Continued Fractions and Sequences

Alan George Beattie Lauder

Royal Holloway and Bedford New College
University of London

Thesis submitted for the Degree of Doctor of Philosophy, 1999

Abstract

Any rational function whose coefficients lie in a finite field may be expanded in a unique way as a finite continued fraction whose partial quotients are polynomials. The field of all rational functions may be embedded in a larger field, known as the field of Laurent series, and an irrational element of this larger field may be written uniquely as an infinite continued fraction. The significance of these expansions is that they reveal how easily the Laurent series may be approximated by other simpler rational functions. If all the partial quotients of the continued fraction have small degree, then the Laurent series may be considered difficult to approximate. Laurent series which have partial quotients all of degree one in their continued fraction expansion are said to be badly approximable. In this thesis we explore questions related to badly approximable rational functions, and more generally, Laurent series which are difficult to approximate.

The orthogonal multiplicity of a polynomial is the number of badly approximable rational functions in reduced form which have that polynomial as their denominator. We classify those polynomials which have an odd number for their orthogonal multiplicity, and put a lower bound on their multiplicity. We also generalise a well-known theorem on badly approximable irrational Laurent series over the binary field. Algorithmic problems related to badly approximable rational functions are considered, and in the final chapter, moving beyond the main theme of the thesis, we present some new results on absolutely irreducible bivariate polynomials.

Any sequence over a finite field may be encoded as a Laurent series. The linear complexity profile of the sequence, which is of interest from a cryptographic viewpoint, may then be read off from the continued fraction expansion of the associated Laurent series. Sequences with desirable profiles correspond to Laurent series which are difficult to approximate, and the new results in this thesis are interpreted in terms of sequences whenever appropriate.

Acknowledgements

I owe thanks to my colleagues and mentors for their guidance and support. Especially to Alfred, the two Peters and Fred for their worldly advice, and to Simon, Steven and Shuhong for sparking my interest. I also thank all of my sponsors: My research in the UK was supervised by Fred Piper and funded by the EPSRC and Vodafone, and my sojourn in the USA was supported by the Fulbright Commission.

Above all, I thank my family and Tomoko for their love and encouragement, and dedicate this thesis to George and Morah Lauder.

Contents

Abstract **2**

Acknowledgements **3**

List of Tables **6**

Notation **7**

1 Introduction **8**

2 The Key Concepts **12**

2.1 Introduction 12

2.2 Rational Functions and Laurent Series 12

2.2.1 Norms, Exponential Valuations, and Completions 12

2.2.2 A Norm on the Field of Rational Functions 14

2.2.3 The Construction of the Field of Laurent Series 15

2.2.4 The Algebraic Properties of the Field of Laurent Series 17

2.3 Continued Fractions 20

2.3.1 General Continued Fractions 20

2.3.2 Simple Continued Fractions and Rational Functions 21

2.3.3 Infinite Continued Fractions 23

2.3.4 Best Approximations 25

2.4 Sequences 29

2.4.1 The Basic Properties of Sequences 29

2.4.2 Linear Complexity Profiles 30

3 Continued Fractions with Partial Quotients of Small Degree **34**

3.1 Introduction 34

3.2 Rational Function Analogues of Zaremba's Conjecture and Theorem . 35

3.3 The Orthogonal Multiplicity of a Polynomial 36

3.3.1 Results for Arbitrary Finite Fields 38

3.3.2 Results for the Binary Field 40

3.4 Motivation 45

3.4.1 The Euclidean Algorithm for Polynomials 45

3.4.2 The Linear Complexity Profiles of Sequences 46

3.4.3 Pseudorandom Number Generation 46

4 Polynomials with Odd Orthogonal Multiplicity **48**
4.1 Introduction . . . 48
4.2 Preliminaries . . . 49
4.2.1 Continued Fractions . . . 49
4.2.2 Folded Polynomials . . . 52
4.3 Theorems . . . 53
4.4 Further Results . . . 55
4.5 Comments and Examples . . . 56

5 Continued Fractions of Algebraic Laurent Series **59**
5.1 Introduction . . . 59
5.2 The Contribution of Baum and Sweet . . . 60

6 Continued Fractions of Laurent Series with Partial Quotients from a Given Set **63**
6.1 Introduction . . . 63
6.2 Preliminaries . . . 64
6.2.1 Lemmas . . . 64
6.2.2 An Equivalence Relation on Sets of Polynomials . . . 66
6.3 The Cardinality of $CF(A)$ up to a Given Rational Approximation . . 66
6.4 The Main Theorem . . . 68
6.4.1 Preliminary Results . . . 68
6.4.2 The Case $\deg u$ Even . . . 70
6.4.3 The Case $\deg u$ Odd . . . 74
6.4.4 A Statement of the Main Theorem . . . 75
6.4.5 Polynomials with Maximal Solution Groups . . . 76
6.5 Corollaries to the Main Theorem . . . 78
6.5.1 Algebraic Laurent Series with Bounded Partial Quotients . . . 78
6.5.2 An Application to Sequences . . . 79

7 Algorithms for Continued Fractions **81**
7.1 Introduction . . . 81
7.2 Computing the Orthogonal Multiplicity . . . 81
7.2.1 The Binary Field . . . 81
7.2.2 General Finite Fields . . . 83
7.3 Polynomials with Odd Orthogonal Multiplicity . . . 84

8 Absolutely Irreducible Bivariate Polynomials **85**
8.1 Introduction . . . 85
8.2 Preliminaries . . . 86
8.2.1 The Newton Polytope of a Multivariate Polynomial . . . 86
8.2.2 Convex Polygons . . . 87
8.3 Algorithms . . . 89
8.4 Absolute Irreducibility Criteria . . . 92
8.5 Comments . . . 93

Bibliography **94**

List of Tables

3.1 Frequencies of Orthogonal Multiplicities for Polynomials of Degree 5 over $\mathbb{F}_3$ 38

4.1 Frequencies of Orthogonal Multiplicities for Polynomials of Degree 5 over $\mathbb{F}_4$ 57

6.1 Polynomials with Maximal Full Solution Groups in $\mathbb{F}_2[x]$ 78

Notation

$\mathbb{Z}$;$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$	the integers; rational, real and complex numbers
$\lfloor r \rfloor$	the greatest integer not greater than the real number r
$\lceil r \rceil$	the least integer not less than the real number r
$\|\|\gamma\|\|$	the absolute value of a complex number γ
$\mathbb{F}_q, \mathbb{F}_q{}^*$	the finite field of q elements, its multiplicative group
$\mathbb{F}_q[x]$	the ring of polynomials in x over $\mathbb{F}_q$
$\mathbb{F}_q(x)$	the field of rational functions in x over $\mathbb{F}_q$
L_q	the field of Laurent series in x^{-1} over $\mathbb{F}_q$
$\gcd(f, g)$	the greatest common divisor of polynomials or integers
$\deg f$	the degree of a polynomial f
$v(\alpha)$	the exponential valuation of the Laurent series α
$\|\alpha\|$	the norm of a Laurent series α
O_q	the subring of L_q whose elements have norm ≤ 1
P_q	the ideal of O_q whose elements have norm < 1
$[\,a_0; a_1, \ldots, a_m\,]$	a continued fraction with partial quotients $a_0, \ldots, a_m$
$K(f/g)$	the degree of the largest partial quotient in the continued fraction expansion of f/g
$m(g)$	the orthogonal multiplicity of polynomial g
M_g	the set of all f/g with $K(f/g) = 1$ and $\deg f < \deg g$
$w = a_1 \ldots a_m$	a word over the alphabet of non-constant polynomials in $\mathbb{F}_q[x]$
$\overleftarrow{w}$	the reversed word $a_m a_{m-1} \ldots a_1$
$[\,w\,]$	the continued fraction $[\,0; a_1, a_2, \ldots, a_m\,]$
$\#(A)$	the cardinality of a set A
$CF(A)$	the set of all continued fractions in P_q which have partial quotients in $A \subseteq \mathbb{F}_q[x]$
S	a sequence $\{s_i\}_{i \geq 1}$
s	its associated Laurent series $\sum_{i \geq 1} s_i x^{-i}$
$l_n(S)$	the nth linear complexity of S
P_f	the Newton Polytope of a multivariate polynomial f
$Q + R$	the Minkowski sum of sets $Q, R \subseteq \mathbb{R}^k$

Chapter 1

Introduction

To explain the contents of this thesis with the minimum of technical language it is easiest to begin by drawing out a relevant analogy. There are some rational numbers with large denominators which may be approximated very closely by other numbers with much smaller denominators. Consider for example the fraction $\frac{11}{34}$. It is very close to the number $\frac{1}{3}$, as a simple subtraction will reveal, but has a much larger denominator. Similarly, there are irrational real numbers which may be closely approximated by relatively simple rational numbers. A famous example is "Liouville's number" ([39]) which is of the form

$$\sum_{k=1}^{\infty} m^{-k!}$$

where m is an integer at least 2. Liouville showed that there is a bound on how closely an algebraic real number may be approximated by an infinite sequence of rational numbers. Observing that the infinite sequence of rational numbers obtained by truncating the above series after a finite number of terms breaks this bound, Liouville deduced that the above number was transcendental. Of equal interest are rational numbers with large denominators which are very difficult to approximate by other rational numbers with smaller denominators. One may check that the rational number with smallest denominator which is as least as close to $\frac{21}{34}$ as $\frac{1}{3}$ is to $\frac{11}{34}$, is $\frac{5}{8}$. Similarly, there are irrational numbers which are difficult to approximate by rational numbers. The most difficult to approximate irrational number of all, which lies between the integers 1 and 2, is the "golden ratio" $\frac{1+\sqrt{5}}{2}$.

All of these ideas may be made more precise using the theory of continued fractions for real numbers. Any rational number x/y may be written as a fraction of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_m}}}}$$

where the a_j are positive integers for $1 \leq j \leq m$, and a_0 is an integer. This expression is unique if we further insist that a_m is at least 2. It is called the continued fraction expansion of x/y, and the integers a_j are known as the partial quotients of x/y. Any irrational number may be written in a similar way, only we require an infinite number of partial quotients. The continued fraction expansion of a rational number may be computed by applying the Euclidean Algorithm to the integers x and y. For example, the continued fraction expansion of $\frac{11}{34}$ has partial quotients $0, 3, 11$, while that of $\frac{21}{34}$ has partial quotients $0, 1, 1, 1, 1, 1, 1, 2$. The 0th partial quotient simply tells us between which integers on the number line the fraction lies, but the remaining partial quotients are of far greater interest. For they reveal how easy or difficult it is to approximate that rational number with other rational numbers whose denominators are smaller. If any of these partial quotients is large relative to the denominator of the fraction then one may conclude that the fraction is easy to approximate. This is the case for $\frac{11}{34}$. However, if all of these partial quotients are small, as with $\frac{21}{34}$, then the rational number is difficult to approximate. Although continued fractions of real numbers have been studied by mathematicians for centuries, there are still many fundamental questions related to them which remain unanswered. For example, investigating a method for numerical integration Zaremba was led to consider the following problem ([47]). For any positive integer y, does there exist a coprime integer x such that x/y is difficult to approximate? We review what is known on this conjecture at the start of Chapter 3. A much older challenge for real numbers is that of exhibiting, or proving a non-trivial fact about, the continued fraction expansion of an algebraic number. The only theorem along these lines is the famous result of Roth which asserts that the partial quotients a_j of an algebraic number cannot grow too fast in magnitude as j tends to infinity ([38]). It is, however, conjectured that the partial quotients of an algebraic real number are unbounded.

One may generalise the theory of continued fraction expansions of real numbers in many different directions. Arguably the most natural way is to replace the field of rational numbers by a field of rational functions, and consider analogous questions. In this context, the role of the real numbers is played by formal power series, known as Laurent series. In this thesis we study how one may approximate rational functions by other rational functions whose denominators have smaller degree, and more generally, how one may approximate irrational Laurent series by rational functions. The rational functions and Laurent series we consider are defined over finite fields. The main tool in our investigation is the theory of continued fractions of Laurent series over finite fields, which we fully develop in Chapter 2. The central two themes which we follow are the study of rational functions which are difficult to approximate, and the continued fraction expansions of Laurent series which are algebraic over the subfield of rational functions. We consider a rational function analogue of Zaremba's question in Chapters 3, 4 and 7. In Chapters 5 and 6 we construct algebraic Laurent series which have partial quotients of bounded degree and may therefore be considered difficult to approximate.

Questions on the approximation of Laurent series are not only of mathematical interest, but can be motivated by the study of pseudorandom sequences over finite fields. Any sequence may be encoded as a Laurent series. The linear complexity profile of a sequence reveals how easy or difficult it is to generate initial segments of the sequence by short linear recurrences. The profile of a given sequence may be read off from the continued fraction expansion of the Laurent series which encodes it. Sequences with desirable linear complexity profiles from a cryptographic point of view correspond to Laurent series which are difficult to approximate. In this thesis, our primary aim is to prove original results on the approximation properties of Laurent series, but we shall interpret our results in terms of sequences whenever it is appropriate.

This thesis also touches upon some important algorithmic problems in the study of polynomials over finite fields in Chapters 7 and 8. Chapter 7 is closely related to the preceding work on rational functions, although Chapter 8 is largely independent of the rest of the thesis.

We now present a breakdown of the contents of the thesis, chapter by chapter.

Chapter 2 lays in place the foundations upon which this thesis is built. The presentation is distilled from many different sources, and in most cases has been adapted from the number field setting. The discussion of the construction of the field of Laurent series is inspired chiefly by the analogous construction of the p-adic field given in Neal Koblitz's beautifully written book on that topic ([18]). The description of the theory of continued fractions is based upon that given for real numbers in the recently published book of Rockett and Szüsz ([37]), and on the classic text of Khinchin ([17]). Once this background theory has been developed, the application to sequences in the final section follows easily. As throughout the thesis, illustrative examples have been interwoven into the text, adding colour to the pattern of definitions, theorems and proofs. Great care has been taken to make Chapter 2 as comprehensive and independent as possible, and the author hopes it will serve as an accessible introduction to this area, as there does not appear to be any other comparable exposition on this topic in the literature.

Chapter 3 introduces the first main theme of this thesis: the study of rational functions which are difficult to approximate. A rational function is said to be badly approximable if all the partial quotients in its continued fraction expansion have degree 1. The orthogonal multiplicity of a polynomial is the number of badly approximable rational functions in reduced form which have that polynomial as their denominator. This chapter describes the existing work which has been done on badly approximable rational functions. Particular attention is paid to Blackburn's results for rational functions over the binary field ([6]), and a slightly modified presentation of these results is given, including some modest generalisations. This new presentation is needed in Chapter 7, where we consider some algorithmic questions related to badly approximable rational functions.

Chapter 4 further develops the theme introduced in the preceding one, and is the first chapter to contain significant new work. The chapter is based upon the author's published paper ([19]) and the contents are entirely original. The main result is a characterisation of polynomials with odd orthogonal multiplicity. A lower bound on the multiplicity of such polynomials is also obtained, and several other related results are proved.

