterminate T_k , thereby obtaining a representation of $p_k(T_k)$ in terms of $p_{k+1}(T_{k+1})$. The other (less frequent) cases can be done by a simple factorization of some reciprocal polynomial. Explicit algorithms to achieve this are presented in Chapter 5.

Definition 3.11 (Predecessor polynomials) *Suppose \mathcal{F} is an explicit tower with representation $(F_i)_{i \geq 0}$ over \mathbb{F}_q generated by the sequence $(f_i)_{i \geq 1}$ of polynomials (resp.) in $(\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$, where $\mathbb{F}_l \subseteq \mathbb{F}_q$. Fix an element $p_{k+1} \in MI_{\mathbb{F}_l}(x_{k+1})$. If $p_{k+1}(x_{k+1}) \in \mathbb{F}_l[x_{k+1}]$, we let $\mathcal{P}_{k+1} = \text{supp}((p_{k+1})_0)$, the support of the zero divisor of $p_{k+1}(x_{k+1})$, otherwise if $p_{k+1}(x_{k+1}) = \frac{1}{x_{k+1}}$, we let $\mathcal{P}_{k+1} = \text{supp}((p_{k+1})_\infty)$. We then define*

$$\text{Pred}_{f_{k+1}}(p_{k+1}) := \{p_k \in MI_{\mathbb{F}_l}(x_k) : p_k(x_k(P_k)) = 0 \text{ for some } P_k \in \mathcal{P}_k\},$$

where $\mathcal{P}_k := \{P \cap F_k : P \in \mathcal{P}_{k+1}\}$.

For any $p_k \in \text{Pred}_{f_{k+1}}(p_{k+1})$, we say that p_k is a predecessor polynomial of p_{k+1} , even if such $p_k(T_k) = \frac{1}{T_k}$.

The definition describes the process of obtaining polynomials at step k of a tower which are induced by (and therefore predecessor polynomials of) polynomials at step $k+1$ of the tower. Theorem 3.10 and the definition above implies that if P_{k+1} and P_k are places of F_{k+1} and F_k respectively with $P_{k+1}|P_k$ in \mathcal{F} , then $x_{k+1}(P_{k+1})$ being a root of $q(x_{k+1})$ will imply that $x_k(P_k)$ is a root of an element of $\text{Pred}_{f_{k+1}}(q(x_{k+1}))$.

We make two extensions to this notation. Firstly, we define the predecessor polynomial set of a set $Q \subseteq MI_{\mathbb{F}_l}(T_i)$ of functions by

$$\text{Pred}_{f_{k+1}}(Q) := \bigcup_{q \in Q} \text{Pred}_{f_{k+1}}(q).$$

Secondly, if we relax the condition that p_{k+1} is irreducible, we can write (for $p_{k+1} = \prod p_{k+1,i}$)

$$\text{Pred}_{f_{k+1}}(\prod_i p_{k+1,i}) := \bigcup_i \text{Pred}_{f_{k+1}}(p_{k+1,i}).$$

where each $p_{k+1,i}$ is an element of $MI_{\mathbb{F}_l}(T_{k+1})$. We leave open the possibility of using non-irreducible polynomials as it will not always be clear whether a given p_{k+1} is in fact irreducible, and that the definition of a predecessor polynomial will still be useful under such circumstances, for example when we consider splitting characteristic polynomials in Chapter 4.

3.2 Ramification-generating sets

The previous section gave us a method to explicitly compute the effect of ramification in step j of the tower on the lower steps 0 to $j - 1$ of the tower. That effect was described by properties (ii) and (iii) of Definition 3.5. In this section we will focus on identifying exactly what elements of a ramification-capturing sequence (or ideal sequence) is contributed by property (i). The central problem is the following:

Problem 3.12 *Let \mathcal{F} be an explicit tower over \mathbb{F}_q with representation $(F_i)_{i \geq 0}$ generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$, where $\mathbb{F}_l \subseteq \mathbb{F}_q$. Suppose that $e(P_{k+1}|P_k) > 1$ for some $k \geq 0$, $P_{k+1} \in S(F_{k+1}/\mathbb{F}_q)$ and $P_k = P_{k+1} \cap F_k$. What is the finite set of possible values of $x_k(P_k) \in \overline{\mathbb{F}} \cup \{\infty\}$?*

By Proposition 3.4, $x_{k+1}(P_{k+1})$ must be a repeated root of some polynomial equation (possibly involving reciprocal polynomials) in $x_k(P_k)$. We can consider the polynomial $f_{k+1}^{(\cdot, \cdot)}(x_k, x_{k+1})$ as an element of $\mathbb{F}_q[x_k][x_{k+1}]$ and compute the discriminants

$$\text{disc}_{x_{k+1}} f_{k+1}^{(\cdot, \cdot)}(x_k, x_{k+1}) = 0$$

for each possibility of $f_{k+1}^{(\cdot, \cdot)}$ (which are f_{k+1} , $f_{k+1}^{(x_k)}$, $f_{k+1}^{(x_{k+1})}$ and $f_{k+1}^{(x_k, x_{k+1})}$), and in each case solve the resulting polynomial in x_k to obtain the possible values of $x_k (P_k)$ for places P_k which are ramified in F_{k+1}/F_k . This can be organized as a theorem:

Theorem 3.13 *Let \mathcal{F} be an explicit tower over \mathbb{F}_q with representation $(F_i)_{i \geq 0}$ generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$, with $\mathbb{F}_l \subseteq \mathbb{F}_q$. Suppose that $e(P_{k+1}|P_k) > 1$ for some $k \geq 0$, $P_{k+1} \in S(F_{k+1}/\mathbb{F}_q)$ and $P_k = P_{k+1} \cap F_k$. Then $x_k (P_k)$ is either*

- (i) *a zero of $\text{disc}_{x_{k+1}} f_{k+1}(x_k, x_{k+1})$, or*
- (ii) *a zero of $\text{disc}_{x_{k+1}} f_{k+1}^{(x_{k+1})}(x_k, 0)$, or*
- (iii) *∞ if 0 is a zero of $\text{disc}_{x_{k+1}} f_{k+1}^{(x_k)}(x_k, x_{k+1})$, or*
- (iv) *∞ if 0 is a zero of $\text{disc}_{x_{k+1}} f_{k+1}^{(x_k, x_{k+1})}(x_k, 0)$.*

Proof. This is just an application of the 4 cases of Proposition 3.4. (i) and (ii) represents the cases where $x_k (P_k) \in \overline{\mathbb{F}}$ and (iii) and (iv) the cases where $x_k (P_k) = \infty$. ■

Theorem 3.13 enables us to, given an explicit description of a tower, find the elements of the residue class $F_k \bmod P_k$ in the k th step of the tower, above which any ramification in the extension F_{k+1}/F_k can occur. This theorem leads to the following definition:

Definition 3.14 (Ramification-generating set of functions) *Let \mathcal{F} be an explicit tower over \mathbb{F}_q with representation $(F_i)_{i \geq 0}$ generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$, with $\mathbb{F}_l \subseteq \mathbb{F}_q$. Then, for each $k \geq 0$, the ramification-generating set at step k of the tower is the minimal set $R_k \subseteq MI_{\mathbb{F}_l}(x_k)$ such that each \mathbb{F}_l -irreducible factor of*

$$\text{disc}_{x_{k+1}} f_{k+1}(x_k, x_{k+1}) \text{ and } \text{disc}_{x_{k+1}} f_{k+1}^{(\cdot, x_{k+1})}(x_k, 0)$$

is in R_k , and $\frac{1}{x_k}$ is in R_k if $x_k = 0$ is a root of

$$\text{disc}_{x_{k+1}} f_{k+1}^{(x_k, \cdot)}(x_k, x_{k+1}) \cdot \text{disc}_{x_{k+1}} f_{k+1}^{(x_k, x_{k+1})}(x_k, 0).$$

Note that the converse of Theorem 3.13 does not hold - we will show a case where it does not hold in Example 3.21, where direct application of Theorem 3.13 in order to compute a superset of a ramification-generating polynomial set will introduce superfluous elements. This problem can be solved by performing a finer analysis which will identify the superfluous elements.

Two cases where the construction of ramification-generating sets of functions can be made precise (i.e. without the introduction of superfluous elements) is the case of Kummer extensions and Artin-Schreier extensions. For example, if step k in the tower is an Artin-Schreier extension given by

$$f_{k+1}(x_k, x_{k+1}) = b(x_k) \left(x_{k+1}^p - x_{k+1} \right) - a(x_k)$$

with $a, b \in \mathbb{F}_q[x_k]$, the set R_k consists of the poles of the rational function $\frac{a(x_k)}{b(x_k)}$. For details on these two cases, we refer to [59, III.7].

3.3 Ramification inheritance

For a fixed k , we can use Definition 3.14 to obtain R_k , and examining the set of solutions of the polynomials in R_k we obtain exactly the elements of $\overline{\mathbb{F}} \cup \{\infty\}$ corresponding to property (i) of Definition 3.5, as a result of Theorem 3.13. We can apply the method of predecessor polynomials (Definition 3.11) to analyze the effect of the set R_k on the lower steps $k-1$, $k-2$, ..., 0 of the tower. This is the effect originally described in Definition 3.5 properties (ii) and (iii).

In order to allow for recursive composition of multi-step predecessors, we extend the notation concerning $\text{Pred}_f(\cdot)$ by, in the context that the full sequence $(f_i)_{i \geq 1}$ is known, writing (for $n \geq m$)

$$\text{Pred}_{f_n}^m(Q) := \text{Pred}_{f_{n-m+1}} \circ \text{Pred}_{f_{n-m+2}} \circ \text{Pred}_{f_{n-m+3}} \circ \dots \circ \text{Pred}_{f_n}(Q), \quad (3.5)$$

where the right-hand side of (3.5) consists of the composition of Pred for step n of the tower down to step $n-m$. We assume the convention that

$\text{Pred}_{f_n}^0(Q) = Q$ for any $Q \subseteq MI_{\mathbb{F}_l}(x_k)$

Theorem 3.15 *Let \mathcal{F} be an explicit tower over \mathbb{F}_q with representation $(F_i)_{i \geq 0}$ generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$. Suppose $(R_i)_{i \geq 0}$ is a sequence of ramification-generating polynomial sets for the steps $i = 0, 1, 2, \dots$ of the tower \mathcal{F} . Let $P_k \in V_{F_k}(\mathcal{F})$, the F_k -ramification locus of \mathcal{F} for some $k \geq 0$. Then $x_k(P_k)$ is a solution of a polynomial in the set*

$$B_k := \bigcup_{j=0}^{\infty} \text{Pred}_{f_{k+j}}^j(R_{k+j}).$$

Proof. Since $P_k \in V_{F_k}(\mathcal{F})$, $P_k \in S(F_k/\mathbb{F}_q)$ is ramified in the extension F_{k+n+1}/F_k for some $n \geq 0$. Suppose n is the smallest integer for which this occurs. Then there exists a place $P_{k+n+1} \in S(F_{k+n+1}/\mathbb{F}_q)$ so that $P_{k+n+1} \cap F_k = P_k$. Let $P_{k+n} := P_{k+n+1} \cap F_{k+n}$. Then $e(P_{k+n+1}|P_{k+n}) > 1$. Since $e(P_{k+n+1}|P_{k+n}) > 1$, Theorem 3.13 and the definition of a ramification-generating polynomial set implies that $x_{k+n}(P_{k+n})$ is a root of an element of R_{k+n} . The discussion after Definition 3.11 then shows that $x_{k+n-1}(P_{k+n-1})$ is a root of an element of $\text{Pred}_{f_{k+n}}(R_{k+n})$. Continuing in this way, we find that $x_k(P_k)$ is a root of an element of

$$\text{Pred}_{f_{k+1}} \circ \text{Pred}_{f_{k+2}} \circ \text{Pred}_{f_{k+3}} \circ \dots \circ \text{Pred}_{f_{k+n}}(R_{k+n}) = \text{Pred}_{f_{k+n}}^n(R_{k+n}) \subseteq B_k,$$

as required. ■

Example 3.16 *We calculate the ramification locus of the tower \mathcal{F}_1 over \mathbb{F}_8 generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_2[x_{i-1}, x_i])_{i \geq 1}$, where each $f_{i+1}(x_i, x_{i+1}) = f(x_i, x_{i+1}) = x_i x_{i+1}^2 + x_i x_{i+1} + x_i^2 + x_i + 1$. This is the tower introduced by van der Geer and van der Vlugt [65], which was the first explicit tower of Artin-Schreier extensions, over a field of non-square cardinality, with good limit. This is a special case of a more general family of towers, introduced later by Bezerra, García and Stichtenoth [12]. The basic function field of this tower is the function field $\mathbb{F}_8(x, y)$ over \mathbb{F}_8 with $xy^2 + xy + x^2 + x + 1 = 0$, or*

written in variable separated form as

$$y^2 + y = \frac{x^2 + x + 1}{x}. \quad (3.6)$$

To ensure that this does indeed define a tower, one can check that the unique pole of x_0 in the rational function field $F_0 = \mathbb{F}_8(x_0)$ is totally ramified in each subsequent extension of the tower. The details are omitted here.

Precomputing the reciprocal polynomials, we find that

$$\begin{aligned} f_{i+1}^{(x_i, \cdot)}(x_i, x_{i+1}) &= f_{i+1}(x_i, x_{i+1}) \\ &= x_i x_{i+1}^2 + x_i x_{i+1} + x_i^2 + x_i + 1 \end{aligned}$$

and

$$\begin{aligned} f_{i+1}^{(x_i, x_{i+1})}(x_i, x_{i+1}) &= f_{i+1}^{(\cdot, x_{i+1})}(x_i, x_{i+1}) \\ &= x_i + x_i x_{i+1} + x_i^2 x_{i+1}^2 + x_i x_{i+1}^2 + x_{i+1}^2. \end{aligned}$$

It turns out that

$$\begin{aligned} \text{disc}_{x_{i+1}} f_{i+1}(x_i, x_{i+1}) &= \text{disc}_{x_{i+1}}^{(x_i, \cdot)} f_{i+1}(x_i, x_{i+1}) \\ &= x_i^2 \\ &= \text{disc}_{x_{i+1}}^{(\cdot, x_{i+1})} f_{i+1}(x_i, x_{i+1}) = \text{disc}_{x_{i+1}}^{(x_i, x_{i+1})} f_{i+1}(x_i, x_{i+1}). \end{aligned}$$

Considering Definition 3.14, we see that $(R_i)_{i \geq 0}$ with each $R_i = \left\{x_i, \frac{1}{x_i}\right\}$ is a ramification-generating polynomial set. This agrees with the result using the ramification theory of Artin-Schreier extensions, as R_i corresponds to the poles of $\frac{x_i^2 + x_i + 1}{x_i}$ for each $i \geq 0$. Suppose that $P \in V_{F_0}(\mathcal{F}_1)$. Then, by Theorem 3.15,

$$B_0 = \bigcup_{k=0}^{\infty} \text{Pred}_{f_k}^k(R_k).$$

As every element of B_k is of the form $\text{Pred}_{f_k}^k(R_k)$ for some k , we can start with the

(finite) set¹ $S_0 := R = \left\{ T, \frac{1}{T} \right\}$, and construct the ascending sequence of sets

$$S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots \quad (3.7)$$

by the simple rule $S_{i+1} := S_i \cup \text{Pred}_f(S_i)$. The predecessors of these elements can now be computed using Theorem 3.10. For example, when computing $\text{Pred}_f(x_{i+1})$ we have that a Gröbner basis for the ideal

$$I = \left\langle x_i x_{i+1}^2 + x_i x_{i+1} + x_i^2 + x_i + 1, x_{i+1} \right\rangle$$

with monomial ordering on $\mathbb{F}_2[x_i, x_{i+1}]$ with $x_{i+1} > x_i$ is easily seen to be

$$\mathcal{G} = \left\{ x_i^2 + x_i + 1, x_{i+1} \right\}$$

and hence Theorem 3.10 (i) yields $\text{Pred}_f(T) = \{T^2 + T + 1\}$. Recursively performing this procedure for this tower, we have

$$\begin{aligned} \text{Pred}_f\left(\frac{1}{T}\right) &= \left\{ T, \frac{1}{T} \right\} \text{ (by (ii) and (iv))}, \\ \text{Pred}_f(T) &= \left\{ T^2 + T + 1 \right\} \text{ (by (i))}, \\ \text{Pred}_f(T^2 + T + 1) &= \{T + 1\} \text{ (by (i))}, \text{ and} \\ \text{Pred}_f(T + 1) &= \left\{ T^2 + T + 1 \right\} \text{ (by (i))}. \end{aligned}$$

This implies that

$$\begin{aligned} S_0 &= \left\{ T, \frac{1}{T} \right\}, \\ S_1 &= \left\{ T, \frac{1}{T}, T^2 + T + 1 \right\}, \text{ and} \\ S_i &= \left\{ T, \frac{1}{T}, T^2 + T + 1, T + 1 \right\} \text{ for } i \geq 2, \end{aligned}$$

¹We now use one designator T for all the T_i as each $f_i = f$.

and therefore $B_0 = \bigcup_{i=0}^{\infty} S_i = \left\{ T, \frac{1}{T}, T^2 + T + 1, T + 1 \right\}$. It follows that

$$V_{F_0}(\mathcal{F}_1) = \left\{ P_{p(x_0)} \in S(F_0/\mathbb{F}_q) : p \in B_0 \right\},$$

implying that \mathcal{F}_1 is of finite ramification type.

3.4 Ramification graphs

The process of identifying a finite ramification locus, as described by the previous two sections, can be reformulated as a graph-traversal algorithm. Given an explicit tower \mathcal{F} over \mathbb{F}_q , ($q = p^n$) with a representation $(F_i)_{i \geq 0}$ generated by the sequence $(f_i)_{i \geq 1}$ of polynomials, one can define the associated *predecessor graph of the tower* over \mathbb{F}_l , for \mathbb{F}_l a subfield of \mathbb{F}_q .

In this section, we will rewrite the notions of the two previous sections in graph-theoretic terms. Representing certain aspects of towers in terms of graph theory is not new, as it was done before in [5]. However, the approach described here is more general, as we allow the possibility of different defining equations at each step, decrease the number of vertices by using irreducible polynomials which each represent more than one place, and thereby making the construction a more natural fit for calculations using Gröbner bases. In Chapter 4, the splitting behaviour of a general $(f_i)_{i \geq 1}$ -tower will be analyzed in an analogous way, but under the assumption that the finite ramification locus, if it exists, is known.

Definition 3.17 (predecessor graph of a tower) *Let \mathcal{F} be a tower over \mathbb{F}_q , which has a representation $(F_i)_{i \geq 0}$ generated by the sequence $(f_i)_{i \geq 1}$ of polynomials in $(\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$. Let \mathbb{F}_l be a subfield of \mathbb{F}_q . Form the edge-labeled directed multigraph $\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}} = (V, E)$ by defining its vertex and (directed) edge sets as follows:*

$$V = \{ p(T_k) \in M_{\mathbb{F}_l}(T_k) : k \geq 0 \},$$

$$E = \left\{ \left(p(T_k) \xrightarrow{f_{k+1}} q(T_{k+1}) \right) : k \geq 0, p \in \text{Pred}_{f_{k+1}}(q) \text{ and } p, q \in V(\Gamma) \right\}.$$

We refer to Γ as the \mathbb{F}_l -predecessor graph² of \mathcal{F} . As $MI_{\mathbb{F}_l}(T_k)$ is an infinite set, the vertex set $V(\Gamma)$ (and hence the edge set $E(\Gamma)$) of Γ is infinite.

Fix some $i \geq 0$ and consider the map $\chi = \chi_{\mathbb{F}_l}$ defined on

$$S(F_i/\mathbb{F}_q) \xrightarrow{\chi} \mathcal{P}(V(\Gamma)) = \mathcal{P}\left(V\left(\Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}\right)\right)$$

where $\mathcal{P}(V(\Gamma))$ denotes the power set of $V(\Gamma)$ and a place P of the function field F_i/\mathbb{F}_q is mapped to the set

$$\chi(P) := \left\{ f_{\chi(P),j} : 0 \leq j \leq i \right\},$$

where $f_{\chi(P),j}(T_j)$ is the unique element of $MI_{\mathbb{F}_l}(T_j)$ such that $a_j = x_j(P)$ is a root of $f_{\chi(P),j}$, or $f_{\chi(P),j} = \frac{1}{T_j}$ if $x_j(P) = \infty$. The map χ embeds places of each step of the tower \mathcal{F} into the graph Γ as paths of length i .

The definition of $\chi(P)$ leads to the following natural property: if Q is a place lying above P with $Q \in S(F_j/\mathbb{F}_q)$ and $P = Q \cap F_i$ (with $i < j$), then $\chi(P) \subseteq \chi(Q)$.

Definition 3.18 (ramification graph) Let \mathcal{F} be an explicit tower over \mathbb{F}_q which is generated by a sequence $(f_i)_{i \geq 1}$ of polynomials (each with coefficient field $F_l \subseteq \mathbb{F}_q$) and its associated predecessor graph $\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$. Let $(R_k)_{k \geq 0}$ be a sequence of ramification-generating sets of functions for the tower \mathcal{F} . Define Γ_B to be the induced subgraph of Γ which consists of the connected components of Γ with the property that

$$p(T_k) \in R_k \text{ for some } k \geq 0 \Rightarrow \text{Pred}_{f_k}^n(p(T_k)) \subseteq V(\Gamma_B) \text{ for each } 0 \leq n \leq k. \quad (3.8)$$

Then, if P is any place of $S(F_i/\mathbb{F}_q)$ for some $i \geq 0$ which is ramified in some extension F_{i+j}/F_i for $j \geq 1$, it follows that

$$\chi(P) \subseteq V(\Gamma_B).$$

Proof. Suppose $f \in \chi(P)$ for some $P \in S(F_i/\mathbb{F}_q)$, where $f \in MI_{\mathbb{F}_l}(T_h)$ for

²In Chapter 4, we will refer to Γ as the \mathbb{F}_l -splitting graph of \mathcal{F} .

some $h \leq i$. Let $j \in \mathbb{N}$ be the smallest natural number so that P is ramified in F_{i+j}/F_i , with $Q|P$ where $Q \in S(F_{i+j}/\mathbb{F}_q)$. As $e(Q|Q \cap F_{i+j-1}) > 1$, we have that the minimum \mathbb{F}_l -irreducible polynomial $m(T_{i+j-1})$ (or $\frac{1}{T_{i+j-1}}$) of $x_{i+j-1}(Q \cap F_{i+j-1})$ is in the ramification-generating set of functions R_{i+j-1} . As $(Q \cap F_{i+j-1})|P$, (3.8) then implies that

$$f \in \text{Pred}_{f_{i+j-1}}^{(j-1)+(i-h)}(m(T_{i+j-1})) \subseteq V(\Gamma_B) \cap MI_{\mathbb{F}_l}(T_h),$$

from which it follows that $\chi(P) \subseteq V(\Gamma_B)$. ■

From here on, we refer to Γ_B as the \mathbb{F}_l -ramification graph of \mathcal{F} . Intuitively, the graph Γ_B from Definition 3.18 is generated as subgraph of Γ by the vertices of Γ which are in the ramification-generating sets $(R_i)_{i \geq 0}$, and then recursively computing predecessors to obtain the full Γ_B . We note that, similarly to the graphs in [5], each place corresponds to a path in Γ , but χ is not one-to-one, implying that different places in the tower can share the same path.

Proposition 3.19 *Let Γ_B be the \mathbb{F}_l -ramification graph of the explicit tower \mathcal{F} . If the intersection of the vertex set $V(\Gamma_B)$ of Γ_B and $MI_{\mathbb{F}_l}(T_i)$ is finite for some $i \geq 0$, \mathcal{F} has a finite ramification locus.*

Proof. As a polynomial can have at most finitely many predecessor polynomial, we need only show the statement for $i = 0$. Suppose $V_{F_0}(\mathcal{F})$ is infinite. For each $P \in V_{F_0}(\mathcal{F})$, $\chi(P) = \{f\}$ for some f , as $i = 0$. As $f \in MI_{\mathbb{F}_l}(x_0)$ by definition, the intersection $MI_{\mathbb{F}_l}(x_0) \cap V(\Gamma_B)$ has infinitely many elements. This contradicts our assumption, and therefore the set $V_{F_0}(\mathcal{F})$ is finite. ■

The result above shows that the graph Γ_B captures all the ramification in all steps of the tower, and therefore that if vertices of Γ_B corresponds to only finitely many places at a specific step i in the tower, the F_i -ramification locus of \mathcal{F} must be finite.

We present some examples of where the finite ramification locus of one-step towers are analyzed in this way. Note that although in each of the examples in this chapter the ramification graph Γ_B is connected, this

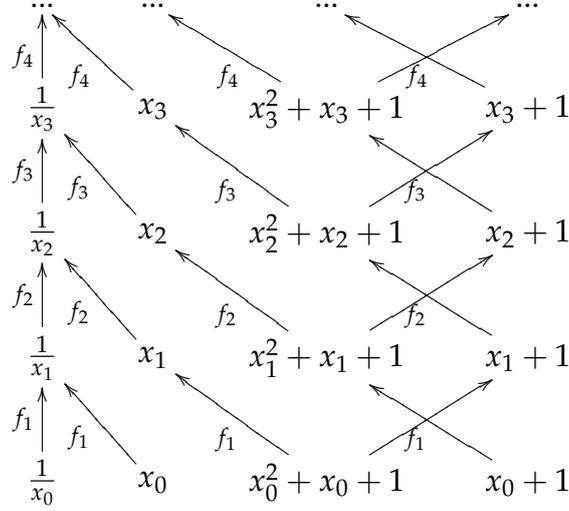


Figure 3.1: Ramification graph Γ_B for Example 3.20

need not be the case. A family of towers which have a disconnected \mathbb{F}_p -ramification graph Γ_B is exhibited in Chapter 6, Figure 6.6.

Example 3.20 (Example 3.16 revisited) As

$$f_{i+1}(x_i, x_{i+1}) = f(x_i, x_{i+1}) = x_i x_{i+1}^2 + x_i x_{i+1} + x_i^2 + x_i + 1$$

for each $i \geq 0$, \mathcal{F}_1 is a one-step tower. Collecting all the information from Example 3.16, we obtain the representation³ of Γ_B given in Figure 3.1. We can again compute the ramification locus and in a similar way to Example 3.16 obtain

$$V_{F_0}(\mathcal{F}_1) = \left\{ P_{p(x_0)} \in S(F_0/\mathbb{F}_q) : p \in V(\Gamma_B) \cap MI_{\mathbb{F}_1}(x_0) \right\},$$

which yields the same result as before since

$$V(\Gamma_B) \cap MI_{\mathbb{F}_1}(x_k) = \left\{ x_k, \frac{1}{x_k}, x_k^2 + x_k + 1, x_k + 1 \right\}$$

for any $k \geq 0$.

³In this and many subsequent representations of graphs related to towers, one should think of the rows (starting at the bottom row) as corresponding to steps in the tower.

We note that the graph encapsulates all the information on predecessor polynomials we obtained during the computations in Example 3.16. As the above example is a one-step tower, the equivalence relation \sim_1 applies and we can obtain a simplified, but complete picture of the ramification behaviour in a much simplified version of Figure 3.1. As \sim_1 implies that $x_i \sim_1 x_j$ for all $i, j \geq 0$ we need not differentiate between the x_i 's, and we denote representatives for x_i and f_i (for all $i \geq 0$) by \tilde{x} and \tilde{f} .

More generally, we can extend an arbitrary equivalence relation \sim on the indeterminates (and therefore the defining polynomials) to the vertex set of the \mathbb{F}_l -ramification graph Γ_B as it also contains univariate functions in the indeterminates $\{x_i : i \geq 0\}$. We abuse notation and define

$$\tilde{\Gamma}_B := \Gamma_B / \sim$$

as the graph induced by the equivalence relation \sim on the vertices of Γ_B . This means that

$$\left(\tilde{p}(\tilde{x}) \xrightarrow{\tilde{f}} \tilde{q}(\tilde{y}) \right) \in E(\tilde{\Gamma}_B) \text{ if and only if } \left(p_i(x_i) \xrightarrow{f_{i+1}} q_{i+1}(x_{i+1}) \right) \in E(\Gamma_B)$$

for some $i \geq 0$, $p_i \in \mathbb{F}_l[x_i]$, $q_{i+1} \in \mathbb{F}_l[x_{i+1}]$ and defining polynomial $f_{i+1}(x_i, x_{i+1}) \in \mathbb{F}_l[x_i, x_{i+1}]$ from step i to $i+1$ of the tower we have that $p_i \sim \tilde{p}$, $q_{i+1} \sim \tilde{q}$ and $f_{i+1} \sim \tilde{f}$ (and hence $x_i \sim \tilde{x}$ and $x_{i+1} \sim \tilde{y}$). We refer to $\tilde{\Gamma}_B$ as the *condensed* version of Γ_B .

By considering the vertex set of the graph Γ_B from Figure 3.1 modulo \sim_1 , we obtain the condensed graph $\tilde{\Gamma}_B$, shown in Figure 3.2 which simplifies the representation in Figure 3.1. In Figure 3.2, as we are employing the (one-step) equivalence relation \sim_1 , the presence of the edge $p(\tilde{x}) \rightarrow q(\tilde{x})$ in $\tilde{\Gamma}_B$ (as now $x_i \sim_1 x_{i+1} \sim_1 \tilde{x}$) should be interpreted as meaning that the edge $p(x_i) \rightarrow q(x_{i+1})$ is an element of Γ_B for all $i \geq 0$.

Example 3.21 Consider the explicit one-step tower \mathcal{F}_2 over the finite field \mathbb{F}_4 , and an explicit description is given by the sequence $(f_i)_{i \geq 1}$ of polynomials where

$$f_{i+1}(x_i, x_{i+1}) = f(x_i, x_{i+1}) = x_{i+1}^3 + (x_i + 1)^3 + 1$$

$$\tilde{f} \circlearrowleft \frac{1}{\tilde{x}} \xleftarrow{\tilde{f}} \tilde{x} \xleftarrow{\tilde{f}} \tilde{x}^2 + \tilde{x} + 1 \xrightleftharpoons[\tilde{f}]{\tilde{f}} \tilde{x} + 1$$

Figure 3.2: Condensed ramification graph $\tilde{\Gamma}_B$ for Example 3.20

for each $i \geq 0$. The sequence $(f_i)_{i \geq 1}$ generates the representation $(F_i)_{i \geq 0}$ of \mathcal{F}_2 in the canonical way. This tamely ramified tower of Kummer extensions is due to García, Stichtenoth and Thomas [37], and is a variation of Example 2.20, a Fermat tower.

We first check that \mathcal{F}_2 is indeed a tower. As before, we write the relation between x_i and x_{i+1} in variable separated form as

$$x_{i+1}^3 = (x_i + 1)^3 + 1 \quad (3.9)$$

and note that x_i is a simple zero of the right-hand side of (3.9) as

$$\frac{d}{dx_i} \left((x_i + 1)^3 + 1 \right) = x_i^2 + 1 \text{ and } \gcd \left((x_i + 1)^3 + 1, x_i^2 + 1 \right) = 1.$$

A place $P \in S(F_i/\mathbb{F}_4)$ corresponding to $x_i = 0$ is therefore totally ramified in the extension F_{i+1}/F_i , with the unique place $Q \in S(F_{i+1}/\mathbb{F}_4)$ lying above P . In the same way as Example 2.20's (2.6) we see that Q is a simple zero of $x_{i+1} = 0$. Repeating this process, we see that the unique place $R \in S(F_{i+2}/\mathbb{F}_4)$ lying above Q is a simple zero of $x_{i+2} = 0$. Starting at $x_0 = 0$ and repeating this process, we see that the unique place in $S(F_0/\mathbb{F}_4)$ which is a simple zero of $x_0 = 0$ is totally ramified in the extension F_n/F_0 for any $n \geq 1$. Therefore \mathcal{F}_2 is a tower.

As in Example 3.16, we use a single $T = T_i$ for each i as indeterminate for the functions, as this is a one-step tower. We now set out to construct a sequence $(R_i)_{i \geq 0}$ of ramification-capturing polynomial sets for this tower. The argument above shows that $T = T_i \in R_i$ for each $i \geq 0$. Blindly applying Theorem 3.13, it seems as if we should include $\frac{1}{T} = \frac{1}{T_i}$ in R_i as well. However, these are superfluous elements⁴ and we therefore only set $R_i = \{T\}$ for each $i \geq 0$.

⁴If P is a simple pole of $x_i = 0$ in $S(F_0/\mathbb{F}_4)$, rewriting the defining equation gives

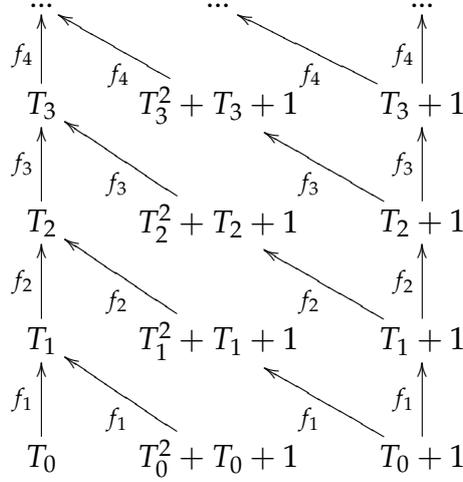


Figure 3.3: Ramification graph Γ_B for Example 3.21

Computing predecessor polynomials using Theorem 3.10, we see that

$$\begin{aligned} \text{Pred}_f(T) &= \{T, T^2 + T + 1\}, \\ \text{Pred}_f(T^2 + T + 1) &= \{T + 1\} \text{ and} \\ \text{Pred}_f(T + 1) &= \{T + 1\}. \end{aligned}$$

This yields the graph Γ_B given in Figure 3.3. Then

$$\begin{aligned} V_{F_0}(\mathcal{F}_2) &= \left\{ P_{p(x_0)} \in S(F_0/\mathbb{F}_q) : p \in V(\Gamma_B) \cap MI_{\mathbb{F}_l}(T_0) \right\} \quad (3.10) \\ &= \left\{ P_{p(x_0)} \in S(F_0/\mathbb{F}_q) : p \in \{x_0, x_0 + 1, x_0^2 + x_0 + 1\} \right\} \\ &= \{x_0, x_0 + 1, x_0^2 + x_0 + 1\}, \end{aligned}$$

which is a finite set. In the last line of (3.10) we abuse notation by representing the places as functions of which they are zeroes.