Chapter 5 introduces the second main theme of this thesis: the study of the continued fraction expansions of Laurent series which are algebraic over the subfield of rational functions, and are difficult to approximate. The contents of two papers of Baum and Sweet are presented ([4, 5]). The main result of the latter of these two papers is generalised in the following chapter.

Chapter 6 is the most technically involved of the thesis and the contents are completely original. It is based upon a paper by the author ([20]) which has been accepted for publication. The main theorem is a generalisation of a well-known and important result of Baum and Sweet on badly approximable binary power series. Some applications to the study of the linear complexity profiles of sequences are also presented.

Chapter 7 is one of the shorter chapters of the thesis. In this chapter some original but far from profound results on algorithmic problems related to badly approximable rational functions are gathered. It also serves as a bridge between the preceding chapters on rational functions, and the final chapter on algorithms for multivariate polynomials.

Chapter 8 is something of an impostor — a large grey egg in a nest full of small white ones — although a link is forged with the main work of this thesis in the preceding chapter. Nevertheless, it is most appropriately seen as lying outwith the central themes of the thesis, fitting roughly within the wider theme of polynomials over finite fields. The chapter contains a new absolute irreducibility testing algorithm for bivariate polynomials, and some original absolute irreducibility criteria. It is elementary in nature and provides a gentle conclusion to the thesis; perhaps a welcome tonic to the technical intricacies of Chapter 6.

We conclude this opening chapter with a discussion of the rather idiosyncratic way in which results are labelled in this thesis. The most significant results are dignified with the title "Theorem". Such results are substantial and entirely original in nature. Next in importance are the "Propositions". Propositions are usually original results, the only exception being Proposition 2.25 which apparently has not appeared in its full form in the literature before and is of such importance that it has been elevated to this rank, but their proofs are less involved. Of slightly lower rank are the "Lemmas" and "Corollaries", which are also mainly original. Finally, the great mass of background results which are presented in Chapters 2, 3 and 5 are referred to simply as "Results", and are usually not original, although the proofs given are in many cases the author's own.

Chapter 2

The Key Concepts

2.1 Introduction

This chapter falls into three parts. In Section 2.2 the field of Laurent series is introduced and its fundamental properties are outlined. Section 2.3 contains a detailed description of the theory of continued fractions for this field, and finally, in Section 2.4 we explain how this theory is intimately connected with the study of the linear complexity profiles of sequences.

2.2 Rational Functions and Laurent Series

Let p be a prime number, and $q = p^e$ where $e \in \mathbb{N}$. Let $\mathbb{F}_q$ denote the unique finite field of order q ([23]). So $\mathbb{F}_q$ has characteristic p. The polynomial ring in the indeterminate x over $\mathbb{F}_q$ is written $\mathbb{F}_q[x]$. This ring is an integral domain and we denote its quotient field by $\mathbb{F}_q(x)$. This field is known as the field of rational functions, or sometimes just the rational field, and it is the smallest field in which $\mathbb{F}_q[x]$ lies. One may extend the field $\mathbb{F}_q(x)$ using an analytical method which mimics the construction of the field of real numbers from the field of rational numbers. The field constructed in this way is called the field of Laurent series in x^{-1} over $\mathbb{F}_q$. This remarkable field has many nice analytic and algebraic properties, and is the appropriate backdrop for our work on continued fractions and sequences.

Section 2.2 of this chapter is laid out in the following manner. In Section 2.2.1 we present the necessary background from algebra and analysis. Section 2.2.2 introduces a notion of size on the rational field which we use in Section 2.2.3 to define the field of Laurent series. Finally, in Section 2.2.4 we discuss some algebraic properties of this field which shall be of interest to us.

2.2.1 Norms, Exponential Valuations, and Completions

Let R be a commutative ring with an identity. A **norm (or valuation)** on R is a mapping $|\,|$ from R to the non-negative real numbers such that

$$\begin{aligned} |r| &= 0 \text{ if and only if } r = 0 && (2.1)\\ |rs| &= |r||s| \text{ for all } r, s \in R && (2.2)\\ |r+s| &\leq |r| + |s| \text{ for all } r, s \in R && (2.3) \end{aligned}$$

The final condition is known as the triangle inequality. We call a norm non-trivial if $|r| \neq 0, 1$ for some $r \in R$. If a norm also satisfies the stronger conditions

$$\begin{aligned} |r+s| &\leq \max\{|r|, |s|\} \text{ for all } r, s \in R && (2.4) \\ |r+s| &= \max\{|r|, |s|\} \text{ for all } r, s \in R \text{ with } |r| \neq |s| && (2.5) \end{aligned}$$

then we say that it is **non-Archimedean**. Property (2.4) is called the ultrametric triangle inequality, and one may show in fact that Property (2.5) is a consequence of Properties (2.2) and (2.4). However, it is convenient for us to explicitly state this final property, as we shall frequently make use of it.

Example 2.1 (Norms on the field of rational numbers $\mathbb{Q}$.) The most familiar example of a norm on $\mathbb{Q}$ is the absolute value norm, which we denote $|\,|_\infty$. This norm does not satisfy the ultrametric triangle inequality, as is seen from

$$|1+1|_\infty = |2|_\infty = 2 > \max\{|1|_\infty, |1|_\infty\}.$$

This is an example of an **Archimedean** norm. It is not, however, the only norm which may be defined on $\mathbb{Q}$, as we now explain. For each prime p in $\mathbb{Z}$, define the map $|\,|_p$ from $\mathbb{Q}$ to the non-negative real numbers in the following way: Let $z \in \mathbb{Z}$ with $z \neq 0$. Define $\text{ord}_p(z)$ to be the highest power of p which divides z and let $|z|_p = (1/p)^{ord_p(z)}$. Now extend this mapping to all rational numbers by letting $|x/y| = |x|/|y|$ where $x, y \in \mathbb{Z}$ with $x, y \neq 0$, and $|0|_p = 0$. One may verify that $|\,|_p$ is a non-Archimedean norm on $\mathbb{Q}$. A theorem of Ostrowski ([18, page 3]) tells us that $|\,|_\infty$ and $|\,|_p$, p a prime, are the only non-trivial norms on $\mathbb{Q}$.

Let $|\,|$ be a non-Archimedean norm on a ring R. Choose $c \in \mathbb{R}$ with $0 < c < 1$. For each non-zero $r \in R$, define $v(r) = \log_c |r|$. Let $v(0) = -\infty$. Then v is a mapping from R to the extended real numbers $\mathbb{R} \cup \{-\infty\}$. It is called the **exponential valuation** associated with $|\,|$. It possesses similar properties to $|\,|$, namely

$$\begin{aligned} v(r) &\in \mathbb{R} \text{ if and only if } r \text{ is non-zero} && (2.6) \\ v(rs) &= v(r) + v(s) \text{ for all } r, s \in R && (2.7) \\ v(r+s) &\geq \min\{v(r), v(s)\} \text{ for all } r, s \in R && (2.8) \\ v(r+s) &= \min\{v(r), v(s)\} \text{ for all } r, s \in R \text{ with } v(r) \neq v(s) && (2.9) \end{aligned}$$

Conversely, given any map v on R which satisfies the above four conditions, we may construct a non-Archimedean norm $|\,|$ on R: Choose some $c \in \mathbb{R}$ with $0 < c < 1$ and let $|r| = c^{v(r)}$ for $r \neq 0$, and $|0| = 0$. For example, the exponential valuation associated with $|\,|_p$ on $\mathbb{Q}$ in Example 2.1 is the map ord_p.

Now let K be a field on which is defined a norm $|\,|$. A **Cauchy sequence** is a sequence $\{c_i\}_{i \geq 1}$ of elements of K with the property that for any real number $\varepsilon > 0$, there exists $N \in \mathbb{N}$, such that $|c_i - c_j| < \varepsilon$ for all $i, j \geq N$. We say that an arbitrary sequence $\{d_i\}_{i \geq 1}$ of elements of K has a **limit** in K if there exists $d \in K$ such that $\lim_{i \to \infty} |d - d_i| = 0$. Finally, we say that K is **complete** with respect to $|\,|$ if any Cauchy sequence in K has a limit in K. Given a norm $|\,|$ on a field K one may construct a field L which is complete with respect to $|\,|$ and contains K. The field L is called the **completion** of K with respect to $|\,|$, and it is the smallest complete field in which K lies. We do not give the details of this construction, but essentially one considers the ring of all Cauchy sequences of K with respect to the norm $|\,|$, and factors out the ideal of all null sequences (Cauchy sequences which have 0 as a limit). A fuller description of the number field case can be found in [18, Page 10-11].

Example 2.2 (Completions of $\mathbb{Q}$.) The completion of $\mathbb{Q}$ with respect to $|\,|_\infty$ is the field of real numbers $\mathbb{R}$. If one completes $\mathbb{Q}$ with respect to $|\,|_p$ for some prime p, one obtains the p-adic field $\mathbb{Q}_p$ ([18, Chapter 1]).

2.2.2 A Norm on the Field of Rational Functions

In this section, we define an exponential valuation on $\mathbb{F}_q(x)$ which in a sense extends the degree map on $\mathbb{F}_q[x]$, and study the norm associated with it.

Definition 2.3 *Let $a, b \in \mathbb{F}_q[x]$ with $b \neq 0$. The exponential valuation v on $\mathbb{F}_q(x)$ maps a/b to $\deg b - \deg a$, and 0 to $-\infty$.*

It is easily verified that v is a well defined map on $\mathbb{F}_q(x)$, and is indeed an exponential valuation.

Definition 2.4 *For $r \in \mathbb{F}_q(x)$ with $r \neq 0$, define $|r| = (1/q)^{v(r)}$. Let $|0| = 0$. So $|\,|$ is the non-Archimedean norm on $\mathbb{F}_q(x)$ associated with the exponential valuation v.*

Thus for a nonzero rational function f/g where f and g are polynomials, $|f/g| = (1/q)^{\deg g - \deg f} = q^{\deg f - \deg g}$. The choice of $1/q$ as the base for converting from the norm to the exponential valuation is somewhat arbitrary, although it does yield a nice "product formula" in a certain context, as we explain in Example 2.6.

Note 2.5 It may appear rather topsy-turvy that for a polynomial f we define $v(f)$ to be the negative of the degree of f, rather than $\deg f$ itself. We do this because, in the parlance of algebraic geometry, we are looking at "the localisation of $\mathbb{F}_q(x)$ at the prime x^{-1}", and consequently we are interested in the "degree of f relative to x^{-1}", which is $-\deg f$. We shall work with the norm $|\,|$ associated with v in most cases, and so the reader may think of $|f|$ as $q^{\deg f}$, and often forget about v altogether.

We observe in the next example that although this is the only norm on the field $\mathbb{F}_q(x)$ which will be of serious interest to us, one can define other norms.

Example 2.6 (Norms on the field $\mathbb{F}_q(x)$.) Associated with every irreducible polynomial $d(x)$ in $\mathbb{F}_q[x]$ there is an exponential valuation $\mathrm{ord}_{d(x)}$ from which one may construct a non-Archimedean norm $|\,|_{d(x)}$: Let f be a non-zero polynomial and define $\mathrm{ord}_{d(x)}(f)$ to be the highest power of $d(x)$ which divides f. For $f, g \in \mathbb{F}_q[x]$ with $f, g \neq 0$ define

$$|f/g|_{d(x)} = (1/q^{\deg d})^{ord_{d(x)}(f) - ord_{d(x)}(g)},$$

and let $|0|_{d(x)} = 0$. One may show that the only non-trivial norms on $\mathbb{F}_q(x)$ are norms of the form $|\,|_{d(x)}$ and the "degree" norm $|\,|$ ([3, page 13-14]). This latter norm is sometimes denoted $|\,|_\infty$ because of a connection with the point of infinity on the projective line. Observe that we have the product formula

$$|a|_\infty \prod_{d(x) \in I_q} |a|_{d(x)} = 1.$$

Here $a \in \mathbb{F}_q(x)$ with $a \neq 0$, and I_q denotes the set of all irreducible polynomials in $\mathbb{F}_q[x]$.

2.2.3 The Construction of the Field of Laurent Series

Having completed our preliminary discussion on the field $\mathbb{F}_q(x)$, we now turn our attention to the field of Laurent series. At this juncture, there are two paths which may be taken. One may formally construct the completion of $\mathbb{F}_q(x)$ with respect to the norm $|\,|$, and then show that every element in this new field has a Laurent series expansion. This longer path is followed in [18]. However, we choose the shorter path, and instead explicitly define a ring of Laurent series, and show that this ring is a complete field, and that one may embed $\mathbb{F}_q(x)$ in this field.

Definition 2.7 *Let q be a prime power. The ring L_q is given by*

$$L_q = \left\{ \sum_{i=n}^{\infty} s_i x^{-i} \mid s_i \in \mathbb{F}_q, n \in \mathbb{Z} \right\}.$$

The addition and multiplication laws in L_q are straightforward and we do not describe them. It is easily seen that L_q is a commutative ring with an identity, although it is not immediately obvious that every non-zero element in the ring L_q has an inverse. This and other basic properties of L_q are proved in Result 2.8.

Before we can state and prove this result, however, we must define a valuation v_L and non-Archimedean norm $|\,|_L$ on L_q. If $s \in L_q$ with $s = \sum_{i \geq n} s_i x^{-i}$ where $s_n \neq 0$ then we let $v_L(s) = n$ and $|s|_L = (1/q)^n = q^{-n}$. Let $v_L(0) = -\infty$ and $|0|_L = 0$. So v can be thought of as telling you the negative of the "degree" of a Laurent series. Once again, it is easy to verify that v_L and $|\,|_L$ satisfy the appropriate properties. In fact, the maps v_L and $|\,|_L$ extend the exponential valuation v and norm $|\,|$ defined on $\mathbb{F}_q(x)$, as we now show.

Result 2.8 *The ring L_q is a field, with $\mathbb{F}_q[x] \subseteq \mathbb{F}_q(x) \subseteq L_q$. The exponential valuation v_L when restricted to the subfield $\mathbb{F}_q(x)$ of L_q is the map v. Similarly, by restricting $|\,|_L$ to $\mathbb{F}_q(x)$ we obtain the norm $|\,|$. The field L_q is complete with respect to the non-Archimedean norm $|\,|_L$. In fact, L_q is the completion of $\mathbb{F}_q(x)$ with respect to $|\,|$.*

Proof: We first show that L_q is a field. It is easily seen that L_q is a commutative ring with an additive identity 0 and multiplicative identity 1. It therefore only remains to show that every non-zero element in L_q has a multiplicative inverse. Let $s = \sum_{i \geq n} s_i x^{-i}$ with $s_n \neq 0$. Then $s = s_n x^{-n} \alpha$ where α has leading term x^0. We show that α is invertible in L_q. Write $\alpha = \sum_{i \geq 0} \alpha_i x^{-i}$ where $\alpha_0 = 1$. Define the sequence β_i $(i \geq 0)$ by

$$\begin{aligned} \beta_0 &= 1 \\ \beta_i &= -(\textstyle\sum_{j=1}^{i} \alpha_j \beta_{i-j}) \quad \text{for } i \geq 1. \end{aligned}$$

Letting $\beta = \sum_{i \geq 0} \beta_i x^{-i}$ we see that $\alpha\beta = 1$. Hence $s(s_n^{-1} x^n \beta) = 1$ as required.