It is interesting to compare the graph Γ_B from Example 3.21 with the analogous representation of the same tower in [9, Example 4.3]. In the

$\left(\frac{x_{i+1}}{x_i}\right)^3 = 1 + 3 \cdot \frac{1}{x_i} + 3 \cdot \frac{1}{x_i^2} = 1 \pmod{P}$. As \mathbb{F}_4 contains all three roots of unity, P splits completely in F_{i+1}/F_i , hence unramified.

representation of the one-step tower by Beelen et al, only a single step of the tower is used, essentially what is done by representing the graph in Figure 3.3 modulo \sim_1 .

Example 3.22 Let \mathbb{F}_q be a finite field of characteristic p . Suppose $q = k^r = l^s$ for some natural numbers $k, l, r, s \geq 2$. Let $m = \frac{q-1}{k-1}$ and $n = \frac{q-1}{l-1}$. Let $a, b, c \in \mathbb{F}_k^*$, $\alpha, \beta, \gamma \in \mathbb{F}_l^*$ and assume further⁵ that $a \cdot b^m + c = 0$ and $\alpha \cdot \beta^n + \gamma = 0$. We construct an explicit two-step tower \mathcal{F}_3 over \mathbb{F}_q by constructing its representation $(F_i)_{i \geq 0}$ from the polynomial sequence $(h_i)_{i \geq 1}$ given by

$$h_{i+1}(x_i, x_{i+1}) = \begin{cases} \tilde{f}(x_i, x_{i+1}) & \text{if } i \equiv 0 \pmod{2}, \text{ and} \\ \tilde{g}(x_i, x_{i+1}) & \text{if } i \equiv 1 \pmod{2}, \end{cases}$$

where

$$\tilde{f}(x_i, x_{i+1}) = x_{i+1}^m - a(x_i + b)^m - c$$

and

$$\tilde{g}(x_i, x_{i+1}) = x_{i+1}^n - \alpha(x_i + \beta)^n - \gamma.$$

This is a variation on a known one-step tower from [30], where the two constituent equations of this tower come from the one-step tower.

We claim that (a) this defines a tower, (b) the tower has a finite ramification locus, (c) it is completely splitting (over \mathbb{F}_q) and (d) it is asymptotically good.

Proof.

(a) The defining equations imply that

$$x_{i+1}^m = a(x_i + b)^m + c \text{ for even } i, \text{ and} \quad (3.11)$$

$$x_{i+1}^n = \alpha(x_i + \beta)^n + \gamma \text{ for even } i. \quad (3.12)$$

It follows from (3.11) that the place P given by $x_0 = 0$ is a simple zero of the right-hand side of (3.11) for $i = 0$, and it therefore ramifies

⁵A necessary and sufficient condition is that a, b, c, α, β and γ are all nonzero, as shown by Wulftange, see [36, Note 3.5], [70]. Our stronger assumptions ensure that \mathcal{F}_3 is *totally* ramified.

totally in the extension F_1/F_0 . The unique place Q above $x_0 = 0$ is then a simple zero of x_1 . Considering (3.12), we have that the simple zero Q of the right-hand side of (3.12) is totally ramified in F_2/F_1 and has a unique place R above $x_1 = 0$ which is a simple zero of x_2 . Continuing in this way and alternatingly using \tilde{f} and \tilde{g} , we see that P is totally ramified in the tower, and hence \mathbb{F}_q is the full constant field of each F_i for $i \geq 0$.

- (b) If we take account the superfluous element $\frac{1}{T_i} \notin R_i$ as in Example 3.21, it turns out that the ramification-generating sets of functions are given by

$$R_i = \begin{cases} \text{the irreducible factors of } \alpha(T_i + \beta)^n + \gamma & \text{if } i \text{ is odd, and} \\ \text{the irreducible factors of } a(T_i + b)^m + c & \text{if } i \text{ is even.} \end{cases}$$

However, as $a, c \in \mathbb{F}_k^*$, it follows that $(T_i + b)^m \in \mathbb{F}_k^*$ and therefore $T_i \in \mathbb{F}_q$, as $z \mapsto z^m$ is the norm map from \mathbb{F}_q to \mathbb{F}_k , for even i . A similar argument shows that $T_i \in \mathbb{F}_q$ for odd i as well (involving the $z \mapsto z^n$ norm map). This implies that R_i is a subset of the set of irreducible factors of $T_i^q - T_i$, which we denote by M_i .

To show that the ramification locus is finite, it suffices to show that $(M_i)_{i \geq 0}$ is a ramification-capturing function sequence for this tower. We have $R_i \subseteq M_i$. We need to show that

$$\text{Pred}_{\tilde{f}}(M_{i+1}) \subseteq M_i \text{ if } i \text{ is even, and } \text{Pred}_{\tilde{g}}(M_{i+1}) \subseteq M_i \text{ if } i \text{ is odd.} \quad (3.13)$$

This can be done without explicitly computing predecessor polynomials by the following argument from [36, Proposition 3.8] (the case for \tilde{g} is similar): Consider the equation $\tilde{f}(x_i, x_{i+1}) = 0$ at some place $P \in S(F_{i+1}/\mathbb{F}_q)$ for some even i , $x_{i+1}(P) \in \mathbb{F}_q$ and (hence) $T_{i+1} - x_{i+1}(P) \in M_{i+1}$. Considering (3.11), we note that as $a, c, (x_{i+1}(P))^m \in \mathbb{F}_k$, it follows that $(x_i(P) + b)^m \in \mathbb{F}_k$. Therefore $x_i(P) \in \mathbb{F}_q$, which implies that $\text{Pred}_{\tilde{f}}(M_{i+1})$ does only contain elements of M_i . This

implies then that

$$\text{Pred}_f^1(M_{\text{odd}}) \subseteq \text{Pred}_g^0(M_{\text{even}}) \text{ and } \text{Pred}_g^1(M_{\text{even}}) \subseteq \text{Pred}_f^0(M_{\text{odd}})$$

and then by alternately applying Pred_f and Pred_g to the two inclusions above, we obtain

$$\text{Pred}_f^{k+1}(M_{\text{odd}}) \subseteq \text{Pred}_g^k(M_{\text{even}}) \text{ and } \text{Pred}_g^{k+1}(M_{\text{even}}) \subseteq \text{Pred}_f^k(M_{\text{odd}})$$

for all $k \geq 0$ and therefore

$$\dots \subseteq \text{Pred}_f^k(M_{\text{odd}}) \subseteq \text{Pred}_g^{k-1}(M_{\text{even}}) \subseteq \text{Pred}_f^{k-2}(M_{\text{odd}}) \subseteq \dots \subseteq M_0$$

for all $k \geq 0$, from which it follows that the ramification locus of \mathcal{F}_3 is generated by a subset of the finite set M_0 , as required.

- (c) The proof that $\#T_{\mathbb{F}_q(x_0)}(\mathcal{F}_3) > 0$ is postponed to Chapter 4 (see Example 4.10) where it is calculated using complete splitting graphs. Without invoking the theory of Chapter 4, this can be seen to hold in a similar manner as the footnote on p. 3.21 by noting that the pole of x_0 in $F_0 = \mathbb{F}_q(x_0)$ splits completely in \mathcal{F}_3 .
- (d) As $(mn, q) = 1$, the tower \mathcal{F}_3 is tamely ramified. Therefore (b), (c) and Corollary 2.18 implies that the tower has positive limit.

■

For specific examples of towers such as in Example 3.22, we can construct ramification graphs Γ_B , or their condensed form $\tilde{\Gamma}_B$ working modulo \sim_2 . For example, if $\mathbb{F}_q = \mathbb{F}_9$ and the two-step defining equations

$$f(x_i, x_{i+1}) = x_{i+1}^4 + (x_i + 1)^4 - 1 \in \mathbb{F}_3[x_i, x_{i+1}]$$

and

$$g(x_i, x_{i+1}) = x_{i+1}^4 + (x_i - 1)^4 + 1 \in \mathbb{F}_3[x_i, x_{i+1}]$$

are used (f when i is even, g when i is odd), we can consider the indeter-

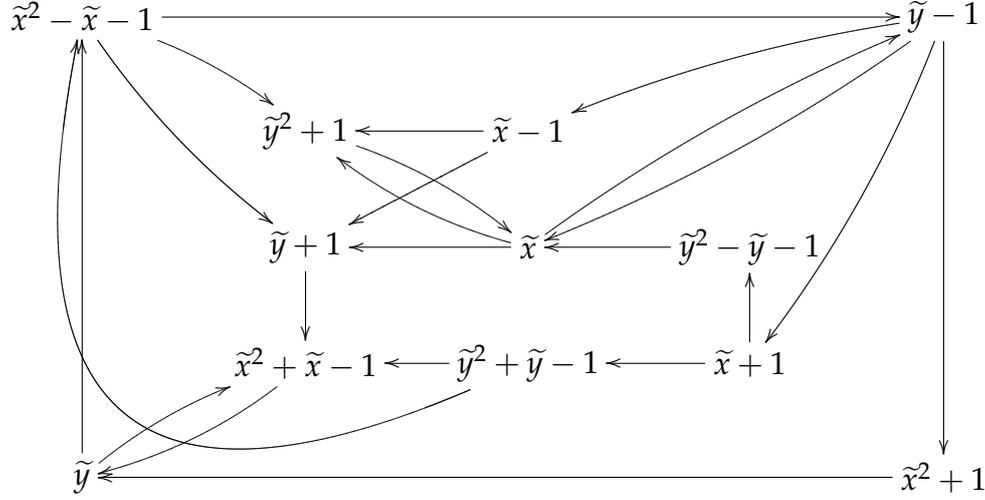


Figure 3.4: Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for Example 3.22 with specific f and g

minates

$$\{x_0, x_1, x_2, \dots\} \bmod \sim_2 \cong \{\tilde{x}, \tilde{y}\}$$

where \tilde{x} corresponds to the even i , and \tilde{y} to the odd i . Similarly, we let

$$\tilde{f}_1 \sim_2 f \text{ and } \tilde{f}_2 \sim_2 g.$$

Constructing the ramification graph (modulo \sim_2) we obtain the condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ as given in Figure 3.4. Note that the presence of an edge $p(\tilde{x}) \xrightarrow{\tilde{f}_1} q(\tilde{y})$ in $\tilde{\Gamma}_B$ implies the presence of the edge $p(x_i) \xrightarrow{f(x_i, x_{i+1})} q(x_{i+1})$ in Γ_B for each even $i \geq 0$, and the presence of an edge $p(\tilde{y}) \xrightarrow{\tilde{f}_2} q(\tilde{x})$ in $\tilde{\Gamma}_B$ implies the presence of the edge $p(x_i) \xrightarrow{g(x_i, x_{i+1})} q(x_{i+1})$ in Γ_B for each odd $i \geq 0$. Moreover, the ramification locus has 6 elements, consisting of the places of $F_0 = \mathbb{F}_9(x_0)$ which are zeros of the 6 polynomials in $\mathbb{F}_3[\tilde{x}]$ in $V(\tilde{\Gamma}_B)$, corresponding to the elements of \mathbb{F}_9 . This two-step tower is asymptotically good with limit $\lambda(\mathcal{F}) \geq \frac{2}{7}$ by Corollary 2.18, which does not improve upon the limit obtained for the one-step Fermat towers generated by either \tilde{f}_1 or \tilde{f}_2 .

Chapter 4

Complete splitting

In the previous chapter, a method was described to systematically test whether an explicit tower \mathcal{F} has a finite ramification locus. This was achieved by explicitly calculating the (finite) ramification locus $V_{F_0}(\mathcal{F})$. In order to focus on the computation of $\lambda(\mathcal{F})$, we will now move to the next important aspect : complete splitting, as emphasised by Theorem 2.16.

As any place P of a function field F cannot be both ramified and completely splitting in an extension E/F , it is clear that any set we eventually identify as a completely splitting set for a tower \mathcal{F} will be disjoint from the ramification locus as identified in Chapter 3 (even for an infinite ramification locus).

Let \mathbb{F}_q be a finite field of characteristic p . In the context of explicit towers, the central problem of this chapter will be to, given an explicit tower

$$\mathcal{F} = (F_0 = \mathbb{F}_q(x_0), F_1, F_2, \dots)$$

generated by the defining polynomials $(f_i)_{i \geq 1} \in (\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$, find a finite field \mathbb{F}_r (if it exists) so that if the constant field of \mathcal{F} is extended to \mathbb{F}_r to form the tower \mathcal{F}' , the new tower \mathcal{F}' will have a nonempty completely splitting locus.

In order to analyze the splitting structure of a tower, we assume without loss of generality that the sequence $(f_i)_{i \geq 1}$ of polynomials are in fact bivariate polynomials over a subfield $\mathbb{F}_l \subseteq \mathbb{F}_q$. A choice of \mathbb{F}_l that we'll

often use is the prime subfield \mathbb{F}_p .

Moreover, we will again make the implicit assumption that we start with a sequence $(f_i)_{i \geq 1} \in (\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$, and that \mathbb{F}_q is an unknown finite extension of the (known) finite field \mathbb{F}_l . If the tower \mathcal{F} is defined over \mathbb{F}_l , it is defined over every finite extension of \mathbb{F}_l (as the ramification behaviour does not change as a result of constant field extensions), and our aim will be to find a suitable finite extension (which we denote by \mathbb{F}_r) of \mathbb{F}_l so that the choice $\mathbb{F}_q := \mathbb{F}_r$ will lead to the set $T_{\mathbb{F}_0/\mathbb{F}_r}(\mathcal{F}/\mathbb{F}_r)$ being nonempty.

In the remainder of this chapter we assume that \mathbb{F}_l is a finite field such that the sequence of defining polynomials $(f_i)_{i \geq 1} \in (\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$ induce an explicit tower \mathcal{F} , with canonical representation (F_0, F_1, F_2, \dots) over some unknown extension \mathbb{F}_q of \mathbb{F}_l (see Definition 2.19). For all practical purposes, we will therefore consider \mathcal{F} as a tower over \mathbb{F}_l , and extend the field of constants to \mathbb{F}_r , so that the new tower \mathcal{F}' over \mathbb{F}_r has a nonempty splitting locus, simultaneously preserving the ramification structure we discerned in Chapter 3.

4.1 Successor polynomials

As an analogue to the definition of predecessor polynomials (Definition 3.11) in Chapter 3, we now introduce *successor polynomials*.

Definition 4.1 (Successor polynomial set) *Let \mathcal{F} be an explicit tower with representation $(F_i)_{i \geq 0}$ over \mathbb{F}_q generated by the sequence $(f_i)_{i \geq 1}$ of polynomials (resp.) in $(\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$. Fix a monic \mathbb{F}_q -irreducible polynomial $p_k(T_k)$ (or $p_k(T_k) = \frac{1}{T_k}$). We define the successor polynomial set in terms of the predecessor polynomial set by*

$$\text{Succ}_{f_k}(p_k) := \left\{ p_{k+1} \in MI_{\mathbb{F}_q}(T_{k+1}) : p_k \in \text{Pred}_{f_k}(p_{k+1}) \right\}$$

where $MI_{\mathbb{F}_q}(T_{k+1})$ is the set of monic \mathbb{F}_q -irreducible polynomials in T_{k+1} , together with the element $\frac{1}{T_{k+1}}$.

For any $p_{k+1} \in \text{Succ}_{f_k}(p_k)$, we say that p_{k+1} is a successor polynomial of p_k . As for the case of predecessor polynomials, we will extend the notation for sets of polynomials in an analogous way to that for predecessor polynomials by setting

$$\text{Succ}_{f_{k+1}}(P) := \bigcup_{p \in P} \text{Succ}_{f_{k+1}}(p).$$

for the successor polynomial set of a set $P \subseteq MI_{\mathbb{F}_q}(T_k)$ of rational functions. For a polynomial p_k which is not necessarily irreducible, we can write (for $p_k = \prod_i p_{k,i}$)

$$\text{Succ}_{f_{k+1}}(\prod_i p_{k,i}) := \bigcup_i \text{Succ}_{f_{k+1}}(p_{k,i})$$

where each $p_{k,i} \in MI_{\mathbb{F}_q}(T_k)$. We also set

$$\text{Succ}_{f_n}^m(P) := \text{Succ}_{f_{n+m-1}} \circ \text{Succ}_{f_{n+m-2}} \circ \text{Succ}_{f_{n+m-3}} \circ \dots \circ \text{Succ}_{f_n}(P)$$

where \circ denotes composition in the usual sense with the convention that $\text{Succ}_{f_n}^0(P) = P$.

Proposition 4.2 *For a set $P \subseteq MI_{\mathbb{F}_q}(T_k)$ with $k \geq 1$, we have*

$$P \subseteq \text{Pred}_f \circ \text{Succ}_f(P) \cap \text{Succ}_g \circ \text{Pred}_g(P)$$

for any $f \in \mathbb{F}_q[T_k, T_{k+1}]$ and $g \in \mathbb{F}_q[T_{k-1}, T_k]$.

Proof. The containments $P \subseteq \text{Pred}_f(\text{Succ}_f(P))$ and $P \subseteq \text{Succ}_g(\text{Pred}_g(P))$ are easily shown using Definition 4.1. ■

The definition of a successor polynomial does not make the method of computation of it immediately clear, but a similar approach as Theorem 3.10 can be used to do so. This is summed up in the following theorem:

Theorem 4.3 *Let $p(T_k) \in MI_{\mathbb{F}_q}(T_{k+1})$, and $q(T_{k+1})$ be an arbitrary element of $\text{Succ}_f(p(T_k))$. Then $q(T_{k+1})$ is*

(i) either (if $p(T_k) \neq \frac{1}{T_k}$)

(a) a factor of the univariate generator polynomial of the elimination ideal

$$\langle p(T_k), f(T_k, T_{k+1}) \rangle \cap \mathbb{F}_q[T_{k+1}], \text{ or}$$

(b) $\frac{1}{T_{k+1}}$ if $\gcd\left(p(T_k), f^{(\cdot, T_{k+1})}(T_k, 0)\right) \neq 1$, or

(ii) either (if $p(T_k) = \frac{1}{T_k}$)

(a) a factor of $f^{(T_k, \cdot)}(0, T_{k+1})$, or

(b) $\frac{1}{T_{k+1}}$ if $f^{(T_k, T_{k+1})}(0, 0) = 0$

Proof.

(i) In this case $p(T_k)$ is a monic \mathbb{F}_q -irreducible polynomial. Then either (a) $q(T_{k+1}) \neq \frac{1}{T_{k+1}}$ (in which an argument similar to that in the proof Theorem 3.10 (i) shows that the statement does hold), or (b) $q(T_{k+1}) = \frac{1}{T_{k+1}}$, which implies that the reciprocal polynomial $f^{(\cdot, T_{k+1})}(z, 0)$ and $p(z)$ must have a common root (in $\overline{\mathbb{F}}$), as

$$f^{(\cdot, T_{k+1})}(z, t) = t^d \cdot f\left(z, \frac{1}{t}\right)$$

(by the definition of a reciprocal polynomial) where $\deg f = d$.

(ii) We have $p(T_k) = \frac{1}{T_k}$ and $q(T_{k+1})$ is either (a) a monic \mathbb{F}_q -irreducible polynomial or (b) $q(T_{k+1}) = \frac{1}{T_{k+1}}$. In case (a), $q(T_k)$ and $f^{(T_k, \cdot)}(0, T_{k+1})$ must have a common root (in $\overline{\mathbb{F}}$), and in case (b) $(T_k, T_{k+1}) = (0, 0)$ must be a root of

$$f^{(T_k, T_{k+1})}(0, 0) \equiv f^{(T_k, T_{k+1})}(T_k, T_{k+1}) \Big|_{(0,0)} = 0.$$

■

4.2 Complete splitting graph

We recall the definition of the predecessor graph of a tower (Definition 3.17). Because of Definition 4.1, we see that the edge set E of the directed graph $\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$ (where \mathbb{F}_l is a subfield of \mathbb{F}_q) of Definition 3.17 can be defined in an equivalent way in terms of successor polynomials as

$$E = \left\{ p(T_k) \xrightarrow{f_{k+1}} q(T_{k+1}) : k \geq 0, q \in \text{Succ}_{f_{k+1}}(p) \text{ and } p, q \in V(\Gamma) \right\}. \quad (4.1)$$

Because of this, we from here on refer to $\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$ as the \mathbb{F}_l -splitting graph of the tower \mathcal{F} with $(f_i)_{i \geq 1}$ generating its canonical representation.

When studying the ramification behaviour of the tower, we constructed the subgraph Γ_B of Γ , see Definition 3.17. In order to analyze complete splitting (in the sense of $T_F(\mathcal{F})$ being positive for some $F < \mathcal{F}$), we construct another subgraph of Γ :

Definition 4.4 (Complete splitting graph) *Let Γ be the \mathbb{F}_l -splitting graph of the tower \mathcal{F} generated by $(f_i)_{i \geq 1}$. Let Γ_T be the maximal subgraph of Γ such that the connected components of Γ_B and Γ_T are disjoint. We call Γ_T the complete \mathbb{F}_l -splitting graph of the tower \mathcal{F} .*

In contrast with the case for \mathbb{F}_l -ramification graphs, the defining property of a complete \mathbb{F}_l -splitting graph of a tower is that, given any vertex, recursively computing successor polynomials (vertices) will never lead to a vertex which is an element of Γ_B . This is due to the restriction on the vertex set in Definition 4.4.

It is however possible that there exist connected components of Γ having vertices in both Γ_B and Γ_T . This can occur when a vertex in Γ_B corresponding to an element of a ramification-generating set of functions has a successor polynomial which is not in Γ_B .

Note the distinction between the \mathbb{F}_l -splitting graph Γ and the complete \mathbb{F}_l -splitting graph Γ_T . In the results that follow, we show that a tower is completely splitting if there exists at least one component of Γ_T for which certain a degree boundedness condition holds. As successor polynomials

can easily be computed, it is in many cases easy to therefore show complete splitting by considering certain connected components of Γ_T . But first we show the following auxillary result:

Proposition 4.5 *Suppose $P \in T_{F_k/\mathbb{F}_q}(\mathcal{F}/\mathbb{F}_q)$ for some $k \geq 0$, where $(f_i)_{i \geq 1} \in (\mathbb{F}_l[x_{i-1}, x_i])_{i \geq 1}$ generates the representation $(F_i)_{i \geq 0}$ of \mathcal{F} and \mathbb{F}_q is some unknown finite extension of \mathbb{F}_l . Let Γ_T be the complete \mathbb{F}_l -splitting graph of \mathcal{F} . Then (a) $\chi(P) \subseteq V(\Gamma_T)$ and (b) the subgraph of Γ_T induced by the elements of $\chi(P)$ (as vertices) is a path of length k , where $\chi = \chi_{\mathbb{F}_l}$ (see page 41).*

Proof. Let $P \in S(F_k/\mathbb{F}_q)$ and $f \in \chi(P) = \chi_{\mathbb{F}_l}(P)$ such that $f(x_j(P)) = 0$ for some $0 \leq j \leq k$. As P splits completely in the steps k and up of the tower \mathcal{F} , there exist sequences

$$P = P_k \subset P_{k+1} \subset P_{k+2} \subset \dots$$

of places (with $P_i \in S(F_i/\mathbb{F}_q)$) where each P_i splits completely as well, for each $i \geq k$. Therefore no ramification occurs above the place P , which implies that $f \in V(\Gamma) \setminus V(\Gamma_B) = V(\Gamma_T)$, implying (a).

Part (b) follows in the following manner: We note that $\chi(P) \cap MI_{\mathbb{F}_q}(T_i)$ has only one element for each $0 \leq i \leq k$ and we denote this unique element by $\chi(P)_i(T_i) \in \chi(P) \cap MI_{\mathbb{F}_q}(T_i)$. Then the definition of the complete splitting graph (4.1) implies that the directed edge

$$\chi(P)_i(T_i) \xrightarrow{f_{i+1}} \chi(P)_{i+1}(T_{i+1})$$

is present in Γ_T for each $0 \leq i \leq k - 1$. ■

We use the following notation: when fixing a subgraph Γ' of the \mathbb{F}_q -splitting graph Γ of a tower \mathcal{F} , we let

$$\mathcal{A}(\Gamma', i) := V(\Gamma') \cap MI_{\mathbb{F}_q}(T_i) \tag{4.2}$$

where $i \geq 0$ is some step of the tower. This yields a short-hand notation for the polynomials at step i of the tower which are in the vertex set of the subgraph Γ' . It can easily be seen that $\mathcal{A}(\Gamma, i) = MI_{\mathbb{F}_q}(T_i)$ for all $i \geq 0$ for

the full \mathbb{F}_l -splitting graph Γ of the tower \mathcal{F} , and for a subgraph Γ' of Γ we have that

$$V(\Gamma') = \bigcup_{i \geq 0} \mathcal{A}(\Gamma', i) \quad (4.3)$$

where the right-hand side of (4.3) is a disjoint union.

The definition of the directed graph $\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$ in (4.1) and Definition 3.17, and the restriction to an arbitrary connected component Γ' of Γ ensures that, for all $i \geq 0$,

$$\text{Succ}_{f_{i+1}}(\mathcal{A}(\Gamma', i)) = \mathcal{A}(\Gamma', i+1) \text{ and } \text{Pred}_{f_{i+1}}(\mathcal{A}(\Gamma', i+1)) = \mathcal{A}(\Gamma', i). \quad (4.4)$$

Therefore, a useful way to interpret $\mathcal{A}(\Gamma', i)$ is as one row (corresponding to one step of the tower) of some of the graphical representations for the graphs that we use. Examples of this include the representations of Γ_B in Figures 3.1 and 3.3, as well as the representation of Γ_T in Figure 4.1. In Figure 3.1, the bottom row (row $i = 0$) of vertices constitute the elements of $\mathcal{A}(\Gamma_B, 0)$, the second row (row $i = 1$) of vertices constitute $\mathcal{A}(\Gamma_B, 1)$, and so on, for $\Gamma' = \Gamma_B$ in (4.2). The same convention (for $\Gamma' = \Gamma_B$) will be used for the complete \mathbb{F}_l -splitting graph Γ_T in the examples that follow.

When considering a graph modulo some equivalence relation \sim on the indeterminates (see page 44) (for example $\tilde{\Gamma}_B$ in Figure 3.4),

$$\mathcal{A}(\Gamma', i) \cong \mathcal{A}(\Gamma', j) \quad (4.5)$$

when $x_i \sim \tilde{x}_j$.

Theorem 4.6 Fix an integer $k \geq 0$. With notation as in Proposition 4.5, let Γ_T^* be a connected component of the subgraph Γ_T of Γ with the property that the degree of the elements of the sets $\mathcal{A}(\Gamma_T^*, i)$ for each $i \geq k$ are bounded, i.e. there exists an integer $m \geq 1$ such that

$$\max_{i \geq k} \{\deg p : p \in \mathcal{A}(\Gamma_T^*, i)\} = m. \quad (4.6)$$

Then there exists an extension $\mathbb{F}_r/\mathbb{F}_q$ such that $\#T_{\mathbb{F}_i, \mathbb{F}_r}(\mathcal{F} \cdot \mathbb{F}_r) > 0$ for each

$i \geq k$, i.e. \mathcal{F} is completely splitting over some (finite) constant field extension of the tower.

Proof. Let $\mathcal{A}_i := \mathcal{A}(\Gamma_T^*, i)$ for each $i \geq 0$, and fix some $i \geq k$. For every $u(T_i) \in \mathcal{A}_i$, there exists only finitely many $z \in \overline{\mathbb{F}} \cup \{\infty\}$ such that $u(z) = 0$. This, together with the fact that as \mathcal{A}_i represents a finite number of places of F_i which are completely splitting, implies that for each $u(T_i) \in \mathcal{A}_i$, there exists only finitely many places $P \in S(F_i/\mathbb{F}_q)$ such that

$$\chi(P)_i(T_i) \mid \prod_{u \in \mathcal{A}_i} u(T_i), \quad (4.7)$$

where $\chi(P)_i(T_i)$ is as defined in Proposition 4.5. These are exactly the places of $S(F_i/\mathbb{F}_q)$ in the support of the zero divisor of the right-hand side of (4.7). For the case $\frac{1}{T_i} \in \mathcal{A}_i$, we allow the possibility $\chi(P)_i(T_i) = \frac{1}{T_i}$ in (4.7).

These places are certainly unramified, but not necessarily of degree one, as it is possible that $\deg_{T_i} u > 1$ for some $u \in \mathcal{A}_i$. To remedy this, and taking into account that the above must hold for each $i \geq k$ simultaneously, we extend \mathbb{F}_q to the splitting field of $\prod_{i \geq k; u \in \mathcal{A}_i} u(T_i)$ over \mathbb{F}_q , i.e.

$$\begin{aligned} \mathbb{F}_r &= \text{splitting field of } \prod_{i \geq k, u \in \mathcal{A}_i} u(T_i) \\ &= \prod_{i \geq k} \left(\text{splitting field of } \prod_{u \in \mathcal{A}_i} u(T_i) \right), \end{aligned}$$

where by products of fields we mean composita of fields. Because of the boundedness condition (4.6), the resulting field \mathbb{F}_r is finite. We denote by

$$\mathcal{F}' = (F'_0 = F_0 \cdot \mathbb{F}_r, F'_1 = F_1 \cdot \mathbb{F}_r, F'_2 = F_2 \cdot \mathbb{F}_r, \dots)$$

the tower $\mathcal{F} = (F_0, F_1, F_2, \dots)$ but now considered over \mathbb{F}_r instead of \mathbb{F}_q . Let Γ'_T be the complete \mathbb{F}_r -splitting graph of \mathcal{F}' , and Γ'^*_T the minimal subgraph of Γ'_T containing all connected components of Γ'_T with polynomials

as vertices which divide vertices (as polynomials) of the original Γ_T^* . It is clear that the $\mathcal{A}'_i := \mathcal{A}(\Gamma_T^*, i)$, which are polynomials in $\mathbb{F}_r[x_{i-1}, x_i]$ instead of $\mathbb{F}_q[x_{i-1}, x_i]$, will consist only of polynomials of degree one for each $i \geq k$. As the places $P \in S(F'_k/\mathbb{F}_r)$ with paths $\chi(P)$ crossing through the elements of \mathcal{A}_i for $i \geq k$ are completely splitting, the tower \mathcal{F}' has a nonempty set of completely splitting places of degree one, the result we set out to prove. ■

When the conditions of Theorem 4.6 are satisfied for $k = 0$, we can explicitly describe the finite set of elements of degree one of the rational function field $F_0 = \mathbb{F}_q(x_0)$ which split completely in \mathcal{F} , corresponding to the component Γ_T^* of Γ_T . For a subgraph Γ' of Γ , this can be done by defining the sunset $\Omega_{\Gamma'} \subseteq \overline{\mathbb{F}} \cup \{\infty\}$ by

$$\Omega_{\Gamma'} = \{\alpha \in \overline{\mathbb{F}} \cup \{\infty\} : p(\alpha) = 0 \text{ for some } p(x_0) \in \mathcal{A}(\Gamma', 0)\}.$$

When the context makes it clear to which subgraph Γ' we are referring, we abbreviate this to Ω . In this notation, Ω_{Γ_T} gives the elements of the projective line $\mathbb{P}^1(\overline{\mathbb{F}})$ (if the tower of function fields is considered as a sequence of covers of curves) corresponding to places in the function field F_0/\mathbb{F}_q which split completely in \mathcal{F} . Similarly, $\Omega_{\Gamma_T^*}$ is a subset of Ω_{Γ_T} describing the points corresponding to the specific component Γ_T^* of Γ_T which split completely. This Ω -notation corresponds to the convention used to describe the completely splitting places in various papers of García and Stichtenoth, for example [36].

Theorem 4.7 *Let \mathcal{F} be a tower defined by the sequence $(f_i)_{i \geq 1}$ of separable polynomials with $f_i \in \mathbb{F}_q[x_{i-1}, x_i]$. Then there exists a finite field extension $\mathbb{F}_r \supseteq \mathbb{F}_q$ such that \mathcal{F} with constant field extended to \mathbb{F}_r is completely splitting if and only if there exists a maximally connected¹ subgraph Γ'_T of Γ_T with the property that*

$$\max_{i \geq 0} \mathcal{A}(\Gamma_T^*, i) = m \tag{4.8}$$

for some $m \geq 1$.

¹The subgraph Γ'_T of Γ_T must consist of the union of connected components of Γ .

Proof. The if part follows directly by applying Theorem 4.6 to a union of connected components Γ_T^* of Γ_T , and $k = 0$. This union is a finite union because of the boundedness condition on the $\mathcal{A}(\Gamma_T^*, i)$.

Conversely, let \mathcal{F}' (with representation $(F'_0, F'_1, F'_2, \dots)$) be the tower \mathcal{F} with constant field extended to \mathbb{F}_r . Then there exists a finite subset of places of degree one of $F'_0 = \mathbb{F}_r(x_0)$ which split completely in \mathcal{F}' (exactly the elements of $T_{F'_0}(\mathcal{F}')$). Noting that $\chi(P)$ has only one element for each $P \in T_{F'_0/\mathbb{F}_r}(\mathcal{F}')$, we consider the set

$$W := \bigcup_{P \in T_{F'_0/\mathbb{F}_r}(\mathcal{F}'/\mathbb{F}_r)} \chi(P)$$

as a subset of the vertex set of Γ_T . As the elements of $T_{F'_0/\mathbb{F}_r}(\mathcal{F}')$ are completely splitting in \mathcal{F}' , all the successor polynomials (computed recursively) of elements of W are contained in $V(\Gamma_T)$ as well. Therefore there exists a minimal subgraph Γ'_T of Γ_T which contains all the successors of elements of W . As \mathbb{F}_r is a finite field, and elements of $V(\Gamma'_T)$ can have degree at most r in order to factorize into linear factors over \mathbb{F}_r ($\frac{1}{T_i}$ is unchanged), the sets $\mathcal{A}(\Gamma'_T, i)$ has cardinality at most r for all $i \geq 0$. ■

In the case of an n -step tower (or more generally, a \sim -finite tower), the maximum of (4.8) in Theorem 4.7 needs only to be computed over n indices i , one for each of the equivalence classes induced by \sim_n . The condition is still nontrivial, as the problem remains to find a suitable component Γ_T^* of Γ_T for which

$$\# \left(\bigcup_{i=1}^n \mathcal{A}(\Gamma_T^*, i) \right) < \infty,$$

using the equivalence relation \sim_n in expression (4.5).