We now show that L_q contains copies of both $\mathbb{F}_q[x]$ and $\mathbb{F}_q(x)$. Identify $\mathbb{F}_q[x]$ with the subring of L_q consisting of those elements of the form $\sum_{n \leq i \leq 0} s_i x^{-i}$, where $s_i \in \mathbb{F}_q$ and $n \leq 0$. This gives an embedding of $\mathbb{F}_q[x]$ in L_q, as is readily verified. Since $\mathbb{F}_q[x] \subseteq L_q$ and L_q is a field, we know that L_q must contain the field of fractions $\mathbb{F}_q(x)$ of $\mathbb{F}_q[x]$. We may describe this embedding explicitly: Let $f, g \in \mathbb{F}_q[x]$ with $g \neq 0$ and consider the rational function f/g. We may assume by cancelling leading coefficients that g is monic. Write $f = \sum_{i \geq m} f_i x^{-i}$ and $g = \sum_{i \geq n} g_i x^{-i}$ where $f_m \neq 0$ and $g_n = 1$. Observe that $f_i, g_i = 0$ for $i > 0$. Define the sequence s_i for $i \geq m - n$ by

$$\begin{aligned} s_{m-n} &= f_m \\ s_{m-n+k} &= f_{m+k} - \textstyle\sum_{j=1}^{k} g_{n+j} s_{m-n+(k-j)} \quad \text{for } k > 0. \end{aligned}$$

Let $s = \sum_{i \geq m-n} s_i x^{-i}$. Then one may verify that $f = sg$ in L_q. Thus we may identify f/g with s. This gives an embedding of $\mathbb{F}_q(x)$ in L_q.

The next two sentences in the statement of the result are easily seen to be true by considering the definitions of $v, |\,|, v_L$ and $|\,|_L$, and the embedding of $\mathbb{F}_q(x)$ in L_q that we have just described.

It is not difficult to prove that L_q is complete: Let $\{c_j\}_{j \geq 1}$ be a Cauchy sequence in L_q with respect to $|\,|_L$. We define a Laurent series $l = \sum_{i \geq n} l_i x^{-i}$ which we claim is the limit of the sequence $\{c_j\}_{j \geq 1}$. For each natural number $k \geq n$, there is an $N_k \in \mathbb{N}$ such that $|c_i - c_{i'}|_L < q^{-k}$ for $i, i' \geq N_k$. Define l_k to the coefficient of x^{-k} in the Laurent series expansion of c_i for any $i \geq N_k$. This is well-defined by the preceding sentence, and it is easily verified that the l thus constructed is the limit of $\{c_j\}_{j \geq 1}$.

Finally, to prove that L_q is the completion of $\mathbb{F}_q(x)$ with respect to $|\,|$, we must show that it is the smallest complete field in which $\mathbb{F}_q(x)$ lies. This is easily seen. For any Laurent series $\sum_{i \geq n} s_i x^{-i}$ is the limit as $m \to \infty$ of the sequence of rational Laurent series $\{\sum_{n \leq i \leq n+m} s_i x^{-i}\}_{m \geq 0}$.

□

We call L_q the **field of Laurent series** in x^{-1} over $\mathbb{F}_q(x)$. The element s constructed in the second paragraph of the above proof is called the **Laurent series expansion** of the rational function f/g. Observe that its sequence of coefficients satisfies a linear recurrence and is therefore eventually periodic. Conversely, it is easily proved (Result 2.31) that any Laurent series whose sequence of coefficients is eventually periodic can be written as a rational function. Identifying $\mathbb{F}_q(x)$ with its image under the embedding, we call Laurent series which lie in $\mathbb{F}_q(x)$ **rational**, and those which do not **irrational**.

From now on, we shall use $|\,|$ and v to denote the exponential valuation $|\,|_L$ and norm v_L on the field L_q.

Example 2.9 We present a simple example of a rational Laurent series over the finite field $\mathbb{F}_3$. The expansion s of the rational function f/g can be verified by checking that $f = gs$ in L_3.

$$\frac{x^3 + x^2 + x + 2}{x^3 + 1} = 1 + x^{-1} + x^{-2} + x^{-3} + 2x^{-4} + 2x^{-5} + 2x^{-6} + \ldots$$

The expansion has period six and the remaining terms can be obtained by repeating the coefficients of the terms $x^{-1}, \ldots, x^{-6}$. We shall compute the initial few terms of the Laurent series expansion of a square root of this rational function in Example 2.12, thus giving our first example of an irrational Laurent series.

We conclude this section by defining the **Frobenius map** ϕ_p on the field L_q. Let $\phi_p : L_q \to L_q$ be given by

$$\alpha \mapsto \alpha^p,$$

where $\alpha \in L_q$ and $\operatorname{char} L_q = p$. It is easily verified that ϕ_p is a monomorphism on the field L_q. One useful fact we shall use in Chapter 6 is that

$$(\sum_{i=n}^{\infty} s_i x^{-i})^p = \sum_{i=n}^{\infty} s_i^p x^{-ip}. \tag{2.10}$$

This may be proved in the following manner. For all $m > n$ we have that

$$(\sum_{i=n}^{m} s_i x^{-i})^p = \sum_{i=n}^{m} s_i^p x^{-ip}. \tag{2.11}$$

This is proved by induction on $m \geq n+1$, the first case following easily from the fact that p divides $\binom{p}{i}$ for all $1 \leq i \leq p-1$. Taking limits as $m \to \infty$ on both sides of (2.11), and using the easily verified fact that the limit of a product is the product of the limits, now establishes equality (2.10).

2.2.4 The Algebraic Properties of the Field of Laurent Series

The field of Laurent series can be thought of as a positive characteristic analogue of the field of real numbers, and like the field of real numbers, it is privileged with many nice properties not shared by other fields. The next result will be of interest in Chapter 6. It is a generalisation to arbitrary positive characteristic, of a result which is proved for fields of characteristic 2 in [4, Proof of Theorem 8].

We must first of all recall a few basic ideas from field theory. An element of L_q is algebraic over $\mathbb{F}_q(x)$ if it is the root of a polynomial which has coefficients in $\mathbb{F}_q(x)$. If a Laurent series α is algebraic over $\mathbb{F}_q(x)$, we call it an **algebraic Laurent series**. In this case, there is a unique monic irreducible polynomial over $\mathbb{F}_q(x)$ of which α is a root, and this is known as the minimal polynomial of α. If the minimal polynomial of α has distinct roots in some suitably large extension field, then we say that α is a separable element. Now let K be a field extension of $\mathbb{F}_q(x)$. If every element of K is algebraic (separable respectively), then we say that K is algebraic (separable respectively).

Result 2.10 *Any algebraic extension of the field $\mathbb{F}_q(x)$ which lies in L_q is separable.*

Proof: Let K be a field such that $\mathbb{F}_q(x) \subseteq K \subseteq L_q$ and let $\alpha \in K$. Denote by $h(T) \in \mathbb{F}_q(x)[T]$ the minimal polynomial of α over $\mathbb{F}_q(x)$. Since α is an arbitrary element of K, we need to show that h has distinct roots. Let u denote the common denominator of all of the coefficients of h. Then $f := uh \in \mathbb{F}_q[x,T]$. Certainly f has distinct roots if and only if h does, and so it is enough to prove that f has distinct roots.

Suppose that f has a repeated root, β say. Then h is also the minimal polynomial of β. For any polynomial $g(T) \in \mathbb{F}_q[x,T]$ write $\deg_T g$ to denote the highest power of T which occurs in g. The derivative df/dT of f with respect to T must then be identically zero, for otherwise β is a root of df/dT which is a non-zero polynomial with $\deg_T(df/dT) < \deg_T f$, which contradicts the minimality of $\deg_T f = \deg_T h$. Thus $f(T) \in \mathbb{F}_q[x, T^p]$, where $p = \operatorname{char} \mathbb{F}_q$. Now a typical summand of f is of the form $x^n T^{pm} = x^b (x^a T^m)^p$ where $0 \leq b < p$. Gathering together all the terms whose "remainders" x^b are the same, we may write $f(T) = \sum_{i=0}^{p-1} x^i (M_i(T))^p$ where $M_i(T) \in \mathbb{F}_q[x,T]$. Observe that $M_i(\alpha) \neq 0$ since $\deg_T M_i < \deg_T f = \deg_T h$. Substituting $T = \alpha$ we have that

$$-(M_0(\alpha))^p = \sum_{i=1}^{p-1} x^i (M_i(\alpha))^p. \tag{2.12}$$

Since $\alpha \in L_q$, both sides of this equation lie in L_q and we may take exponential valuations. Now for $0 \leq i \leq p-1$

$$\begin{aligned} v(x^i(M_i(\alpha))^p) &= -i + pv(M_i(\alpha)) \\ &\equiv -i \bmod p. \end{aligned}$$

Here we use Property (2.7) of v, and the fact that $M_i(\alpha) \neq 0$ for $0 \leq i \leq p-1$ and so $v(M_i(\alpha))$ lies in $\mathbb{Z}$. Hence $v(x^i(M_i(\alpha))^p) \neq v(x^j(M_j(\alpha))^p)$ for $0 \leq i \neq j \leq p-1$. So using Property (2.9) of v

$$\begin{array}{rcl} v(\sum_{i=1}^{p-1} x^i(M_i(\alpha))^p) & = & \min\{v(x^i(M_i(\alpha))^p)\} \\ & = & \min_{1\leq i\leq p-1}\{-i + pv(M_i(\alpha))\} \\ & \not\equiv & 0 \bmod p. \end{array}$$

But $v(-M_0(\alpha)^p) = v(M_0(\alpha)^p) \equiv 0 \bmod p$. This contradicts (2.12), and so f, and hence the minimal polynomial of α, must have distinct roots, as we wished to show. □

The second result of this section is known as Hensel's Lemma, and can be thought of as an analogue of Newton's Method for computing roots of equations over $\mathbb{R}$. Before we can describe this result, we need to introduce two important subrings of L_q.

Define

$$\begin{array}{rcl} O_q & = & \{s \in L_q \,|\, |s| \leq 1\}, \\ P_q & = & \{s \in L_q \,|\, |s| < 1\}. \end{array}$$

It is easily shown that O_q is a ring and P_q an ideal of O_q. We have the natural homomorphism of rings

$$\begin{array}{rcl} O_q & \to & O_q/P_q \cong \mathbb{F}_q \\ s & \mapsto & \bar{s} \end{array}$$

where $\bar{s}$ denotes the coefficient of x^0 in s.

Result 2.11 (Hensel's Lemma) *Let $f(T) \in O_q[T]$ and denote by $\bar{f}$ its image in $(O_q/P_q)[T] \cong \mathbb{F}_q[T]$ under the natural homomorphism. If $\bar{f}(T)$ has a root a in $O_q/P_q \cong \mathbb{F}_q$ with $d\bar{f}/dT(a) \neq 0$, then $f(T)$ has a root α in O_q with $\bar{\alpha} = a$.*

Observe that given a polynomial $f(T) \in L_q[T]$, one may multiply it by a suitable power n of x to obtain a polynomial $g(T) = x^n f(T) \in O_q[T]$. Any roots of $f(T)$ are also roots of $g(T)$ and vice-versa, and so Hensel's Lemma in fact allows one to attempt to solve arbitrary algebraic equations over L_q.

A proof of Result 2.11 can be modelled on that given for the number field case in [18, page 16-17]. We content ourselves with illustrating the methods used in the proof in Example 2.12.

Example 2.12 In this example, we consider the Laurent series expansions of the square roots of the rational function over $\mathbb{F}_3$ considered in Example 2.9. Consider the polynomial

$$f(T) := T^2 - \frac{x^3 + x^2 + x + 2}{x^3 + 1}.$$

This polynomial is defined over $\mathbb{F}_3(x)$ and one may show that, since $x^3 + x^2 + x + 2$ is irreducible in $\mathbb{F}_3[x]$, $f(T)$ does not factor in $\mathbb{F}_3(x)$. However, Hensel's Lemma tells us that $f(T)$ has two roots in L_3 and so factors over L_3, as we now explain. Using Example 2.9 we can expand the constant term in $f(T)$ as a Laurent series to obtain

$$f(T) = T^2 - (1 + x^{-1} + x^{-2} + x^{-3} + 2x^{-4} + 2x^{-5} + 2x^{-6} + \ldots).$$

Reducing $f(T)$ modulo x^{-1} we have that $\bar{f}(T) \equiv T^2 - 1 \equiv (T-1)(T-2) \bmod x^{-1}$. So $\bar{f}(T)$ has two roots, $a = 1$ and $b = 2$ say, in $O_3/P_3 \cong \mathbb{F}_3$. Now $d\bar{f}/dT = 2T$ and so $d\bar{f}/dT(1) = 2 \neq 0$ and $d\bar{f}/dT(2) = 1 \neq 0$. Thus $f(T)$ satisfies the conditions of Hensel's Lemma for both a and b, and so there exist elements α and β such that $f(\alpha) = f(\beta) = 0$, and $\alpha \equiv a \equiv 1 \bmod x^{-1}$, $\beta \equiv b \equiv 2 \bmod x^{-1}$.

We can say more. For the proof of Hensel's Lemma is constructive and allows us to compute as many of the initial terms in the Laurent series expansions of the roots of $f(T)$ as we please. We demonstrate this for α.

Let $\alpha = \sum_{i\geq 0} a_i x^{-i}$. Then $a_0 = 1$ and we have

$$\begin{aligned} 1 + x^{-1} &\equiv \alpha^2 \bmod x^{-2} \\ &\equiv (a_0 + a_1 x^{-1})^2 \bmod x^{-2} \\ &\equiv a_0^2 + 2a_0 a_1 x^{-1} \bmod x^{-2}. \end{aligned}$$

Putting $a_0^2 = 1$ we get the equation

$$x^{-1} \equiv 2a_0 a_1 x^{-1} \bmod x^{-2},$$

which is the same as

$$1 \equiv 2a_0 a_1 \bmod x^{-1}.$$

Since $d\bar{f}/dT(a_0) \equiv 2a_0 \not\equiv 0 \bmod x^{-1}$, we can solve this equation to get $a_1 = 2$. To uncover the values of the coefficients $a_2, a_3, \ldots$ we look at the equation $f(T) = 0$ modulo successively higher powers $x^{-3}, x^{-4}, \ldots$. At each stage, we are presented with a linear equation modx^{-1}, which we can solve since $d\bar{f}/dT(a_0) \not\equiv 0 \bmod x^{-1}$. Thus solving the above quadratic equation in L_3 reduces to solving an initial quadratic equation in $\mathbb{F}_3$, and then solving a succession of linear ones in $\mathbb{F}_3$. Following this method we find that

$$\alpha = 1 + 2x^{-1} + 2x^{-3} + x^{-5} + 2x^{-7} + 2x^{-8} + x^{-9} + 2x^{-10} + 2x^{-11} + 2x^{-12} + \ldots$$

The next example of this section is the first of a series of examples on a single theme which illustrate an important point discussed in Chapter 5.