However, this means that we do not need the explicit boundedness condition (an explicit value for m) for n -step towers where each $\mathcal{A}(\Gamma_T^*, i)$ is known to be finite, as the finiteness of the $\mathcal{A}(\Gamma_T^*, i)$ for each $i = 0, 1, 2, \dots, n-1$, together with the finiteness of the number of equivalence classes modulo \sim_n would imply that a suitable m exists (the splitting field of finitely many irreducible polynomials). For the same reason, general \sim -finite tow-

ers do not need the condition either. In these two cases, the remaining problem is therefore to find a suitable finite component Γ_T^* of Γ_T .

In order to work with examples, we would like to explicitly determine the finite field \mathbb{F}_r over which a tower defined by the sequence $(f_i)_{i \geq 1}$ will split completely. The field \mathbb{F}_r must be a (finite) field extension of the coefficient ring (which is a field) of the polynomial rings from which the f_i come. The proof of Theorem 4.6 shows that once a component Γ_T^* of Γ_T is fixed, a field \mathbb{F}_r can be found by taking the compositum of the splitting fields of all the polynomials in $V(\Gamma_T^*) \cap MI_{\mathbb{F}_q}(T_i)$ for $i \geq k$ such that $T_{\mathbb{F}_k'/\mathbb{F}_r}(\mathcal{F} \cdot \mathbb{F}_r)$ is nonempty. This observation leads to the following corollary.

Corollary 4.8 *Suppose \mathcal{F} is an explicit tower with representation $(F_i)_{i \geq 0}$ over \mathbb{F}_q generated by the sequence $(f_i)_{i \geq 1}$ of polynomials (resp.) in $(\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$. Let Γ_T^* be a connected component of Γ_T (Definition 4.4), and suppose that the set*

$$U_{\Gamma_T^*} := \left\{ \deg_{T_i} p(T_i) : i \geq 0, p(T_i) \in \Gamma_T^* \right\} \subseteq \mathbb{N}$$

is bounded (where we assume that $\deg(1/T_i) = 1$). Then \mathcal{F} is completely splitting over \mathbb{F}_r where

$$r = q^{\text{lcm } U_{\Gamma_T^*}}.$$

Proof. Note that, in the notation of Theorem 4.6,

$$V(\Gamma_T^*) = \bigcup_{i \geq 0} \mathcal{A}(\Gamma_T^*, i).$$

As the splitting field of an \mathbb{F}_q -irreducible polynomial $p(T)$ is $\mathbb{F}_{q^{\deg p(T)}}$ and the compositum of such fields are given by the least common multiple in the way shown, Theorem 4.6 implies the desired result. ■

We conclude this section with two examples of applications of the above theorem and corollary.

Example 4.9 (Example 3.16, 3.20 revisited) *We return to the tower \mathcal{F}_1 by Van der Geer and Van der Vlugt to finally show that it is completely splitting, using Theorem 4.6. It is helpful to note a key feature of the analysis of this tower so*

far: while we have stated in Example 3.16 that the tower is defined over the finite field \mathbb{F}_8 , this fact has not been used at all so far. The only feature of the field of definition that was used in the ramification analysis (Example 3.20) is the fact that it is a finite field of characteristic 2. We therefore make the following change to our notation used in the preliminary examples, and start with the minimal assumption that the tower is defined over $\mathbb{F}_q = \mathbb{F}_2$, and that we wish to find some extension field $\mathbb{F}_r/\mathbb{F}_2$ such that \mathcal{F}_1 will be completely splitting if defined over \mathbb{F}_r . Our first aim will be to determine a connected component Γ_T^* of Γ_T which satisfies the conditions of Corollary 4.8. We do this by picking polynomials in $MI_{\mathbb{F}_2}(T_0)$, ensuring that they are not in Γ_B , and then generating the subgraph of Γ_T they belong to by recursively computing successor polynomials.

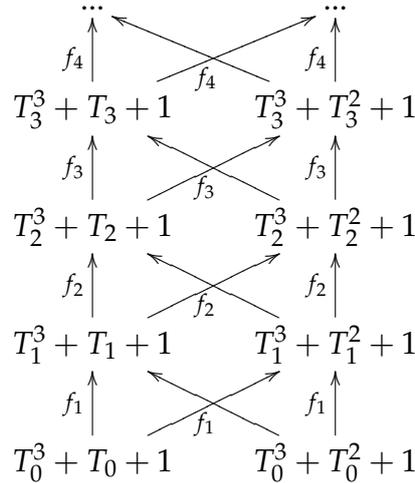


Figure 4.1: Complete \mathbb{F}_2 -splitting graph Γ_T^* for Example 4.9

In Example 3.20 $V(\Gamma_B)$ was completely described, and we note that the minimal-degree elements of $MI_{\mathbb{F}_2}(T_0) \setminus V(\Gamma_B)$ are the polynomials $T_0^3 + T_0 + 1$ and $T_0^3 + T_0^2 + 1$. By computing predecessors and successors, we see that they are in fact members of the same component of Γ_T , which we denote by Γ_T^* (see Figure 4.1). As the degree of each polynomial in the vertex set of Γ_T^* is 3, \mathcal{F}_1 splits completely over $\mathbb{F}_r = \mathbb{F}_{2^3} = \mathbb{F}_8$ by Corollary 4.8.

The work in Examples 3.16, 3.20 and 4.9 show that the tower \mathcal{F}_1 has a

finite ramification locus and is completely splitting. As it is wildly ramified, Corollary 2.18 does not apply, and we must find suitable values for a_p so that Theorem 2.16 can be used to find a lower bound for the limit $\lambda(\mathcal{F}_1)$. García and Stichtenoth [28] showed that one can choose $a_p = 2$ for each $P \in V_{F_0}(\mathcal{F}_1)$, leading to the limit $\lambda(\mathcal{F}_1) \geq 3/2$ with much less effort than the original derivation by Van der Geer and Van der Vlugt [65].

Example 4.10 (Example 3.22 revisited) We complete the proof of the two-step Kummer tower example by finishing part (c) (see page 49). In order to apply Corollary 4.8 to \mathcal{F}_3 , we first need to identify a connected component Γ_T^* of Γ_T . We claim that the subset $V = \left\{ \frac{1}{T_i} : i \geq 0 \right\}$ of the full vertex set of Γ induces a full connected component of Γ_T . Indeed, as $\frac{1}{T_i} \notin \Gamma_B$ for all i ($\frac{1}{T_i} \notin M_i$), the subgraph of Γ induced by the vertices in V is indeed contained in Γ_T . It remains to show that it is a full connected component. From the theory of Kummer extensions (see [59]) and the proof of Example 3.22(b), we observe that $\text{Pred}_{h_{i+1}}\left(\frac{1}{T_{i+1}}\right) = \frac{1}{T_i}$ for all $i \geq 1$. The comments above together with the fact that Γ_T and Γ_B are disjoint subgraphs of Γ then implies that the edge $\frac{1}{T_i} \xrightarrow{h_{i+1}} T_{i+1}$ cannot occur in Γ_T , and therefore a connected component Γ_T^* of Γ_T is induced by the set V on the vertices of Γ . Now Corollary 4.8 applies, and it follows that \mathcal{F}_3 splits completely

$$\frac{1}{T_0} \xrightarrow{h_1=\tilde{f}} \frac{1}{T_1} \xrightarrow{h_2=\tilde{g}} \frac{1}{T_2} \xrightarrow{h_3=\tilde{f}} \frac{1}{T_3} \xrightarrow{h_4=\tilde{g}} \dots$$

Figure 4.2: Complete \mathbb{F}_q -splitting graph Γ_T^* for Example 4.10

over $\mathbb{F}_r := \mathbb{F}_{q^1} = \mathbb{F}_q$. A representation of Γ_T^* is given in Figure 4.2, and of $\tilde{\Gamma}_T^* = \Gamma_T^* / \sim_2$ in Figure 4.3 (with $\tilde{x} \sim_2 x_i$ for even i and $\tilde{y} \sim_2 x_i$ for odd i).

$$\begin{array}{ccc} & \tilde{f} & \\ & \curvearrowright & \\ \frac{1}{\tilde{x}} & & \frac{1}{\tilde{y}} \\ & \curvearrowleft & \\ & \tilde{g} & \end{array}$$

Figure 4.3: Condensed complete \mathbb{F}_q -splitting graph $\tilde{\Gamma}_T^*$ for Example 4.10

4.3 Splitting characteristic polynomials

For an explicit tower \mathcal{F} as described in the notation of Corollary 4.8, and a fixed component Γ_T^* of Γ_T , we refer to the polynomial

$$\tau_{\Gamma_T^*,i}(T_i) := \prod_{u \in \mathcal{A}(\Gamma_T^*,i)} u \quad (4.9)$$

as the splitting characteristic polynomial at step i for the tower \mathcal{F} , if

$$\#\mathcal{A}(\Gamma_T^*,i) < \infty \text{ and } \frac{1}{T_j} \notin \mathcal{A}(\Gamma_T^*,j)$$

for all $j \geq i$. In this case we say that the splitting characteristic polynomial $\tau_{\Gamma_T^*,i}(T_i)$ is defined at step i of the explicit tower \mathcal{F} generated by the sequence $(f_i)_{i \geq 1}$. As $\mathcal{A}(\Gamma_T^*,i)$ contains distinct monic irreducible polynomials, the polynomial $\tau_{\Gamma_T^*,i}(T_i)$ is separable.

Proposition 4.11 *Let \mathcal{F} be an explicit tower with generating polynomials $(f_i)_{i \geq 1}$ (with coefficients in \mathbb{F}_q), and Γ_T^* a fixed component of the \mathbb{F}_q -complete splitting graph Γ_T . Suppose that $\tau_{\Gamma_T^*,i}(T_i)$ is defined for \mathcal{F} for all $i \geq 0$. Then*

$$\tau_{\Gamma_T^*,i+1}(T_{i+1}) = \prod \left\{ p(T_i) : p(T_i) \in \text{Succ}_{f_{i+1}} \left(\tau_{\Gamma_T^*,i}(T_i) \right) \right\}$$

for each $i \geq 0$, where $\prod S$ denotes the product of the elements of the set S .

Proof. Note that as $\tau_{\Gamma_T^*,i}(T_i)$ is defined for all $i \geq 0$, it also holds that for any $i \geq 0$, $\frac{1}{T_{i+1}} \notin \text{Succ}_{f_{i+1}}(\mathcal{A}(\Gamma_T^*,i))$. Then

$$\tau_{\Gamma_T^*,i+1}(T_{i+1}) = \prod_{u \in \mathcal{A}(\Gamma_T^*,i+1)} u = \prod_{v \in \text{Succ}_{f_{i+1}}(\mathcal{A}(\Gamma_T^*,i))} v = \prod_{v \in \text{Succ}_{f_{i+1}}(\tau_{\Gamma_T^*,i}(T_i))} v.$$

■

Because of the condition on Γ_T^* for the definition of $\tau_{\Gamma_T^*,i}(T_i)$ to be defined that $\frac{1}{T_j} \notin V(\Gamma_T^*)$ (4.9), any computation of predecessor or successor polynomials, which respectively require application of Theorem 3.10 and Theorem 4.3, will only require those cases of these theorems applying to

finite elements of $\overline{\mathbb{F}} \cup \{\infty\}$. In other words, only the elimination ideal methods of Theorem 3.10(i) (for predecessor polynomials) and Theorem 4.3(i)(a) (for successor polynomials) apply. This leads to the following theorem which gives a sufficient condition for complete splitting to occur in an n -step tower (see Definition 2.21), without knowledge of the field of definition of the tower.

Theorem 4.12 *Let $(f_i)_{i \geq 1}$ generate an n -step tower \mathcal{F} defined from the set of representatives*

$$\{f_1, f_2, f_3, \dots\} / \sim_n = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$$

where $f_i(x_{i-1}, x_i) \in \mathbb{F}_l[x_{i-1}, x_i]$ and f_i is uniquely defined by $f_i = \tilde{f}_j$ where $i \equiv j \pmod n$. We assume that the tower \mathcal{F} has some unknown finite extension of \mathbb{F}_l as field of constants, and has canonical representation (F_0, F_1, F_2, \dots) induced by the $(f_i)_{i \geq 1}$. Let $\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$ be the \mathbb{F}_l -splitting graph of \mathcal{F} , and let Γ_T be the associated complete \mathbb{F}_l -splitting graph of \mathcal{F} . Suppose that Γ_T^* is a component of Γ_T such that $\tau_{\Gamma_T^*, 0}(T_0)$ is defined, and that

$$\text{Succ}_{\tilde{f}_1}^n \left(\tau_{\Gamma_T^*, 0}(T_0) \right) \mid \tau_{\Gamma_T^*, 0}(T_n). \quad (4.10)$$

Then $\#T_{F_0}(\mathcal{F}/\mathbb{F}_r) > 0$ where \mathbb{F}_r is the splitting field of $\tau_{\Gamma_T^*, 0}(T_0) \in \mathbb{F}_l[T_0]$.

Proof. As the irreducible factors of $\tau_{\Gamma_T^*, 0}(T_0)$ correspond to vertices at step 0 of a component of the completely \mathbb{F}_l -splitting graph of \mathcal{F} , the set of places

$$Z = \left\{ P \in S(F_0/\mathbb{F}_q) : a_0 = x_0(P) \text{ is a root of } \tau_{\Gamma_T^*, 0}(T_0) \right\}$$

is unramified in the tower \mathcal{F} . In order to analyze the complete splitting behaviour, consider that by using Equation (2.1),

$$v_F(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{N(F_i/\mathbb{F}_l)}{[F_i : F]} = \lim_{i \rightarrow \infty} \frac{N(F_{ni}/\mathbb{F}_l)}{[F_{ni} : F]}$$

where $0 \leq i < \infty$. Moreover, we see that successively applying

$$\text{Succ}_{\tilde{f}_{n+1}}^n(\cdot), \text{Succ}_{\tilde{f}_{2n+1}}^n(\cdot), \text{Succ}_{\tilde{f}_{3n+1}}^n(\cdot), \dots$$

to both sides of (4.10), it follows that, for any $m \geq 1$,

$$\text{Succ}_{\tilde{f}_{kn+1}}^{(m-k)n} \left(\tau_{\Gamma_T^*, 0}(T_{kn}) \right) \mid \text{Succ}_{\tilde{f}_{(k+1)n+1}}^{(m-k-1)n} \left(\tau_{\Gamma_T^*, 0}(T_{(k+1)n}) \right)$$

for each $k = 0, 1, 2, \dots, m-1$ and that as

$$\tau_{\Gamma_T^*, 0}(T_{mn}) = \text{Succ}_{\tilde{f}_{mn+1}}^{(m-m)n} \left(\tau_{\Gamma_T^*, 0}(T_{mn}) \right),$$

this implies that

$$\text{Succ}_{\tilde{f}_1}^{mn} \left(\tau_{\Gamma_T^*, 0}(T_0) \right) \mid \tau_{\Gamma_T^*, 0}(T_{mn}),$$

because of each n th step of the tower having the same defining equations modulo \sim_n , noting that respectively the indeterminates $T_0, T_n, T_{2n}, \dots, T_{mn}$ and the defining polynomials $\tilde{f}_1, \tilde{f}_{n+1}, \tilde{f}_{2n+1}, \dots, \tilde{f}_{mn+1}$ are all equal modulo \sim_n . Therefore, for every $k \geq 1$, every place $Q \in S(F_{kn}/\mathbb{F}_q)$ lying above some $P \in Z$ must have the property that $x_{kn}(Q)$ is a root of $\tau_{\Gamma_T^*, 0}(T_{kn})$.

Now the conditions of Theorem 4.6 are satisfied, and it follows that \mathcal{F} is completely splitting over some extension of \mathbb{F}_l . By Corollary 4.8 this extension field \mathbb{F}_r is the splitting field of the polynomial $\tau_{\Gamma_T^*, 0}$. ■

The set of places of F_0/\mathbb{F}_r which split completely in the n -step tower \mathcal{F} described by Theorem 4.12 corresponds to the set

$$\Omega = \left\{ \alpha \in \overline{\mathbb{F}} : \tau_{\Gamma_T^*, 0}(\alpha) = 0 \right\} = \left\{ \alpha \in \mathbb{F}_r : \tau_{\Gamma_T^*, 0}(\alpha) = 0 \right\}.$$

The second equality holds since \mathbb{F}_r is the splitting field of $\tau_{\Gamma_T^*, 0}$ over \mathbb{F}_l .

The following corollary describes the situation when the polynomial H we are considering has irreducible factors belonging to different components of Γ_T . We are therefore considering the possibility that the complete splitting locus of such an n -step tower is not described by a single connected component of Γ_T only.

Corollary 4.13 *Suppose the sequence $(f_i)_{i \geq 1}$ generates an n -step tower \mathcal{F} defined from the set of representatives given by*

$$\{f_1, f_2, f_3, \dots\} / \sim_n = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$$

with $f_i(x_{i-1}, x_i) \in \mathbb{F}_l[x_{i-1}, x_i]$, where f_i is uniquely defined by $f_i = \tilde{f}_j$ where $i \equiv j \pmod n$. We assume that \mathcal{F} has some unknown finite extension of \mathbb{F}_l as field of constants. Suppose $H(T_0)$ is a monic polynomial in $\mathbb{F}_l[T_0]$ such that

$$\text{Succ}_{f_1}^n(H(T_0)) \mid H(T_n) \quad (4.11)$$

and $H(T_0)$ has no repeated roots. Then $\#T_{F_0}(\mathcal{F}/\mathbb{F}_r) > 0$ where \mathbb{F}_r is the splitting field of $H(T_0) \in \mathbb{F}_l[T_0]$.

Proof. Let $H(T_0) = \prod_{i=1}^t H_i(T_0)$ where, for each i , $H_i(T_0) \mid \tau_{\Gamma_T^i, 0}(T_0)$ where $\Gamma_T^1, \Gamma_T^2, \dots, \Gamma_T^t$ are t distinct components of Γ_T . As the set of successor polynomials at each step for $H_i(T_0)$ and $H_j(T_0)$ (for $i \neq j$) are distinct, equation (4.11) will apply, and we can apply Theorem 4.12 to the polynomial $H_i(T_0) \mid \tau_{\Gamma_T^i, 0}(T_0)$ in component Γ_T^i separately for each $1 \leq i \leq t$. This implies that the set of places

$$Z_i = \{P \in S(F_0/\mathbb{F}_r) : x_0(P) \text{ is a root of } H_i(T_0)\}$$

are completely splitting for each $1 \leq i \leq t$. Then the places in the set

$$Z := \bigcup_{i=1}^t Z_i = \left\{ P \in S(F_0/\mathbb{F}_r) : x_0(P) \text{ is a root of } \prod_{i=1}^t H_i(T_0) = H(T_0) \right\}$$

are completely splitting in some constant field extension of \mathcal{F} . By Corollary 4.8 the adequate extension field \mathbb{F}_r is the splitting field of $H(T_0)$. ■

Corollary 4.13 considers the possibility of more than one component of Γ_T which satisfy the conditions of Theorem 4.12. It is worthwhile to note that if an explicit tower \mathcal{F} over \mathbb{F}_q meets the Drinfeld-Vladut bound, it is not possible for it to have more places which split completely when considered over a constant field extension of the tower, see [62]. In the context

of components of Γ_T , this means that if a component already exists which guarantees complete splitting and the tower attains the Drinfeld-Vladut bound for \mathbb{F}_q , there cannot exist components of the complete \mathbb{F}_l -splitting graph Γ_T which (a) for which the vertex set contains \mathbb{F}_l -irreducible polynomials of degree greater than $\log_l q$ and (b) satisfy Corollary 4.13. This restriction does not hold if \mathcal{F} is not asymptotically maximal.

In both Theorem 4.12 and Corollary 4.13 we can write the relation between $\tau_{\Gamma^*,0}(T_0)$ and $\tau_{\Gamma^*,0}(T_n)$ (resp. $H(T_0)$ and $H(T_n)$) for an n -step tower in terms of Gröbner bases. If a monomial ordering on the polynomial ring $\mathbb{F}_l[T_0, T_1, \dots, T_n]$ with $T_0 > T_1 > \dots > T_n$ is used, (4.10) and (4.11) are equivalent to checking that the univariate generator polynomial for the elimination ideal

$$I = \left\langle H(T_0), \tilde{f}_1(T_0, T_1), \tilde{f}_2(T_1, T_2), \dots, \tilde{f}_n(T_{n-1}, T_n) \right\rangle \cap \mathbb{F}_l[T_n]$$

divides $H(T_n)$. When this occurs, the polynomial H is a splitting characteristic polynomial for some unknown component Γ^* of Γ which has the degree-boundedness property of Theorem 4.6. When we know $\frac{1}{T_i}$ to be a vertex of a ramification graph Γ_B for each $i \geq 0$ where Γ_B consists of a single connected component, Γ^* is guaranteed to be a component of Γ_T satisfying Theorem 4.6, yielding a nonempty complete splitting locus.

It is sometimes useful to consider the splitting characteristic polynomial $\tau_{\Gamma^*,0}(T)$ as the solution of a functional equation, by which the set Ω can be described.

Proposition 4.14 *Suppose the defining equation of a one-step tower \mathcal{F} with basic function field $F_1 \cong \mathbb{F}_q(x, y)$ can be written in variable separated form as*

$$h(y) = \frac{f_1(x)}{f_2(x)} \tag{4.12}$$

where $h(y) \in \mathbb{F}_q[y]$, $f_1(x), f_2(x) \in \mathbb{F}_q[x]$ and $\deg h = \deg f_1 > \deg f_2$. Suppose further that all monic irreducible factors of the polynomials f_1, f_2 and h appear as vertices in the \mathbb{F}_q -ramification graph Γ_B of \mathcal{F} , and that $\frac{1}{x_i} \in V(\Gamma_B)$ for all $i \geq 0$. Suppose the squarefree polynomial $G(T) \in \mathbb{F}_q[T]$ is a solution of the

functional equation

$$G(h(T)) = (f_2(T))^{\deg G \cdot (\deg f_1 - \deg f_2)} \cdot G\left(\frac{f_1(T)}{f_2(T)}\right) \quad (4.13)$$

and that the monic irreducible factors of $G(h(T))$ are distinct from those of f_1, f_2 and h . Then $\tau_{\Gamma_T^*, 0}(x_0) := G(h(x_0))$ is a splitting characteristic polynomial for the tower \mathcal{F} , representing $\deg h \cdot \deg G$ places of degree one splitting completely in \mathcal{F} defined over the splitting field of $\tau_{\Gamma_T^*, 0}$.

Proof. We follow the general idea in [9] and [10]. Let $\deg G = g$, $\deg f_1 = m$ and $\deg f_1 - \deg f_2 = d$. We note that the exponent of $(f_2(T))$ in the right-hand side of (4.13) ensures that the right-hand side is a polynomial of degree mg , as is the left-hand side. Let Ω be a subset of $\bar{\mathbb{F}}$ representing the places of degree one of F_0/\mathbb{F}_q that split completely in \mathcal{F} . In order to prove that $\tau_{\Gamma_T^*, 0}(x_0) := G(h(x_0))$ is a splitting characteristic polynomial for some component Γ_T^* of the complete \mathbb{F}_q -splitting graph Γ_T , we need to show that if $(x, y) = (\alpha, \beta) \in \mathbb{F}_r \times \bar{\mathbb{F}}$ is a solution of (4.12) and $\tau_{\Gamma_T^*, 0}(\alpha) = 0$, then $\tau_{\Gamma_T^*, 0}(\beta) = 0$ and $\beta \in \mathbb{F}_r$, where $\mathbb{F}_r \supseteq \mathbb{F}_q$ is the splitting field of $\tau_{\Gamma_T^*, 0}$. Indeed, suppose $\tau_{\Gamma_T^*, 0}(\alpha) = 0$ and that $h(\beta) = f_1(\alpha) / f_2(\alpha)$. Then

$$0 = \tau_{\Gamma_T^*, 0}(\alpha) = G(h(\alpha)) = (f_2(\alpha))^{\deg G \cdot (\deg f_1 - \deg f_2)} \cdot G\left(\frac{f_1(\alpha)}{f_2(\alpha)}\right).$$

As $f_2(\alpha) \neq 0$ due to the disjointness of Γ_T^* from Γ_B , this implies that $G\left(\frac{f_1(\alpha)}{f_2(\alpha)}\right) = 0$. Hence $G(h(\beta)) = 0$, implying that $\beta \in \mathbb{F}_r$ and is a zero of $\tau_{\Gamma_T^*, 0}$, as required. ■

When a splitting characteristic polynomial has been found for a specific tower, we can recover both the field \mathbb{F}_r and the vertices of Γ_T^* by factorizing $\tau_{\Gamma_T^*}(x_0)$ and observing the degrees of its factors and the factors themselves.

We note that knowing that we can find a polynomial G satisfying (4.13) is a useful step towards showing modularity of the tower, as for suitable h, f_1 and f_2 , (4.13) will satisfy a necessary condition for $\tau_{\Gamma_T^*, 0}(T) = G(h(T))$ to define a modular form of weight $\deg G \cdot (\deg f_2 - \deg f_1)$. For an exposition on modular towers, we refer to the work of Elkies [21], [22] on showing that many known explicit asymptotically good towers correspond to

towers of modular curves.

The functional equation of (4.13) is also related to that in [9] where it is shown, in the language of our graphs, that each (finite) component of $\tilde{\Gamma}_T = \Gamma_T / \sim_1$ corresponds to a essentially unique solution of (4.13). When such a solution is found, we therefore know that a unique finite component exists solving (4.13).

To conclude the chapter, we give an example of an explicit, one-step tower \mathcal{F} which is asymptotically maximal.

Example 4.15 *Let $q = p^n$ be an arbitrary power of a prime p . We consider a tower \mathcal{F}_4 with canonical representation $F_0 \subset F_1 \subset F_2 \subset \dots$ of García and Stichtenoth [31] recursively defined by the polynomials $(f_i)_{i \geq 1}$ where*

$$f_{i+1}(x_i, x_{i+1}) = (x_{i+1}^q + x_{i+1}) (x_i^{q-1} + 1) - x_i^q.$$

Performing an analysis of the ramification behaviour using the results of Chapter 3, we construct the \mathbb{F}_q -ramification graph following Theorems 3.10, 3.13 and 3.18, and obtain the representation for Γ_B shown² in Figure 4.4 which makes it clear that \mathcal{F} has a finite ramification locus, as also shown by García and Stichtenoth [31]. We apply Corollary 4.13 to confirm their result that there are $q^2 - q$ places of F_0 which split completely in the one-step tower \mathcal{F}_4 . Indeed, consider the polynomial

$$H(T_0) := \frac{T_0^{q^2} - T_0}{T_0^q + T_0} = \sum_{i=0}^{q-1} (T_0^{q-1})^i \quad (4.14)$$

of which the irreducible factors are all in Γ_T because of the denominator in the fraction. In order to show that H is a splitting characteristic polynomial for \mathcal{F}_4 , it suffices to show that

$$\text{Succ}_{f_1}(H(T_0)) \mid H(T_1).$$

For a specific example where q is known, this can be confirmed using the Gröbner basis approach discussed in Theorem 3.10, and this is the method we will employ

²In Figure 4.4, the expressions $x^{q-1} + 1$ are not necessarily irreducible for certain q . In such case, we assume that for each edge sequence $p(x_i) \rightarrow x_{i+1}^{q-1} + 1 \rightarrow q(x_{i+2})$ the edges $p(x_i) \rightarrow h(x_{i+1})$ and $h(x_{i+1}) \rightarrow q(x_{i+2})$ are present for each monic irreducible factor $h(x_{i+1})$ of $x_{i+1}^{q-1} + 1$.

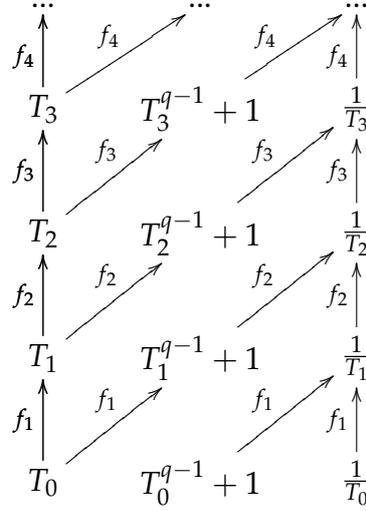


Figure 4.4: Ramification graph Γ_B for Example 4.15

for algorithms in Chapter 5, and examples in Chapter 6. We can evade the successor computations by considering that every root $z \in \overline{\mathbb{F}}$ of $H(T_0)$ has $T_0^q + T_0 \neq 0$. Note that $z \in \mathbb{F}_{q^2}^\times$ because of the numerator of (4.14). As

$$T_1^q + T_1 = \frac{z^q}{z^{q-1} + 1} = \frac{z^{q+1}}{z^q + z}$$

for some z and the right-hand side has nonzero denominator which is the trace from \mathbb{F}_{q^2} onto \mathbb{F}_q and nonzero numerator which acts as the norm from \mathbb{F}_{q^2} onto \mathbb{F}_q , $T_1^q + T_1 = \alpha$ where $\alpha \in \mathbb{F}_q^\times$. Hence T_1 is a root of H , which implies that $\text{Succ}_{f_1}(H(T_0)) \mid H(T_1)$. Corollary 4.13 (with $n = 1$) then implies that \mathcal{F}_4 is completely splitting over \mathbb{F}_{q^2} with $\deg H = q^2 - q$ places of degree one splitting completely.

Chapter 5

Algorithms

Let \mathcal{F} over \mathbb{F}_q be an explicit tower of function fields with explicit equations given by the sequence $(f_i)_{i \geq 1}$ of separable polynomials where $f_i(x_{i-1}, x_i) \in \mathbb{F}_q[x_{i-1}, x_i]$ for each $i \geq 1$. Then $F_0 = \mathbb{F}_q(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ where $f_{i+1}(x_i, x_{i+1}) = 0$ for all $i \geq 0$. This yields the representation

$$\mathcal{F} = (F_0/\mathbb{F}_q, F_1/\mathbb{F}_q, F_2/\mathbb{F}_q, \dots)$$

of the tower \mathcal{F} .

In Chapter 3 we described methods by which to test whether such a tower \mathcal{F} has a finite ramification locus, largely motivated due to its importance for satisfying one of the conditions of Theorem 2.16. Chapter 4 was devoted to finding a finite extension $\mathbb{F}_r/\mathbb{F}_q$ such the tower \mathcal{F} , if redefined over the extended constant field \mathbb{F}_r , will be completely splitting. If one can find a tower \mathcal{F} where both these properties are satisfied, only the existence of relative bounds for the different exponents still has to be shown for Theorem 2.16 to apply. If $\mathcal{F}' = \mathcal{F} \cdot \mathbb{F}_r = (F'_0/\mathbb{F}_r, F'_1/\mathbb{F}_r, F'_2/\mathbb{F}_r, \dots)$ denotes the constant field extension of \mathcal{F} from \mathbb{F}_q to \mathbb{F}_r , the lower bound

$$\lambda(\mathcal{F}'/\mathbb{F}_r) \geq \frac{2 \cdot \#T_{F'_0}(\mathcal{F}'/\mathbb{F}_r)}{2g(F'_0/\mathbb{F}_r) - 2 + \sum_{P \in V_{F'_0}(\mathcal{F}'/\mathbb{F}_r)} a_P \cdot \deg P}$$

for the limit of the tower is obtained from Theorem 2.16, where the a_P are

appropriate different exponent bounds, see Theorems 2.12 and 2.16 and a finite ramification locus $V_{F'_0}(\mathcal{F}')$. When \mathcal{F} (equivalently \mathcal{F}') is tamely ramified, the different exponents are automatically bounded (Corollary 2.13), in which case finite ramification and complete splitting suffices in order to obtain a lower bound for the limit.

The problem of finding adequate values for the a_p in the wildly ramified case is inherently difficult. Usually some explicit formula or upper bound for the genus of each F_i is determined in this case. Interesting examples include a family of wildly ramified explicit towers attaining the Drinfeld-Vladut bound (with fields of square cardinality) by García and Stichtenoth [29] and a family of wildly ramified explicit towers (with finite fields of cubic cardinality) by Bezerra, García and Stichtenoth [12] with good limit.

Because of the above, the algorithms described in this chapter will directly apply to tamely ramified towers, but still require some extra work to be done to analyze wildly ramified towers. The difficulty in finding appropriate a_p can be alleviated in some cases, for example certain families of Artin-Schreier extensions, see [28].

5.1 Finite ramification

For the theoretical derivation of the results used in this section, we refer to Chapter 3. Note that in the following algorithms, we assume that \mathcal{F} is a tower defined over \mathbb{F}_q , but that \mathbb{F}_l is a finite field contained in \mathbb{F}_q such that the bivariate separable polynomials $(f_i)_{i \geq 1}$ are defined with \mathbb{F}_l as coefficient ring. In almost all practical situations, \mathbb{F}_l is the prime subfield of \mathbb{F}_q , although it can be equal to \mathbb{F}_q itself.

This containment condition allows us to analyze the ramification behaviour of a tower without a priori knowledge of the field of definition \mathbb{F}_q of the tower. We will therefore only assume that the coefficients of the polynomial ring $\mathbb{F}_l[y]$ come from some known subfield \mathbb{F}_l of the unknown full constant field \mathbb{F}_q .

The subsections 5.1.1 and 5.1.2 will outline the algorithmic aspects of the two ingredients in determining a finite ramification locus, as respectively derived in Sections 3.1 and 3.3. Subsection 5.1.3 will then unify these to give a single algorithm that takes the defining polynomials of an explicit tower as input.

5.1.1 Predecessor polynomials

To compute the predecessor polynomial $\text{Pred}_f(q)$ of a polynomial q , we use Definition 3.11 and the notation introduced directly thereafter. This can be implemented using the next two algorithms as basis.

Require: $f(x, y) \in \mathbb{F}_l[x, y]$ separable, monic, irreducible, $q(y) \in \mathbb{F}_l[y]$ monic, irreducible, \mathbb{F}_l is contained in \mathbb{F}_q

Ensure: $P = \text{Pred}_f(q)$

- 1: $P \leftarrow \emptyset$
- 2: $I \leftarrow \langle f(x, y), q(y) \rangle$
- 3: $\mathcal{G} \leftarrow$ Gröbner basis for the ideal I using `grevlex` with $y > x$
- 4: $u \leftarrow$ univariate generator polynomial for $I \cap \mathbb{F}_l[x]$ using \mathcal{G}
- 5: **for all** monic irreducible factors $u_i(x)$ of $u(x)$ **do**
- 6: $P \leftarrow P \cup \{u_i(x)\}$
- 7: **end for**
- 8: $g \leftarrow f^{(x)}(x, y)$
- 9: **if** $\deg(\gcd(g(0, y), q(y))) > 0$ **then**
- 10: $P \leftarrow P \cup \{\frac{1}{x}\}$
- 11: **end if**
- 12: **return** P .

Algorithm 1: Calculate $\text{Pred}_f(q)$ for a monic \mathbb{F}_l -irreducible $q(y) \in \mathbb{F}_l[y]$.

Algorithm 1 covers cases (i) and (iii) of Theorem 3.10. Lines 2-7 adds irreducible polynomials to the predecessor set as derived from Theorem 3.10(i), whereas lines 8-11 adds $\frac{1}{x}$ to the predecessor set depending on the condition in Theorem 3.10(iii).

The computationally most expensive step is the calculation of the Gröbner basis \mathcal{G} , for which one may use Buchberger's algorithm [14] (also see [16]), or the Faugere F4 algorithm [25]. The monomial ordering used in line 3

need not necessarily be grevlex, any ordering which will eliminate y before x will be sufficient. In practice, however, grevlex appears to be much more efficient.

Require: $f(x, y) \in \mathbb{F}_l[x, y]$ separable, monic, irreducible, \mathbb{F}_l is contained in \mathbb{F}_q

Ensure: $P = \text{Pred}_f(\frac{1}{y})$

- 1: $P \leftarrow \emptyset$
- 2: $g \leftarrow f^{(y)}(x, y)$
- 3: **for all** monic irreducible factors $g_i(x)$ of $g(x, 0)$ **do**
- 4: $P \leftarrow P \cup \{g_i(x)\}$
- 5: **end for**
- 6: $h \leftarrow f^{(x,y)}(x, y)$
- 7: **if** $h(0, 0) = 0$ **then**
- 8: $P \leftarrow P \cup \{\frac{1}{x}\}$
- 9: **end if**
- 10: **return** P .

Algorithm 2: Calculate $\text{Pred}_f(q)$ for $q(y) = \frac{1}{y}$.

Algorithm 2 covers cases (ii) and (iv) of Theorem 3.10. As it does not require the computation of a Gröbner basis as in the case of Algorithm 1, it runs much more quickly.

5.1.2 Ramification-generating polynomial sets

The next problem is the construction of ramification-generating polynomial sets for \mathcal{F} . Here we will follow Theorem 3.13 and use the notation from Definition 3.14.

As R_k needs to be computed at each step $k \geq 0$ of the tower, this algorithm will apply only to the case where the sequence $(f_i)_{i \geq 1}$ with $f_i(x_{i-1}, x_i) \in \mathbb{F}_l[x_{i-1}, x_i]$ contains only finitely many distinct polynomials. To define distinctness of polynomials exactly in this sense, we consider the equivalence relation \sim where, for $i, j \geq 1$

$$f_i(x_{i-1}, x_i) \sim f_j(x_{j-1}, x_j) :\Leftrightarrow f_i(x_{i-1}, x_i) \equiv f_j(x_{i-1}, x_i),$$

see (2.9) on page 20. This includes the family of n -step towers given by the equivalence relation \sim_n (including the usual one-step tower), for which there are at most n distinct f_i in this sense.

Suppose \mathcal{F} is a tower over \mathbb{F}_q , for which the sequence $(f_i)_{i \geq 1}$ contains only finitely many distinct polynomials modulo \sim , in other words \mathcal{F} is a \sim -finite tower. We relabel these essentially unique polynomials as $\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m$ (now the subscripts do not refer to the relevant step in the tower any more). Because of the equivalence relation \sim , there exist index sets $\Lambda_1, \Lambda_2, \dots, \Lambda_m$ which form a partition of \mathbb{N} , such that for each $i \geq 1$, $i \in \Lambda_j$ if and only if $f_i \sim \tilde{f}_j$. Therefore we need only to compute R_k for one representative k from each set Λ_i for $1 \leq i \leq m$, and we denote these by $R_{\Lambda(1)}, R_{\Lambda(2)}, \dots, R_{\Lambda(m)}$ respectively.

The following algorithm then yields a sequence of sets R_k for each $k \geq 0$ which constitute a sequence of (not necessarily minimal) ramification-generating polynomial sets:

Require: $\{f_i : i \geq 1\} \bmod \sim = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m\}$
Ensure: $R_i = R_{\Lambda(j)}$ is a ramification-generating polynomial set for each $i \in \Lambda(j), 1 \leq j \leq m$

- 1: **for** $j = 1$ to m **do**
- 2: $R_{\Lambda(j)} \leftarrow \emptyset$
- 3: $f(x, y) \leftarrow \tilde{f}_j$
- 4: $u(x) \leftarrow \text{disc}_y f(x, y) \cdot \text{disc}_y f^{(y)}(x, 0)$
- 5: $v(x) \leftarrow \text{disc}_y f^{(x)}(x, y) \cdot \text{disc}_y f^{(x, y)}(x, 0)$
- 6: **for all** monic \mathbb{F}_l -irreducible factors $u_i(x)$ of $u(x)$ **do**
- 7: $R_{\Lambda(j)} \leftarrow R_{\Lambda(j)} \cup \{u_i(x)\}$
- 8: **end for**
- 9: **if** $v(0) = 0$ **then**
- 10: $R_{\Lambda(j)} \leftarrow R_{\Lambda(j)} \cup \{\frac{1}{x}\}$
- 11: **end if**
- 12: **end for**
- 13: **return** $\{R_{\Lambda(1)}, R_{\Lambda(2)}, \dots, R_{\Lambda(m)}\}$

Algorithm 3: Calculate R_k for each $k \geq 0$.

The sets R_k for each $k \geq 0$ obtained by Algorithm 3 are not necessarily

minimal, as mentioned in Definition 3.14. The advantage however is that one can mechanically compute these R_k using the algorithm, and if a finer analysis reveals a superfluous element, remove it (see Example 3.21). Even if some superfluous elements are retained, the analysis can be continued (as in the next subsection), risking that a tower with a finite ramification locus is identified as having an infinite ramification locus.

The discriminants in Algorithm 3 are computed using resultants, see for example [17].

5.1.3 Ramification locus

We will now combine Algorithms 1 and 2 (for computing predecessors) and Algorithm 3 (the residue classes generating ramification) to algorithmically obtain a sufficient condition for the ramification locus to be finite. If the choices of R_k for $k \geq 0$ are not minimal, it is possible that the test will not be able to positively identify finite ramification, as the superfluous elements in R_k , for infinitely many positive values of k , will generate infinitely many (transitive) predecessor polynomials (see the discussion on page 36).

By the same argument, if almost all R_k (for $k \geq 0$) are minimal, there are at most finitely many steps $k \geq 0$ for which R_k contains superfluous elements. This finite set of superfluous elements (and their superfluous predecessors) will be included by the method described by Theorem 3.15 in the set B_0 , thereby not letting a finite ramification locus appear infinite, but with the possibility of extraneous elements in the obtained (finite) superset of $V_{F_0}(\mathcal{F})$ by the method described.

As in subsection 5.1.2, it is therefore desirable that the set of defining polynomials $\{f_i : i \geq 1\}$ is finite modulo \sim , this constitutes a \sim -finite tower \mathcal{F} , for which

$$\{f_i : i \geq 1\} / \sim = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m\}. \quad (5.1)$$

An often-used family of explicit towers for which this holds is the family

of n -step towers (employing the equivalence relation \sim_n), for which a set of representative defining polynomials is given by

$$\{f_i : i \geq 1\} / \sim_n = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}, \quad (5.2)$$

with the additional property that the representatives $\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n$ are applied in order in subsequent steps in the tower, see Definition 2.21. We exhibit two algorithms. Algorithms 5 and 4 will take the sequence $(f_i)_{i \geq 1}$ as input, then use the preceding algorithms of this section to either return a positive result (the tower has a finite ramification locus), or return **false**, indicating no result (it is unable to determine whether the tower has a finite ramification locus).

Algorithm 5 will assume that the input is an n -step tower, and implicitly uses the order of the representatives $\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n$ from (5.2). An important step in this algorithm is the fact that the use of the equivalence relation \sim_n implies that

$$p(x_i) \in \mathcal{A}(\Gamma_B, i) \implies p(x_j) \in \mathcal{A}(\Gamma_B, j)$$

for any $p(T) \in MI_{\mathbb{F}_l}(T)$ and $i \equiv j \pmod n$.

In contrast with this situation, Algorithm 4 applies to an arbitrary \sim -finite tower, considerably relaxing the conditions of Algorithm 5. The order of appearance of the representatives $\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m$ from (5.1) is now arbitrary at each step of the tower. We therefore assume that for the \mathbb{F}_l -ramification graph Γ_B of such a tower \mathcal{F} , that

$$p(x_i) \in \mathcal{A}(\Gamma_B, i) \implies p(x_j) \in \mathcal{A}(\Gamma_B, j)$$

for any $p(T) \in MI_{\mathbb{F}_l}(T)$ and all $j \geq 0$.

Algorithm 5 is therefore a more refined test than Algorithm 4, as it takes into account the ordering of the n representatives from (5.2), as well as the fact that the defining polynomials are equal n steps apart in the chain of extensions. Both algorithms are generalizations of the one-step tower case illustrated in Example 3.16. When the ascending chain from (3.7) stabilizes,

recursively adding more predecessors cannot increase the ramification locus, and the algorithm terminates, returning a finite superset of $V_{F_0}(F)$ represented as functions in x_0 . The positive integer M_B is the maximum allowable degree for a function (polynomial) in this set. Larger values of M_B are stronger in the sense that they increase the probability that a finite ramification locus can be found, although at the cost of a longer running time.

5.1.3.1 \sim -finite towers

Require: $\{f_i : i \geq 1\} \bmod \sim = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m\}$, $M_B \in \mathbb{N}$
Ensure: if **false** not returned, S_i represents a finite superset of $V_{F_0}(\mathcal{F})$

- 1: $\{R_{\Lambda(1)}, R_{\Lambda(2)}, \dots, R_{\Lambda(m)}\} \Leftarrow$ Output of Algorithm 3
- 2: $i \Leftarrow 0$
- 3: $S_i \Leftarrow \bigcup_{j=1}^m R_{\Lambda(j)}$
- 4: **while** $S_i \neq S_{i-1}$ **do**
- 5: $i \Leftarrow i + 1$
- 6: $S_i \Leftarrow S_{i-1}$
- 7: $S_i \Leftarrow S_i \cup \bigcup_{i=1}^m \text{Pred}_{\tilde{f}_j}(S_{i-1})$
- 8: **if** $\max\{\deg a : a \in S_i\} > M_B$ **then**
- 9: **return false**
- 10: **end if**
- 11: **end while**
- 12: **return** S_i

Algorithm 4: Decide whether the ramification locus for \mathcal{F} generated by $(f_i)_{i \geq 1}$ is finite, for arbitrary (finite modulo \sim) tower \mathcal{F}

Algorithm 4 is constructive : if **false** is not returned but S instead, the last computed value of S_i contains a set of monic \mathbb{F}_l -irreducible polynomials in x and possibly $\frac{1}{x}$. The (finite) ramification locus $V_{F_0}(\mathcal{F})$ then corresponds to places of the rational function field F_0/\mathbb{F}_l (equivalently, F_0/\mathbb{F}_q) which are zeroes of the elements of a subset¹ of S_i (with $x := x_0$).

¹Because, as in earlier discussions, S_i may contain superfluous elements.

5.1.3.2 n -step towers

Require: $\{f_i : i \geq 1\} \bmod \sim_n = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$, $M_B \in \mathbb{N}$

Ensure: if **true** returned, $S_i^{(0)}$ represents a finite superset of $V_{F_0}(\mathcal{F})$

- 1: $\{R_{\Lambda(1)}, R_{\Lambda(2)}, \dots, R_{\Lambda(n)}\} \Leftarrow$ Output of Algorithm 3
- 2: $i \Leftarrow 0$
- 3: **for** $j = 1$ to n **do**
- 4: $S_i^{(j)} \Leftarrow R_{\Lambda(j)}$
- 5: **end for**
- 6: **while** $S_i^{(j)} \neq S_{i-1}^{(j)}$ (for some $1 \leq j \leq n$) **do**
- 7: $i \Leftarrow i + 1$
- 8: **for** $j = 1$ to n **do**
- 9: $S_i^{(j)} \Leftarrow S_{i-1}^{(j)} \cup \text{Pred}_{\tilde{f}_{j+1}} S_{i-1}^{(j+1)}$
- 10: **end for**
- 11: **if** $\max\{\deg a : a \in S_i^{(0)}\} > M_B$ **then**
- 12: **return false**
- 13: **end if**
- 14: **end while**
- 15: **return** $S_i^{(0)}$

Algorithm 5: Decide whether the ramification locus for \mathcal{F} generated by $(f_i)_{i \geq 1}$ is finite, for n -step tower \mathcal{F}

Note that wherever the index j appears, we work modulo n . Therefore, when $j = n$ in line 9, we will set $S_i^{(n)} := S_{i-1}^{(n)} \cup \text{Pred}_{\tilde{f}_1}(S_{i-1}^{(1)})$. For the same reasons as for Algorithm 4, Algorithm 5 successfully terminating (not returning **false**) also reveals information on the ramification locus $V_{F_0}(\mathcal{F})$ by construction of a finite set in which $V_{F_0}(\mathcal{F})$ is contained.

The n classes of steps in the tower are also kept separate, in order to cater for the possibility that for steps i and j (where $i \neq j \bmod n$), the ramification-capturing function sequence elements $M_i \neq M_j$. In other words, we are anticipating the possibility that not all steps in the tower have identical ramification behaviour, which refines the brute-force approach of Algorithm 4.

5.1.3.3 One-step towers

A special case of Algorithm 5 is the much-studied family of one-step towers. For convenience, we write this as a separate algorithm:

Require: $\tilde{f} \in \mathbb{F}_l[x, y]$, $M_B \in \mathbb{N}$
Ensure: if **false** is not returned, S_i represents a finite superset of $V_{F_0}(\mathcal{F})$

- 1: $R \leftarrow$ Output of Algorithm 3
- 2: $i \leftarrow 0$
- 3: $S_i \leftarrow R$
- 4: **while** $S_i \neq S_{i-1}$ **do**
- 5: $i \leftarrow i + 1$
- 6: $S_i \leftarrow S_{i-1} \cup \text{Pred}_{\tilde{f}} S_{i-1}$
- 7: **if** $\max\{\deg a : a \in S_i\} > M_B$ **then**
- 8: **return false**
- 9: **end if**
- 10: **end while**
- 11: **return** S_i

Algorithm 6: Decide whether the ramification locus for \mathcal{F} generated by $(f_i)_{i \geq 1}$ is finite, for 1-step tower \mathcal{F} ($f_i \sim_1 \tilde{f}$)

It should be noted that all the algorithms described in this section blindly take a sequence $(f_i)_{i \geq 1}$ as input, and implicitly assumes that they do in fact define a tower over their field of definition (see Remark 2.3 (i)-(iii)). As this is not guaranteed for an arbitrary sequence $(f_i)_{i \geq 1}$, one should check this by hand. One way to ensure that the sequence $(f_i)_{i \geq 1}$ defines a tower is to choose them in such a way that there will exist at least one place $P \in S(F_0/\mathbb{F}_q)$ such that P is totally ramified in F_k/F_0 for each $k \geq 0$.

5.2 Complete splitting

The algorithms in this section are derived from the results of Chapter 4. As in the previous section, we will assume that the defining polynomials have a known coefficient ring (field) \mathbb{F}_l , which is a subfield of the unknown full field of definition of the tower, \mathbb{F}_q .

In contrast with the case of finite ramification where the cardinality of \mathbb{F}_q was not important but only the characteristic, the true cardinality of \mathbb{F}_q is essential when computing a complete splitting locus for the tower \mathcal{F} over \mathbb{F}_q . Because of this, we treat \mathbb{F}_q as an arbitrary extension of \mathbb{F}_l , which we can tailor to our needs to ensure that the set $T_{\mathbb{F}_0/\mathbb{F}_q}(\mathcal{F}/\mathbb{F}_q)$ is nonempty. This is done by constructing the extension $\mathbb{F}_r/\mathbb{F}_l$ following the construction in the proof of Theorem 4.6 and setting $\mathbb{F}_q := \mathbb{F}_r$.

Because of this, we assume that $(f_i)_{i \geq 1}$ consists of polynomials with \mathbb{F}_l as coefficient ring, and that our aim is to obtain a suitable extension $\mathbb{F}_q/\mathbb{F}_l$ so that \mathcal{F} with \mathbb{F}_l as full constant field becomes completely splitting if extended to \mathbb{F}_q . To do this, we will use Theorems 4.6 and 4.7, as well as Corollary 4.8.

5.2.1 Successor polynomials

We will require the computation of successor polynomials (Definition 4.1), which is derived in Theorem 4.3. As for predecessor polynomials, we distinguish between the successor sets for an element of $\mathbb{F}_l[x]$ and for $\frac{1}{x}$, given the defining polynomial $f(x, y) \in \mathbb{F}_l[x, y]$ at the relevant step of the tower.

Require: $f(x, y) \in \mathbb{F}_l[x, y]$ separable, monic, irreducible, $p(x) \in \mathbb{F}_l[x]$ monic, irreducible, \mathbb{F}_l is contained in \mathbb{F}_q

Ensure: $Q = \text{Succ}_f(p)$

- 1: $Q \leftarrow \emptyset$
- 2: $I \leftarrow \langle f(x, y), p(x) \rangle$
- 3: $\mathcal{G} \leftarrow$ Gröbner basis for the ideal I using `grevlex` with $x > y$
- 4: $v \leftarrow$ univariate generator polynomial for $I \cap \mathbb{F}_l[y]$ using \mathcal{G}
- 5: **for all** monic irreducible factors $v_i(y)$ of $v(y)$ **do**
- 6: $Q \leftarrow Q \cup \{v_i(y)\}$
- 7: **end for**
- 8: $g \leftarrow f^{(y)}(x, y)$
- 9: **if** $\deg(\gcd(g(x, 0), p(x))) > 0$ **then**
- 10: $Q \leftarrow Q \cup \{\frac{1}{y}\}$
- 11: **end if**
- 12: **return** Q .

Algorithm 7: Calculate $\text{Succ}_f(p)$ for a monic \mathbb{F}_l -irreducible $p(x) \in \mathbb{F}_l[x]$.

Algorithm 7 is very similar to the predecessor case in Algorithm 1. The computation spanning lines 2-7 covers the case of Theorem 4.3(i)(a), whereas lines 8-11 cover the case of Theorem 4.3(i)(b).

Require: $f(x, y) \in \mathbb{F}_l[x, y]$ separable, monic, irreducible, \mathbb{F}_l is contained in \mathbb{F}_q

Ensure: $Q = \text{Succ}_f(\frac{1}{x})$

- 1: $Q \leftarrow \emptyset$
- 2: $g \leftarrow f^{(x)}(x, y)$
- 3: **for all** monic irreducible factors $g_i(y)$ of $g(0, y)$ **do**
- 4: $Q \leftarrow Q \cup \{g_i(y)\}$
- 5: **end for**
- 6: $h \leftarrow f^{(x,y)}(x, y)$
- 7: **if** $h(0, 0) = 0$ **then**
- 8: $Q \leftarrow Q \cup \{\frac{1}{y}\}$
- 9: **end if**
- 10: **return** Q .

Algorithm 8: Calculate $\text{Succ}_f(p)$ for $p(x) = \frac{1}{x}$.

Algorithm 8 is the successor analogy of Algorithm 2. Lines 2-5 cover the case of Theorem 4.3(ii)(a), whereas lines 6-9 cover the case of Theorem 4.3(ii)(b).

5.2.2 Computing \mathbb{F}_r

We now use the main results from Theorems 4.6 and 4.7 to compute an appropriate extension field \mathbb{F}_r of \mathbb{F}_l such that the tower \mathcal{F} , considered over \mathbb{F}_r , will be completely splitting.

The strategy is as follows. We assume that there exists a connected component Γ_T^* of the complete \mathbb{F}_l -splitting graph Γ_T such that the boundedness condition (4.6) of Theorem 4.6 holds. To restrict our algorithm and make it computationally feasible, we assume that $m \leq M_T$ where M_T is some arbitrary positive integer. The variable M_T will denote the maximum allowable degree of a polynomial in $\mathcal{A}(\Gamma_T^*, i)$ for each $i \geq 0$.

We then pick either an arbitrary monic irreducible polynomial $p(x_0) \in \mathbb{F}_l[x_0]$ such that $\deg p \leq M_T$, or $p(x_0) = \frac{1}{x_0}$. If the \mathbb{F}_l -ramification graph has been precomputed, it should be checked that $p(x_0) \notin V(\Gamma_B)$. We implicitly assume that the candidate function $p(x_0)$ is in the vertex set of Γ_T^* , i.e. $p(x_0) \in \mathcal{A}(\Gamma_T^*, 0)$, and that the boundedness condition holds for some $m \leq M_T$. This assumption is tested by iteratively computing successor polynomials of $p(x_0)$, using Algorithms 7 and 8, which are added to $\mathcal{A}(\Gamma_T^*, 1)$, $\mathcal{A}(\Gamma_T^*, 2)$, ... respectively. The process terminates either when a monic irreducible successor polynomial of degree greater than M_T is found in which case a nonempty completely splitting locus could not be found, or the ascending chain of candidates for $\mathcal{A}(\Gamma_T^*, 1)$, $\mathcal{A}(\Gamma_T^*, 2)$, ... stabilizes, implying that a nonempty locus has been found.

If the algorithm described in the previous paragraph never terminates while performing a breadth-first traversal of the tree of paths in Γ_T originating from $p(x_0)$, all (recursive) successor polynomials of $p(x_0)$ have degree less than or equal to M_T . For this infinite tree there will therefore exist a positive integer $m \leq M_T$ so that $\mathcal{A}(\Gamma_T^*, i)$ contains polynomials of degree at most m for each $i \geq 0$ simultaneously. Then Theorem 4.6 applies, and it follows that $\#_{T_{\mathbb{F}_l, \mathbb{F}_r}}(\mathcal{F} \cdot \mathbb{F}_r) > 0$ where \mathbb{F}_r is some subfield of \mathbb{F}_{l^m} .

Moreover, for each of the algorithms for complete splitting described in this section, the assumption that the ramification locus has already been precomputed to be finite by means of the algorithms of the previous chapter can be relaxed when we are only interested in complete splitting for a tower. However, taking this into account ensures that the (unknown) component Γ_T^* of Γ that we are considering is disjoint from Γ_B . In cases where the ramification behaviour of a tower is well-known, the relevant vertices of Γ can easily be avoided to ensure that the candidates for Γ_T^* are indeed represent completely splitting places.

5.2.2.1 n -step towers

We now explicitly describe the algorithm for complete splitting in n -step towers:

Require: $\{f_i : i \geq 1\} \bmod \{\sim_n\} = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$, $M_T \in \mathbb{N}$

Ensure: $A = \mathcal{A}(\Gamma_T^*, 0)$

- 1: $P \leftarrow MI_{\mathbb{F}_l}(x_0) \setminus (\text{Output of Algorithm 5, if not false})$
- 2: $P \leftarrow \{p \in P : \deg p \leq M_T\}$
- 3: **for** p in P **do**
- 4: $A \leftarrow \{p\}$
- 5: $B \leftarrow \emptyset$
- 6: **while** $A \neq B$ and $\max\{\deg a : a \in A\} \leq M_T$ **do**
- 7: $\pi \leftarrow$ minimal degree element of $A \setminus B$
- 8: $A \leftarrow A \cup \text{Succ}_{f_1}^n(\pi) = A \cup \text{Succ}_{f_n}(\text{Succ}_{f_{n-1}}(\dots(\text{Succ}_{f_1}(\pi))\dots))$
- 9: $B \leftarrow B \cup \{\pi\}$
- 10: **end while**
- 11: **if** $\max\{\deg a : a \in A\} \leq M$ **then**
- 12: **return** A
- 13: **end if**
- 14: **end for**
- 15: **return false**

Algorithm 9: Compute a representation of a connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T of \mathcal{F} , for n -step tower \mathcal{F}

Algorithm 9 returns either **false** if no completely splitting set could be found. If it does return a set, this set is $A = \mathcal{A}(\Gamma_T^*, 0)$ for some connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T . At any time during the run, the set A contains the n -step successor polynomials of monic \mathbb{F}_l -irreducible polynomials which themselves have been added to B . The set B is therefore always contained in A , but equal only when no new successors can be added to A , meaning $A = \tilde{\mathcal{A}}(\Gamma_T^*, n)$.

The outer loop ensures that all possible components Γ_T^* of Γ_T (with the additional property that the maximum degree of an element is at most M_T) are considered.

The algorithm exploits the n -step repetitive structure of this family of towers as described in Theorem 4.12. Employing the equivalence relation \sim_n on the defining polynomials, the n representatives are given by

$$\{f_i : i \geq 1\} / \sim_n \cong \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}.$$

As $x_i \sim_n x_{i+n}$ for all $i \geq 0$, it also follows that $\mathcal{A}(\Gamma_T^*, i) \sim_n \mathcal{A}(\Gamma_T^*, i+n)$ for each $i \geq 0$. Therefore only finitely many $\mathcal{A}(\Gamma_T^*, i)$ needs to be considered, namely the n distinct representatives given by

$$\mathcal{C} := \left\{ \tilde{\mathcal{A}}(\Gamma_T^*, 1), \tilde{\mathcal{A}}(\Gamma_T^*, 2), \dots, \tilde{\mathcal{A}}(\Gamma_T^*, n) \right\}. \quad (5.3)$$

This characterization of the $\mathcal{A}(\Gamma_T^*, i)$ allows Algorithm 9 to run in finite time.

By analyzing $\mathcal{A}(\Gamma_T^*, 0)$ and the representatives $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$, we can recover all the representative classes in \mathcal{C} , where $A = \mathcal{A}(\Gamma_T^*, 0) \equiv \tilde{\mathcal{A}}(\Gamma_T^*, n)$. This allows us to recover a representation (modulo \sim_n) of the component Γ_T^* of Γ_T by

$$\begin{aligned} \tilde{\mathcal{A}}(\Gamma_T^*, n) &:= A = \mathcal{A}(\Gamma_T^*, 0), \\ \tilde{\mathcal{A}}(\Gamma_T^*, 1) &:= \text{Succ}_{\tilde{f}_1} \left(\tilde{\mathcal{A}}(\Gamma_T^*, 0) \right), \\ \tilde{\mathcal{A}}(\Gamma_T^*, 2) &:= \text{Succ}_{\tilde{f}_2} \left(\tilde{\mathcal{A}}(\Gamma_T^*, 1) \right), \\ \tilde{\mathcal{A}}(\Gamma_T^*, 3) &:= \text{Succ}_{\tilde{f}_3} \left(\tilde{\mathcal{A}}(\Gamma_T^*, 2) \right), \\ &\dots \\ \tilde{\mathcal{A}}(\Gamma_T^*, n-1) &:= \text{Succ}_{\tilde{f}_{n-1}} \left(\tilde{\mathcal{A}}(\Gamma_T^*, n-2) \right). \end{aligned}$$

Determining the field \mathbb{F}_r over which \mathcal{F} splits completely is done by the procedure of Corollary 4.8, and therefore requires the n elements of \mathcal{C} to compute. A nonempty subset of $T_{\mathbb{F}_0, \mathbb{F}_r}(\mathcal{F} \cdot \mathbb{F}_r)$ is found by considering only the elements of $\mathcal{A}(\Gamma_T^*, 0) \equiv \tilde{\mathcal{A}}(\Gamma_T^*, n)$, split into linear factors over \mathbb{F}_r .

5.2.2.2 One-step towers

For convenience, we exhibit the one-step version of Algorithm 9 which is applicable to the family of one-step towers.

<p>Require: $f \in \mathbb{F}_l[x, y], M_T \in \mathbb{N}$</p> <p>Ensure: $A = \mathcal{A}(\Gamma_T^*, 0)$ for some component Γ_T^* of Γ_T.</p> <ol style="list-style-type: none"> 1: $P \leftarrow MI_{\mathbb{F}_l}(x) \setminus (\text{Output of Algorithm 6, if not false})$ 2: $P \leftarrow \{p \in P : \deg p \leq M_T\}$ 3: for p in P do 4: $A \leftarrow \{p\}$ 5: $B \leftarrow \emptyset$ 6: while $A \neq B$ and $\max\{\deg a : a \in A\} \leq M_T$ do 7: $\pi \leftarrow$ minimal degree element of $A \setminus B$ 8: $A \leftarrow A \cup \text{Succ}_f(\pi)$ 9: $B \leftarrow B \cup \{\pi\}$ 10: end while 11: if $\max\{\deg a : a \in A\} \leq M_T$ then 12: return A 13: end if 14: end for 15: return false
--

Algorithm 10: Compute a representation of a connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T of \mathcal{F} , for one-step tower \mathcal{F}

5.2.2.3 \sim -finite towers

As an analogue to the brute-force approach of Algorithm 4 for computing ramification loci for \sim -finite towers, we exhibit a similar relaxed-conditions algorithm for complete splitting. For a \sim -finite tower \mathcal{F} with representative polynomials $\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m$, we make the assumption that if $p(x_i) \in \mathcal{A}(\Gamma_T^*, i)$ for some $i \geq 0$, then $p(x_j) \in \mathcal{A}(\Gamma_T^*, j)$ for all $j \geq 0$.

Require: $\{f_i : i \geq 1\} \bmod \sim = \{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m\}$, $M_T \in \mathbb{N}$
Ensure: $A = \mathcal{A}(\Gamma_T^*, 0)$ for some component Γ_T^* of Γ_T .

- 1: $P \leftarrow MI_{\mathbb{F}_l}(x) \setminus (\text{Output of Algorithm 4, if not false})$
- 2: $P \leftarrow \{p \in P : \deg p \leq M_T\}$
- 3: **for** p in P **do**
- 4: $A \leftarrow \{p\}$
- 5: $B \leftarrow \emptyset$
- 6: **while** $A \neq B$ and $\max\{\deg a : a \in A\} \leq M_T$ **do**
- 7: $\pi \leftarrow \text{minimal degree element of } A \setminus B$
- 8: $A \leftarrow A \cup \bigcup_{i=1}^m \text{Succ}_{\tilde{f}_i}(\pi)$
- 9: $B \leftarrow B \cup \{\pi\}$
- 10: **end while**
- 11: **if** $\max\{\deg a : a \in A\} \leq M_T$ **then**
- 12: **return** A
- 13: **end if**
- 14: **end for**
- 15: **return false**

Algorithm 11: Compute a representation of a connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T of \mathcal{F} , for \sim -finite tower \mathcal{F}

5.3 Tamely ramified towers

We are now in a position to use the combination of Algorithms 5 and 9 to determine whether the conditions of Corollary 2.18 are satisfied for a tower \mathcal{F} defined by a sequence of defining polynomials $(f_i)_{i \geq 1}$ over a finite field \mathbb{F}_l , in the case that \mathcal{F} is tamely ramified. When this occurs, we can explicitly compute a positive lower bound for $\lambda(\mathcal{F})$ from a superset of $V_{F_0}(\mathcal{F})$, such as S obtained from Algorithms 4, 5 and 6.

To test for the extra condition on the boundedness of the different exponents for wildly ramified towers (see Theorem 2.16) it is outside the scope of the algorithmic approach described here. In some cases it is possible to determine such bounds explicitly, see for example [28].

5.3.1 n -step towers

Given an n -step tower \mathcal{F} with defining polynomials $(f_i)_{i \geq 1}$ having \mathbb{F}_l as coefficient ring, we obtain the n representatives

$$\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\} \cong \{f_i : i \geq 1\} / \sim_n$$

in the manner described in the previous section. We choose elements $M_B, M_T \in \mathbb{N}$ which will denote the maximum allowable degrees² of polynomials in $V(\Gamma_B)$ and $V(\Gamma_T^*)$ respectively, where Γ_T^* is a connected component of the complete \mathbb{F}_l -splitting graph Γ_T which will be explicitly constructed using Algorithm 9 (if it exists, with polynomial degrees less than or equal to M_T) and Γ_B is the \mathbb{F}_l -ramification graph of \mathcal{F} .

Applying Algorithm 5 with M_B and $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$ as input, we either obtain **false** as a returned value (in which we cease the analysis of the given tower), or $S_i^{(0)}$ (see Algorithm 5 line 10) is returned. In this case, $S_i^{(0)}$ is a set of monic \mathbb{F}_l -irreducible polynomials in $\mathbb{F}_l[x_0]$ (and possibly the element $\frac{1}{x_0}$) representing the elements of $V_{F_0/\mathbb{F}_l}(\mathcal{F}/\mathbb{F}_l)$, which corresponds to a subset of the places of F_0/\mathbb{F}_l . As $S_i^{(0)}$ is finite, the ramification locus is found to be finite in this case, and we continue to the analysis of the splitting behaviour.

Algorithm 9 now uses the output from Algorithm 5 in the previous paragraph to restrict our analysis to elements of Γ_T , still using M_T and the set $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$ as input. If **false** is returned, no complete splitting locus involving polynomials of degree at most M_T could be found, and we stop. If the set A is returned (Algorithm 9, line 12), A contains monic \mathbb{F}_l -irreducible polynomials in $\mathbb{F}_l[x_0]$ (and possibly the element $\frac{1}{x_0}$) corresponding to places of degree one of F_0/\mathbb{F}_r (note that polynomials in $\mathbb{F}_l[x_0]$ are factored into linear polynomials in $\mathbb{F}_r[x_0]$ in this case). The cardinality of the finite field \mathbb{F}_r can be obtained by applying Corollary 4.8.

²We may also choose different natural numbers M_B and M_T for Algorithms 5 and 9 respectively. As the ramification-generating sets are known, M_B can be set high at relatively low computational cost.

5.3.2 \sim -finite towers

For a \sim -finite tower which is not an n -step tower, the analysis continues in the same way as for n -step towers, except that the ramification test of Algorithm 5 is replaced by Algorithm 4, and the complete splitting locus test of Algorithm 9 is replaced by Algorithm 11. The tests for \sim -finite towers are considerably weaker than the specialized test for n -step towers, as the strong assumptions used by Algorithms 4 and 11 may easily lead to them returning **false** when the specific tower does possess a finite ramification locus or is completely splitting, respectively.