Example 2.13 Let $z_c = c + \sum_{i=0}^{\infty} x^{-p^i} \in L_q$, where char $\mathbb{F}_q = p$ and $c \in \mathbb{F}_p$. Then it is easily seen from our discussions on the Frobenius map that $\phi_p(z_c) = z_c^p = z_c - x^{-1}$ and hence $z_c^p - z_c + x^{-1} = 0$. Thus z_c is algebraic over L_q of degree not greater than p. In fact we can say more. For the equation

$$T^p - T + x^{-1} \tag{2.13}$$

over $\mathbb{F}_q(x)$ factors as $\prod_{c=0}^{p-1}(T - z_c)$ in L_q. This tells us that the equation is irreducible over $\mathbb{F}_q(x)$, as we now explain. If $f \in \mathbb{F}_q(x)[T]$ is monic and divides $T^p - T + x^{-1}$ then $f = \prod_{c\in J}(T - z_c)$ where $J \subseteq \{0, 1, \ldots, p-1\}$. The coefficient of $T^{\#(J)-1}$ in f is $\sum_{c\in J} z_c = (\sum_{c\in J} c) + \#(J)z_0$. Since f is defined over $\mathbb{F}_q(x)$, this coefficient must lie in $\mathbb{F}_q(x)$, which implies that $\#(J)z_0 \in \mathbb{F}_q(x)$. Now $z_0 \notin \mathbb{F}_q(x)$ since its Laurent series expansion is not eventually periodic. Hence we must have that $\#(J) \equiv 0 \bmod p$. Thus either $j = \emptyset$ and $f = 1$, or $J = \{0, 1, \ldots, p-1\}$ and $f = T^p - T + x^{-1}$. So each irrational Laurent series z_c has $T^p - T + x^{-1}$ for its minimal polynomial, and therefore has exact degree p as an algebraic element over $\mathbb{F}_q(x)$.

We will return to this example in Example 2.13 of Section 2.3.4 in which we will consider the continued fraction expansion of $z := z_0 = \sum_{i=0}^{\infty} x^{-p^i}$. Following Mahler, we will then see in Chapter 5 that the properties of z imply that a version of Liouville's theorem in positive characteristic is sharp.

2.3 Continued Fractions

The theory of continued fractions of rational functions and Laurent series proceeds in parallel with that for rational numbers and real numbers, and is simpler in many places. To give a completely rigorous presentation, one must first discuss the rational function case, before proceeding to general Laurent series. We begin by defining a general continued fraction, and describing how one may associate a unique such continued fraction with each rational function.

Section 2.3 is arranged in the following way. In Section 2.3.1 we give the most general definition of a finite continued fraction which we shall need, and outline the fundamental properties of such continued fractions. Section 2.3.2 describes the connection between simple continued fractions and rational functions, and we widen the net in Section 2.3.3 to encompass irrational Laurent series and infinite continued fractions. With the basic ideas in place, we then present the central idea of a best approximation in Section 2.3.4, and cement the whole structure together with Proposition 2.25, which is arguably the most important result in the theory of continued fractions.

2.3.1 General Continued Fractions

The most general definition of a "continued fraction" which we give is not a standard definition, but rather is tailored to our purposes. (Note that our general "continued fractions" only play an auxiliary role in defining and manipulating simple and infinite continued fractions, and our definitions of these latter more important continued fractions are standard.)

Definition 2.14 *A* ***continued fraction*** *in the field* L_q *is an expression of the form*

$$a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots + 1/a_m))),$$

where $a_j \in \mathbb{F}_q[x]$ *for* $0 \leq j \leq m-1$ *with* $\deg a_j \geq 1$ *for* $1 \leq j \leq m-1$*. Also,* $a_m \in L_q$ *with* $|a_m| > 1$*.*

The freedom to choose the final entry a_m in the continued fraction to be any Laurent series such that $|a_m| > 1$ will allow use to manipulate both simple continued fractions in Section 2.3.2 and infinite ones in Section 2.3.3.

We denote such an expression by

$$[\, a_0\, ; a_1, a_2, \ldots, a_m\,].$$

For $-1 \leq j \leq m$, define Laurent series f_j and g_j recursively by

$$\begin{array}{llll} f_{-1} = 1, & f_0 = a_0, & f_j = a_j f_{j-1} + f_{j-2}, & \text{for } 1 \leq j \leq m, \\ g_{-1} = 0, & g_0 = 1, & g_j = a_j g_{j-1} + g_{j-2}, & \text{for } 1 \leq j \leq m. \end{array} \tag{2.14}$$

Then

Result 2.15 *For any* $0 \leq j \leq m$

1. $f_j/g_j = [\, a_0; a_1, a_2, \ldots, a_j\,]$.
2. $f_j g_{j-1} - f_{j-1} g_j = (-1)^{j-1}$.
3. $|g_j| = \prod_{k=1}^{j} |a_k|$ *(here* $j > 1$*).*

4. $|(f_k/g_k) - (f_j/g_j)| = 1/|g_j||g_{j+1}|$ *for* $j < k \le m$.

Proof: We shall prove that $f_j/g_j = [\, a_0; a_1, a_2, \ldots, a_j \,]$ by induction on j. Observe that if $j = 0$ or 1 the result is true. So suppose $j > 1$. We may write

$$[\, a_0; a_1, a_2, \ldots, a_j \,] = [\, a_0; a_1, \ldots, a_{j-2}, \zeta_{j-1} \,],$$

where $\zeta_{j-1} = a_{j-1} + (1/a_j)$. Observe that $|\zeta_{j-1}| > 1$ since $1/|a_j| < 1$ and $|a_{j-1}| > 1$. By induction, we may assume that this latter continued fraction equals

$$\frac{\zeta_{j-1} f_{j-2} + f_{j-3}}{\zeta_{j-1} g_{j-2} + g_{j-3}}.$$

Substituting $\zeta_{j-1} = a_{j-1} + (1/a_j)$ we see that this reduces to f_j/g_j.

We now prove that $f_j g_{j-1} - f_{j-1} g_j = (-1)^{j-1}$. This is easily verified for $j = 0$. For $0 < j \le m$ we have

$$\begin{aligned} f_j g_{j-1} - f_{j-1} g_j &= (a_j f_{j-1} + f_{j-2}) g_{j-1} - f_{j-1}(a_j g_{j-1} + g_{j-2}) \\ &= f_{j-2} g_{j-1} - f_{j-1} g_{j-2} \\ &= (-1)^{j-1}. \end{aligned}$$

Part 3 follows easily from the recurrences (2.14) which defines g_j.

To prove the Part 4, observe that $f_k/g_k = [\, a_0; a_1, \ldots, a_j, \zeta_{j+1} \,]$ where $\zeta_{j+1} = [\, a_{j+1}; a_{j+2}, \ldots, a_k \,]$. Therefore

$$\frac{f_k}{g_k} = \frac{\zeta_{j+1} f_j + f_{j-1}}{\zeta_{j+1} g_j + g_{j-1}}.$$

Hence

$$\begin{aligned} |f_k/g_k - f_j/g_j| &= 1/|(\zeta_{j+1} g_j + g_{j-1}) g_j| \\ &= 1/|a_{j+1}||g_j|^2 \\ &= 1/|g_j||g_{j+1}|. \end{aligned}$$

Here we use the identity $f_{j-1} g_j - g_{j-1} f_j = (-1)^j$, and the fact that $|g_j| > |g_{j-1}|$, $|\zeta_{j+1}| = |a_{j+1}|$ and $|a_j||g_j| = |g_{j+1}|$.

□

2.3.2 Simple Continued Fractions and Rational Functions

We shall mainly be interested in a particular type of continued fraction known as a **simple continued fraction**, although it is extremely useful to be able to work with continued fractions of a more general form when proving results on simple continued fractions. In a simple continued fraction $[\, a_0; a_1, a_2, \ldots, a_m \,]$ we have that $a_j \in \mathbb{F}_q[x]\,(0 \le j \le m)$, with $\deg a_j \ge 1$ for $1 \le j \le m$. Thus simple continued fractions lie in $\mathbb{F}_q(x)$. In this case, both f_j and g_j for $-1 \le j \le m$ as defined above are polynomials. For $0 \le j \le m$, the polynomial a_j is called the **jth partial quotient** of $[\, a_0\,; a_1, \ldots, a_m]$ and the rational function f_j/g_j is called the **jth convergent**.

Part 3 of Result 2.15 tells us that $\deg g_j = \sum_{1 \le k \le j} \deg a_k$ for $1 \le j \le m$. We also have

Result 2.16 *If* f_j/g_j *is the* j*th convergent to* $f/g = [\, a_0; a_1, a_2, \ldots, a_m \,]$ *then for* $0 \le j \le m-1$,

$$\begin{aligned} |(f/g) - (f_j/g_j)| &= 1/|g_j||g_{j+1}| \\ &= 1/|a_{j+1}||g_j|^2. \end{aligned}$$

This result is just a restatement of Part 4 of Result 2.15, using Part 3 to obtain the second equality.

We have seen that a simple continued fraction is just a rational function presented in a rather curious way. In fact, any rational function f/g may be written as a simple continued fraction by applying the Euclidean Algorithm for polynomials to f and g, as we now explain. First observe that we may assume f and g are coprime, for otherwise we can cancel factors. Applying the Euclidean Algorithm we obtain

$$\begin{array}{rcl} f & = & a_0 g + r_0 \\ g & = & a_1 r_0 + r_1 \\ r_0 & = & a_2 r_1 + r_2 \\ r_1 & = & a_3 r_2 + r_3 \\ \vdots & \vdots & \vdots \\ r_{m-3} & = & a_{m-1} r_{m-2} + r_{m-1} \\ r_{m-2} & = & a_m r_{m-1}. \end{array}$$

In anticipation of what follows, we call the polynomials a_j the partial quotients of f/g, and the polynomials r_j are known as the **partial remainders**. Observe that $\deg r_j < \deg r_{j-1}$ for $1 \leq j \leq m-1$ and so, by comparing the degrees of the lefthand side and the righthand side in the $(j+1)$th equation in the list, we see that $\deg a_j \geq 1$ for $1 \leq j \leq m$. Also, since f and g are coprime, we have that $r_{m-1} \in \mathbb{F}_q{}^*$.

We may now recover a continued fraction which is equal to f/g from the above list of polynomials. Dividing the first equation through by g we see

$$f/g = a_0 + 1/(g/r_0).$$

The rational function g/r_0 may be written as $a_1 + 1/(r_0/r_1)$ from the second equation in the list. Continuing in this way we find that

$$f/g = a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots + 1/a_m))).$$

Thus we have written f/g as a continued fraction.

We now present a formal proof that we can write any rational function as a continued fraction, and further observe that it may be done in a unique way.

Result 2.17 *For every rational function f/g there is a unique simple continued fraction to which it is equal.*

Proof: Let f/g be a rational function. We may assume that it is in reduced form i.e. f and g are coprime. We argue by induction on the degree of the denominator that any rational function in reduced form may be written in a unique way as a simple continued fraction. Any rational function whose denominator has degree zero can certainly be written as a simple continued fraction in a unique way. Suppose then that $\deg g \geq 1$. We may write $f = a_0 g + r_0$ where $0 \leq \deg r_0 < \deg g$. Observe that g and r_0 have no common factors. Therefore, by induction we may assume that g/r_0 can be written uniquely as a simple continued fraction. Now $f/g = a_0 + 1/(g/r_0)$, and so f/g can certainly be written as a simple continued fraction. That it can be done so in a unique way follows easily.

□

We may now make the following definition.

Definition 2.18 *The* ***continued fraction expansion*** *or just* ***continued fraction*** *of a rational function is the unique simple continued fraction to which it is equal.*

Example 2.19 The continued fraction expansion of the rational function of which we computed the square roots in Example 2.12 is

$$\frac{x^3+x^2+x+2}{x^3+1} = [\,1; x+2, 2x^2+2x+2\,].$$

This may be verified using the Euclidean Algorithm.

2.3.3 Infinite Continued Fractions

We wish to extend our notion of a simple continued fraction so that irrational as well as rational elements in the field L_q may be written in this form. We begin by defining an infinite continued fraction as a limit of finite simple ones, and then present a general method for constructing, given any irrational Laurent series, an infinite continued fraction to which it is equal.

Let $\{a_j\}_{j\geq 0}$ be an infinite sequence of polynomials with $\deg a_j \geq 1$ for $j \geq 1$. We define the **infinite continued fraction** $l = [\,a_0\,; a_1, a_2 \ldots]$ to be the limit of the sequence of finite simple continued fractions $l_k = [\,a_0\,; a_1, a_2, \ldots, a_k\,]$ as $k \to \infty$. Here we take the "limit" to mean the limit with respect to the norm $|\,|$ on the field L_q. We must first verify that this limit exists.

It follows easily from Result 2.15 Part 4 that

$$|l_j - l_k| = 1/|g_k||g_{k+1}|,$$

for $j > k$. Here f_k/g_k $(0 \leq k \leq j)$ denotes the kth convergent to l_j, which is equal to l_k. Hence

$$|l_j - l_{j'}| \leq 1/|g_k||g_{k+1}|,$$

for all $j, j' > k$. From Result 2.15 Part 2, we know that $\{|g_k||g_{k+1}|\}_{k\geq 0}$ is an increasing unbounded sequence. It therefore follows that $\{l_k\}_{k\geq 0}$ is a Cauchy sequence, and so has a limit in the complete field L_q.

As before, we call the polynomials a_j the partial quotients of $l = [\,a_0; a_1, a_2, \ldots]$ and the rational functions $f_j/g_j = [\,a_0; a_1, \ldots, a_j\,]$ the convergents of l. Here f_j and g_j are the polynomials given by

$$\begin{array}{llll} f_{-1} = 1, & f_0 = a_0, & f_j = a_j f_{j-1} + f_{j-2}, & \text{for } j \geq 1, \\ g_{-1} = 0, & g_0 = 1, & g_j = a_j g_{j-1} + g_{j-2}, & \text{for } j \geq 1. \end{array} \tag{2.15}$$

We now wish to show how one may associate with each irrational Laurent series $\alpha \in L_q$ a unique infinite continued fraction $[\,a_0\,; a_1, a_2, \ldots]$. This is done by means of an algorithm which is a generalisation of the one used to compute the continued fraction expansion of a rational function.

Let $\alpha \in L_q$ with $\alpha \notin \mathbb{F}_q(x)$. For any $\beta \in L_q$, let $Poly(\beta)$ and $Frac(\beta)$ denote the polynomial part and fractional part of β. So if $\beta = \sum_{i\geq n} b_i x^{-i}$ then $Poly(\beta) = \sum_{n\leq i\leq 0} b_i x^{-i}$ and $Frac(\beta) = \sum_{i\geq 1} b_i x^{-i}$. We recursively define a sequence of polynomials a_j which we shall see are the partial quotients of α.