Chapter 6

Applications

The algorithms of Chapter 5 were implemented using the Magma V2.11-1 computer algebra system [13]. A subset of the program code is given in Appendix A. Implementation in Magma makes it possible to automate much of the process of determining finite ramification loci, complete splitting loci, and the limit $\lambda(\mathcal{F})$ itself of a tower in the tamely ramified case.

We will focus almost exclusively on the tamely ramified case for n -step towers, involving the n -step Algorithms 5 and 9 (for finite ramification and complete splitting, respectively), and apply the specialization of this to one-step towers. In each of the examples we will consider, we choose defining polynomials for \mathcal{F} beforehand, as well as suitable values for $M_B, M_T \in \mathbb{N}$, then attempt to determine the ramification structure and complete splitting of the induced tower by constructing suitable ramification and complete splitting graphs.

In many cases the program code will generate sets of candidate equations for defining polynomials. When applicable, we eliminate many candidates from these sets by only using one candidate $f(x, y)$ from each $GL(\mathbb{F}_q, 2)$ -orbit of $f(x, y)$. We will therefore only use one representative from the set

$$\left\{ f^A(x, y) : A \in GL(\mathbb{F}_q, 2) \right\},$$

following the notation in Section 2.3.

The chapter is divided into two sections, the first covering examples of

computations involving tamely ramified towers, the second considering wildly ramified towers.

6.1 Tame towers

In [36] various tamely ramified towers are considered. We first consider a restricted family of towers of Fermat type, earlier alluded to in Example 3.21, then move on to more general towers of Kummer extensions of the type considered in [36] and higher degrees.

6.1.1 Towers of Fermat type

Following [36, Definition 3.3], the defining polynomial of a one-step tower of Fermat type over \mathbb{F}_q is given by

$$f(x, y) = y^m + a(x + b)^m + c \quad (6.1)$$

where $a, b, c \in \mathbb{F}_q$ and $(m, q) = 1$. However, to ensure that (6.1) does indeed define a tower, a sufficient condition is that $a \cdot b^m + c = 0$, see [36, Proposition 3.4]. It can be shown then that the place corresponding to $x_0 = 0$ being a simple zero of $a(x + b)^m + c$ implies that the unique place above it is a simple zero for the function x_1 , and that $x_0 = 0$ is totally ramified in the tower \mathcal{F} . If we further assume that $m \mid (q - 1)$ and a is an m th power in \mathbb{F}_q , the pole of x_0 is completely splitting in \mathcal{F} . In this case, the tower is asymptotically good, with $\lambda(\mathcal{F}) \geq \frac{2}{q-2}$.

As it is in each case the zero of the functions x_0, x_1, x_2, \dots that is ramified in this sequence, one can easily construct an n -step Fermat tower where each of the n representatives $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\}$ are of the form (6.1) for possibly different choices of a, b and c at each step. As the argument above still holds, such an n -step tower will still be defined, with the place $x_0 = 0$ totally ramified in it.

We enumerated the possible defining polynomials (6.1) at each step for various m, n and \mathbb{F}_q using a Magma program. The tower considered in

Figure 3.4 was found in this way, and is an example of an asymptotically good two-step Fermat tower for $m = 4$, $n = 2$ and $\mathbb{F}_q = \mathbb{F}_9$ in (6.1). Another example we found in this way is the two-step tower given by the representatives

$$\tilde{f}_1(\tilde{x}, \tilde{y}) = \tilde{y}^6 - (\tilde{x} + 1)^6 + 1 \text{ and } \tilde{f}_2(\tilde{y}, \tilde{x}) = \tilde{x}^6 + (\tilde{y} - 1)^6 - 1$$

over \mathbb{F}_{25} (as $6 \mid (25 - 1)$). Both these towers have ramification locus

$$V_{F_0}(\mathcal{F}) = \{P \in S(F_0/\mathbb{F}_q) : x_0(P) \in \mathbb{F}_q\},$$

resulting in a limit of $\lambda(\mathcal{F}) \geq \frac{2}{q-2}$, not improving the one-step case.

In general one can construct a tower over \mathbb{F}_p where the defining polynomial at each step varies, but is of the form described in (6.1) with $m = p + 1$, as the argument used in the proof of Example 3.22 (b) and the comments above together imply that such a tower will have a finite ramification locus corresponding to the \mathbb{F}_{p^2} -rational elements of $S(F_0/\mathbb{F}_p)$. When $q = p^2$ we have that $m \mid (q - 1)$, implying that the pole of x_0 splits completely up the tower. As the number of admissible choices of $a, b, c \in \mathbb{F}_q$ for (6.1) is finite, such a tower is \sim -finite but not n -step for any $n \geq 1$. While it is hoped that certain combinations of defining polynomials of this type will yield ramification loci with elements not corresponding to a subfield¹ \mathbb{F}_l of \mathbb{F}_q in order to improve the limit $\lambda(\mathcal{F})$, we could not find such examples through computer search.

6.1.2 Towers of Kummer extensions

In [36, Section 4] the ramification structure and complete splitting structure of various tamely ramified one-step towers of Kummer extensions are considered. For an overview of the ramification theory of Kummer extensions, we refer to [59, III.7]. The following proposition (which restates [36, Proposition 4.1] more generally) describes a family of sequences of Kum-

¹To ensure that this does not coincide with the ramification loci found in the Fermat towers in [37] with limit $\lambda(\mathcal{F}) \geq \frac{2}{l-2}$.

mer extensions which are guaranteed to induce totally ramified towers of function fields.

Proposition 6.1 *Let \mathbb{F}_q be a finite field of characteristic p . Fix a sequence of natural numbers $(m_i)_{i \geq 1}$ so that for each i we have $1 < m_i < p$ and two sequences of univariate polynomials $(g_i)_{i \geq 1}, (h_i)_{i \geq 1} \in (\mathbb{F}_q[x_{i-1}])_{i \geq 1}$ where for each $i \geq 1$ we have that $\deg g_i = m_i$, $\deg h_i = m_i - 1$ and $(g_i, h_i) = 1$. Define the sequence $(f_i)_{i \geq 1} \in (\mathbb{F}_q[x_{i-1}, x_i])_{i \geq 1}$ of bivariate polynomials by*

$$f_{i+1}(x_i, x_{i+1}) := x_{i+1}^{m_{i+1}} h_{i+1}(x_i) - g_{i+1}(x_i) \quad (6.2)$$

for each $i \geq 0$. Then the sequence $(f_i)_{i \geq 1}$ defines an explicit, tamely ramified tower \mathcal{F} for which the pole of x_0 in $S(F_0/\mathbb{F}_q)$ is totally ramified in \mathcal{F} , with representation

$$\mathcal{F} = (\mathbb{F}_q(x_0) = F_0, F_1, F_2, \dots)$$

where $[F_{i+1} : F_i] = m_{i+1}$ for each $i \geq 0$.

Proof. Writing (6.2) for each $i \geq 0$ as an equation in variable separated form, we have

$$x_{i+1}^{m_{i+1}} = \frac{g_{i+1}(x_i)}{h_{i+1}(x_i)}. \quad (6.3)$$

As $\deg g_{i+1} = 1 + \deg h_{i+1}$, we see that the x_i is a simple pole of the right-hand side, and hence it is totally ramified in the (separable) extension $\mathbb{F}_q(x_i, x_{i+1})/\mathbb{F}_q(x_i)$. The unique place above the pole of x_i is then a simple pole of x_{i+1} . By induction, this place is totally ramified in F_n/F_0 for each $n \geq 1$, and hence the sequence $(f_i)_{i \geq 1}$ does define a tower. ■

The restriction of Proposition 6.1 to the case of a one-step tower for $m_i = m = 2$ yields the case considered in [36]. As $1 < m_i < p$, the fields \mathbb{F}_q considered are of odd characteristic. We further note that if $x_i = 0$ is a simple zero of the right-hand side of (6.3) for each $i \geq 0$, then the zero of x_0 in $S(F_0/\mathbb{F}_q)$ is also totally ramified in the tower.

We now consider a subfamily of the family of towers of Proposition 6.1.

Proposition 6.2 Let \mathbb{F}_q be a finite field of characteristic p , and $\overline{\mathbb{F}}$ its algebraic closure. Fix a sequence of natural numbers $(m_i)_{i \geq 1}$ with $1 < m_i < p$ for each $i \geq 1$. Let $(A_i)_{i \geq 1}$ be a sequence of elements of $\text{PGL}(\overline{\mathbb{F}}, 2)$ so that A_{i+1} is an element of order m_{i+1} in $\text{PGL}(\overline{\mathbb{F}}, 2)$ for each $i \geq 0$. Let $(B_i)_{i \geq 1}$ be a sequence of (upper triangular) matrices of the form

$$B_{i+1} = \begin{bmatrix} \alpha_{i+1} & \beta_{i+1} \\ 0 & 1 \end{bmatrix}$$

where $\alpha_i \neq 0$ for each $i \geq 0$. Consider the sequence of defining polynomials $(f_{i+1}(x_i, x_{i+1}))_{i \geq 1}$ where $f_{i+1}(x_i, x_{i+1})$ is induced by the variable separated form equation

$$x_{i+1}^{m_{i+1}} = \prod_{j=0}^{m_{i+1}-1} \left((B_{i+1} A_{i+1}^j) \cdot x_i \right) \quad (6.4)$$

and we further assume that the right-hand side of (6.4), can be written as a rational function in lowest terms in x_i as

$$x_{i+1}^{m_{i+1}} = \frac{g_{i+1}(x_i)}{h_{i+1}(x_i)} \quad (6.5)$$

with $g_{i+1}, h_{i+1} \in \mathbb{F}_q[x_i]$, has $\deg g_{i+1} = m_{i+1} = 1 + \deg h_{i+1}$, for each $i \geq 0$. Then

- (i) The sequence $(f_i)_{i \geq 1}$ defines a tamely ramified tower \mathcal{F} over \mathbb{F}_q .
- (ii) The pole of x_0 in $S(F_0/\mathbb{F}_q)$ is totally ramified in \mathcal{F} .
- (iii) The right-hand side of (6.4) is invariant under the linear fractional transformation $x_i \mapsto A_{i+1}^k \cdot x_i$ for each $k \geq 0$.
- (iv) The function

$$\sum_{j=0}^{m_{i+1}-1} A_{i+1}^j \cdot x_i$$

is invariant under the linear fractional transformation $x_i \mapsto A_{i+1}^k \cdot x_i$ for each $k \geq 0$.

(v) If $\beta_i = 0$ for all $i \geq 1$, then both the zero and pole of x_0 in $S(F_0/\mathbb{F}_q)$ are totally ramified in \mathcal{F} .

(vi) If the edge $p(x_i) \xrightarrow{f_{i+1}} q(x_{i+1})$ is in the edge set of $\Gamma_T = \left(\Gamma_{\mathcal{F}, \overline{\mathbb{F}}, (f_i)_{i \geq 1}}\right)_T$ then for each $\alpha, \beta \in \overline{\mathbb{F}}$ with $p(\alpha) = 0 = q(\beta)$ we have that $P_k(x_i) \xrightarrow{f_{i+1}} Q_l(x_{i+1})$ is in the edge set of Γ_T as well for each $k, l \in \mathbb{Z}$, where $P_k(x_i) = x_i - A_{i+1}^k \cdot \alpha$ for any $k \in \mathbb{Z}$ and $Q_l(x_{i+1}) = x_{i+1} - \beta \gamma_{i+1}^l$ and γ_{i+1} is a primitive m_{i+1} th root of unity.

Proof. We note that under the assumptions, the tower \mathcal{F} is of the type described in Proposition 6.1. Therefore (i) and (ii) follows immediately. Both (iii) and (iv) follow by noting that the set

$$\left\{ A_{i+1}^0, A_{i+1}^1, \dots, A_{i+1}^{m_{i+1}-1} \right\},$$

for each $i \geq 0$, is unchanged under left multiplication by A_{i+1} , as $A_{i+1}^{m_{i+1}} = I$ where I is the 2×2 identity matrix in $PGL(\overline{\mathbb{F}}, 2)$. Under the assumption of (v), the action of B_{i+1} is just scalar multiplication by α_{i+1} , ensuring that, for the factor $(B_{i+1}A_{i+1}^0) \cdot x_i$ of the right-hand side of (6.4) we have

$$\left(B_{i+1}A_{i+1}^0 \right) \cdot x_i = \alpha_{i+1} \cdot (I \cdot x_i) = \alpha_{i+1}x_i$$

and hence $x_i = 0$ is a zero of the right-hand side of (6.4). If it was not a simple zero, then we would have for some $0 < j < m_{i+1}$ that

$$\alpha_{i+1}x_i = \alpha_{i+1} \cdot \left(A_{i+1}^j \cdot x_i \right) \Rightarrow A_{i+1}^j = I,$$

which cannot occur as $j < m_{i+1}$. It then follows that the zero of x_0 is totally ramified in \mathcal{F} .

For (vi), we note that $\frac{1}{x_i} \notin V(\Gamma_T)$ for each $i \geq 0$ as the pole of x_0 is totally ramified in \mathcal{F} . We have that $f_{i+1}(\alpha, \beta) = 0$, and need to show that

$$f_{i+1} \left(A_{i+1}^k \cdot \alpha, \beta \gamma_{i+1}^l \right) = 0$$

for each $k, l \in \mathbb{Z}$. As the transformation $x_i \mapsto A_{i+1} \cdot x_i$ is an automorphism of (6.4), we have $f_{i+1}(A_{i+1}^k \cdot \alpha, \beta) = 0$ for each $k \in \mathbb{Z}$. The action $x_i \mapsto x_i \gamma_{i+1}$ obviously fixes the expression $x_{i+1}^{m_{i+1}}$, and the result follows. ■

The invariants of the types described in Proposition 6.2 (iii) and (iv) yield expressions by which we can form subtowers of a given tower. In the next subsection we will illustrate cases where subtowers can be constructed of towers using this method.

The result in (vi) suggests a method by which we can construct more edges in a component of Γ_T given one edge of Γ_T . Consider the step F_{i+1}/F_i of the tower, and suppose $P_0(x_i) \xrightarrow{f_{i+1}} Q_0(x_{i+1})$ is an edge of Γ_T , belonging to some unknown connected component Γ_T^* . Here we choose Γ_T as we know that $\frac{1}{x_i} \in V(\Gamma_B)$ for each i for the family of towers considered in both Proposition 6.1 and 6.2. By definition, there exist elements $\alpha, \beta \in \overline{\mathbb{F}}$ so that $f_{i+1}(\alpha, \beta) = 0$. By Proposition 6.2 (vi), for each

$$\alpha' = A_{i+1}^k \cdot \alpha \text{ and } \beta' = \gamma_{i+1}^l \beta \quad (6.6)$$

we also have $f_{i+1}(\alpha', \beta') = 0$. Therefore, there exists monic irreducible polynomials $P_k(x_i)$ and $Q_l(x_{i+1})$, respectively the minimum irreducible polynomials of α' and β' , with the edge $P_k(x_i) \xrightarrow{f_{i+1}} Q_l(x_{i+1})$ present in Γ for each possible (α', β') defined by (6.6), i.e. for each $k, l \in \mathbb{Z}$. In fact, this edge is in the component Γ_T^* of Γ_T , as $P_0(x_i) \xrightarrow{f_{i+1}} Q_0(x_{i+1}) \in \Gamma_T^*$ implies that $P_0(x_i) \xrightarrow{f_{i+1}} Q_l(x_{i+1}) \in \Gamma_T^*$ with $\beta' = \gamma_{i+1}^l \beta$, from which it follows that $P_k(x_i) \xrightarrow{f_{i+1}} Q_l(x_{i+1}) \in \Gamma_T^*$ with $\alpha' = A_{i+1}^k \cdot \alpha$. Hence each of the obtained edges (by varying k and l) belong to the same component Γ_T^* of Γ_T .

Given $f_{i+1}(x_i, x_{i+1}) \in \mathbb{F}_q[x_i, x_{i+1}]$, $P_0(x_i) \in \mathbb{F}_q[x_i]$, $Q_0(x_{i+1}) \in \mathbb{F}_q[x_{i+1}]$ and $m_{i+1} > 1$, we can construct each of these edges by using an elimination ideal. If we form the ideal

$$I_{i+1} = \left\langle \begin{array}{l} f_{i+1}(\alpha, \beta), P_0(\alpha), Q_0(\beta), \gamma_{i+1}^{m_{i+1}} - 1, \\ \beta' - \gamma_{i+1}^l \beta, (a_{21}\alpha + a_{22})\alpha' - (a_{11}\alpha + a_{12}) \end{array} \right\rangle$$

of the polynomial ring $\mathbb{F}_q[\alpha, \beta, \alpha', \beta', \gamma_{i+1}]$ where

$$A_{i+1}^k \equiv \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

representations for the vertices (polynomials) $P_k(x_i)$ and $Q_l(x_{i+1})$ can be found by computing a univariate polynomial basis for $I_{i+1} \cap \mathbb{F}_l[\alpha']$ and $I_{i+1} \cap \mathbb{F}_l[\beta']$ respectively.

It can therefore be seen that for towers of the form of those described in Proposition 6.2, the action of A_{i+1} on x_i and multiplication of x_{i+1} by γ_{i+1} induces automorphisms on the set of vertices of a connected component Γ_T^* of Γ_T .

6.1.2.1 Towers of quadratic extensions

An extensive study of one-step towers of quadratic extensions has been made in [36] and [47]. We focus on one-step towers of the family described in Proposition 6.1 (for $m_i = 2$) and show that many of these can be expressed in the form (6.4) of Proposition 6.2.

A Magma implementation allowed us to test the family of towers of Proposition 6.2 over various small finite fields. For the (quadratic) case $m_i = 2$ similar studies have been done for the primes $p \leq 11$ in [45] and [47], although in those cases the whole² family of q^9 defining polynomials $f(x, y) \in \mathbb{F}_q[x, y]$ of balanced degree was tested using computer methods. For larger m_i and larger p this is impractical, and promising subfamilies must be tested.

6.1.2.1.1 A tower over \mathbb{F}_p , $p \geq 3$ A quadratic one-step tower \mathcal{F} over \mathbb{F}_p ($p \geq 3$) considered in [36] is generated by the defining equations

$$x_{i+1}^2 = \frac{x_i(1-x_i)}{x_i+1}$$

²With the exception of some subfamilies of equations known to not define towers or yield bad towers.

for each $i \geq 0$. It can be written in the form of Proposition 6.2 by letting $m_i = 2$,

$$A_{i+1} = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } B_{i+1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

for all $i \geq 0$. Proposition 6.2 (v) applies, and we have that both $x_0 = 0$ and $x_0 = \infty$ are totally ramified in \mathcal{F} .

This tower was shown by Beelen and Bouw [6] to be asymptotically optimal over \mathbb{F}_{p^2} when $p \equiv \pm 1 \pmod{8}$. This is confirmed by explicit computations using the algorithms from Chapter 5 for many cases, which yields a representation of the \mathbb{F}_p -ramification graph shown in Figure 6.1. It should be noted that the vertices $\tilde{x}^2 + 1$, $\tilde{x}^2 - 2\tilde{x} - 1$ and $\tilde{x}^2 + 2\tilde{x} - 1$ are not guaranteed to be irreducible in $\mathbb{F}_p[\tilde{x}]$, this is dependent on whether -1 (for $\tilde{x}^2 + 1$) and 2 (for $\tilde{x}^2 - 2\tilde{x} - 1$ and $\tilde{x}^2 + 2\tilde{x} - 1$) are quadratic residues modulo p . From the theory of Legendre symbols these two cases occur respectively when $p \equiv 1 \pmod{4}$ and when $p^2 \equiv 1 \pmod{16}$. When such reducibility occurs, the ramification graph will have the relevant vertices split into two vertices each, but will still present a finite ramification locus. It follows that, independently from p , $\sum_{P \in V_{\mathbb{F}_0}(\mathcal{F})} \deg P = 10$.

The complete splitting of the tower \mathcal{F} can be computed using the algorithms in Chapter 5 for various primes. In [36] the case $p = 3$ was considered, resulting in 8 places of degree one splitting completely over \mathbb{F}_{81} . The cases $p = 5, 7$ and 11 was considered in [47], showing that the tower is completely splitting respectively over the fields \mathbb{F}_{5^4} , \mathbb{F}_{7^2} and \mathbb{F}_{11^4} . A representation of the finite component $\tilde{\Gamma}_T^*$ of $\tilde{\Gamma}_T$ obtained using the Magma implementation for $p = 5$ is shown in Figure 6.2.

We continued the analysis for all the odd primes less than 100. The experimental results seem to indicate that whenever $p^2 \equiv 1 \pmod{16}$, the tower is asymptotically optimal over \mathbb{F}_{p^2} , otherwise it is asymptotically good (but not optimal) over \mathbb{F}_{p^4} . A computer-generated representation of the completely splitting component of Γ_T for $p = 13$ is presented in the Appendix, Figure B.2.

We construct two subtowers of the tower \mathcal{F} defined on page 6.1.2.1.1,

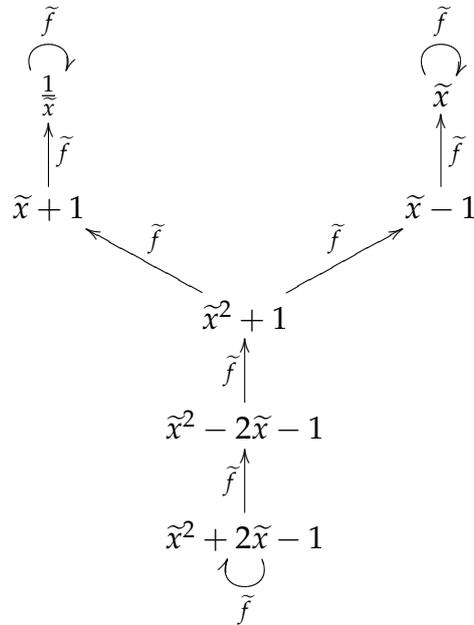


Figure 6.1: Condensed \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$ for \mathcal{F}

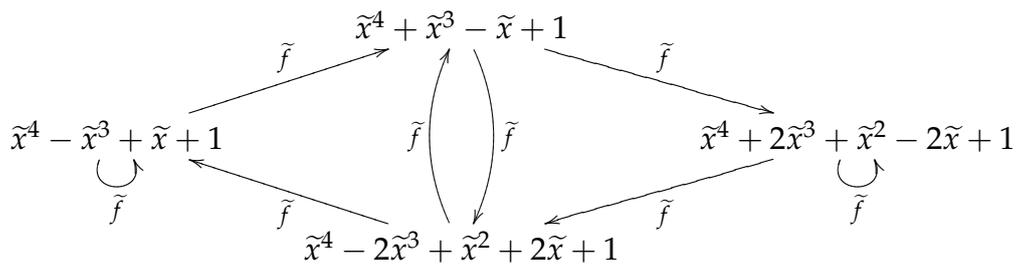


Figure 6.2: Condensed component of $\tilde{\Gamma}_T^*$ for \mathcal{F} , $p = 5$

using the functions in x_i in Proposition 6.2 (iii) and (iv) respectively, using a method of Elkies [45]. In the first case (using (iii)) we define

$$y_i := \prod_{j=0}^{m_{i+1}-1} \left((B_{i+1} A_{i+1}^j) \cdot x_i \right)$$

for each $i \geq 0$, and obtain using elimination theory (over \mathbb{Z}) the relation

$$g_{i+1}(y_i, y_{i+1}) = y_{i+1}^2 y_i^2 + 2y_{i+1} y_i^2 + y_i^2 - 4y_{i+1} y_i + y_{i+1}^2 - 2y_{i+1} + 1 = 0$$

for each $i \geq 0$ and any prime $p \geq 3$. If we let $\mathcal{G} = (G_0, G_1, G_2, \dots)$ with $G_i = \mathbb{F}_p(y_0, y_1, \dots, y_i)$ be the explicit one-step tower induced by these equations, we obtain a tower which has (over \mathbb{F}_3) isomorphic ramification and complete splitting graphs as \mathcal{F} , i.e.

$$\left(\Gamma_{\mathcal{F}, \mathbb{F}_p, (f_i)_{i \geq 1}} \right)_B \cong \left(\Gamma_{\mathcal{G}, \mathbb{F}_p, (g_i)_{i \geq 1}} \right)_B \quad \text{and} \quad \left(\Gamma_{\mathcal{F}, \mathbb{F}_p, (f_i)_{i \geq 1}} \right)_T \cong \left(\Gamma_{\mathcal{G}, \mathbb{F}_p, (g_i)_{i \geq 1}} \right)_T.$$

The second case, in which we use Proposition 6.2 (iv), we define

$$z_i := \sum_{j=0}^{m_{i+1}-1} A_{i+1}^j \cdot x_i$$

for each $i \geq 0$ in order to define the quotient subtower, and similarly obtain the equation

$$h_{i+1}(z_i, z_{i+1}) = z_{i+1}^2 z_i + 2z_{i+1} z_i - 4z_{i+1} + z_i^2 - 4z_i + 4 = 0$$

for each $i \geq 0$ and any prime $p \geq 3$. If we let $\mathcal{H} = (H_0, H_1, H_2, \dots)$ with $H_i = \mathbb{F}_p(z_0, z_1, \dots, z_i)$ be the explicit one-step tower induced by these equations, we obtain a tower with ramification and complete splitting graphs nonisomorphic (as graphs) to that of \mathcal{F} . Indeed, the ramification locus is

$$V_{H_0/\mathbb{F}_p}(\mathcal{H}) = \left\{ z_0, z_0 - 1, z_0 - 2, z_0^2 + 4z_0 - 4, \frac{1}{z_0} \right\},$$

and for $p = 5$, $\#T_{H_0}(\mathcal{H}) = 8$, whereas $\#T_{F_0}(\mathcal{F}) = 16$. However, the lower

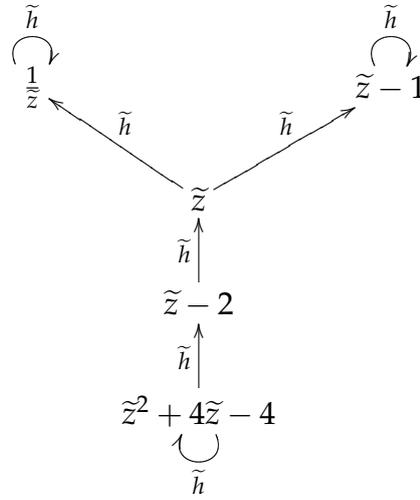


Figure 6.3: Condensed \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$ for \mathcal{H}

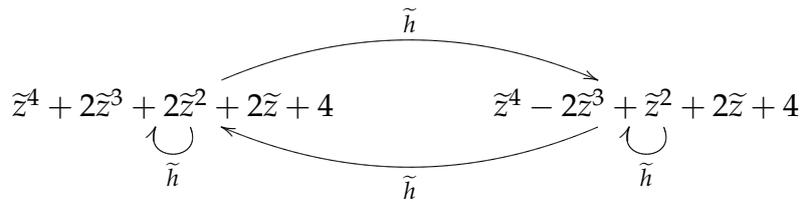


Figure 6.4: Condensed component of $\tilde{\Gamma}_T^*$ for \mathcal{H} , $p = 5$

bound for $\lambda(\mathcal{H})$ given by Corollary 2.18 is not better than that of $\lambda(\mathcal{F})$, although $\lambda(\mathcal{H}) \geq \lambda(\mathcal{F})$ as \mathcal{H} is a subtower of \mathcal{F} . Graphical representations of $(\Gamma_{\mathcal{H}, \mathbb{F}_p})_B$ and $(\Gamma_{\mathcal{H}, \mathbb{F}_5})_T$ are respectively given in Figures 6.3 and 6.4.

Considering Figure 6.3, we see that for an arbitrary prime $p \geq 3$, the tower \mathcal{H} has the places $z_0 = \infty$ and $z_0 = 1$ in $S(H_0/\mathbb{F}_p)$ totally ramified in the tower, the place $z_0 = 0$ is unramified in H_1/H_0 but is totally ramified above H_1 , and the place $z_0 = 2$ is unramified in H_2/H_0 , but is totally ramified from H_2 onwards. The places in $S(H_0/\mathbb{F}_p)$ corresponding to roots of $z_0^2 + 4z_0 - 4$ are unramified in H_3/H_0 , but totally ramified in H_i/H_3 for each $i \geq 4$.

6.1.2.1.2 An optimal tower over \mathbb{F}_p , $p \geq 3$ We briefly consider the one-step tower of Kummer extensions \mathcal{F} given by the recursive equations

$$x_{i+1}^2 = \frac{x_i^2 + 1}{2x_i} \quad (6.7)$$

for each $i \geq 0$. This tamely ramified tower was shown in [36] to be asymptotically optimal over \mathbb{F}_{p^2} for each prime $p \geq 3$. If the defining polynomials of the tower are considered to have coefficient ring \mathbb{F}_{p^4} , the tower is also of the type described in Proposition 6.2 by letting $m_i = 2$,

$$A_{i+1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } B_{i+1} = \begin{bmatrix} s^{-1}r^{-1} & s^{-1}r \\ 0 & 1 \end{bmatrix}$$

for all $i \geq 0$ and $r, s \in \mathbb{F}_{p^4}$ with $r^4 + 1 = 0$ and $s^2 - 2 = 0$. It then follows that

$$\begin{aligned} x_{i+1}^2 &= \prod_{j=0}^{m_i-1} \left((B_{i+1}A_{i+1}^j) \cdot x_i \right) = (B_{i+1} \cdot x_i) (B_{i+1}A_{i+1} \cdot x_i) \\ &= \frac{1}{rs} (x_i + r^2) \frac{1}{rs} \left(\frac{1}{x_i} + r^2 \right) = \frac{(x_i + r^2) (1 + x_i r^2)}{2r^2 x_i} \\ &= \frac{r^2 x_i^2 + (r^4 + 1) x_i + r^2}{2r^2 x_i} = \frac{x_i^2 + 1}{2x_i}, \end{aligned}$$

as required. This also shows that, due to the coefficients in B_i , in order to study towers with defining polynomials with a certain finite coefficient field of the form of Proposition 6.2, matrices B_i with entries in a potentially larger finite coefficient field should be considered.

Showing that the tower has a finite ramification locus follows easily by constructing a \mathbb{F}_p -ramification graph. It was shown [36] that a splitting characteristic polynomial for \mathcal{F} is given by

$$\tau_{\Gamma_T^*}(x_0) = H_p(x_0^4) \quad (6.8)$$

where

$$H_p(T) = \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j}^2 \cdot T^j \in \mathbb{F}_p[T] \quad (6.9)$$

is Deuring's polynomial, which is used to classify supersingular elliptic curves based on the Legendre form: the elliptic curve given by $y^2 = x(x-1)(x-\lambda)$ is supersingular iff $H_p(\lambda) = 0$. As the separable polynomial $H_p(T)$ has $\deg H_p = \frac{p-1}{2}$, this implies that \mathcal{F} has $2(p-1)$ places which split completely. It is shown in [36] that $\tau_{T^*}(x_0)$ as in (6.8) is a solution for the functional equation described in Proposition 4.14. Showing that \mathbb{F}_{p^2} is the splitting field of $\tau_{T^*}(x_0) \in \mathbb{F}_p[x_0]$ requires that the roots of $H_p(T)$ are fourth powers in \mathbb{F}_{p^2} . This is shown by Auer and Top in [3] and Rück in the Appendix of [36].

Proposition 6.2 (iv) yields the involution $x_i \mapsto \frac{1}{x_i}$, for which the substitution $y_i := x_i + \frac{1}{x_i}$ leads to a subtower \mathcal{G} of \mathcal{F} (see [36]) with defining equations

$$y_{i+1}^2 = \frac{(1 + y_i)^2}{4y_i} \quad (6.10)$$

for each $i \geq 0$.

Proposition 4.14 can be applied to the tower \mathcal{F} . In [36] it is shown that the solution to the functional equation is also a solution to a differential equation that has the Gaussian hypergeometric function

$${}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; z\right) \quad (6.11)$$

as solution, where the general form of a hypergeometric function (see [39, (5.76)]) is given by

$${}_mF_n(\alpha_1, \alpha_2, \dots, \alpha_m; \beta_1, \beta_2, \dots, \beta_n; z) = \sum_{k=0}^{\infty} \frac{(\alpha_1)_k (\alpha_2)_k \dots (\alpha_m)_k}{k! (\beta_1)_k (\beta_2)_k \dots (\beta_n)_k} z^k \quad (6.12)$$

where

$$(x)_k = x(x+1)(x+2)\dots(x+k-1). \quad (6.13)$$

The special case $m = 2, n = 1$ which applies for (6.11) yields the Gaus-

sian hypergeometric function, for which an explicit differential equation is known (see [39, 5.108]).

6.1.2.1.3 A tower with delayed ramification Finally, consider the explicit one-step tower \mathcal{F} over \mathbb{F}_7 which is induced by the sequence

$$x_{i+1}^2 = \frac{x_i^2 - x_i}{5x_i - 1}$$

of defining equations for each $i \geq 0$, resulting in the canonical representation

$$F_0 \subset F_1 \subset F_2 \subset \dots$$

of function fields over \mathbb{F}_7 . Construction of the \mathbb{F}_7 -ramification graph leads to Figure 6.5. Proposition 6.1 shows that this does define a tower, with the places $x_0 = 0$ and $x_0 = \infty$ in $S(F_0/\mathbb{F}_7)$ both totally ramified in \mathcal{F} .

In the representation of $\tilde{\Gamma}_B$ given in Figure 6.5, we have emphasised the vertices in boldface which correspond to elements of the ramification-generating sets of functions for the tower \mathcal{F} . By applying Definition 3.14, we have that these sets are given by $R_i = \left\{ x_i, \frac{1}{x_i}, x_i + 4, x_i + 6 \right\}$ for each $i \geq 0$. As the minimum path length from the vertex $\tilde{x}^2 + \tilde{x} + 3$ to a vertex belonging to $\tilde{R} := \left\{ \tilde{x}, \frac{1}{\tilde{x}}, \tilde{x} + 4, \tilde{x} + 6 \right\}$ in $\tilde{\Gamma}_B$ (and hence in Γ_B) is 5, it follows that the zero of $x_0^2 + x_0 + 3$ in $S(F_0/\mathbb{F}_7)$ is unramified in the extension F_5/F_0 but ramified in F_k/F_0 for any $k > 5$.

An exhaustive test for complete splitting in this tower with $M_T = 4$ did not result in the discovery of a non-empty complete splitting locus. Therefore, if it is completely splitting, it is so over a finite field of cardinality exceeding $7^4 = 2401$.

6.1.2.2 Towers of cubic extensions

We now consider the case of $m_i = 3$. When we want Proposition 6.2 (vi) to apply, we require that the m_i th root of unity is in the field \mathbb{F}_q over which our tower is to be defined. In this case, we assume that $m_i | q - 1$. For $p \geq 5$ we have that $3 | q - 1$ for $q = p^2$, and we consider the sequence of defining

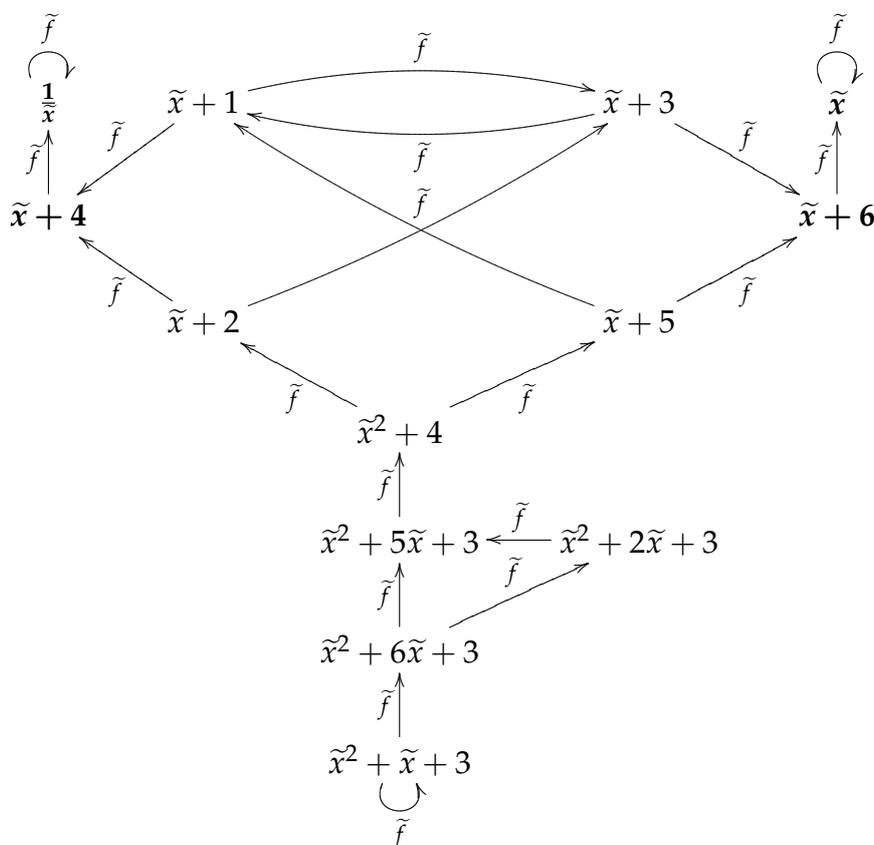


Figure 6.5: Condensed \mathbb{F}_7 -ramification graph $\tilde{\Gamma}_B$

equations given by

$$x_{i+1}^3 = \frac{x_i^3 + 2x_i^2 + 4x_i}{x_i^2 - x_i + 1} \tag{6.14}$$

for each $i \geq 0$. Computational results and careful consideration of the defining polynomials and the results in the rest of this section suggest that the towers defined by equations (6.14) give an analogue of degree 3 of the asymptotically optimal tower of García, Stichtenoth and Rück in [36] of degree 2 which was discussed on page 103, see defining equations (6.7).

First, explicit computation of Γ_B over \mathbb{Z} (as we want Γ_B for any $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ for $p \geq 5$) leads to the finite representation of a disconnected \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$ given in Figure 6.6. It therefore follows that the tower is of finite ramification type for any prime $p \geq 5$. The vertices

$\tilde{x}^2 + 2\tilde{x} + 4$ and $\tilde{x}^2 - \tilde{x} + 1$ of $\tilde{\Gamma}_B$ split into linear factors over \mathbb{F}_p when -3 is a quadratic residue mod p , which occurs when $p \equiv 1 \pmod{6}$.

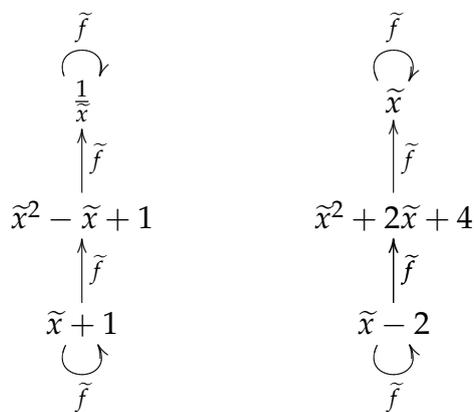


Figure 6.6: Condensed \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$

Before studying the complete splitting, we recall that the n th Franel number of order r is given by the expression

$$a_n^{(r)} = \sum_{k=0}^n \binom{n}{k}^r, \tag{6.15}$$

and assume the convention that $\binom{n}{k} = 0$ if $n, k \geq p$ as the binomial coefficient is considered in \mathbb{F}_p . Let

$$f^{(r)}(z) = \sum_{l=0}^{\infty} a_l^{(r)} z^l \tag{6.16}$$

be the generating function for the sequence $(a_0^{(r)}, a_1^{(r)}, a_2^{(r)}, \dots)$. In characteristic p the right-hand side of (6.16) is a finite sum, yielding $\deg f^{(r)} = p - 1$. For the case $r = 2$ it is well-known that

$$a_n^{(2)} = \binom{2n}{n},$$

the central binomial coefficients, which implies that the generating function $f^{(2)}(z)$ can be expressed as a (Gaussian) hypergeometric function.

Franel [26] considered the case $r = 3$, and derived the second-order recurrence

$$a_{n+1}^{(3)} = \frac{(7n^2 + 7n + 2) a_n^{(3)} + 8n^2 a_{n-1}^{(3)}}{(n+1)^2} \quad (6.17)$$

with $a_0 = 1$ and $a_1 = 2$. As (6.17) is second-order and Cusick [18] showed that all recurrences for the Franel numbers of order $r \geq 3$ has order greater than one, the analogous generating function $f^{(r)}(z)$ for $r \geq 3$ cannot be expressed as a hypergeometric series in closed form as for the case $r = 2$.

Numerical experiments using our Magma implementation, using all the primes $5 \leq p \leq 97$ and various larger primes confirm the following conjecture for those primes p :

Conjecture 6.3 *Let p be a prime number with $p \geq 5$. Consider the tower \mathcal{F} defined by the sequence of recursive equations as given in (6.14). Then the polynomial*

$$\tau(x_0) := x^{3(p-1)} f^{(3)}\left(\frac{1}{x^3}\right)$$

has the following properties:

- (i) $\tau(x_0)$ is a splitting characteristic polynomial for a component Γ_T^* of the \mathbb{F}_p -splitting graph Γ_T for \mathcal{F} .
- (ii) The splitting field of $\tau(x_0)$ is \mathbb{F}_{p^2} .

We have that $\deg \tau(x_0) = 3(p-1)$ as $a_0^{(3)} = 1$, and that $\tau(x_0)$ is separable as $a_1^{(3)} = 2 \neq 0 \pmod{p}$. It is an easy consequence of Wilson's theorem that $a_{p-1}^{(r)} \equiv 1 \pmod{p}$ when r is odd, which implies that the constant term of $\tau(x_0)$ is 1.

Together with the construction of Γ_B above which shows that

$$\sum_{P \in V_{\mathbb{F}_0}(\mathcal{F})} \deg P = 8$$

for this tower, and Conjecture 6.3(ii) implying that $\#T_{F_0}(\mathcal{F}) \geq 3(p-1)$, application of Corollary 2.18 shows that,

$$\lambda(\mathcal{F}) \geq \frac{2 \cdot \#T_{F_0}(\mathcal{F})}{\sum_{P \in V_{F_0}(\mathcal{F})} \deg P - 2} \geq \frac{6(p-1)}{8-2} = p-1,$$

implying that $\lambda(\mathcal{F}) = p-1$, as it meets the Drinfeld-Vladut bound for a tower defined over \mathbb{F}_{p^2} , the splitting field of $\tau(x_0)$ as implied by Conjecture 6.3(i). A representation of the \mathbb{F}_7 -splitting graph $\tilde{\Gamma}_T$ for the case $p=7$, with corresponding splitting characteristic polynomial

$$\tau_{\Gamma_7^*}(x_0) = x_0^{18} + 2x_0^{15} + 3x_0^{12} + 3x_0^6 + 5x_0^3 + 1$$

is presented in Figure B.1 in Appendix B.

We observe that this family of towers is also of the type described in Proposition 6.2 by using, for any $p \geq 5$, the matrices

$$A_{i+1} = \begin{bmatrix} 1 & 1+s \\ \frac{1}{2}(1+s) & \frac{1}{2}(1-s) \end{bmatrix} \text{ and } B_{i+1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

where $s \in \mathbb{F}_{p^2}$ with $s^2 + 3 = 0$ and observing that $A_{i+1}^3 = I$ in $PGL(\overline{\mathbb{F}}, 2)$ for each $i \geq 0$. This yields the automorphism

$$x_i \longmapsto \frac{2x_i + 2(1+s)}{(1+s)x_i + (1-s)}$$

for the right-hand side of (6.14) for each $i \geq 0$.

A general proof of Conjecture 6.3 for all $p \geq 5$ appears difficult, as no (hypergeometric) closed form expression for $f^{(3)}(z)$ exists, see [53, Theorem 8.8.1]. Hence a solution of the functional equation described in Proposition 4.14 cannot be found as readily as in the quadratic case with Deuring's polynomial which yield the hypergeometric central binomial coefficients.

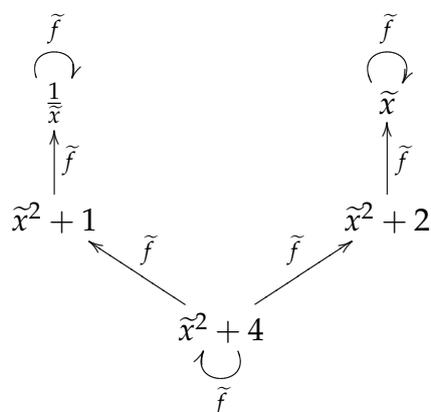


Figure 6.7: Condensed \mathbb{F}_7 -ramification graph $\tilde{\Gamma}_B$ for \mathcal{F}_1

6.1.2.2.1 Two towers of finite ramification type over \mathbb{F}_7 If we relax the condition that the tower must be of the form described in Proposition 6.2 but still have the form of Proposition 6.1, more towers can be found. Two examples of one-step tame towers over \mathbb{F}_7 which have finite ramification loci found using computer search are the towers \mathcal{F}_1 generated by

$$x_{i+1}^3 = \frac{x_i^3 + 2x_i}{x_i^2 + 1}$$

for each $i \geq 0$ in which both $x_0 = 0$ and $x_0 = \infty$ in $S(F_0/\mathbb{F}_7)$ are totally ramified, and the tower \mathcal{F}_2 generated by

$$x_{i+1}^3 = \frac{3x_i^3 + x_i^2 + 2}{x_i^2}$$

for each $i \geq 0$ in which only $x_0 = \infty$ in $S(F_0/\mathbb{F}_7)$ is totally ramified. While \mathcal{F}_1 results in a symmetric ramification graph with polynomials of degree 1 and 2 as vertices, the tower \mathcal{F}_2 has a very asymmetric ramification graph, involving polynomials of degree 1 and a single polynomial of degree 3. Representations of these \mathbb{F}_7 -ramification graphs modulo \sim_1 of \mathcal{F}_1 and \mathcal{F}_2 are respectively given in Figure 6.7 and 6.8.

Testing of the towers \mathcal{F}_1 and \mathcal{F}_2 for complete splitting with $M_T = 4$

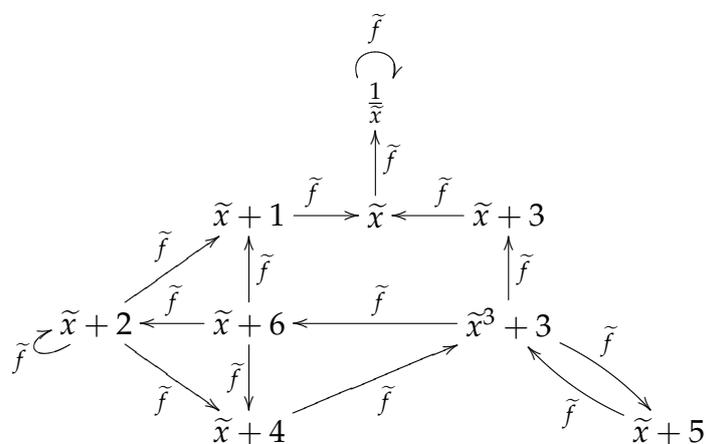


Figure 6.8: Condensed \mathbb{F}_7 -ramification graph $\tilde{\Gamma}_B$ for \mathcal{F}_2

does not yield a positive splitting rate.

6.1.2.3 Towers of quintic extensions

6.1.2.3.1 An asymptotically good tower over \mathbb{F}_{7^4} For $m_i = 5$, consider the explicit tower \mathcal{F} given by the sequence of defining equations

$$x_{i+1}^5 = \frac{x_i^5 + 5x_i^4 + x_i^3 + 2x_i^2 + 4x_i}{2x_i^4 + 5x_i^3 + 2x_i^2 + x_i + 1}$$

defined over \mathbb{F}_7 . Applying Algorithms 5 and 9 to this one-step tower of the type described in Proposition 6.1 leads to the ramification locus

$$V_{F_0/\mathbb{F}_7}(\mathcal{F}) = \left\{ \begin{array}{l} x_0^4 + 5x_0^3 + x_0^2 + 2x_0 + 4, x_0^4 + 6x_0^3 + x_0^2 + 4x_0 + 4, \\ x_0^2 + 3x_0 + 5, x_0, \frac{1}{x_0} \end{array} \right\}$$

and a complete splitting locus consisting of 30 places of degree one in $S(F_0/\mathbb{F}_{2401})$ with splitting characteristic polynomial

$$\tau_{\Gamma_T^*}(x_0) = x_0^{30} + 6x_0^{25} + 6x_0^{20} + 3x_0^{10} + 2x_0^5 + 1,$$

which factorizes into \mathbb{F}_7 -irreducible polynomials of degree 2 and 4. By Corollary 2.18, $\lambda(\mathcal{F}) \geq 6$, not meeting the Drinfeld-Vladut bound which gives $\lambda(\mathcal{F}) \leq 48$.

6.1.2.3.2 A tower of finite ramification type over \mathbb{F}_{11} For $m_i = 5$, considering all possible matrices A_{i+1} and B_{i+1} of the form described in Proposition 6.2 with entries in \mathbb{F}_{11} takes 9 hours on a 3GHz computer, and yields no asymptotically good towers (with $M_T = 2$) using Algorithms 5 and 9. Many towers in this family have a finite ramification locus however, for example the tower given by the choice of matrices

$$A_{i+1} = \begin{bmatrix} 1 & 1 \\ 3 & -4 \end{bmatrix}, B_{i+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL(\mathbb{F}_{11}, 2)$$

for each $i \geq 0$. This yields the sequence $(f_i)_{i \geq 1}$ of defining polynomials where $f_{i+1}(x_i, x_{i+1})$ is obtained from the equation

$$x_{i+1}^5 = \frac{5x_i^5 + 3x_i^4 + 3x_i^3}{x_i^4 + 4x_i^3 + 5x_i^2 + 2x_i + 5}$$

for each $i \geq 0$. Proposition 6.1 shows that this defines a one-step tower in which the place $x_0 = \infty$ is totally ramified. We deduce that the tower is of finite ramification type by examining the \mathbb{F}_{11} -ramification graph $\tilde{\Gamma}_B$, of which a representation is given in Figure 6.9.

6.1.2.3.3 Asymptotically optimal towers over \mathbb{F}_{11} Again, relaxing the conditions of the previous example, we consider the wider family of towers of the type described by Proposition 6.1. While an exhaustive search is currently impossible due to the size of the family, some sequences of defining polynomials result in distinct splitting characteristic polynomials $\tau_{\Gamma_T^*}$ for the completely splitting component Γ_T^* found, resulting in each of these cases in an asymptotically optimal tower over \mathbb{F}_{121} with limit $\lambda(\mathcal{F}) = 10$.

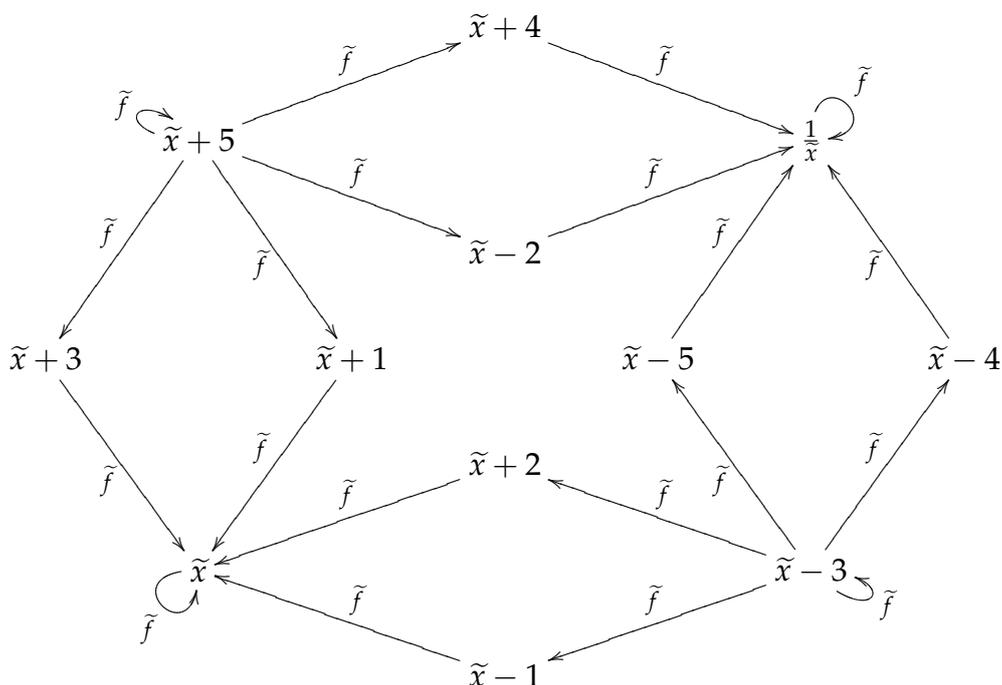


Figure 6.9: Condensed \mathbb{F}_{11} -ramification graph $\tilde{\Gamma}_B$

For example, the tower \mathcal{F} defined by the sequence

$$x_{i+1}^5 = \frac{x_i^5 + 4x_i^4 + x_i^3 + 8x_i^2 + 9x_i}{5x_i^4 + 5x_i^3 + 5x_i^2 - 5x_i + 1}$$

yields

$$\tau_1(x_0) = x_0^{50} + 3x_0^{45} - 3x_0^{40} + 4x_0^{35} - 3x_0^{30} - 3x_0^{20} - 4x_0^{15} - 3x_0^{10} - 3x_0^5 + 1,$$

implying that 50 places of degree one of $F_0 = \mathbb{F}_{121}(x_0)$ splits completely. The ramification locus contains the 12 places of degree one in $S(F_0/\mathbb{F}_{11})$. As the tower is tamely ramified, 2.18 implies that $\lambda(\mathcal{F}) = 10$.

6.1.3 Multi-step towers

We now show some examples of 2-step and 3-step towers which were obtained through computer search. For these, use of respectively Algorithms 5 and 9 were required instead of the one-step special cases in the form of Algorithms 6 and 10. As the families of defining equations which can define n -step towers for $n > 1$ are significantly larger than the case for one-step towers, we again focus on subfamilies where each constituent step consists of an extension of the type described by Proposition 6.1 or a variation thereof. An exception to this is the two-step Fermat tower already demonstrated at the end of Chapter 3 (see Figure 3.4).

For each of the cases considered in this section, we have chosen the defining polynomials of each distinct step to be in a different $GL(\mathbb{F}_p, 2)$ -orbit than those in the others. For example, for a two-step tower with representatives of the sequence of defining polynomials modulo \sim_2 given by \tilde{f} and \tilde{g} , we ensure that \tilde{f} and \tilde{g} are in different $GL(\mathbb{F}_p, 2)$ -orbits when considering a tower in characteristic p .

6.1.3.1 Two-step towers

6.1.3.1.1 An asymptotically optimal two-step tower over \mathbb{F}_9 Consider the 2-step tower \mathcal{F} over \mathbb{F}_9 generated by the representative defining polynomials

$$\begin{aligned}\tilde{f}(x_i, x_{i+1}) &= (x_i^2 + 1)x_{i+1}^2 - x_i \text{ for } i \equiv 0 \pmod{2} \\ \tilde{g}(x_i, x_{i+1}) &= x_i x_{i+1}^2 - (x_i^2 + 1) \text{ for } i \equiv 1 \pmod{2}\end{aligned}$$

with canonical representation $(F_i)_{i \geq 0}$.

We write \tilde{f} and \tilde{g} respectively as the equations

$$x_{i+1}^2 = \frac{x_i}{x_i^2 + 1} =: a(x_i) \tag{6.18}$$

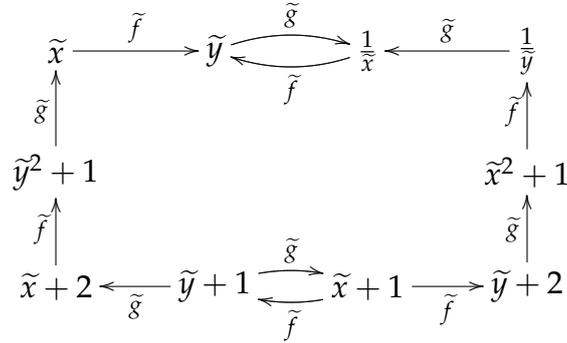


Figure 6.10: Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for 2-step tower \mathcal{F} over \mathbb{F}_3

and

$$x_{i+1}^2 = \frac{x_i^2 + 1}{x_i} =: b(x_i), \tag{6.19}$$

and then imitate the proof of Proposition 6.1 to show that the pole P of x_0 in $S(F_0/\mathbb{F}_9)$ is totally ramified in \mathcal{F} .

Indeed, as the degree of the numerator of $a(x_i)$ is one more than the denominator of $a(x_i)$, $x_0 = \infty$ is a simple zero of the right-hand side of (6.18), for $i = 0$. This implies that P is totally ramified in F_1/F_0 , with the unique place Q above P in F_1 being a simple zero of $x_1 = 0$. We then observe that the place Q , which is a simple zero of $x_1 = 0$, is totally ramified in F_2/F_1 as it is a simple pole of $b(x_i)$ in (6.19) for $i = 1$, for which the same properties hold for the denominator and numerator interchanged as (6.18). The resulting unique place R in $S(F_2/\mathbb{F}_9)$ above $x_1 = 0$ is a simple pole of x_2 . Continuing this two-step process, we see that the tower \mathcal{F} is well-defined, with the totally ramified place $x_0 = \infty$ in $S(F_0/\mathbb{F}_9)$ corresponding to alternating poles and zeros of the indeterminates x_0, x_1, x_2, \dots introduced at each step of the tower.

Applying Algorithms 5 and 9 leads respectively to a finite representation of $\tilde{\Gamma}_B$ for \mathcal{F} as given in Figure 6.10 and a (squarefree) splitting characteristic polynomial

$$\tau_{\Gamma_T^*}(x_0) = (x_0^2 + x_0 - 1)(x_0^2 - x_0 - 1) = x_0^4 + 1$$

yielded by an explicit finite component of $\tilde{\Gamma}_T$. Corollary 2.18 then applies, and we obtain

$$\begin{aligned} \lambda(\mathcal{F}) &\geq \frac{2 \cdot \#T_{F_0}(\mathcal{F})}{-2 + \sum_{P \in V_{F_0}(\mathcal{F})} \deg P} \\ &= \frac{2 \cdot \deg \tau_{\Gamma_T^*}}{-2 + 6} \\ &= \frac{8}{4} \\ &= 2 = \sqrt{9} - 1, \end{aligned}$$

implying that the two-step tower is asymptotically optimal over \mathbb{F}_9 .

By eliminating the intermediate variable x_{2i+1} from the successive defining polynomials $\tilde{f}(x_{2i}, x_{2i+1})$ and $\tilde{g}(x_{2i+1}, x_{2i+2})$ by an elimination ideal for each $i \geq 0$, we obtain a one-step subtower \mathcal{G} of \mathcal{F} with defining polynomials

$$\tilde{h}(x_{2i}, x_{2i+2}) = x_{2i+2}^4 (x_{2i}^3 + x_{2i}) - (x_{2i}^4 + 2x_{2i}^3 + 2x_{2i} + 1)$$

and canonical representation $(G_{2i})_{i \geq 0}$ where clearly $G_{2i} \subseteq F_{2i}$ for each $i \geq 0$. Hence $\mathcal{G} \subseteq \mathcal{F}$, and therefore the tower \mathcal{G} is an asymptotically optimal one-step tower of quartic extensions over \mathbb{F}_9 .

One may generalize the two-step tower \mathcal{F} to arbitrary characteristic $p > 3$ in the following manner. Suppose $a \in \mathbb{F}_q$ with the property that $16a^8 - 1 = 0$. Then $b = 2a^2$ is a fourth root of unity and it follows from the definition that $a^2 + 2b^3 = 0$. Consider the representative defining polynomials

$$\begin{aligned} \tilde{f}'(x_i, x_{i+1}) &= (x_i^2 + b) x_{i+1}^2 - ax_i \text{ for } i \equiv 0 \pmod{2} \\ \tilde{g}'(x_i, x_{i+1}) &= ax_i x_{i+1}^2 - (x_i^2 + b) \text{ for } i \equiv 1 \pmod{2} \end{aligned}$$

which we let define the two-step tower \mathcal{F}' over $\mathbb{F}_q = \mathbb{F}_{p^2}$. For $p = 3$, $a = 1$ this defines the tower \mathcal{F} above. For characteristic $p > 3$, the fact that $a^2 + 2b^3 = 0$ ensures that the completely splitting locus of \mathcal{F}' over \mathbb{F}_{p^2} is

not empty. However, numerical experiments using our Magma programs show that these higher characteristic towers do not have a finite ramification locus for $q = p$, $3 < p < 150$ by in each case considering all the a satisfying the given condition in the field of definition.

6.1.3.1.2 A two-step tower over \mathbb{F}_3 with finite ramification We present a two-step tower which has a finite ramification locus, but for which it is unknown whether it is completely splitting. Let \mathcal{H} be the 2-step tower over \mathbb{F}_3 generated by the representative defining polynomials

$$\begin{aligned} \tilde{f}(x_i, x_{i+1}) &= x_i x_{i+1}^2 - (x_i^2 - 1) \text{ for } i \equiv 0 \pmod{2}, \text{ and} & (6.20) \\ \tilde{g}(x_i, x_{i+1}) &= (x_i^2 + x_i) x_{i+1}^2 - (x_i - 1) \text{ for } i \equiv 1 \pmod{2}, \end{aligned}$$

with canonical representation $(H_i)_{i \geq 0}$. By a similar argument as in the previous example (subsection 6.1.3.1.1) we see that the zero of x_0 in $S(H_0/\mathbb{F}_3)$ is totally ramified, ensuring that \tilde{f} and \tilde{g} do indeed define a tower.

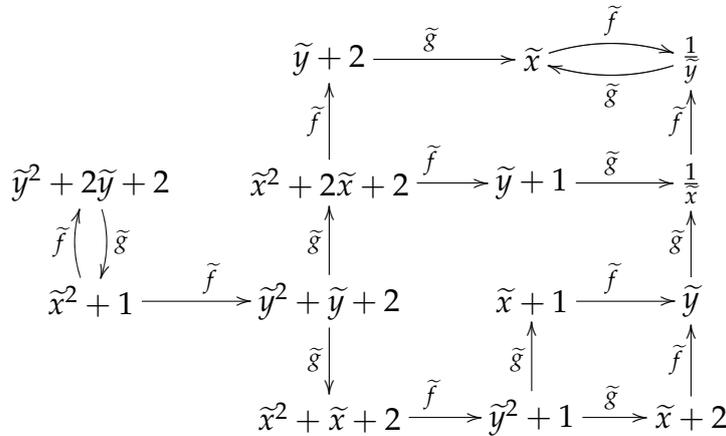


Figure 6.11: Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for 2-step tower \mathcal{H} over \mathbb{F}_3

Using Algorithm 5, we can construct the \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ (see Figure 6.11), where \tilde{x} and \tilde{y} are defined to be equivalent modulo \sim_2 to

respectively even and odd indices i for x_i . This shows that

$$V_{H_0}(\mathcal{H}) = \left\{ x_0, x_0 + 1, x_0 + 2, \frac{1}{x_0}, x_0^2 + 1, x_0^2 + x_0 + 2, x_0^2 + 2x_0 + 2 \right\}.$$

The equations (6.20) which define the tower \mathcal{H} can be extended to yield towers which are finitely ramified for characteristics $p = 3, 5$ and 7 . Let

$$\begin{aligned} \tilde{f}(x_i, x_{i+1}) &= x_i x_{i+1}^2 + 2x_i^2 - 2 \text{ for } i \equiv 0 \pmod{2}, \text{ and} & (6.21) \\ \tilde{g}(x_i, x_{i+1}) &= \left(x_i^2 + 4x_i \right) x_{i+1}^2 + 2x_i + 1 \text{ for } i \equiv 1 \pmod{2}. \end{aligned}$$

Then (6.21), which can be seen to be equivalent to (6.20) in characteristic 3 , define towers with finite ramification when considered in characteristic $p = 3, 5$ and 7 , but not for characteristic $p = 11$.

6.1.3.1.3 A two-step tower of cubic extensions over \mathbb{F}_5 with finite ramification Let \mathcal{I} be a two-step tower defined over \mathbb{F}_5 with representatives \tilde{f} and \tilde{g} given by

$$\tilde{f}(x_i, x_{i+1}) = \left(x_i^3 - x_i^2 + x_i \right) x_{i+1}^3 - \left(x_i^2 - 2x_i + 4 \right) \text{ for } i \equiv 0 \pmod{2}, \text{ and} \quad (6.22)$$

$$\tilde{g}(x_i, x_{i+1}) = \left(x_i^3 - 2x_i^2 + 4x_i \right) x_{i+1}^3 - \left(x_i^2 + x_i + 1 \right) \text{ for } i \equiv 1 \pmod{2},$$

with canonical representation $(I_i)_{i \geq 0}$. By a similar argument as that for the tower \mathcal{F} on page 115, we observe that both the place $x_0 = 0$ and $x_0 = \infty$ in $S(I_0/\mathbb{F}_5)$ is totally ramified in \mathcal{I} . Using Algorithm 5 leads to the representation of the \mathbb{F}_5 -ramification graph $\tilde{\Gamma}_B$ given in Figure B.3 in Appendix B, yielding

$$V_{I_0}(\mathcal{I}) = \left\{ \begin{array}{l} x_0, x_0 + 1, x_0 + 2, x_0 + 3, x_0 + 3, \frac{1}{x_0}, x_0^2 + 3, \\ x_0^2 + 4x_0 + 1, x_0^2 + 2x_0 + 3, x_0^2 + 2x_0 + 4, \\ x_0^2 + x_0 + 1, x_0^2 + 3x_0 + 3, x_0^2 + 3x_0 + 4 \end{array} \right\}$$

so that

$$\sum_{P \in V_{I_0}(\mathcal{I})} \deg P = 20.$$

Interestingly, the defining equations of this tower appears to be related to our one-step tower involving the Franel numbers by comparing the reciprocal polynomials $\tilde{f}^{(x_i)}$ and $\tilde{g}^{(x_i)}$ from (6.22) with (6.14).

6.1.3.2 A three-step tower

We define the polynomials $\tilde{f}, \tilde{g}, \tilde{h} \in \mathbb{F}_3[u, v]$ by

$$\begin{aligned} \tilde{f}(u, v) &:= (u - 1)v^2 - u^2, \\ \tilde{g}(u, v) &:= (u + 1)v^2 - (u - 1)^2 \text{ and} \\ \tilde{h}(u, v) &:= uv^2 - (u + 1)^2, \end{aligned} \tag{6.23}$$

and consider the 3-step tower \mathcal{F} (with canonical representation $(F_i)_{i \geq 0}$) over \mathbb{F}_3 generated by the sequence $(f_i)_{i \geq 1} \in (\mathbb{F}_3[x_{i-1}, x_i])$ of defining polynomials with

$$f_{i+1}(x_i, x_{i+1}) = \begin{cases} \tilde{f}(x_i, x_{i+1}) & \text{if } i \equiv 0 \pmod{3} \\ \tilde{g}(x_i, x_{i+1}) & \text{if } i \equiv 1 \pmod{3} \\ \tilde{h}(x_i, x_{i+1}) & \text{if } i \equiv 2 \pmod{3} \end{cases}$$

for each $i \geq 0$. Explicit calculations show that polynomials \tilde{f}, \tilde{g} and \tilde{h} are in disjoint $GL(\mathbb{F}_3, 2)$ -orbits.

We let $\tilde{x} \sim_3 x_i$ when $i \equiv 0 \pmod{3}$, $\tilde{y} \sim_3 x_i$ when $i \equiv 1 \pmod{3}$, and $\tilde{z} \sim_3 x_i$ when $i \equiv 2 \pmod{3}$. Each of \tilde{f}, \tilde{g} and \tilde{h} are of the type described by Proposition 6.1. As the coefficient of x_{i+1}^2 in each of $\tilde{f}, \tilde{g}, \tilde{h} \in \mathbb{F}_3[x_i][x_{i+1}]$ is of degree one, the same argument as in the proof of Proposition 6.1 implies that the place $x_0 = \infty$ in $S(F_0/\mathbb{F}_3)$ is totally ramified in \mathcal{F} .