Let $\zeta_0 = \alpha$ and $a_0 = Poly(\alpha)$. For $j \geq 1$ let

$$\begin{aligned} \zeta_j &= 1/(\zeta_{j-1} - a_{j-1}), \\ a_j &= Poly(\zeta_j). \end{aligned}$$

This sequence is well defined as one may verify that the irrationality of α ensures that $\zeta_{j-1} - a_{j-1} \neq 0$ for all $j \geq 1$. Observe that for each $m \geq 1$,

$$\begin{aligned} \alpha &= a_0 + 1/(a_1 + 1/(a_2 + 1/\ldots + 1/(a_{m-1} + 1/\zeta_m))) \\ &= [\,a_0; a_1, \ldots, a_{m-1}, \zeta_m\,]. \end{aligned}$$

This is easily verified by induction on $m \geq 1$. Now let $l_{m-1} = [\,a_0\,; a_1, a_2, \ldots, a_{m-1}]$ and suppose that f_{m-1}/g_{m-1} is the $(m-1)$th convergent to l_{m-1}. Then by Result 2.15 Part 4,

$$\begin{aligned} |\alpha - l_{m-1}| &= 1/|\zeta_m||g_{m-1}|^2 \\ &= 1/|a_m||g_{m-1}|^2, \end{aligned}$$

since $|\zeta_j| = |a_j + Frac(\zeta_j)| = |a_j|$. So we see that $\alpha = \lim_{m\to\infty} l_m$. Hence $\alpha = [\,a_0; a_1, a_2, \ldots]$.

Result 2.20 *Every irrational element in L_q may be written uniquely as an infinite continued fraction.*

Proof: We have shown that every irrational Laurent series may be written as an infinite continued fraction. Now suppose that $\alpha = [\,a_0; a_1, a_2, \ldots] = [\,b_0; b_1, b_2 \ldots]$ and that these two continued fractions are "different". That is to say, for some $m \geq 0$, $a_j = b_j\ (0 \leq j < m)$ but $a_m \neq b_m$. Let $\mu_m = [\,a_m; a_{m+1}, \ldots]$ and $\nu_m = [\,b_m; b_{m+1}, \ldots]$. For $0 \leq j \leq m-1$, let f_j/g_j denote the jth convergent to $[\,a_0; a_1, \ldots, a_{m-1}\,] = [\,b_0; b_1, \ldots, b_{m-1}\,]$. Now $\alpha = [\,a_0; a_1, \ldots, a_{m-1}, \mu_m\,] = [\,b_0; b_1, \ldots, b_{m-1}, \nu_m\,]$. Hence from recurrences (2.14)

$$\frac{\mu_m f_{m-1} + f_{m-2}}{\mu_m g_{m-1} + g_{m-2}} = \frac{\nu_m f_{m-1} + f_{m-2}}{\nu_m g_{m-1} + g_{m-2}},$$

from which we may deduce that $\mu_m = \nu_m$. In particular $a_m = Poly(\mu_n) = Poly(\nu_m) = b_m$. But we assumed that $a_m \neq b_m$. This contradiction establishes that $a_j = b_j$ for all j, as we wished to show.

□

Definition 2.21 *The* ***continued fraction expansion*** *or* ***continued fraction*** *of an irrational Laurent series is the unique infinite continued fraction to which it is equal.*

So every Laurent series has a unique continued fraction expansion, which is finite if the Laurent series is rational, and infinite otherwise.

Example 2.22 Recall that in Example 2.12 we consider the quadratic element $\alpha \in L_3$ given by

$$\alpha = 1 + 2x^{-1} + 2x^{-3} + x^{-5} + 2x^{-7} + 2x^{-8} + x^{-9} + 2x^{-10} + 2x^{-11} + 2x^{-12} + \ldots$$

One may use the continued fraction algorithm for irrational Laurent series to compute the continued fraction of α. The first few partial quotients are found to be

$$\alpha = [\,1; 2x, x, 2x, x^2, x+1, \ldots].$$

It is claimed in [4, page 593] that an analogue of Lagrange's theorem — an irrational element has an eventually periodic expansion if and only if it is quadratic — holds in L_q. Thus an "effective version" of this result, giving a bound on the length of the period and initial stem in terms of the coefficients of the quadratic polynomial, would enable one to completely determine the continued fraction of α. One may bound the length of the period for quadratic real numbers ([37, page 50]), and so it is possible that an effective version of Lagrange's theorem for Laurent series could be obtained, although the author is not aware of any such result.

2.3.4 Best Approximations

Having spent several pages showing how one may expand any Laurent series as a continued fraction in a unique way, the natural question to now address is what use such expansions are. We shall see that the continued fraction expansion of a Laurent series is closely related to the sequence of "best approximations" to the Laurent series.

Definition 2.23 *Let $\alpha \in L_q$.*

1. *A rational function f/g is called a* ***best approximation of the first kind*** *to α if*
$$|\alpha - (f/g)| < |\alpha - (r/s)|$$
for all rational functions r/s with $\deg s < \deg g$, and
$$|\alpha - (f/g)| \leq |\alpha - (r/s)|$$
for all rational functions r/s with $\deg s = \deg g$.

2. *A rational function f/g is a called a* ***best approximation of the second kind*** *to α if*
$$|g\alpha - f| < |s\alpha - r|,$$
for all rational functions r/s with $\deg s < \deg g$.

Thus a best approximation of the first kind, is a rational function which approximates a given Laurent series better than any other rational function whose denominator has smaller degree, and as least as well as any other whose denominator has the same degree. We discuss some of the finer points concerning this definition in Note 2.26 following the proof of Proposition 2.25.

The next result explains the apparent omission of a "second requirement" for best approximations of the second kind.

Result 2.24 *Let f/g be a best approximation of the second kind to α. Then*
$$|g\alpha - f| < |s\alpha - r|,$$
for all rational functions r/s distinct from f/g with $\deg s = \deg g$.

Proof: Suppose that there exists r/s with $\deg s = \deg g$ but $s \neq g$ and
$$|s\alpha - r| \leq |g\alpha - f|.$$
We may assume that s and g have the same leading coefficient. We then have that
$$\begin{aligned} |(s-g)\alpha - (r-f)| &\leq \max\{|s\alpha - r|, |g\alpha - f|\} \\ &= |g\alpha - f|, \end{aligned}$$
which is a contradiction, since $0 \leq \deg(s-g) < \deg g$.

□

We now present the main result of this section.

Proposition 2.25 *Let $\alpha \in L_q$ and $f/g \in \mathbb{F}_q(x)$. The following are equivalent*

1. *f/g is a best approximation of the first kind to α.*
2. *f/g is a best approximation of the second kind to α.*
3. *f/g is a convergent of α.*

Proof: $(2 \Rightarrow 1)$. Let f/g be a best approximation of the second kind to α. Suppose it is not a best approximation of the first kind. Then there exists a rational function r/s distinct from f/g with either $\deg s < \deg g$ and $|\alpha - (r/s)| \leq |\alpha - (f/g)|$, or $\deg s = \deg g$ and $|\alpha - (r/s)| < |\alpha - (f/g)|$. In either case multiplying through by s we see that

$$\begin{aligned} |s\alpha - r| &= |s||\alpha - (r/s)| \\ &< |g||\alpha - (f/g)| \\ &= |g\alpha - f|, \end{aligned}$$

which is a contradiction, by Definition 2.23 and Result 2.24.

$(1 \Rightarrow 3)$. Let f/g be a best approximation of the first kind to α. If α is rational and $f/g = \alpha$ then f/g is the final convergent to α, and the result is true. So assume that this is not the case. We claim that then there exists $k \geq 0$ such that

$$\deg g_k \leq \deg g < \deg g_{k+1},$$

where f_j/g_j is the jth convergent of α. It is easily seen that this claim is true when α is irrational. Let us now consider the case where α is rational with $\alpha = f_m/g_m$, the mth and final convergent to α. If $\deg g > \deg g_m$ then f/g cannot be a best approximation, and if $\deg g = \deg g_m$ then f/g can only be a best approximation if $f/g = \alpha = f_m/g_m$, which we have assumed is not the case. Hence $\deg g < \deg g_m$ and so, when α is rational, there exists $k \geq 0$ such that $\deg g_k \leq \deg g < \deg g_{k+1}$. This proves the claim.

Now f/g is a best approximation of the first kind. Suppose that $\deg g > \deg g_k$, so in particular $f/g \neq f_k/g_k$, as we may assume that f/g is in reduced form. Then

$$\begin{aligned} |\alpha - (f/g)| &< |\alpha - (f_k/g_k)| \\ &= |g_k g_{k+1}|^{-1}, \end{aligned}$$

the final equality coming from Result 2.16. Hence

$$\begin{aligned} |f/g - f_k/g_k| &= |(\alpha - (f_k/g_k)) - (\alpha - (f/g))| \\ &= |g_k g_{k+1}|^{-1}, \end{aligned}$$

by Property (2.5) of $|\,|$. So we have that

$$\begin{aligned} |g_k g|^{-1} &\leq |g_k f - f_k g|/|g||g_k| \\ &= |g_k g_{k+1}|^{-1}, \end{aligned}$$

and so $\deg g \geq \deg g_{k+1}$, which is a contradiction. So we must have that $\deg g = \deg g_k$. If $f/g \neq f_k/g_k$ we may argue in a similar fashion as before to once again deduce that $\deg g = \deg g_{k+1}$, another contradiction. Hence $f/g = f_k/g_k$, and f/g is a convergent of α as we wished to show.

$(3 \Rightarrow 2)$. Let f_k/g_k be the kth convergent to α. We now show that f_k/g_k is a best approximation of the second kind to α. Let

$$S_k = \{|g\alpha - f| \mid f, g \in \mathbb{F}_q[x],\ 0 \leq \deg g \leq \deg g_k\}.$$

Let $t = \min S_k$ and $M_k = \{f/g \mid |g\alpha - f| = t\}$. Observe that such a t exists since there are only finitely many f/g with $\deg g \leq \deg g_k$ and $|g\alpha - f| \leq |g_k\alpha - f_k| < 1$. We wish to show that $M_k = \{f_k/g_k\}$, as this is equivalent to f_k/g_k being a best approximation of the second kind to α.

Choose the subset of M_k of rational functions whose denominators have lowest degree; degree l say. Let r/s lie in this set. Then r/s approximates α in the second sense better than any rational function whose denominator has smaller degree than l, and so is a best approximation of the second kind to α. Now we have already shown that best approximations of the second kind are convergents, and so r/s must be a convergent of α. So let $r/s = f_j/g_j$, the jth convergent of α. Certainly $0 \leq j \leq k$ since $\deg s \leq \deg g_k$.

Recall that $|g_j\alpha - f_j| = |g_{j+1}|^{-1}$ where $\{|g_j|\}_{0 \leq j \leq k}$ is a strictly increasing sequence. Thus f_k/g_k certainly approximates α better than any f_j/g_j with $j < k$. Hence we must have that $j = k$. Therefore $r/s = f_k/g_k$, and so f_k/g_k is a best approximation of the second kind to α.

□

Note 2.26 From Result 2.24 and Proposition 2.25 ($1 \Leftrightarrow 2$) it can be seen that best approximations of the first kind actually approximate the given Laurent series *better* than any other rational function whose denominator has the same degree. However, we make slighty weaker requirements when defining a best approximation of the first kind so that we may use the theory we develop in the proof of Result 2.36 (see the comments preceding Result 2.36). Observe also that a rational function f/g which approximates a Laurent series α better than any other rational function whose denominator has *smaller* degree need not be a best approximation. In general, such a rational function is either a convergent or an **intermediate** convergent of α. (If $\alpha = [0; a_1, a_2, \dots]$ with convergents f_k/g_k, then intermediate convergents are rational functions of the form $(bf_k + f_{k-1})/(bg_k + g_{k-1})$ where $\deg b = \deg a_{k+1}$ and b and a_{k+1} have the same leading coefficient, but $b \neq a_{k+1}$.)

In traditional applications of diophantine approximation to number theory, such as minimising linear forms, real number analogues of best approximations of the second kind are studied. Not only are they the correct type of approximations to consider in this context, but the theory connecting these approximations and continued fraction expansions of real numbers is far neater than that connecting best approximations of the first kind with continued fractions. More specifically, with a few trivial exceptions, the best approximations of the second kind to a number and its convergents are one and the same thing. This statement is not true for best approximations of the first kind to real numbers. All that one can say about the best approximation of the first kind to a real number is that it is a convergent or an “intermediate convergent”. It is particularly satisfying that when one considers Laurent series rather than real numbers, the three ideas — best approximations of the first and second kind and convergents — fit together so well.

As a first application of Proposition 2.25, we prove a result from [4, Lemma 1, Part (a)], which we shall use in Section 3.3.2 of Chapter 3.

Result 2.27 *Let $\alpha \in L_q$ and $f, g \in \mathbb{F}_q[x]$ with $g \neq 0$. If $|\alpha - (f/g)| = 1/|g|^2 q^d$, where $\gcd(f, g) = 1$ and $d \geq 1$, then f/g is a convergent of α with next partial quotient of degree d.*

We shall first of all need a lemma.

Lemma 2.28 *Let $\alpha \in L_q$ with convergents f_k/g_k. Then*

$$|\alpha - (f_k/g_k)| \leq |\alpha - (f/g)|,$$

for all f/g with

$$\deg g_k \leq \deg g < \deg g_{k+1}.$$

Proof: Suppose that the lemma is not true for a given k. Choose f/g with $\deg g$ of minimum degree subject to the conditions

$$|\alpha - (f_k/g_k)| > |\alpha - (f/g)|,$$

and $\deg g_k \leq \deg g < \deg g_{k+1}$. Then f/g must be a best approximation of the first kind to α and hence a convergent by Proposition 2.25. Since $\deg g_k \leq \deg g < \deg g_{k+1}$ we must have that $f/g = f_k/g_k$. But $|\alpha - (f/g)| < |\alpha - (f_k/g_k)|$, which is a contradiction.

□

Observe that this lemma implies that

$$|g_k\alpha - f_k| \leq |g\alpha - f|,$$

for all $f, g \in \mathbb{F}_q[x]$ with $\deg g_k \leq \deg g < \deg g_{k+1}$.

We now prove Result 2.27.

Proof: Suppose that $|\alpha - (f/g)| = 1/|g|^2 q^d < |g|^{-2}$ and $\gcd(f,g) = 1$. Choose k so that

$$\deg g_k \leq \deg g < \deg g_{k+1},$$

where f_k/g_k is the kth convergent to α. It is easily verified that one may do this even when α is rational. Then

$$|\alpha - (f/g)| < |g|^{-2} \leq |g_k g|^{-1}.$$

By the remarks following the proof of Lemma 2.28 we also have that

$$|g_k\alpha - f_k| \leq |g\alpha - f| < |g|^{-1}$$

and so

$$|\alpha - (f_k/g_k)| < |g_k g|^{-1}.$$

Therefore

$$\begin{array}{rcl} |f/g - f_k/g_k| & = & |(\alpha - (f_k/g_k)) + ((f/g) - \alpha)| \\ & \leq & \max\{|\alpha - (f/g)|, |\alpha - (f_k/g_k)|\} \\ & < & |g_k g|^{-1} \end{array}$$

If $f/g \neq f_k/g_k$ then we also have that

$$\begin{array}{rcl} |f/g - f_k/g_k| & = & |(fg_k - gf_k)/g_k g| \\ & \geq & |g_k g|^{-1}. \end{array}$$

This is a contradiction, and so we must have that $f/g = f_k/g_k$. Thus f/g is a convergent. That the next partial quotient has degree d follows from Result 2.16 and the fact that $\gcd(f,g) = 1$.

□

Example 2.29 Recall in Example 2.13 we considered the algebraic element $z = \sum_{i=0}^{\infty} x^{-p^i}$ of L_q which satisfies the equation $z^p - z + x^{-1} = 0$. We now consider its continued fraction expansion. In this example, we shall assume that $p > 2$, and we shall look at the case $p = 2$ in Example 2.39.

For $n \geq 1$ let

$$\begin{aligned} a_n &= x^{p^{n-1}}(x^{-1} + x^{-p} + \ldots + x^{-p^{n-1}}) \\ b_n &= x^{p^{n-1}}. \end{aligned}$$

Then gcd $(a_n, b_n) = 1$ and $|b_n| = q^{p^{n-1}}$. Now

$$\begin{aligned} |z - (a_n/b_n)| &= |x^{-p^n} + x^{-p^{n+1}} + \ldots| \\ &= q^{-p^n} \\ &= |b_n|^{-p} \\ &= 1/|b_n|^2 q^{p^{n-1}(p-2)} \end{aligned}$$

Thus since $p > 2$, by Result 2.27 we have that a_n/b_n is a convergent to z. The next partial quotient therefore has degree $p^{n-1}(p-2)$. Thus the sequence $\{a_n/b_n\}_{n\geq 1}$ is a subsequence of the sequence of convergents to z, $\{f_j/g_j\}_{j\geq 0}$ say. However, these do not give us all the convergents. For since $\deg b_n = p^{n-1}$ the degree of the denominator of the next convergent after a_n/b_n is $p^{n-1}(p-2)+p^{n-1} = p^n - p^{n-1} < p^n = \deg b_{n+1}$. In Example 4.12 of Chapter 4 we shall uncover the complete continued fraction expansion of z, and determine exactly which special convergents of z the rational functions a_n/b_n give us.

In the next section we shall see that best approximations of the first kind play a natural role in the study of sequences. We have already seen that best approximations of the second kind are the same as those of the first, but other than through this connection, one cannot motivate interest in these approximations in terms of sequences. Nevertheless, in a full exposition on the theory of continued fraction expansions of Laurent series, it is appropriate to initially distinguish between these two types of approximations, as there may well be other applications of this theory where approximations of the second type arise more naturally.

2.4 Sequences

One immediate and useful application of the theory we have just described is to the study of the algebraic properties of sequences. In Section 2.4.1 we outline the basic properties of sequences over finite fields, before moving on in Section 2.4.2 to discuss linear complexity profiles, and describing how this is related to continued fraction theory.

2.4.1 The Basic Properties of Sequences

Throughout this chapter, we have assumed a familiarity with the basic mathematical notion of a sequence. For example, sequences of convergents and Cauchy sequences. As the study of sequences over finite fields is one of the main topics of this thesis, it is appropriate at this stage to take a step backwards, and give a formal definition.

Definition 2.30 *A* ***sequence*** *over a finite field $\mathbb{F}_q$ is a map S from the natural numbers $\mathbb{N}$ to $\mathbb{F}_q$. We write $S(i) = s_i$ and denote the sequence by $\{s_i\}_{i\geq 1}$. The sequence is called* ***eventually periodic*** *if there exists $m, n \in \mathbb{N}$ such that $s_i = s_i + n$*

for all $i > m$. If such an m and n exists, then the least such n is called the ***period*** *of S.*

With any sequence $S = \{s_i\}_{i\geq 1}$ over a field $\mathbb{F}_q$ we may associate the Laurent series $s := \sum_{i\geq 1} s_i x^{-i}$ in L_q. We call s the **generating function** of the sequence S.

Result 2.31 *Let S be a sequence with generating function s. Then S is eventually periodic if and only if s is a rational function.*

Proof: Suppose first that S is an eventually periodic sequence. Then there exists $m, n > 0$ such that $s_i = s_{i+n}$ for all $i > m$. Now the coefficient of $x^{-i}\,(i \geq 1)$ in $(x^{m+n} - x^m)s$ is $s_{i+(m+n)} - s_{i+m}$. For $i \geq 1$ this is equal to 0. Hence $(x^{m+n} - x^m)s$ lies in $\mathbb{F}_q[x]$ and we may write $s = r/(x^{m+n} - x^m)$ for some $r \in \mathbb{F}_q[x]$.

Conversely, suppose that s is a rational function. We write $s = f/g$ with $f, g \in \mathbb{F}_q[x]$ and $g \neq 0$. We claim that there exists $m, n \in N$ such that g divides $x^{m+n} - x^m$. This follows from the fact that the factor ring $\mathbb{F}_q[x]/g\mathbb{F}_q[x]$ is finite and so not all powers of x modulo g can be distinct. So $(x^{m+n} - x^m) = hg$ for some $h \in \mathbb{F}_q[x]$. Hence $s = hf/(x^{m+n} - x^m)$. Therefore $s_i = s_{i+n}$ for all $i > m$, and so S is eventually periodic.

□

The generating function s of any sequence S which is eventually periodic may therefore be written as $s = f/g$ where f and g are coprime polynomials.

Definition 2.32 *A sequence S satisfies a* ***linear recurrence of length*** *l if there exists $g_0, g_1, \ldots, g_l \in \mathbb{F}_q$ with $g_l \neq 0$ such that $\sum_{0\leq j\leq l} g_j s_{i+j} = 0$ for all $i \geq 0$. We call $g(x) = \sum_{0\leq j\leq l} g_j x^j$ a* ***characteristic polynomial*** *of the sequence S. The* ***linear complexity*** *of s is the length of the shortest linear recurrence satisfied by s.*

Result 2.33 *Let S be a sequence with associated Laurent series $s = f/g$, where* $\gcd(f, g) = 1$. *The linear complexity of S is* $\deg g$.

Proof: We claim that S satisfies a linear recurrence with coefficients $b_0, b_1, \ldots, b_t$ if and only if $bs \in \mathbb{F}_q[x]$, where $b = \sum_{0\leq j\leq t} b_j x^j$. This is easily verified by considering the coefficients of $x^{-i}\,(i \geq 1)$ in bs. From this it follows that b is a characteristic polynomial of s if and only if $g|b$, and so the set of characteristic polynomials of s is the principal ideal in $\mathbb{F}_q[x]$ generated by g. In particular, the linear complexity of s is the degree of the smallest non-zero polynomial in this ideal, which is just $\deg g$.

□

Definition 2.34 *If S is an eventually periodic sequence with $s = f/g$ where* $\gcd(f, g) = 1$ *and g is monic, then g is called the* ***minimal polynomial*** *of S.*

2.4.2 Linear Complexity Profiles

The linear complexity of a sequence is a rather inadequate measure of the unpredictability of the sequence for many reasons. In particular, it may be that although the whole sequence is difficult to generate by a linear recurrence, long initial segments of the sequence might be much easier to generate. This is one reason for considering the linear complexity profile of a sequence. In essence, the linear complexity profile of a sequence reveals how easy or difficult it is to generate not just the whole sequence by a linear recurrence, but initial segments of the sequence of any given length. Indeed, the sequence being considered need not even be eventually periodic.

Definition 2.35 *Let $S = \{s_i\}_{i\geq 1}$ be a sequence over $\mathbb{F}_q$. The n**th linear complexity** of S, denoted $l_n(S)$, is the length of the shortest linear recurrence which will generate a sequence of the form $s_1, s_2, \ldots, s_n, r_{n+1}, r_{n+2}, \ldots$ where $r_i \in \mathbb{F}_q$ $(i > n)$ may be chosen arbitrarily. The **linear complexity profile** of S is the positive integer sequence $\{l_n(S)\}_{n\geq 1}$.*

The above definition comes very clearly into focus when one interprets it in terms of generating functions. The nth linear complexity of a sequence S with generating function s is the degree of the smallest polynomial g such that

$$|s - (f/g)| < q^{-n},$$

for some $f \in \mathbb{F}_q[x]$. Now suppose that g is such a polynomial. Then we have that

$$|s - (f/g)| < q^{-n} \leq |s - (u/v)|,$$

for all rational functions u/v with $\deg v < \deg g$. Thus f/g is almost a best approximation of the first kind, except that we do not know whether f/g approximates s as least as well as any rational function whose denominator has degree $\deg g$. In general f/g need not be a best approximation of the first kind, but rather is either an intermediate convergent or a convergent (see Note 2.26). However, for each $n \geq 1$, out of all the rational functions which approximate s to the "nth coefficient", we may always choose one that is a best approximation of the first kind — just choose one which approximates s at least as well as any other. (If we had defined a best approximation of the first kind to be a rational function which approximates a given Laurent series better than any other rational function whose denominator does not have a larger degree, then it would not be clear that we could make such a choice. Thus the slightly more complicated definition which we give is appropriate for our application.) Therefore the nth linear complexity of S must always be the degree of some best approximation of the first kind to s. In fact we have ([31, Theorem 1]).

Result 2.36 *Let S be a sequence with generating function s. Suppose that the kth convergent and partial quotient of s are denoted f_k/g_k and a_k respectively. Further let $l_n(S)$ denote the nth linear complexity of S. Suppose*

$$\deg g_{k-1} + \deg g_k \leq n < \deg g_k + \deg g_{k+1},$$

where $k \geq 0$. Then $l_n(S) = \deg g_k$. Also, if s is a rational function with final convergent f_m/g_m and we have that $\deg g_{m-1} + \deg g_m \leq n$, then $l_n(S) = \deg g_m$.

Proof: For a given $n \geq 1$, let f/g be a rational function such that

$$|s - (f/g)| < q^{-n} \leq |s - (u/v)|,$$

for all rational functions u/v with $\deg v < \deg g$. We may choose f/g so that

$$|s - (f/g)| \leq |s - (u/v)|$$

for all rational functions u/v with $\deg v = \deg g$. Observe that the nth linear complexity is just $\deg g$ by definition. Now f/g is a best approximation of the first kind to s, and hence a convergent of s by Proposition 2.25. Therefore $f/g = f_k/g_k$ for some $k \geq 0$. Thus $l_n(S) = \deg g_k$. It only remains to show that n must lie in the range specified by the theorem.

Suppose firstly that $k = 0$. Now $f_0/g_0 = a_0/1 = 0$. So

$$\begin{array}{rcl} q^{-n} > |s - (f_0/g_0)| & = & |s| \\ & = & |g_0 g_1|^{-1} \\ & = & |a_1|^{-1} \end{array}$$

Thus in this case $1 \leq n < \deg a_1$. Now $\deg a_1 = \deg g_0 + \deg g_1$ and $-\infty = \deg g_{-1} + \deg g_0 < 1$. Hence for n in the range

$$\deg g_{-1} + \deg g_0 \leq n < \deg g_0 + \deg g_1,$$

the nth linear complexity is just $\deg g_0 = 0$.

If s is rational and f_k/g_k is the final convergent to s, so $s = f_k/g_k = f_m/g_m$, then

$$\begin{array}{rcl} |s - (f_{m-1}/g_{m-1})| & = & |g_{m-1} g_m|^{-1} \\ & \geq & q^{-n}, \end{array}$$

and so $\deg g_{m-1} + \deg g_m \leq n$, which proves the final claim.

Suppose now that $k \geq 1$ and f_k/g_k is not the final convergent to s. Then

$$\begin{array}{rcl} |s - (f_k/g_k)| & = & |g_k g_{k+1}|^{-1} \\ & < & q^{-n}, \end{array}$$

and

$$\begin{array}{rcl} |s - (f_{k-1}/g_{k-1})| & = & |g_{k-1} g_k|^{-1} \\ & \geq & q^{-n}, \end{array}$$

since $\deg g_{k-1} < \deg g_k$. So

$$\deg g_{k-1} + \deg g_k \leq n < \deg g_k + \deg g_{k+1}.$$

From this we see that for all n with

$$\deg g_{k-1} + \deg g_k \leq n < \deg g_k + \deg g_{k+1},$$

the nth linear complexity of S must be $\deg g_k$. This completes the proof.

□

It is the next and final result in this chapter which will be of most interest to us when interpreting our new theorems on continued fractions of Laurent series in Chapters 4 and 6 in terms of sequences. We first need a definition.

Definition 2.37 *The* ***jumps profile*** *of a sequence S is the subsequence of positive terms in the sequence*

$$l_1(S), l_2(S) - l_1(S), l_3(S) - l_2(S), \ldots$$

This may be an infinite or a finite sequence.

Result 2.38 *Let S be a sequence with generating function s. Let s have continued fraction expansion $[0; a_1, a_2, \ldots]$. The jumps profile of S is $\{\deg a_k\}_{k \geq 1}$.*

Proof: By Result 2.36 the subsequence of non-zero terms in the linear complexity profile is the sequence $\{\deg g_k - \deg g_{k-1}\}_{k\geq 1}$. The result now follows from the observation that $\deg g_k = \deg a_k + \deg g_{k-1}$, which is obvious from recurrences (2.14), in the case that s is rational, and (2.15) when s is irrational.

□

Example 2.39 In this final example we consider a binary sequence which is well-known in the study of the linear complexity profiles of sequences. Let R be the sequence over $\mathbb{F}_2$ whose generating function z is given by

$$z = \sum_{i=0}^{\infty} x^{-2^i}.$$

Recall that we considered this Laurent series in Examples 2.13 and 2.29. This is sometimes called the Rueppel sequence. We show that

$$z = [\,0; x+1, x, x, \dots]$$

and so R has the jumps profile $111\dots$.

Let $\alpha = [\,0; x+1, x, x, \dots]$. Then $\alpha = [\,0; x+1, (1/\beta)]$ where $\beta = [\,0; x, x, \dots]$. Now $(1/\beta) + x = \beta$ and hence $\beta^2 + x\beta + 1 = 0$. Substituting $\beta = (1+x) + (1/\alpha)$ into this equation we have that

$$\alpha^2 + \alpha + x^{-1} = 0.$$

Hence from the case $p = 2$ of Example 2.13, we have that α must be z_0 or z_1. Comparing polynomial parts we see that $\alpha = z_0 = z$, as we wished to show.

The sequence whose generating function is $\beta = [\,0; x, x, \dots]$ is sometimes called the Morii-Kasahara sequence. Both the Rueppel sequence and the Morii-Kasahara sequence are discussed in [16, pages 38-39].

Chapter 3

Continued Fractions with Partial Quotients of Small Degree

3.1 Introduction

We begin by stating a long-standing conjecture in number theory.

Conjecture 3.1 *For any positive integer n there exists a coprime positive integer m such that all the partial quotients of the continued fraction expansion of m/n are not greater than* 5.