Constructing $\tilde{\Gamma}_B$ by Algorithm 5 shows that the tower has a finite ramification locus given by

$$V_{F_0/\mathbb{F}_3}(\mathcal{F}) = \left\{ x_0, x_0 + 1, x_0 + 2, \frac{1}{x_0} \right\}.$$

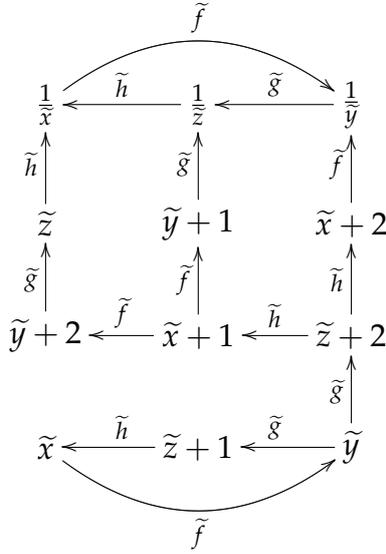


Figure 6.12: Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for 3-step tower over \mathbb{F}_3

A representation of the \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ of \mathcal{F} in terms of the representatives \tilde{x} , \tilde{y} and \tilde{z} defined above is given in Figure 6.12.

When the equations (6.23) are used to define a 3-step tower over \mathbb{F}_5 , \mathbb{F}_7 or \mathbb{F}_{11} , no finite ramification locus is found for $M_B = 8$.

6.2 Wild towers

In this section, we focus on the case of towers where some wild ramification occurs. Because of this, we cannot apply Corollary 2.18 when the limit $\lambda(\mathcal{F})$ is to be computed, but merely focus on a study of the ramification structure and finding an appropriate field \mathbb{F}_r so that the tower is completely splitting when defined over that field.

We follow [10] in computing the ramification and complete splitting behaviour of certain Artin-Schreier towers. In particular, the following classification theorem was proven by Beelen, García and Stichtenoth:

Theorem 6.4 ([10, Theorem 6.4]) *Let \mathcal{F} be a one-step tower over \mathbb{F}_q of which the basic function field $F_1 = \mathbb{F}_q(x, y)$ can be described by the equation $h(y) =$*

$g(x)$, with $h(T), g(T) \in \mathbb{F}_q(T)$, where $\deg g = \deg h = p^r$ for some $r \geq 1$. Suppose that both extensions $F_1/\mathbb{F}_q(x)$ and $F_1/\mathbb{F}_q(y)$ are Galois. Then \mathcal{F} is recursively defined (in one-step fashion) by one of the equations

$$\varphi(y) = \begin{cases} \text{(i)} & \frac{a}{\varphi(\alpha x) + b} + c \quad \text{where } \alpha \notin \mathbb{F}_p, \\ \text{(ii)} & a \cdot \varphi\left(\frac{\alpha}{x}\right) + b \quad \text{where } a \notin \mathbb{F}_p, \text{ or} \\ \text{(iii)} & \frac{a}{\varphi\left(\frac{\alpha}{x}\right) + b} + c \end{cases} \quad (6.24)$$

with $a, \alpha \in \mathbb{F}_q^\times$, $b, c \in \mathbb{F}_q$, and $\varphi(T) = T^p - e^{p-1}T \in \mathbb{F}_q[T]$ with $e \in \mathbb{F}_q^\times$.

Proof. A proof is given in [10], hinging on cases considered for the representation of the defining equations of \mathcal{F} as

$$\varphi(y) = A \cdot \varphi(B \cdot x)$$

where A and B are elements of $PGL(\mathbb{F}_q, 2)$ and $\varphi(T) \in \mathbb{F}_q[T]$, following the notation of Section 2.3. ■

Using Theorem 6.4, it is possible to enumerate all possible defining polynomials over \mathbb{F}_q of one-step towers of Galois extensions (of degree p^r) over \mathbb{F}_q , by constructing bivariate polynomials $f(x, y) \in \mathbb{F}_q[x, y]$ from the separated variable equations in (6.24). If we restrict ourself to the case where the defining polynomials are defined over the prime field $\mathbb{F}_q = \mathbb{F}_p$, the conditions of (i) and (ii) in (6.24) imply that only (iii) can apply. An explicit enumeration of such towers can be done for small primes p using the subroutine BGS64 which was implemented in Magma, with code shown in Appendix A. For $\mathbb{F}_q = \mathbb{F}_2$ the calculation was done in [10], yielding (up to $PGL(\mathbb{F}_2, 2)$ -orbits) the four defining equations

$$y^2 + y \in \left\{ \frac{x^2}{x+1}, \frac{x^2+x+1}{x}, \frac{x^2}{x^2+x+1}, \frac{x}{x^2+x+1} \right\}. \quad (6.25)$$

The first equation yields the tower considered in Example 4.15 and the second equation the tower considered in Example 3.16. The third equation defines a tower dual to the second. The algorithms of Chapter 5

successfully identifies (using $M_B = 100$ and $M_T = 6$) both a finite ramification locus and nonempty complete splitting locus for each of these towers, except for a complete splitting locus for the last tower, given by $y^2 + y = \frac{x}{x^2+x+1}$. The first three towers are known to be asymptotically good, and optimal in the case of the first tower. Considering the tower induced by $y^2 + y = \frac{x}{x^2+x+1}$ for which the complete splitting locus is unknown, we have the following result:

Proposition 6.5 *Consider the one-step tower \mathcal{F} given by*

$$f(x, y) = (y^2 + y)(x^2 + x + 1) - x \quad (6.26)$$

over some constant field extension of \mathbb{F}_2 . If there exists an extension $\mathbb{F}_r/\mathbb{F}_2$ such that $T_{\mathbb{F}_0}(\mathcal{F}/\mathbb{F}_r)$ is nonempty, then $r > 2^{25}$.

Proof. Suppose there exists a finite field \mathbb{F}_r of characteristic 2 and cardinality at most 2^{25} such that $\#T_{\mathbb{F}_0}(\mathcal{F}/\mathbb{F}_r) > 0$. By considering the ramification locus of the tower generated using (6.26) which equals that of the tower considered in Example 3.16, it is clear that $2^2 < r \leq 2^{25}$. Using the Magma procedures shown in Appendix A, one can list the elements of $MI_{\mathbb{F}_2}(T_0)$ of degree d , for each $3 \leq d \leq 25$. Performing recursive successor polynomial computations on each of these elements, one finds that each monic irreducible polynomial (over \mathbb{F}_2) of degree at most 25 and at least 3 has a successor of degree exceeding 25. To illustrate one case, for the monic irreducible polynomial $T_0^3 + T_0 + 1 \in MI_{\mathbb{F}_2}(T_0)$ the 8-step successor polynomial set

$$\text{Succ}_f^8(T_0^3 + T_0 + 1) \subseteq MI_{\mathbb{F}_2}(T_8)$$

contains at least one monic \mathbb{F}_2 -irreducible polynomial of degree 48 in T_8 . As each successor polynomial set contains a polynomial of degree exceeding 25, Theorem 4.7 implies that $r > 2^{25}$. This contradicts our initial assumption, and therefore \mathcal{F} does not split over any field of cardinality less than or equal to 2^{25} . ■

The large lower bound on the cardinality of \mathbb{F}_r in Proposition 6.5 makes it appear unlikely that the complete \mathbb{F}_2 -splitting graph Γ_T for the tower

possesses a component Γ_T^* satisfying the conditions of Theorem 4.7.

We continue applying Theorem 6.4 to some small finite fields. For $\mathbb{F}_q = \mathbb{F}_3$ we obtain (up to orbits of $GL(\mathbb{F}_3, 2)$) two distinct defining equations

$$y^3 - y \in \left\{ \frac{x^3}{1-x^2}, \frac{2x^3}{1-x^2} \right\} \quad (6.27)$$

for which Algorithm 6 (with $M_B = 100$) yields a finite ramification locus. For each of these towers the ramification loci are the zeroes of the four functions $x_0, x_0 + 1, x_0 + 2$ and $\frac{1}{x_0}$. Algorithm 10 (with $M_T = 6$) shows that both these towers are completely splitting over \mathbb{F}_9 , in both cases with splitting characteristic polynomial

$$\tau_{\Gamma_T^*}(x_0) = (x_0^2 - x_0 - 1) (x_0^2 + x_0 - 1) (x_0^2 + 1) = x_0^6 + x_0^4 + x_0^2 + 1 \quad (6.28)$$

For $\mathbb{F}_q = \mathbb{F}_5$ we obtain (up to $GL(\mathbb{F}_5, 2)$ -orbits) four distinct defining equations, namely

$$y^5 - y \in \left\{ \frac{x^5}{1-x^4}, \frac{2x^5}{1-x^4}, \frac{3x^5}{1-x^4}, \frac{4x^5}{1-x^4} \right\} \quad (6.29)$$

for which Algorithm 6 (with $M_B = 100$) yields a finite ramification locus. For each of these towers the ramification locus is the set of zeroes of the six functions $x_0, x_0 + 1, x_0 + 2, x_0 + 3, x_0 + 4$ and $\frac{1}{x_0}$. Algorithm 10 (with $M_T = 6$) shows that all these towers are completely splitting over \mathbb{F}_{25} , in each of these cases with splitting characteristic polynomial

$$\tau_{\Gamma_T^*}(x_0) = x_0^{20} + x_0^{16} + x_0^{12} + x_0^8 + x_0^4 + 1. \quad (6.30)$$

The towers obtained in this way for $\mathbb{F}_q \in \{\mathbb{F}_3, \mathbb{F}_5\}$ are in the $GL(\overline{\mathbb{F}}_q, 2)$ -orbit of the family of towers considered in Example 4.15, and are therefore asymptotically optimal over \mathbb{F}_{q^2} for each q .

We note that both splitting characteristic polynomials in (6.28) and (6.30) are special cases of the splitting characteristic polynomial obtained in Example 4.15, equation (4.14).

We now consider the case of $\mathbb{F}_q = \mathbb{F}_4 = \mathbb{F}_2(\rho)$ where $\rho^2 + \rho + 1 = 0$. Equation (6.24) yields 288 candidate equations of type (i), 72 candidate equations of type (ii) and 432 candidate equations of type (iii). Considering only one candidate equation from each $GL(\mathbb{F}_4, 2)$ -orbit, we reduce these numbers to respectively 72, 72 and 144.

Application of Algorithm 6 (with $M_B = 100$) and Algorithm 10 (with $M_T = 7$) yields many towers with a finite ramification locus, and only 9 with a non-empty complete splitting locus. These 9 are all of type (iii), and yield towers which split completely over \mathbb{F}_{4^1} , \mathbb{F}_{4^2} and \mathbb{F}_{4^3} . In each of these cases the ramification locus $V(\mathcal{F}/\mathbb{F}_4)$ consists of either 3 or 5 elements.

An example of the largest ramification locus occurring in a tower which is not necessarily completely splitting is for the tower (of type (i)) with basic function field $F_1 = \mathbb{F}_4(x, y)$ with

$$\tilde{f}(x, y) = x^2y^2 + \rho xy^2 + y^2 + x^2y + \rho xy + \rho y + x^2 + \rho x = 0.$$

This results in the condensed \mathbb{F}_4 -ramification graph given in Figure 6.13.

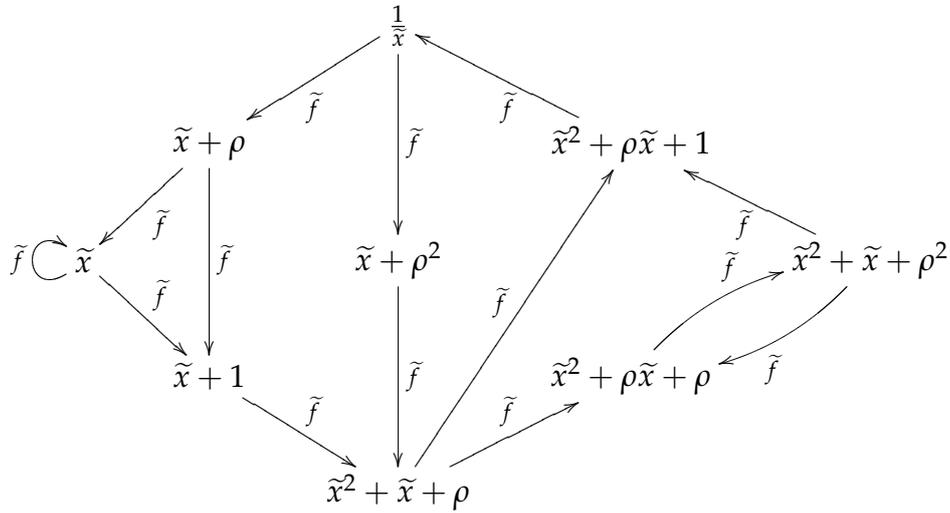


Figure 6.13: Condensed \mathbb{F}_4 -ramification graph $\tilde{\Gamma}_B, \rho^2 + \rho + 1 = 0$

For $\mathbb{F}_q = \mathbb{F}_8 = \mathbb{F}_2(\alpha)$ where $\alpha^3 + \alpha + 1 = 0$, equation (6.24) yields

a total of 43120 candidate equations. Running Algorithm 6 and 10 (with $M_B = 100, M_T = 5$) we obtain various ramification graphs with $\#V(\tilde{\Gamma}_B) \in \{3, 4, 5, 7, 10\}$ of types (i) and (iii), as well as various towers which are completely splitting over \mathbb{F}_8 and \mathbb{F}_{64} .

An exhaustive test of the candidate equations for $\mathbb{F}_q = \mathbb{F}_{32} = \mathbb{F}_2(\beta)$ with $\beta^5 + \beta^2 + 1 = 0$ was not feasible due to the size of the family. However, a partial test (180000 candidate equations with $M_B = 20, M_T = 2$) of the family yields two towers which are completely splitting. These are both of type (iii) and have $\#V(\tilde{\Gamma}_B) = 3$ and 62 places of degree one which split completely. They are respectively defined by

$$x_{i+1}^2 + \beta^{29}x_{i+1} = \frac{x_i^2}{\beta^{24}x_i + \beta^{22}} \quad (6.31)$$

and

$$x_{i+1}^2 + \beta^{29}x_{i+1} = \frac{x_i^2}{\beta^{25}x_i + \beta^{23}}, \quad (6.32)$$

for all $i \geq 0$, where the right-hand sides of (6.31) and (6.32) differ by only a factor of β .

The difference between the towers generated by (6.31) and (6.32) is that the finite component of their condensed complete \mathbb{F}_{32} -splitting graphs differ in the sense that the former tower's graph contains only quadratic polynomials as vertices, while the latter contains linear (corresponding to \mathbb{F}_{32} -rational places) as well as quadratic polynomials as vertices. If an equation could be found for which only linear polynomials would occur, the tower would be completely splitting over \mathbb{F}_{32} .

Chapter 7

Conclusions

In this dissertation we have considered the problem of obtaining explicit equations for towers of function fields from both a graph-theoretic and algorithmic viewpoint. As Chapters 3 and 4 have shown, the behaviour of ramified places and completely splitting places in a tower \mathcal{F} over \mathbb{F}_q can be viewed as subgraphs of the \mathbb{F}_l -splitting (directed) graph

$$\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$$

where \mathbb{F}_l is a subfield of the finite field \mathbb{F}_q . In this case the canonical representation of \mathcal{F} is given by the sequence

$$\mathbb{F}_q(x_0) = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$$

where each separable extension F_{i+1}/F_i is defined by the balanced-degree bivariate polynomial $f_{i+1}(x_i, x_{i+1}) = 0$ (with coefficient ring \mathbb{F}_l) for each $i \geq 0$. In most of the examples we discussed, n -step towers were discussed with the indeterminates x_i for $i \geq 0$ satisfying the equivalence relation \sim_n .

For both the study of the ramification and complete splitting, it is not necessary to know \mathbb{F}_q a priori. Fixing a finite subfield \mathbb{F}_l of the possibly unknown finite field \mathbb{F}_q , Chapter 3 described how every place $P \in S(F_0/\mathbb{F}_q)$ which is ramified in F_k/F_0 for some $k \geq 1$ can be described as a directed path of length k in the subgraph Γ_B of Γ such that at least

one of its constituent vertices (except the terminal vertex) has out-degree less than the degree of the corresponding polynomial $f_k(x_{k-1}, x_k)$. Then, by analyzing the defining polynomials $f_i(x_{i-1}, x_i) = 0$ at each step $i \geq 1$, predecessor polynomials were defined to traverse the graph downwards (meaning that we traverse the steps of the tower from higher steps to lower steps) in order to find all possible residue classes for which ramification occurs in places corresponding to them. This culminated in the algorithms described in the first part of Chapter 5.

The process of testing for a finite ramification locus may identify some completely splitting places as ramified places (for example, the place $P_\infty \in S(F_0/\mathbb{F}_4)$ of Example 2.20 which splits completely in that tower). This would mean that $\frac{1}{x_0}$ is a superfluous element of the ramification locus obtained through Algorithm 5, but would not cause the algorithm to identify the ramification locus as infinite. When continuing on to the case of complete splitting, such fringe cases should be taken into account, as we would then want to consider $\frac{1}{x_0}$ as an element of $V(\Gamma_T) = V(\Gamma) \setminus V(\Gamma_B)$.

In the case of complete splitting, selecting a small finite field $\mathbb{F}_l \supset \mathbb{F}_p$ and analyzing the splitting behaviour in the n distinct steps of an n -step tower allows us to, under certain conditions, deterministically find a suitable finite field $\mathbb{F}_q \supset \mathbb{F}_l$ such that \mathcal{F} defined over \mathbb{F}_q will be completely splitting (Theorem 4.6). This yields a highly practical Algorithm 9 allowing us to test the complete splitting behaviour of n -step towers for various n and (finite) defining polynomial sequences

$$\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_n\} \cong \{f_i(x_{i-1}, x_i) : i \geq 1\} / \sim_n.$$

For both ramification and complete splitting, rudimentary algorithms were also described for \sim -finite towers, where the ordering of the constituent steps $\{\tilde{f}_1, \tilde{f}_2, \dots, \tilde{f}_m\}$ are not fixed.

All these algorithms were implemented using the Magma computer algebra system, which allowed computational experiments to be run on certain families of defining polynomials over various small finite fields. We demonstrated the usefulness of the above algorithms in finding new

asymptotically good tamely ramified towers. We have shown that there exists many asymptotically optimal tame towers of extensions of degree greater than two, and made such constructions of degree 3 and 5. We then considered two-step and three-step towers, showing that their ramification structure can be effectively described using ramification graphs.

Many interesting questions are motivated by some of the constructions and algorithms in this dissertation. Amongst these is the question implied by the construction of splitting characteristic polynomials and Corollary 4.13: given a bivariate balanced-degree polynomial $f(x, y) \in \mathbb{F}_q[x, y]$, can we find a polynomial $H(T) \in \mathbb{F}_q[T]$ so that

$$\langle H(x) \rangle = \langle f(x, y), H(y) \rangle \cap \mathbb{F}_q[x] ?$$

Finding such a polynomial H or non-constructively showing that its degree is bounded can be very useful in showing that an f -tower has a non-empty complete splitting locus over some finite field.

The tamely ramified tower of quadratic extensions of García, Stichtenoth and Rück in [36] which involves Deuring's polynomial had the squares of binomial coefficients appearing in its splitting characteristic polynomial, whereas our tower of cubic extensions had the sum of cubes of binomial coefficients appearing in its splitting characteristic polynomial. An interesting problem can be to find higher-order constructions of tamely ramified towers to generalize this.

Appendix A

Magma program code

```
// initialization
l := 8;
F_1<rho> := GF(l);
p := Characteristic(F_1);
F_p := GF(p);
F_1x<x> := PolynomialRing(F_1);
FFF_1x<x> := FieldOfFractions(F_1x);
FF_1<x,y> := PolynomialRing(F_1,2, "grevlex");
FFF_1<x,y> := FieldOfFractions(FF_1);
FF_1<x,y> := PolynomialRing(F_1,2, "grevlex");
SHOWRAMIFICATIONONLY := true;
SHOW_GRAPH := true;

// auxillary
function IsSeparable(f);
    return (Derivative(f,1) ne 0) or (Derivative(f,2) ne 0);
end function;

function MonIrrPolsUpTo(Deg);
    return &join{AllIrreduciblePolynomials(F_1,i) : i in [1..Deg]};
end function;

function PolsUpTo(Deg);
    if (Deg eq 0) then
        return {FF_1!a : a in Set(F_1)};
    else
        return {(FF_1!f)*(FF_1!x)+(FF_1!a) : a in F_1, f in (PolsUpTo(Deg-1))};
    end if;
end function;

function MonPolsUpTo(Deg);
    return {f/LeadingCoefficient(f) : f in PolsUpTo(Deg) | f ne 0};
end function;
```

```

function Reciprocal(f, xr, yr);
  if (xr eq 0) and (yr eq 0) then
    return FF_1!f;
  elif (xr eq 1) and (yr eq 0) then
    d := hom<FFF_1 -> FFF_1 | 1/x, y>;
  elif (xr eq 0) and (yr eq 1) then
    d := hom<FFF_1 -> FFF_1 | x, 1/y>;
  elif (xr eq 1) and (yr eq 1) then
    d := hom<FFF_1 -> FFF_1 | 1/x, 1/y>;
  end if;
  return FF_1!(Numerator(d(FF_1!f)));
end function;

procedure printGraph(f, someSet);
  printf "### begin GraphViz code ###\ndigraph \"%o\" {\n", f;
  for p in someSet, q in Succ(f, {p}) do
    if q eq 1 then
      printf "  \"%o\" -> \"1/x\";\n", (p eq 1 select "1/x" else p);
    else
      printf "  \"%o\" -> \"%o\";\n", (p eq 1 select "1/x" else p), q;
    end if;
  end for;
  printf "}\n### end GraphViz code ###\n";
end procedure;

function IrrFactors(u); // u is a univariate polynomial
  if IsZero(u) then
    return {};
  end if;
  return &join{FF_1!factor[1] : factor in Factorization(u)};
end function;

function isoPols(f);
  IsoClass := {};
  for A in GeneralLinearGroup(2, F_1) do
    A_action := hom<FFF_1 -> FFF_1 | (A[1][1]*x+A[1][2])/(A[2][1]*x+A[2][2]), \
      (A[1][1]*y+A[1][2])/(A[2][1]*y+A[2][2])>;
    Include(~IsoClass, FF_1!Numerator(FFF_1!A_action(FF_1!f)));
  end for;
  return IsoClass;
end function;

function IsIsomorphicToSymmetricPolynomial(f);
  for g in isoPols(f) do
    if IsSymmetric(g) then
      return true;
    end if;
  end for;
  return false;
end function;

```

```

procedure reduceModGL2(~Set);
  NewSet := {};
  while #Set gt 0 do
    f := Representative(Set);
    fClass := isoPols(f);
    if #fClass gt 1 then
      Set := Set diff fClass;
      Include(~NewSet, f);
    end if;
  end while;
  Set := NewSet;
end procedure;

// U is a set of univariate polynomials
function IrrFactorsSet(U);
  return &join{IrrFactors(u) : u in U};
end function;

function XDegreeBelow(A, degreeBound);
  return (Max({Degree(a,1) : a in A} join {1}) le degreeBound);
end function;

function LCMofDegrees(MVPs);
  return LCM({Degree(f,1) : f in MVPs});
end function;

procedure printHx(CSL);
  printf "H(x) = %o\n", &#{h : h in CSL};
end procedure;

procedure printSet(Set);
  printf "{ ";
  for s in Set do
    printf "%o ",(s ne 1) select s else "1/x";
  end for;
  printf "}";
end procedure;

function degSumSet(Set);
  return &+{(s eq 1 select 1 else Degree(s,1)) : s in Set};
end function;

// compute Predecessors
function Pred(f, Q);
  P := {};
  d := hom<FF_1 -> FF_1 | y, 0>;
  for q in Q do
    if (q ne 1) then
      // algorithm 1, q is a polynomial
      qy := d(q);
    end if;
  end for;
end function;

```

```

I := ideal<FF_1 | f, qy>;
if Dimension(I) eq 0 then
    p := UnivariateEliminationIdealGenerator(I, 1);
    P := P join IrrFactors(p);
end if;
fx := Reciprocal(f, 1, 0);
if Degree(GCD(Evaluate(fx,1,0),qy),2) gt 0 then
    P := P join {FF_1!1}; // 1/x
end if;
else
    // algorithm 2, q is 1/x
    fy := Reciprocal(f, 0, 1);
    P := P join IrrFactors(Evaluate(fy,2,0));
    fxy := Reciprocal(f, 1, 1);
    if (Evaluate(Evaluate(fxy,1,0),2,0) eq 0) then
        P := P join {FF_1!1}; // 1/x
    end if;
end if;
end for;
return P;
end function;

// compute Successors
function Succ(f, P);
Q := {};
d := hom<FF_1 -> FF_1 | 0, x>;
for p in P do
    if (p ne 1) then
        // algorithm 7, p is a polynomial
        I := ideal<FF_1 | f, p>;
        if Dimension(I) eq 0 then
            q := UnivariateEliminationIdealGenerator(I, 2);
            Q := Q join IrrFactors(d(q));
        end if;
        fy := Reciprocal(f, 0, 1);
        if Degree(GCD(FF_1!Evaluate(fy,2,0),FF_1!p),1) gt 0 then
            Q := Q join {FF_1!1}; // 1/x
        end if;
    else
        // algorithm 8, p is 1/x
        fx := Reciprocal(f, 1, 0);
        Q := Q join d(IrrFactors(Evaluate(fx,1,0)));
        fxy := Reciprocal(f, 1, 1);
        if (Evaluate(Evaluate(fxy,1,0),2,0) eq 0) then
            Q := Q join {FF_1!1}; // 1/x
        end if;
    end if;
end for;
return Q;
end function;

```

```

// algorithm 3
function RamificationGeneratingSet(f);
  R := {};
  ff := FF_1!f;
  fx := FF_1!Reciprocal(f, 1, 0);
  fy := FF_1!Reciprocal(f, 0, 1);
  fxy := FF_1!Reciprocal(f, 1, 1);
  Discf := Resultant(ff, Derivative(ff,2),2);
  Discfx := Resultant(fx, Derivative(fx,2),2);
  Discfy := Resultant(fy, Derivative(fy,2),2);
  Discfxy := Resultant(fxy, Derivative(fxy,2),2);
  for u in IrrFactors(Discf) join IrrFactors(Discfy) do
    R := R join {u};
  end for;
  V := Discfx * Discfxy;
  if (Evaluate(V,1,0) eq 0) then
    R := R join {FF_1!1};
  end if;
  return R;
end function;

// algorithm 4
function FiniteRamificationLocusTest_BF(fSeq, MB);
  S := {} join &join{RamificationGeneratingSet(fSeq[i]) : \
    i in [1..#fSeq]};
  while Max({Degree(f,1) : f in S}) le MB do
    Sprev := S;
    S := S join &join{Pred(fSeq[j],Sprev) : j in [1..#fSeq]};
    if S eq Sprev then
      return S, true;
    end if;
  end while;
  return false, false;
end function;

// algorithm 5 (algorithm 6 is a special case of this)
function FiniteRamificationLocusTest_Nstep(fSeq, MB);
  S := [RamificationGeneratingSet(fSeq[i]) : i in [1..#fSeq]];
  while Max({Degree(f,1) : f in &join{S[i] : i in [1..#fSeq]}}) le MB do
    Sprev := S;
    for j in [1..(#fSeq-1)] do
      S[j] := Sprev[j] join Pred(fSeq[j+1],Sprev[j+1]);
    end for;
    S[#fSeq] := Sprev[#fSeq] join Pred(fSeq[1],Sprev[1]);
    if S eq Sprev then
      return S[#fSeq], true;
    end if;
  end while;
  return {}, false;
end function;

```

```

// algorithm 9 (algorithm 10 is a special case of this)
function CSlocusTest_Nstep_with_seed(fSeq, fSeed, MT);
  A := IrrFactorsSet(fSeed);
  B := {};
  while (A ne B) and XDegreeBelow(A,MT) do
    pi := Random(A diff B);
    Succ_n := {pi};
    for i in [1..#fSeq] do
      Succ_n := Succ(fSeq[i],Succ_n);
      if not XDegreeBelow(Succ_n,MT) then
        return A, false;
      end if;
    end for;
    A := A join Succ_n;
    B := B join {pi};
  end while;
  return A, ((A eq B) and (#A gt 0) select true else false);
end function;

function CSlocusTest(fSeq, MT, Exceptions);
  MI := {MultivariatePolynomial(FF_1, f, 1) : \
    f in MonIrrPolsUpTo(MT)} join {FF_1!1} diff Exceptions;
  while #MI gt 0 do
    MinDeg := Minimum({Degree(f,1) : f in MI});
    fSeed := Random({f : f in MI | (Degree(f,1) eq MinDeg)});
    ResultingSet, Success := \
      CSlocusTest_Nstep_with_seed(fSeq, {fSeed}, MT);
    if (Success) and (#(ResultingSet meet Exceptions) eq 0) then
      return ResultingSet, Success;
    else
      MI := MI diff (ResultingSet join {fSeed});
    end if;
  end while;
  return {}, false;
end function;

procedure CompleteTestNStep(fSeq, MB, MT);
  startTime := Realtime();
  V, foundFiniteVLocus := FiniteRamificationLocusTest_Nstep(fSeq, MB);
  if (foundFiniteVLocus) then
    if (SHOWRAMIFICATIONONLY) then
      printf "\n\nf = "; printSet(fSeq); printf "\n";
      f := fSeq[1];
      printf "Characteristic = %o, MB = %o, MT = %o \n", p, MB, MT;
      printf "V(F)\t\t = "; printSet(V); printf "\n";
      printf "#V(F)\t\t = %o\nSUM(deg P : P in V) = %o\n", \
        #V, degSumSet(V);
    if (SHOW_GRAPH) then
      printf "Gamma_B: (first step) \n";
      printGraph(f,V);
    end if;
  end if;
end procedure;

```

```

    end if;
end if;
T, foundCSLocus := CSLocusTest(fSeq, MT, V);
if (foundCSLocus) then
  if (not SHOWRAMIFICATIONONLY) then
    printf "\n\nf = "; printSet(fSeq); printf "\n";
    f := fSeq[1];
    printf "Characteristic = %o, MB = %o, MT = %o \n", p, MB, MT;
    printf "V(F)\t\t = "; printSet(V); printf "\n";
    printf "#V(F)\t\t = %o\nSUM(deg P : P in V) = %o\n", \
      #V, degSumSet(V);
    if (SHOW_GRAPH) then
      printf "Gamma_B: (first step) \n";
      printGraph(f,V);
    end if;
  end if;
end if;
r := LCMofDegrees(T);
numT := degSumSet(T);
numV := degSumSet(V)/2-1;
if (numV gt 0) then // and (numT/numV le (1^(r/2))-1) then
  printf "r\t\t = %o\n", r;
  printf "T(F/GF(%o))\t = ", 1^r; printSet(T); printf "\n";
  if (SHOW_GRAPH) then
    printf "Gamma_T: (first step) \n";
    printGraph(f,T);
  end if;
  printHx(T);
  printf "If tame, lambda(F) >= (%o)/(%o) = %o <= %o.\n", numT,\
    numV, (numV ne 0) select numT/numV else "undefined", \
    (1^(r/2))-1;
end if;
end if;
end if;
end procedure;

function KummerTypesSatisfyingProp41(m);
Set := {};
for gamma in {0} do // F_1 do
  printf "... gamma = %o ... \n", gamma;
  if gamma ne 1 then
    for A in GeneralLinearGroup(2,F_1) do
      f2 := FF_1!(A[2][1]*(x+1)^m+A[2][2]*(x+gamma)^m);
      f1 := FF_1!(A[1][1]*(x+1)^m+A[1][2]*(x+gamma)^m);
      f := FF_1!(f2*y^m-f1);
      if IsSeparable(f) and not IsUnivariate(f) \
        and IsIrreducible(f) and (Degree(f1,1) eq m) \
        and (Degree(f2,1) eq m-1) then
        Set := Set join {f};
      end if;
    end for;
  end for;
end function;

```

```

    end if;
  end for;
  return Set;
end function;

procedure KummerTowers(m);
  printf "Starting test for tame towers with deg f = %o,
    of form y^m=x*f1(x)/f2(x) ... \n",m;
  printf "GF(q) = %o\n", F_1;
  startTime := Realtime();
  i := 0;
  Pols := MonPolsUpTo(m-1);
  for f in {FF_1!(y^m*a*Q-x*P) : P in Pols, Q in Pols, a in F_1 | \
    (Degree(P,1) eq m-1) and (Degree(Q,1) eq m-1)} do
    if (FF_1!f ne FF_1!0) and (IsIrreducible(FF_1!f)) then
      i := i + 1;
      printf "[%o]\n",i;
      CompleteTestNStep([FF_1!f], 50, 5);
    end if;
  end for;
  printf "... took %o seconds.\n", Realtime(startTime);
end procedure;

procedure FermatTowersMultiStep(m);
  FTypes := {FF_1!(y^m-(a1)^m*(x+b)^m+(a1)^m*b^m) : \
    a1 in F_1, b in F_1 | a1 ne 0};
  reduceModGL2(~FTypes);
  for f in FTypes, g in FTypes diff {f}, h in FTypes diff {f, g} do
    CompleteTestNStep([FF_1!(f),FF_1!(g),FF_1!(h)],100,2);
  end for;
end procedure;

procedure GSRProp41Generalized(m);
  printf "Generating cases of type y^m = (B.x)(B.A.x)...(B.A^(m-1).x)\n";
  startTime := Realtime();
  Done := {};
  for alpha in F_1, beta in F_1 do
    if alpha ne 0 then
      for A in GeneralLinearGroup(2,1) do
        if (Order(A) eq m) and ((A[1][1] eq 1) or \
          ((A[1][1] eq 0) and (A[1][2] eq 1))) then
          RHS := FFF_1!1;
          Apower := A;
          for i in [1..m] do
            factor := FFF_1!(alpha*((Apower[1][1]*x+Apower[1][2])/
              (Apower[2][1]*x+Apower[2][2]))+beta);
            Apower := Apower*A;
            RHS := RHS*factor;
          end for;
          g := FF_1!Numerator(RHS);