We shall call this **Zaremba's Conjecture** as a form of it first appeared in print in a paper of S.K. Zaremba in 1972 ([47]). Zaremba's interest in finding "good lattice points for numerical integration" led him to consider rational numbers whose partial quotients were small. He conjectured that there is a constant C, such that for any positive integer n, there exists a coprime positive integer m such that the partial quotients of m/n are all not greater than C. Thomas Cusick believes that we may take this constant to be 5 ([10]), as we have stated in our version of Zaremba's original conjecture. Zaremba was able to prove a weaker version of this conjecture, which we shall call **Zaremba's Theorem** ([48]).

Result 3.2 *For any positive integer n, there exists a coprime positive integer m, such that all the partial quotients of the continued fraction expansion of m/n are less than $D \log_e n$, where D is some constant.*

Cusick provides a much shortened proof of this result in [10], in which he also shows that we make take the constant D to be 3.

In this chapter, we study a rational function analogue of Zaremba's Conjecture. The main protagonists in this act are Harald Niederreiter and Simon Blackburn, both of whose work contributes elegantly to different aspects of this problem. It is of historical interest to note that Niederreiter, who is best known for his work in finite fields, began academic life as a numerical analyst, and actually contributed a paper to the conference proceedings in which Zaremba's original conjecture first appeared.

We organise the remainder of this chapter as follows: in Section 3.2 we discuss rational function analogues of Zaremba's conjecture and theorem; in Section 3.3 the orthogonal multiplicity of a polynomial is defined; and Sections 3.3.1 and 3.3.2 contain detailed discussions of existing results on this topic. Finally, in Section 3.4 we present some applications which have motivated research in this area.

3.2 Rational Function Analogues of Zaremba's Conjecture and Theorem

To avoid the continual repetition of the phrase "all of whose partial quotients have degree not greater than", we start with a definition.

Definition 3.3 *Let f/g be a rational function over a finite field $\mathbb{F}_q$ with $\gcd(f, g) = 1$ and $\deg g \geq 1$. Let $f/g = [a_0; a_1, a_2, \ldots, a_m]$ with $a_j \in \mathbb{F}_q[x]$ for $0 \leq j \leq m$ and $\deg a_j \geq 1$ for $1 \leq j \leq m$. Define*

$$K\left(\frac{f}{g}\right) = \max_{1 \leq j \leq m} \deg a_j.$$

Rational functions f/g with $K(f/g)$ "small" relative to $\deg g$ can be thought of as being difficult to approximate, as we now explain. Recall that the convergents of a rational function are the same as its best approximations of both the first and second kinds (Result 2.25). We also know (by Result 2.16) that if f_k/g_k is the kth convergent to f/g then

$$|f/g - f_k/g_k| = 1/|a_{k+1}||g_k|^2,$$

and so

$$|g_k(f/g) - f_k| = 1/|a_{k+1}||g_k|.$$

Further recall that $|g_k| = \prod_{i=1}^{k} |a_i|$. Suppose that $\deg a_{k+1}$ is "small". Then $1/|a_{k+1}|$ is "large" and so the kth convergent f_k/g_k does not approximate f/g particularly well, in either the first or the second sense. If $K(f/g)$ is "small" then this means that $|a_{k+1}|$ is "small" for every $0 \leq k \leq m-1$, where $f/g = f_m/g_m$. So in this case, none of the convergents to f/g approximate this rational function well. Thus all the best approximations, both of the first and second kind, approximate f/g rather poorly, and f/g can be considered difficult to approximate.

The worst possible case is when $K(f/g) = 1$; here the best approximations are always as far from f/g as one could expect. These are of particular interest.

Definition 3.4 *We say that f/g is* ***badly approximable*** *if $K(f/g) = 1$.*

We may now state our rational function analogue of Zaremba's conjecture. It falls into two parts.

Conjecture 3.5 *[6, page 110] Let $\mathbb{F}_q$ be a finite field with $q \neq 2$. For all $g \in \mathbb{F}_q[x]$ with $\deg g \geq 1$ there exists a coprime polynomial $f \in \mathbb{F}_q[x]$ such that f/g is badly approximable.*

(It should be pointed out that Blackburn does not in fact make such a conjecture in [6], but only asks if this is true.)

Conjecture 3.6 *[28, page 145] For all $g \in \mathbb{F}_2[x]$ with $\deg g \geq 1$ there exists a coprime polynomial $f \in \mathbb{F}_2[x]$ with $K(f/g) \leq 2$.*

Both of these conjectures remain open; however, several partial results on these conjectures have been obtained. We delve more deeply into the questions surrounding these conjectures in Section 3.3. But first, we present a result due to Niederreiter, which can be thought of as a rational function analogue of Zaremba's Theorem.

Result 3.7 *[30, Theorem 4] Let $g \in \mathbb{F}_q[x]$ be monic of degree $n \geq 1$, and exclude the case where $q = n = 2$ and $g = x^2 + x + 1$. Then there exists a monic irreducible $f \in \mathbb{F}_q[x]$ with $\deg f = n$, $\gcd(f, g) = 1$ and*

$$K\left(\frac{f}{g}\right) < 2 + 2\log_q n.$$

We do not discuss in detail the methods used by Niederreiter to prove this result, but content ourselves with the following outline of the proof.

Proof: For $0 \leq t < n$, Niederreiter defines $I_n(t)$ to be the number of monic irreducible polynomials $f \in \mathbb{F}_q[x]$ with $\deg f = n$, such that f divides some polynomial $H_1 + H_2 g$, with $H_1, H_2 \in \mathbb{F}_q[x]$, $H_1 H_2 \neq 0$ and $\deg H_1 + \deg H_2 \leq t$. Letting $t_0 = \lfloor n - 2 - 2\log_q n \rfloor$, he obtains an upper bound on the cardinality of $I_n(t_0)$. In particular, he observes that this upper bound is at least two less than the total number of monic irreducible polynomials of degree n. Thus one can conclude that there exists a monic irreducible polynomial f distinct from g such that f does not lie in $I_n(t_0)$. For this polynomial f, the rational function f/g is in reduced form and we will show that $K(f/g) < 2 + 2\log_q n$.

Let f_j/g_j denote the jth convergent to f/g, where $0 \leq j \leq m$, say. Then

$$|g_{j-1}(f/g) - f_{j-1}| = 1/|a_j||g_{j-1}|,$$

where a_j is the jth partial quotient of f/g. Thus

$$\deg(g_{j-1}f - f_{j-1}g) = n - \deg f_j.$$

Here we use that fact that $a_0 = 1$ and so $\deg f_j = \sum_{1 \leq i \leq j} \deg a_i = \deg g_j$. For a fixed j with $1 \leq j \leq m$, put $H_1 = g_{j-1}f - f_{j-1}g$ and $H_2 = f_{j-1}$. Then f divides $H_1 + H_2 g$ and we have $H_1 H_2 \neq 0$. Since $f \notin I_n(t_0)$ this implies that

$$\deg H_1 + \deg H_2 \geq t_0 + 1 > n - 2 - 2\log_q n.$$

Now

$$\deg H_1 + \deg H_2 = (n - \deg f_j) + \deg f_{j-1} = n - \deg a_j,$$

and so

$$\deg a_j < 2 + 2\log_q n.$$

Since this holds for every $1 \leq j \leq m$ we have the desired bound.

□

3.3 The Orthogonal Multiplicity of a Polynomial

We begin with a definition.

Definition 3.8 *Let g be a monic polynomial over $\mathbb{F}_q$ of degree $n \geq 1$. The **orthogonal multiplicity** of g is the number of coprime polynomials f in $\mathbb{F}_q[x]$ with $\deg f < n$ and $K(f/g) = 1$. We denote this by $m(g)$.*

This appellation is motivated by the "orthogonal sequences of polynomials" studied in classical analysis: one may show that the orthogonal multiplicity of a polynomial $g \in \mathbb{F}_q[x]$ of degree n is the number of choices for $g_0, g_1, \ldots, g_{n-1} \in \mathbb{F}_q[x]$, such that $g_0, \ldots, g_{n-1}, g$ is the initial segment of an orthogonal sequence of polynomials ([40]).

Thus Conjecture 3.5 claims that all polynomials over a finite field of size greater than 2 have positive orthogonal multiplicity. More generally, we consider the following related questions.

- For a given q, do all polynomials over $\mathbb{F}_q$ have positive orthogonal multiplicity?
- Can one put non-trivial bounds on the multiplicity of a polynomial?
- Can one characterise polynomials in terms of their multiplicities in any way?

We also broach the corresponding algorithmic problems in Chapter 7 where we ask

- Can one efficiently compute the orthogonal multiplicity of a given polynomial?

In the next two sections we describe the results which have been obtained and conjectures made for both general finite fields and specific fields. However, we first consider a few elementary ideas which throw some light on these problems.

Niederreiter was the first to observe that the average value of the orthogonal multiplicity of a monic polynomial of degree n over $\mathbb{F}_q$ is $(q-1)^n$ ([30, Page 281]). This is easily seen, as we now explain. The total number of continued fractions of the form $[\,0; a_1, a_2, \ldots, a_n\,]$ where $\deg a_j = 1$ for $1 \le j \le n$ is $q^n(q-1)^n$. Each of these corresponds to a unique pair of polynomials f and g, where g is monic of degree n and $f/g = [\,0; a_1, a_2, \ldots, a_n\,]$. From this it follows that

$$\sum_g m(g) = q^n(q-1)^n,$$

where the sum is taken over all monic polynomials in $\mathbb{F}_q[x]$ of degree n. There are q^n such polynomials, and Niederreiter's result now follows.

Thus if $q > 2$ the "expected value" for the orthogonal multiplicity of a monic polynomial grows exponentially with its degree. Unless there is very large "deviation" from this value, one would expect that all polynomials of sufficiently large degree have positive orthogonal multiplicity. Unfortunately, this has not yet been proved. When $q = 2$, the "expected value" is 1, and in this case unless all polynomials have the same multiplicity, some polynomials must have multiplicity zero. We shall see that indeed some polynomials over the binary field do have multiplicity zero.

Elementary considerations also allow one to put an upper bound on the orthogonal multiplicity. We have that

Proposition 3.9 *The orthogonal multiplicity of a monic polynomial of degree n over $\mathbb{F}_q$ is not greater than $(q-1)^{\lceil n/2 \rceil} q^{\lfloor n/2 \rfloor}$.*

Proof: We first consider the case n even. Suppose that $K(f/g) = 1$ where $\deg f < n$ and $\gcd(f, g) = 1$. Then $f/g = [\,0; a_1, a_2, \ldots, a_n\,]$ where $\deg a_j = 1$ for $1 \le j \le n$. Let f_j/g_j denote the jth convergent to f/g. Then

$$\begin{aligned} |f/g - f_{n/2}/g_{n/2}| &= 1/|a_{(n/2)+1}||g_{n/2}|^2 \\ &= q^{-(n+1)}, \end{aligned}$$

since $\deg g_{n/2} = \sum_{j=1}^{n/2} \deg a_j = n/2$. Thus f/g and $f_{n/2}/g_{n/2}$ agree on the first n coefficients $s_1, s_2, \ldots, s_n$, say, in their Laurent series expansions.

Suppose now that

$$h/g = [\,0; a_1, a_2, \ldots, a_{n/2}, b_{(n/2)+1}, b_{(n/2)+2}, \ldots, b_n\,],$$

where $h \in \mathbb{F}_q[x]$ and $\deg b_j = 1$ for $(n/2)+1 \le j \le n$. (Thus h is necessarily coprime to g and of degree less than n.) Then the $(n/2)$th convergent to h/g equals the

Mult.	Freq.	Mult.	Freq.	Mult.	Freq.
8	3	22	15	34	12
12	3	24	21	36	36
14	6	26	6	38	18
16	12	28	21	44	24
18	3	30	18	48	24
20	12	32	3	56	6

Table 3.1: Frequencies of Orthogonal Multiplicities for Polynomials of Degree 5 over $\mathbb{F}_3$

$(n/2)$th convergent to f/g. Thus f/g and h/g must agree on the first n coefficients $s_1, s_2, \ldots, s_n$ of their Laurent series expansions. But the remaining coefficients of each are entirely determined by the first n, in each case by the recurrence obtained from g. Thus we must have that $f/g = h/g$ and so $f = h$. From this it follows that the number of polynomials f of degree less than n and coprime to g such that $K(f/g) = 1$, is not greater than the number of choices of linear polynomials $a_1, a_2, \ldots, a_{n/2}$. This is $(q-1)^{n/2} q^{n/2}$, which proves the result in the even degree case.

The odd case is proved in a similar way. Let $a_1, \ldots, a_{\lfloor n/2 \rfloor}$ be fixed linear polynomials over $\mathbb{F}_q$ and a a fixed element of $\mathbb{F}_q{}^*$. Consider all rational functions of the form

$$[\,0; a_1, a_2, \ldots, a_{\lfloor n/2 \rfloor}, ax + b, b_{\lceil n/2 \rceil + 1}, \ldots, b_n\,],$$

where b_j $(\lceil n/2 \rceil \leq j \leq n)$ are linear polynomials and $b \in \mathbb{F}_q$. One may show that the Laurent series expansions of any two such rational functions agree in the first n coefficients. It follows as before that the orthogonal multiplicity of g, where $\deg g$ is odd, cannot be greater than the number of such rational functions, which is $(q-1)^{\lceil n/2 \rceil} q^{\lfloor n/2 \rfloor}$. This completes the proof.

□

Example 3.10 (Some experimental data for $\mathbb{F}_3$.) There are $3^5 = 243$ monic polynomials of degree 5 over $\mathbb{F}_3$. The average value of the orthogonal multiplicity is $2^5 = 32$ and by Proposition 3.9 the upper bound is 72. Computation reveals that the lowest orthogonal multiplicity which occurs is 8, and the highest is 56. Table 3.1 gives a complete breakdown of the frequencies of multiplicities of such polynomials.

3.3.1 Results for Arbitrary Finite Fields

Blackburn is able to prove a general result for arbitrary finite fields by working with the Laurent series expansions and sequences associated with the rational functions, rather than with rational functions themselves. We outline Blackburn's work in this section. Following Blackburn, we will show

Result 3.11 *[6, Theorem 2] Let g be a monic polynomial over $\mathbb{F}_q$ of degree $n \geq 1$. If $n(n-1)/2 \leq q$ then g has positive orthogonal multiplicity.*

We now introduce the ideas necessary to sketch a proof of Result 3.11.

Let $s = f/g$ be a rational function over a finite field $\mathbb{F}_q$, with $\deg f < \deg g = n$. Suppose s has Laurent series expansion $\sum_{i\geq 1} s_i x^{-i}$, and continued fraction expansion $[\,0; a_1, a_2, \ldots, a_m\,]$. For $j \geq 1$, define the ***j*th Hankel determinant** to be

$$H_j(s) = \begin{vmatrix} s_1 & s_2 & \ldots & s_j \\ s_2 & s_3 & \ldots & s_{j+1} \\ \vdots & \vdots & & \vdots \\ s_j & s_{j+1} & \ldots & s_{2j-1} \end{vmatrix}$$

One may show that $H_j(s) \neq 0$ for some j, if and only if there is a convergent to s whose denominator has degree j ([6, Lemma 2]). Now $K(s) = 1$ and $\gcd(f, g) = 1$ if and only if there is a convergent to s whose denominator has degree j for every $1 \leq j \leq n$. This is easily seen by considering the recurrence (2.14) which defines the denominators g_j of the convergents f_j/g_j $(1 \leq j \leq m)$ to s. Tying these together, we see that $K(s) = 1$ and $\gcd(f, g) = 1$ if and only if $H_j(s) \neq 0$ for $1 \leq j \leq n$.