```

```

        h := FF_1!Denominator(RHS);
        f := FF_1!(y^m*FF_1!h-FF_1!g);
        if (Degree(g,1) eq m) and (Degree(h,1) eq m-1) and \
            (f notin Done) then
            printf "\nConsidering alpha=%o, beta=%o, A=\n%o", alpha,beta,A;
            CompleteTestNStep([f],4,2);
        end if;
    end if;
end for;
end if;
end for;
printf "\n... took %o seconds.\n", Realtime(startTime);
end procedure;

procedure GSRProp41withX(m);
    printf "Generating all towers of type y^%o = f1(x)/f2(x) where
        x is a simple zero of f1(x), deg f1=1+deg f2\n",m;
    startTime := Realtime();
    P := {p : p in MonPolsUpTo(m-1) | Degree(p,1) eq m-1};
    printf "#P = %o\n", #P;
    for f1 in P do
        if Evaluate(f1,1,0) ne 0 then
            for f2 in P, a in F_1 do
                if (GCD(x*f1,f2) eq 1) and (a ne 0) then
                    f := y^m*a*f2-x*f1;
                    CompleteTestNStep([f],10,2);
                end if;
            end for;
        end if;
    end for;
    printf "\n... took %o seconds.\n", Realtime(startTime);
end procedure;

procedure KummerTotallyRamified(n,m);
    printf "Generating all %o-step towers with [F_{i+1}:F_{i}]=%o,
        and totally ramified at each step ... \n",n,m;
    startTime := Realtime();
    P := {p : p in MonPolsUpTo(m) | Degree(p,1) eq m};
    Q := {p : p in MonPolsUpTo(m-1) | Degree(p,1) eq m-1};
    printf "#P = %o, #Q = %o\n", #P, #Q;
    MB := 50; MT := 5;
    TopHeavyCandidates := {qx*y^m-px : px in P, qx in Q | \
        IsIrreducible(qx*y^m-px)};
    BottomHeavyCandidates := {px*y^m-qx : px in P, qx in Q | \
        IsIrreducible(px*y^m-qx)};
    AllCandidates := TopHeavyCandidates join BottomHeavyCandidates;
    if (n eq 1) then
        for f in AllCandidates do
            CompleteTestNStep([f],MB,MT);
        end for;
    end if;
end procedure;

```

```

end if;
if (n eq 2) then
  for f in AllCandidates, \
    g in (TopHeavyCandidates join BottomHeavyCandidates) \
      diff isoPols(f) do
    CompleteTestNStep([f,g],MB,MT);
  end for;
end if;
if (n eq 3) then
  for f in AllCandidates,
    g in (AllCandidates) diff isoPols(f),
    h in (AllCandidates) diff \
      (isoPols(f) join isoPols(g)) do
    CompleteTestNStep([f,g,h],MB,MT);
  end for;
end if;
printf "\n... took %o seconds.\n", Realtime(startTime);
end procedure;

procedure BGS64(reduce);
// reduce = true mods by orbit of GL(F_1)
MB := 50; MT := 5;
printf "Generating BGS64 (Galois) Candidates ... \n";
startTime1 := Realtime();
Type1 := {}; Type2 := {}; Type3 := {};
E := {e^(p-1) : e in F_1};
for ep in E, a in F_1, alpha in F_1 do
  if (a*alpha ne 0) then
    for b in F_1, c in F_1 do
      if not (alpha in F_p) then
        f := FF_1!(alpha^p*x^p-ep*alpha*x+b)*(y^p-ep*y-c)-a;
        if IsSeparable(f) then
          Type1 := Type1 join {f};
        end if;
      end if;
      if not (a in F_p) then
        f := FF_1!(y^p-ep*y-b)*x^p-a*(alpha^p-ep*alpha*x^(p-1));
        if IsSeparable(f) then
          Type2 := Type2 join {f};
        end if;
      end if;
      f := FF_1!(alpha^p-ep*alpha*x^(p-1)+b*x^p)*(y^p-ep*y-c)-a*x^p;
      if IsSeparable(f) then
        Type3 := Type3 join {f};
      end if;
    end for;
  end if;
end for;
type1Reduced := Type1; type2Reduced := Type2; type3Reduced := Type3;
if (reduce eq true) then

```

```

    reduceModGL2(~type1Reduced);
    reduceModGL2(~type2Reduced);
    reduceModGL2(~type3Reduced);
end if;
printf "... took %o seconds.\n", Realtime(startTime);
printf "There are %o (%o) defining polynomials of type (i)\n", \
    #Type1, #type1Reduced;
printf "There are %o (%o) defining polynomials of type (ii)\n", \
    #Type2, #type2Reduced;
printf "There are %o (%o) defining polynomials of type (iii)\n", \
    #Type3, #type3Reduced;

printf "Starting test for type (i) ...\n";
startTime := Realtime();
i := 0;
for f in (reduce select type1Reduced else Type1) do
    i := i + 1;
    printf "\n\n(i)[%o]", i;
    CompleteTestNStep([FF_1!f], MB, MT);
end for;
printf "\n... took %o seconds.\n", Realtime(startTime);

printf "Starting test for type (ii) ...\n";
startTime := Realtime();
i := 0;
for f in (reduce select type2Reduced else Type2) do
    i := i + 1;
    printf "\n\n(ii)[%o]", i;
    CompleteTestNStep([FF_1!f], MB, MT);
end for;
printf "\n... took %o seconds.\n", Realtime(startTime);

printf "Starting test for type (iii) ...\n";
startTime := Realtime();
i := 0;
for f in (reduce select type3Reduced else Type3) do
    i := i + 1;
    printf "\n\n(iii)[%o]", i;
    CompleteTestNStep([FF_1!f], MB, MT);
end for;
printf "\n... took %o seconds.\n", Realtime(startTime);

printf "There were %o (%o) defining polynomials of type (i)\n", \
    #Type1, #type1Reduced;
printf "There were %o (%o) defining polynomials of type (ii)\n", \
    #Type2, #type2Reduced;
printf "There were %o (%o) defining polynomials of type (iii)\n", \
    #Type3, #type3Reduced;
end procedure;

```

Appendix B

Supplemental graphs

In this appendix, we exhibit ramification and components of complete splitting graphs for one and two-step towers. The graphs were generated using the GraphViz [23] graph drawing software.

For each of the graphs that follow, vertices should be considered as functions in \tilde{x} and (for Figure B.3) \tilde{y} . Directed edges should be considered as labeled as \tilde{f} for directed edges from functions in \tilde{x} to either functions in \tilde{x} or \tilde{y} , whereas edges from functions in \tilde{y} to functions in \tilde{x} should be considered as labeled with \tilde{g} .

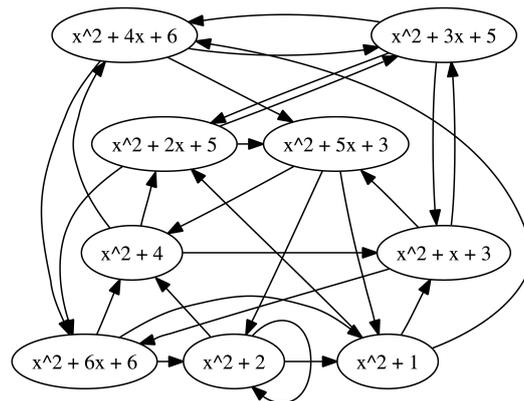


Figure B.1: Computer-generated representation of $\tilde{\Gamma}_T^*$ for tower defined by $y^3 = \frac{x^3+2x^2+4x}{x^2-x+1}$ over \mathbb{F}_7

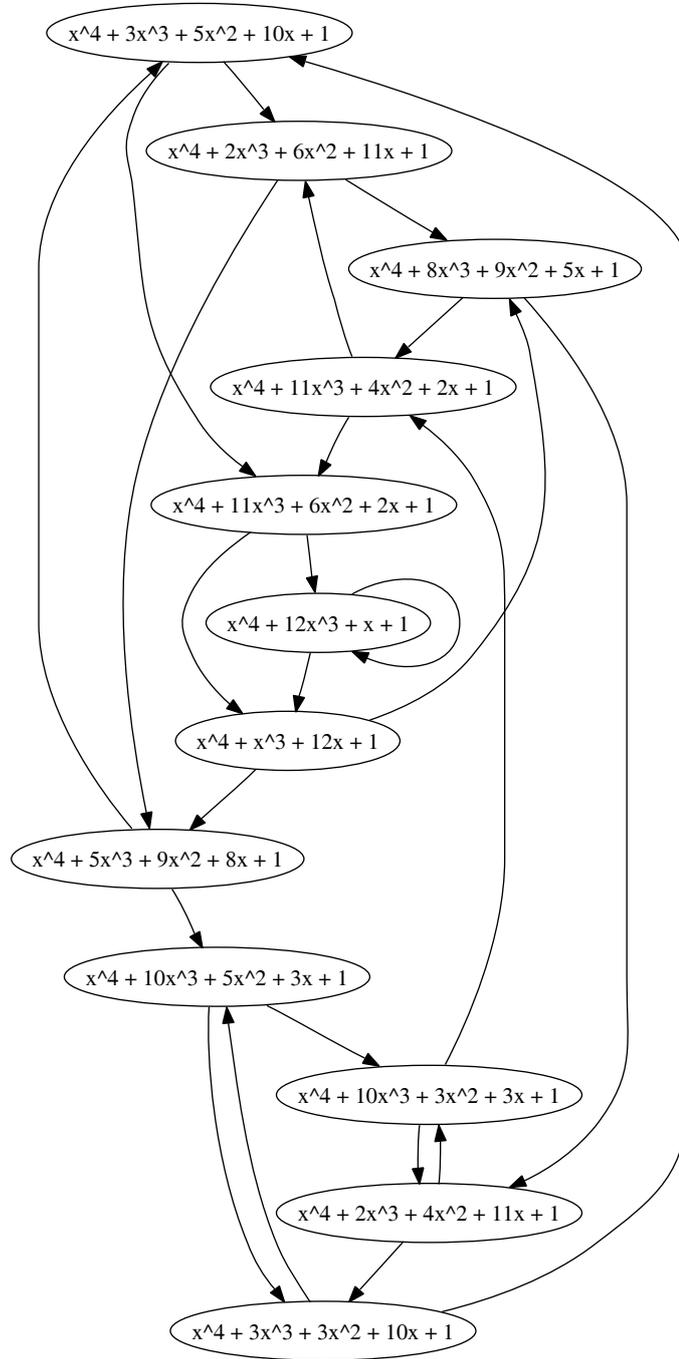


Figure B.2: Computer-generated representation of $\tilde{\Gamma}_T^*$ for tower defined by $y^2 = \frac{x(1-x)}{x+1}$ over \mathbb{F}_{13}

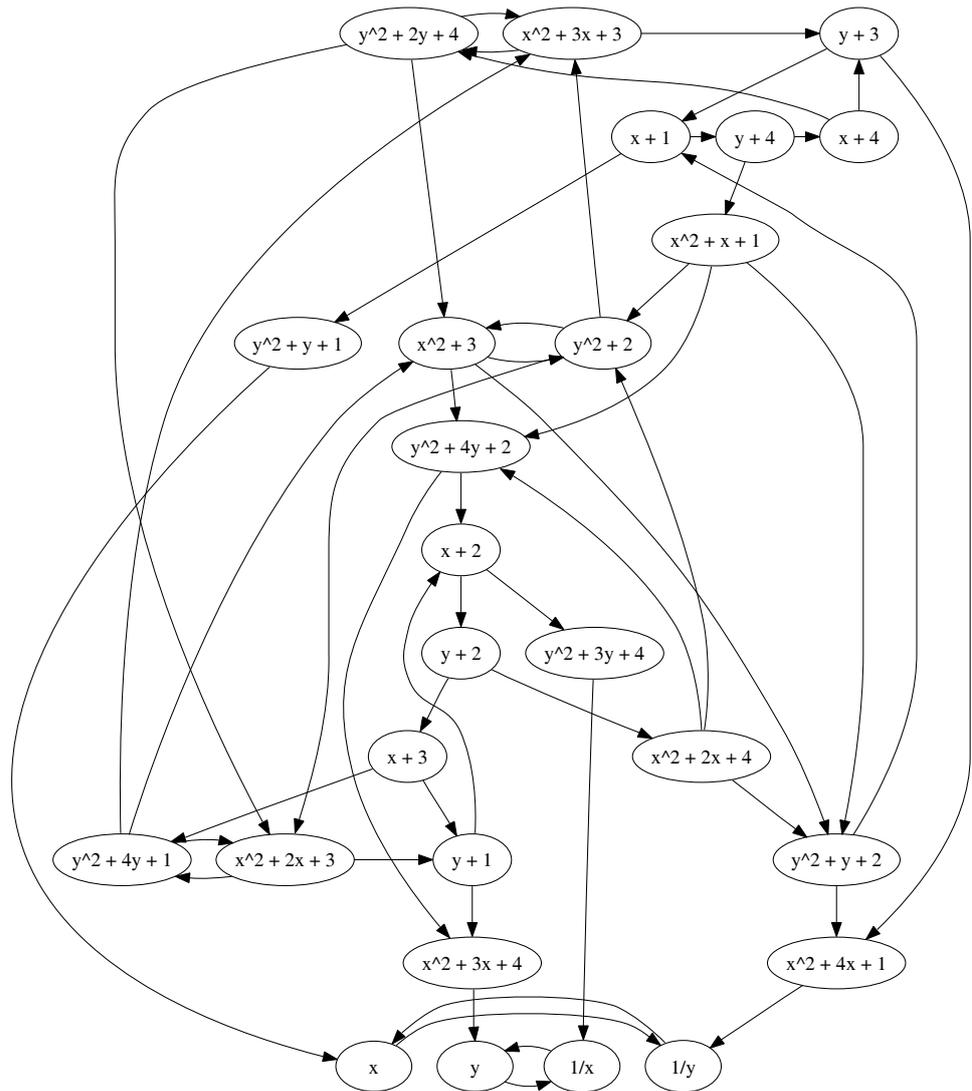


Figure B.3: Computer-generated representation of $\tilde{\Gamma}_B$ for two-step tower of cubic extensions over \mathbb{F}_5

List of Notation

- q A power of a prime p .
- \mathbb{F}_q Finite field with q elements, usually the field over which a tower will be defined.
- $\overline{\mathbb{F}}$ Algebraic closure of \mathbb{F}_q .
- \mathbb{F}_l Field of coefficients of the polynomial ring over which the defining polynomials of a tower are defined. A subfield of \mathbb{F}_q .
- \mathbb{F}_r Smallest finite extension of \mathbb{F}_l so that the tower will be completely splitting if defined over $\mathbb{F}_q = \mathbb{F}_r$.
- F/\mathbb{F}_q Function field with full constant field \mathbb{F}_q
- \mathcal{F}/\mathbb{F}_q Tower of function fields over the finite field \mathbb{F}_q , see p. 9.
- F_i/\mathbb{F}_q Function field (with full constant field \mathbb{F}_q) constituting the i th step ($i \geq 0$) of a representation of a tower.
- $S(F_i/\mathbb{F}_q)$ Set of places of the function field F_i/\mathbb{F}_q .
- $(x_i = \alpha)$ Place of the function field $F_i = \mathbb{F}_q(x_0, x_1, \dots, x_i)$ which is a zero of $x_i - \alpha$ for some $\alpha \in \mathbb{F}_q$, or the pole of x_i for $\alpha = \infty$.
- $N(F_i/\mathbb{F}_q)$ Number of places of degree one of the function field F_i/\mathbb{F}_q .
- $g(F_i/\mathbb{F}_q)$ Genus of the function field F_i/\mathbb{F}_q .
- $v_F(\mathcal{F})$ F -splitting rate of the tower \mathcal{F} , see p. 10.

$\gamma_F(\mathcal{F})$ F -genus rate of the tower \mathcal{F} , see p. 10.

$\lambda(\mathcal{F})$ Limit of the tower \mathcal{F} .

$A(q)$ Minimal upper bound for the limit of a tower defined over the field with q elements.

$V_F(\mathcal{F})$ F -ramification locus of the tower \mathcal{F} , for some $F < \mathcal{F}$.

$e(Q|P)$ Ramification index of the place Q lying above the place P .

$\text{Diff}(E/F)$ Different divisor of the extension E/F .

$d(Q|P)$ Different exponent of the place Q lying above the place P .

$T_F(\mathcal{F})$ F -completely splitting locus of the tower \mathcal{F} , for some $F < \mathcal{F}$.

$(f_i(x_{i-1}, x_i))_{i \geq 1}$ Sequence of defining polynomials of an explicit tower \mathcal{F} .

\sim Equivalence relation on the indeterminates $\{x_0, x_1, x_2, \dots\}$, or on the defining polynomials $\{f_1, f_2, f_3, \dots\}$ of an explicit tower \mathcal{F} .

\tilde{x}_i Representative of an element of the sequence of indeterminates $\{x_0, x_1, x_2, \dots\}$ modulo \sim .

\tilde{f}_i Representative of an element of the sequence of defining polynomials $\{f_1, f_2, f_3, \dots\}$ modulo \sim .

\sim_n n -step equivalence relation on the indeterminates $\{x_0, x_1, x_2, \dots\}$, or on the defining polynomials $\{f_1, f_2, f_3, \dots\}$.

$GL(\mathbb{F}_q, 2)$ General linear group of nonsingular 2×2 matrices over \mathbb{F}_q .

$PGL(\mathbb{F}_q, 2)$ Projective general linear group of nonsingular 2×2 matrices over \mathbb{F}_q .

$\tilde{\mathcal{F}}$ Algebraic closure of the tower \mathcal{F} .

$f^{(x)}, f^{(y)}$ and $f^{(x,y)}$ Reciprocal polynomials of $f(x, y)$.

$(U_i)_{i \geq 0}$ Ramification-capturing sequence, see Definition 3.5.

$MI_{\mathbb{F}_l}(T)$ Set of monic irreducible functions, see Definition 3.8.

$(M_i)_{i \geq 0}$ Ramification-capturing function sequence, see Definition 3.9.

$(f(x))$ Principal divisor of the function $f(x)$.

$\text{supp}(D)$ Support of the divisor D .

$\text{Pred}_f(p)$ Predecessor polynomials, see Definition 3.11.

$(R_i)_{i \geq 0}$ Ramification-generating set of functions, see Definition 3.14.

$\text{disc}_y f(x, y)$ Discriminant of $f(x, y)$, with $\text{disc}_y f(x, y) \in \mathbb{F}_l[x]$.

\mathcal{G} Gröbner basis

$\Gamma = \Gamma_{\mathcal{F}, \mathbb{F}_l, (f_i)_{i \geq 1}}$ \mathbb{F}_l -splitting graph of the explicit tower \mathcal{F} over \mathbb{F}_q induced by the defining polynomials $(f_i)_{i \geq 1}$.

$V(\Gamma)$ Vertex set of the graph Γ .

$E(\Gamma)$ Edge set of the graph Γ .

Γ_B \mathbb{F}_l -ramification graph, see Definition 3.18.

χ Map from $S(F_i/\mathbb{F}_q)$ to the power set of $V(\Gamma)$, see p. 41.

$f_{\chi(P), j}$ Unique element of $MI_{\mathbb{F}_l}(T_j)$ such that $f_{\chi(P), j}(x_j(P)) = 0$.

$\tilde{\Gamma}_B$ \mathbb{F}_l -ramification graph modulo \sim , see page 44.

$\text{Succ}_f(p)$ Successor polynomials, see Definition 4.1.

Γ_T Complete \mathbb{F}_l -splitting graph, see Definition 4.4.

$\chi(P)_i(T_i)$ Unique element in the intersection of $\chi(P)$ and $MI_{\mathbb{F}_l}(T_i)$, see the proof of Proposition 4.5.

$\mathcal{A}(\Gamma', i)$ Subset of vertices of the subgraph Γ' of Γ representing functions in x_i .

- Ω_{Γ} Subset of $\overline{\mathbb{F}} \cup \{\infty\}$ corresponding to a set of places of degree one, see p. 59.
- $\tau_{\Gamma^*, i}(T_i)$ Splitting characteristic polynomial, see (4.9) on p. 64.
- M_B Maximum allowable degree of element in $V(\Gamma_B)$.
- M_T Maximum allowable degree of element in $V(\Gamma_T)$.
- $H_p(T)$ Deuring's polynomial, see p. 104.
- ${}_mF_n$ Generalized hypergeometric function, see (6.12) on p. 104.
- $a_n^{(r)}$ n th Franel number of order r , see (6.15) on p. 107.
- $f^{(r)}(z)$ Generating function for the sequence $(a_n^{(r)})_{n \geq 0}$.

List of Figures

3.1	Ramification graph Γ_B for Example 3.20	43
3.2	Condensed ramification graph $\tilde{\Gamma}_B$ for Example 3.20	45
3.3	Ramification graph Γ_B for Example 3.21	46
3.4	Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for Example 3.22 with specific f and g	50
4.1	Complete \mathbb{F}_2 -splitting graph Γ_T^* for Example 4.9	62
4.2	Complete \mathbb{F}_q -splitting graph Γ_T^* for Example 4.10	63
4.3	Condensed complete \mathbb{F}_q -splitting graph $\tilde{\Gamma}_T^*$ for Example 4.10	63
4.4	Ramification graph Γ_B for Example 4.15	71
6.1	Condensed \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$ for \mathcal{F}	100
6.2	Condensed component of $\tilde{\Gamma}_T^*$ for \mathcal{F} , $p = 5$	100
6.3	Condensed \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$ for \mathcal{H}	102
6.4	Condensed component of $\tilde{\Gamma}_T^*$ for \mathcal{H} , $p = 5$	102
6.5	Condensed \mathbb{F}_7 -ramification graph $\tilde{\Gamma}_B$	106
6.6	Condensed \mathbb{F}_p -ramification graph $\tilde{\Gamma}_B$	107
6.7	Condensed \mathbb{F}_7 -ramification graph $\tilde{\Gamma}_B$ for \mathcal{F}_1	110
6.8	Condensed \mathbb{F}_7 -ramification graph $\tilde{\Gamma}_B$ for \mathcal{F}_2	111
6.9	Condensed \mathbb{F}_{11} -ramification graph $\tilde{\Gamma}_B$	113
6.10	Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for 2-step tower \mathcal{F} over \mathbb{F}_3	115
6.11	Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for 2-step tower \mathcal{H} over \mathbb{F}_3	117
6.12	Condensed \mathbb{F}_3 -ramification graph $\tilde{\Gamma}_B$ for 3-step tower over \mathbb{F}_3	120

6.13	Condensed \mathbb{F}_4 -ramification graph $\tilde{\Gamma}_B, \rho^2 + \rho + 1 = 0$	124
B.1	Computer-generated representation of $\tilde{\Gamma}_T^*$ for tower defined by $y^3 = \frac{x^3+2x^2+4x}{x^2-x+1}$ over \mathbb{F}_7	140
B.2	Computer-generated representation of $\tilde{\Gamma}_T^*$ for tower defined by $y^2 = \frac{x(1-x)}{x+1}$ over \mathbb{F}_{13}	141
B.3	Computer-generated representation of $\tilde{\Gamma}_B$ for two-step tower of cubic extensions over \mathbb{F}_5	142

List of Algorithms

1	Calculate $\text{Pred}_f(q)$ for a monic \mathbb{F}_l -irreducible $q(y) \in \mathbb{F}_l[y]$. . .	74
2	Calculate $\text{Pred}_f(q)$ for $q(y) = \frac{1}{y}$	75
3	Calculate R_k for each $k \geq 0$	76
4	Decide whether the ramification locus for \mathcal{F} generated by $(f_i)_{i \geq 1}$ is finite, for arbitrary (finite modulo \sim) tower \mathcal{F} . . .	79
5	Decide whether the ramification locus for \mathcal{F} generated by $(f_i)_{i \geq 1}$ is finite, for n -step tower \mathcal{F}	80
6	Decide whether the ramification locus for \mathcal{F} generated by $(f_i)_{i \geq 1}$ is finite, for 1-step tower \mathcal{F} ($f_i \sim_1 \tilde{f}$)	81
7	Calculate $\text{Succ}_f(p)$ for a monic \mathbb{F}_l -irreducible $p(x) \in \mathbb{F}_l[x]$	82
8	Calculate $\text{Succ}_f(p)$ for $p(x) = \frac{1}{x}$	83
9	Compute a representation of a connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T of \mathcal{F} , for n -step tower \mathcal{F}	85
10	Compute a representation of a connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T of \mathcal{F} , for one-step tower \mathcal{F}	87
11	Compute a representation of a connected component Γ_T^* of the \mathbb{F}_l -complete splitting graph Γ_T of \mathcal{F} , for \sim -finite tower \mathcal{F}	88

Bibliography

- [1] I. Aleshnikov, V. Deolalikar, P. V. Kumar, and H. Stichtenoth. Towards a basis for the space of regular functions in a tower of function fields meeting the Drinfeld-Vladut bound. In *Finite fields and applications (Augsburg, 1999)*, pages 14–24. Springer, Berlin, 2001.
- [2] B. Angles and C. Maire. A note on tamely ramified towers of global function fields. *Finite Fields Appl.*, 8(2):207–215, 2002.
- [3] R. Auer and J. Top. Legendre elliptic curves over finite fields. *J. Number Theory*, 95(2):303–312, 2002.
- [4] S. Ballet. Curves with many points and multiplication complexity in any extension of \mathbb{F}_q . *Finite Fields Appl.*, 5(4):364–377, 1999.
- [5] P. Beelen. Graphs and recursively defined towers of function fields. *J. Number Theory*, 108(2):217–240, 2004.
- [6] P. Beelen and I. Bouw. Asymptotically good towers and differential equations. *Compos. Math.*, 141(6):1405–1424, 2005.
- [7] P. Beelen, A. García, and H. Stichtenoth. On towers of function fields of Artin-Schreier type. *Bull. Braz. Math. Soc. (N.S.)*, 35(2):151–164, 2004.
- [8] P. Beelen, A. García, and H. Stichtenoth. On ramification and genus of recursive towers. *Port. Math. (N.S.)*, 62(2):231–243, 2005.
- [9] P. Beelen, A. García, and H. Stichtenoth. On towers of function fields over finite fields. In *Arithmetic, geometry and coding theory (AGCT*

- 2003), volume 11 of *Sémin. Congr.*, pages 1–20. Soc. Math. France, Paris, 2005.
- [10] P. Beelen, A. García, and H. Stichtenoth. Towards a classification of recursive towers of function fields over finite fields. *Finite Fields Appl.*, 12(1):56–77, 2006.
- [11] J. Bezerra and A. García. A tower with non-Galois steps which attains the Drinfeld-Vladut bound. *J. Number Theory*, 106(1):142–154, 2004.
- [12] J. Bezerra, A. García, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink’s lower bound. *J. Reine Angew. Math.*, 589:159–199, 2005.
- [13] W. Bosma, J. Cannon, and C. Playoust. The MAGMA Algebra System i: the user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.
- [14] B. Buchberger. Theoretical basis for the reduction of polynomials to canonical forms. *SIGSAM Bull.*, 39:19–24, 1976.
- [15] C. Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable, volume 6 of Mathematical Surveys*. American Mathematical Society, New York, 1951.
- [16] D. Cox, J. Little, and O’Shea. *Ideals, Varieties, and Algorithms: An Introduction to Algebraic Geometry and Commutative Algebra, 2nd ed.* Springer Verlag, 1996.
- [17] D. A. Cox and B. Strumfels, editors. *Applications of Computational Algebraic Geometry*. American Mathematical Society, American Mathematical Society, January 1997.
- [18] T. W. Cusick. Recurrences for sums of powers of binomial coefficients. *J. Combin. Theory Ser. A*, 52(1):77–83, 1989.
- [19] 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.
- [20] V. Deolalikar. Extensions of algebraic function fields with complete splitting of all rational places. *Comm. Algebra*, 30(6):2687–2698, 2002.
- [21] N. D. Elkies. Explicit modular towers. In *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997, T. Basar, A. Vardy, eds.)*, pages 23–32. Univ. of Illinois at Urbana-Champaign, 1998.
- [22] 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.
- [23] J. Ellson, E.R. Gansner, E. Koutsofios, S.C. North, and G. Woodhull. Graphviz and Dynagraph – Static and Dynamic Graph Drawing Tools. In M. Junger and P. Mutzel, editors, *Graph Drawing Software*, pages 127–148. Springer-Verlag, 2003.
- [24] O. Endler. *Valuation theory*. Springer-Verlag, New York, 1972.
- [25] J.-C. Faugere. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.
- [26] J. Franel. On a Question of Laisant. *L'intermédiaire des mathématiciens*, 1:45–47, 1894.
- [27] A. Frölich and M. Taylor. *Algebraic Number Theory*. Cambridge 27, 1991.
- [28] A. García and H. Stichtenoth. Some Artin-Schreier towers are easy. *Moscow Math. J.*
- [29] A. García and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfel'd-Vlăduț bound. *Invent. Math.*, 121(1):211–222, 1995.

- [30] 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.
- [31] A. García and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61:248–273, 1996.
- [32] A. García and H. Stichtenoth. A class of polynomials over finite fields. *Finite Fields Appl.*, 5(4):424–435, 1999.
- [33] A. García and H. Stichtenoth. Skew pyramids of function fields are asymptotically bad. In *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 111–113. Springer, Berlin, 2000.
- [34] A. García and H. Stichtenoth. Asymptotics for the genus and the number of rational places in towers of function fields over a finite field. *Finite Fields Appl.*, 11, 2005.
- [35] A. García and H. Stichtenoth. On the Galois closure of towers. *Preprint*, 2005.
- [36] A. García, H. Stichtenoth, and Hans-Georg Rück. On tame towers over finite fields. *J. Reine Angew. Math.*, 557:53–80, 2003.
- [37] 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.
- [38] V.D. Goppa. Codes on algebraic curves. *Sov. Math. Dokl.*, 24:170–172, 1981.
- [39] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed. Addison-Wesley, Reading, MA, second edition, 1999.
- [40] Y. Ihara. Congruence relations and Shimura curves. *J. Fac. Sci. Univ. Tokyo*, 25:301–361, 1979.

- [41] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo*, 28:721–724, 1981.
- [42] S. Lang. *Algebraic Number Theory*. Addison-Wesley, 1970.
- [43] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [44] W. W. Li. Modularity of asymptotically optimal towers of function fields. In *Coding, cryptography and combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, pages 51–65. Birkhäuser, Basel, 2004.
- [45] W. W. Li, H. Maharaj, H. Stichtenoth, and N. D. Elkies. New optimal tame towers of function fields over small finite fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 372–389. Springer, Berlin, 2002.
- [46] E. C. Lötter. Explicit constructions of asymptotically good towers of function fields. Master’s thesis, University of Stellenbosch, Stellenbosch, 2003.
- [47] H. Maharaj and J. Wulftange. On the construction of tame towers over finite fields. *J. Pure Appl. Algebra*, 199(1-3):197–218, 2005.
- [48] Y. I. Manin. What is the maximal number of points on a curve over \mathbb{F}_2 ? *J. Fac. Sci. Univ. Tokyo*, 28:715–720, 1981.
- [49] P.J. McCarthy. *Algebraic Extensions of Fields*. Dover Publications, 1991.
- [50] 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.
- [51] 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.

- [52] H. Niederreiter and C. Xing. *Rational Points on Curves over Finite Fields, Theory and Applications*. Cambridge University Press, 2001.
- [53] M. Petkovšek, H. S. Wilf, and D. Zeilberger. *A = B*. A K Peters Ltd., Wellesley, MA, 1996.
- [54] O. Pretzel. *Codes and algebraic curves*. Oxford University Press, New York, NY, USA, 1998.
- [55] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [56] J.P. Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.
- [57] J.P. Serre. *Lecture notes on curves over finite fields*. 1985.
- [58] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
- [59] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.
- [60] 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.
- [61] A. Temkine. Hilbert class field towers of function fields over finite fields and lower bounds for $A(q)$. *J. Number Theory*, 87(2):189–210, 2001.
- [62] M. A. Tsfasman. Some remarks on the asymptotic number of points. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 178–192. Springer, Berlin, 1992.

- [63] M. A. Tsfasman, S. G. Vlăduț, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.
- [64] 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.
- [65] 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.
- [66] G. van der Geer and M. van der Vlugt. Tables of curves with many points, January 2006. Available at <http://www.science.uva.nl/~geer/>.
- [67] A. B. van der Merwe. Towers of global function fields with asymptotically many rational places. 2001. Unpublished preprint.
- [68] S.G. Vlăduț and V.G. Drinfeld. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.
- [69] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948.
- [70] J. Wulftange. *Zahme Türme algebraischer Funktionkörper*. PhD thesis, Essen, 2003.
- [71] C. Xing and S. L. Yeo. Algebraic Curves with Many Points over the Binary Field. Preprint.
- [72] Th. Zink. Degeneration of Shimura surfaces and a problem in coding theory. In *Fundamentals of computation theory (Cottbus, 1985)*, volume 199 of *Lecture Notes in Comput. Sci.*, pages 503–511. Springer, Berlin, 1985.

Index

- asymptotically
 - bad, 11
 - good, 11
 - maximal, 12
 - optimal, 12
- balanced degree, 18
- basic function field, 19, 37
- complete splitting, 58
- completely splitting, 15, 51
- completely splitting locus, 15
- condensed graph, 44
- Dedekind different theorem, 19
- defining polynomials, 17
- Deuring's polynomial, 104
- different
 - exponent, 13
- discriminant, 34
- Drinfeld-Vladut
 - bound, 11, 109, 112
- equivalence relation, 19
- extension
 - Artin-Schreier, 37, 120
 - Kummer, 45, 93, 103
- Fermat tower, 45, 92
- finite ramification type, 13, 40
- Franel number, 107
- functional equation, 68, 104, 109
- general linear group, 21, 22
- Gröbner basis, 33, 68, 70, 74, 75, 83
- graph
 - complete splitting, 55
 - predecessor, 40, 41
 - ramification, 41, 42
 - splitting, 41, 55
 - theory, 40
- Hurwitz genus formula, 14, 19
- hypergeometric function, 104
- Legendre
 - form, 104
 - symbol, 99, 107
- limit, 11
- linear fractional transformation, 22, 95
- locus
 - completely splitting, 15
 - ramification, 13

- Möbius transformation, *see* linear fractional transformation
- Magma, 91
- modular tower, 70
- predecessor polynomial, 33
- projective general linear group, 22
- ramification
 - finite, *see* finite ramification type
 - tame, 13, 92
 - wild, 13, 120
- ramification locus, 13, *see* locus
- ramification-capturing
 - function sequence, 31, 48
 - sequence, 29
- ramification-generating
 - set of functions, 35
- reciprocal polynomials, 25, 38
- repeated roots, 25, 34
- splitting characteristic polynomial, 64
- subtower, 12, 99, 104
- successor polynomial, 52
- superfluous elements, 36, 45
- totally ramified, 13, 18
- tower
 - finite, 20, 21
 - Galois, 19
 - n-step, 80
 - one-step, 19, 45, 81
 - two-step, 19, 47
- tower of function fields, 9
 - algebraic closure, 24
 - explicit, 17
 - Van der Geer and Van der Vlugt, 37
 - variable separated form, 17, 95
 - Wilson's theorem, 108