Let Z be the set of all rational functions of the form f/g where $\deg f < \deg g = n$. For each $1 \leq j \leq n$, let $V_j \subseteq Z$ be the subset defined by

$$V_j = \{s \in Z \mid H_j(s) = 0\}.$$

If $s = f/g \in Z$, then $K(s) = 1$ and $\gcd(f, g) = 1$, if and only if $s \notin V_j$ for $1 \leq j \leq n$. Thus g has positive orthogonal multiplicity if and only if $\cup_{j=1}^n V_j \neq Z$.

We now prove Blackburn's theorem.

Proof: We may regard Z as an n dimensional vector space over $\mathbb{F}_q$: Any element of Z is uniquely determined by the first n coefficients $s_1, s_2, \ldots, s_n$ of its Laurent series expansion, later terms being fixed linear combinations of these coefficients, the linear combination determined by the recurrence associated with g (see Definition 2.32). Thus for every positive integer j, we may find a polynomial $h_j \in \mathbb{F}_q[X_1, X_2, \ldots, X_j]$ which has degree at most j and is such that $H_j(s) = h_j(s_1, s_2, \ldots, s_n)$ for all $s = \sum_{i\geq 1} s_i x^{-i}$. When $j \in \{1, 2, \ldots, n\}$, we have that $h_j \neq 0$, since the Laurent series $s = \sum_{i\geq 1} s_i x^{-i}$ defined by

$$s_i = \begin{cases} 0 & \text{if } i \leq n \text{ and } i \neq j \\ 1 & \text{if } i = j \\ -\sum_{j=0}^{n-1} a_j s_{i-n+j} & \text{if } i > n \end{cases}$$

has the property that $h_j(s_1, s_2, \ldots, s_n) = H_j(s) = 1 \neq 0$.

The set V_j is equal to the affine variety corresponding to the principal ideal in $\mathbb{F}_q[X_1, X_2, \ldots, X_n]$ generated by h_j. Define $h = h_1 h_2 \ldots h_n$. The set $\cup_{j=1}^n V_j$ is equal to the variety corresponding to the principal ideal generated by h. Clearly h is non-zero and has degree at most $\frac{1}{2}n(n+1)$. We have that $\cup_{j=1}^n V_i = Z$ if and only if $h(s_1, s_2, \ldots, s_n) = 0$ for all $s_1, s_2, \ldots, s_n \in \mathbb{F}_q$. Now a standard result ([23, Theorem 6.13]) tells us that the cardinality of the zero set of h is at most $(\deg h)q^{n-1}$. Thus if $q > \frac{1}{2}n(n+1) \geq \deg h$ then h is not zero everywhere, which proves the result in this case. If $q = \frac{1}{2}n(n+1)$ then $q = 3$ and $n = 2$ and the result is easily checked by hand. This completes the proof.

□

It is of interest to observe that this argument may be adapted to prove that all polynomials defined over infinite fields have "positive multiplicity" ([6]).

We conclude this section with an explicit example which illustrates the above proof.

Example 3.12 (Computing the orthogonal multiplicity of a polynomial over $\mathbb{F}_3$.) Consider the polynomial $g = x^3 + 2x^2 + x = x(x+1)^2$ over $\mathbb{F}_3$. Then $\deg g = 3$ and $\frac{1}{2}3(3+1) > 3$. So the above theorem does not apply. However, we can use the methods of the theorem to calculate the orthogonal multiplicity of g. We need to compute the trivariate polynomial h associated with g and calculate the size of its zero set. Now $h = h_1h_2h_3$ where $h_j \in \mathbb{F}_q[X_1,\dots,X_j]$ is given by

$$h_1 \;=\; |X_1|, \quad h_2 \;=\; \begin{vmatrix} X_1 & X_2 \\ X_2 & X_3 \end{vmatrix}, \quad h_3 \;=\; \begin{vmatrix} X_1 & X_2 & X_3 \\ X_2 & X_3 & 2X_2+X_3 \\ X_3 & 2X_2+X_3 & 2X_2+2X_3 \end{vmatrix}.$$

Multiplying out and simplifying we see that

$$h = X_1(X_1X_3 - X_2^2)(X_1X_2X_3 + X_1X_3^2 - X_1X_2^2 + X_2^3 - X_2X_3^2 - X_2^2X_3 - X_3^3).$$

Letting the zero sets of h_j be denoted V_j it is easily seen that

$$\begin{array}{rcl} V_1 & = & \{(0,a,b) \mid a,b \in \mathbb{F}_3\} \\ V_2 & = & \{(0,0,a),(a,0,0),(1,b,1),(2,b,2) \mid a,b \in \mathbb{F}_3,\ b \neq 0\} \end{array}$$

Thus the cardinality of $V_1 \cup V_2$ is 15. It only remains to check which of the 12 points that do not lie on $V_1 \cup V_2$ lie on V_3. It may be checked by hand that exactly 6 of these points lie on V_3 (the points $(1,0,1),(1,1,0),(1,2,2),(2,0,2),(2,1,1),(2,2,0)$). Hence the orthogonal multiplicity of g, which is just the cardinality of the complement of the zero set of h, is $27-(15+6) = 6$. Observe that applying Proposition 3.9 to this polynomial, we see that its multiplicity must be not more than 12. We will return to this polynomial in Example 4.10 at the end of Chapter 4.

3.3.2 Results for the Binary Field

All results prior to those in this thesis for polynomials over the binary field depend upon a simple characterisation of binary Laurent series s with partial quotients all of degree 1 first obtained by Baum and Sweet. In [5] they observe that if $s = \sum_{i\geq 1} s_i x^{-i} = [\,0; a_1, a_2, \dots]$ is an irrational Laurent series over $\mathbb{F}_2$ then $\deg a_j = 1\,(j \geq 1)$ if and only if

$$\begin{array}{rcl} s_1 & = & 1 \\ s_i + s_{2i} + s_{2i+1} & = & 0 \quad \text{for } i \geq 1. \end{array} \tag{3.1}$$

We do not prove this here, as it will follow as a corollary of a more general investigation in Chapter 6 (see Example 6.20). Baum and Sweet then observe ([4, page 577]) that if $s = f/g = \sum_{i\geq 1} s_i x^{-i}$ where $\deg g = n$ then $K(s) = 1$ and $\gcd(f,g) = 1$ if and only if

$$\begin{array}{rcl} s_1 & = & 1 \\ s_i + s_{2i} + s_{2i+1} & = & 0 \quad \text{for } 1 \leq i \leq n-1. \end{array} \tag{3.2}$$

This observation is not difficult to prove, given the characterisation of irrational Laurent series with partial quotients all of degree 1 mentioned above. For suppose that f/g satisfies recurrences (3.2). Let the irrational Laurent series $t = \sum_{i\geq 1} t_i x^{-i}$ be given by

$$\begin{array}{rcll} t_i & = & s_i & \text{for } 1 \leq i \leq 2n-1 \\ t_{2i} & = & s_{2i} & \text{for } 2i \geq 2n \\ t_{2i+1} & = & t_{2i} + t_i & \text{for } 2i+1 \geq 2n+1. \end{array}$$

Then all of the partial quotients of t, excluding the 0th, have degree 1, since t satisfies recurrences (3.1). Now

$$|(f/g) - t| \leq 2^{-(2n+1)},$$

and thus by Result 2.27 in Chapter 2, we have that f/g is a convergent to t and so $K(f/g) = 1$. Conversely, suppose that $K(f/g) = 1$ with $f/g = [\,0; a_1, a_2, \ldots, a_n\,]$. Letting $t = [\,0; a_1, a_2, \ldots, a_n, x, x, \ldots\,]$ we see that the coefficients in the Laurent series expansion of t satisfy recurrence (3.1), as all the partial quotients of t have degree 1. Since $|t - (f/g)| = 2^{-(2n+1)}$ we have that the coefficients in the Laurent series expansion of f/g must satisfy recurrence (3.2), as we wished to show.

Thus for the binary field, the difficult non-linear problem we confronted in the last section miraculously collapses down to a tractable linear one. An application of linear algebra now allows one to make great progress in tackling the pertinent questions. In particular, we have

Result 3.13 *[6, Proposition 2] Let $g \in \mathbb{F}_2[x]$ with $\deg g \geq 1$. Then the orthogonal multiplicity of g is either 0 or 2^k where k is the number of distinct non-linear irreducible factors of g.*

Result 3.14 *[28] A non-linear irreducible polynomial over $\mathbb{F}_2$ has orthogonal multiplicity 2.*

Recall that the average value for $m(g)$ over all polynomials of degree n in $\mathbb{F}_2[x]$ is 1. Since there certainly exist irreducible polynomials of each degree, by Result 3.14 we immediately see that for each degree greater than 1 there must be polynomials of orthogonal multiplicity zero.

We outline the proof of the first of these results for the case x does not divide g; a full proof can be found in [6]. We also give the proof of a modest generalisation of the second. Once again, we follow the elegant approach taken by Blackburn.

We begin by stating a result due to Blackburn which generalises the well-known trace representation of "M-sequences". A proof of this result can be found in [6, page 103].

Result 3.15 *[6, Proposition 1] Let $g \in \mathbb{F}_q[x]$ be a non-zero polynomial of degree n. Define $R_g = \mathbb{F}_q[x]/g\mathbb{F}_q[x]$. Let $\pi : R_g \to \mathbb{F}_q$ be a non-degenerate linear functional. (That is to say, π is non-trivial on all non-zero ideals of R_g, and so the map $(x, y) \mapsto \pi(xy)$ is a non-degenerate symmetric bilinear form on R_g.) Let $S = \{s_i\}_{i\geq 1}$ be a sequence of elements of $\mathbb{F}_q$. Then S has characteristic polynomial g if and only if there exists $r \in R_g$ such that*

$$s_i = \pi(rx^{i-1}) \text{ for } i \geq 1.$$

Moreover, the element r is unique.

Let $g \in \mathbb{F}_q[x]$ with $\deg g = n$, and π be a non-degenerate linear functional on R_g. Suppose that there exists an $r \in R_g$ such that

$$\begin{aligned} \pi(rx^0) &= 1 \\ \pi(r(x^{i-1} + x^{2i-1} + x^{2i})) &= 0 \quad \text{for } 1 \leq i \leq n-1. \end{aligned} \tag{3.3}$$

Then the sequence $S = \{s_i\}_{i\geq 1}$ given by $s_i = \pi(rx^{i-1})$ will have characteristic polynomial g and satisfy condition (3.2). Hence for $f/g := \sum_{i\geq 1} s_i x^{-i}$ we will have that

$K(f/g) = 1$ and $\gcd(f, g) = 1$. Conversely, if $\gcd(f, g) = 1$ and $K(f/g) = 1$, then if we write $f/g = \sum_{i \geq 1} s_i x^{-i}$ we shall find that the unique element $r \in R_g$ such that $s_i = \pi(rx^{i-1})$ $(i \geq 1)$ satisfies conditions (3.3). Thus the orthogonal multiplicity of g is the number of $r \in R_g$ such that r satisfies conditions (3.3). By "duality", such an r exists provided x^0 does not lie in the subspace of R_g generated by the set $\{x^{i-1} + x^{2i-1} + x^{2i} \,|\, 1 \leq i \leq n-1\}$. This can be checked efficiently for any g, as we shall explain in Section 7.2.1 of Chapter 7. In the case that x does not divide g, we can transform this condition into an alternative simpler condition which we use to prove this case of Result 3.13.

So suppose now that x does not divide g. Then x is invertible in the ring R_g and so given any $r \in R_g$ we may write $r = mx$ where $m \in R_g$. This may be done in a unique way. Thus the orthogonal multiplicity of g is the number of elements $m \in R_g$ such that

$$\begin{aligned} \pi(mx) &= 1 \\ \pi(m(x^i + x^{2i} + x^{2i+1})) &= 0 \quad \text{for } 1 \leq i \leq n-1. \end{aligned} \tag{3.4}$$

So the orthogonal multiplicity of g is positive provided x does not lie in the subspace generated by the set $\{x^i + x^{2i} + x^{2i+1} \,|\, 1 \leq i \leq n-1\}$. We reformulate this condition by considering a particular linear transformation on R_g.

Define the linear map $T : R_g \to R_g$ by

$$h \mapsto h + (1+x)h^2.$$

Note that $T(1) = x$ and $T(x^i) = x^i + x^{2i} + x^{2i+1}$. Let

$$V = \{x^i + x^{2i} + x^{2i+1} \,|\, 0 \leq i \leq n-1\}.$$

So V is the image of R_g under T. Hence

$$\begin{aligned} \dim V &= \dim R_g - \dim \ker T \\ &= n - \dim \ker T. \end{aligned}$$

If we let

$$W = \{x^i + x^{2i} + x^{2i+1} \,|\, 1 \leq i \leq n-1\}$$

then we see that W is the image under T of the subspace U generated by $x, x^2, \ldots, x^{n-1}$.

Thus

$$\begin{aligned} \dim W &= \dim U - \dim \ker T|_U \\ &= (n-1) - \dim(\ker T \cap U). \end{aligned}$$

Let

$$W^\perp = \{e \in R_g \,|\, \pi(ew) = 0 \text{ for all } w \in W\},$$

and

$$V^\perp = \{e \in R_g \,|\, \pi(ev) = 0 \text{ for all } v \in V\},$$

denote the orthogonal complements of W and V with respect to the non-degenerate symmetric bilinear form given by π. An element $m \in R_g$ will satisfy conditions (3.4) if and only if $m \in W^\perp$ but $m \notin V^\perp$. Since $W \subseteq V$ we have that $V^\perp \subseteq W^\perp$. Thus the orthogonal multiplicity of g is the cardinality of $W^\perp - V^\perp$. Now

$$\begin{aligned} \dim W^\perp &= n - ((n-1) - \dim(\ker T \cap U)) \\ &= 1 + \dim(\ker T \cap U), \end{aligned}$$

and

$$\begin{aligned}\dim V^{\perp} &= n-(n-\dim\ker T)\\ &= \dim\ker T.\end{aligned}$$

So $\dim W^{\perp}-\dim V^{\perp}=1-(\dim\ker T-\dim(\ker T\cap U))$. Therefore if $\ker T\not\subseteq U$ then $W^{\perp}=V^{\perp}$ and the orthogonal multiplicity of g is zero. If $\ker T\subseteq U$ then the cardinality of $W^{\perp}-V^{\perp}$ is $2^{1+\dim(\ker T\cap U)}-2^{\dim\ker T}=2^{1+\dim\ker T}-2^{\dim\ker T}=2^{\dim\ker T}$.

We have shown

Proposition 3.16 *Let $g\in\mathbb{F}_2[x]$ with g not divisible by x. Let R_g and T be as in the preceding discussion. Then g has positive orthogonal multiplicity if and only if* $\ker T\subseteq U$. *In this case, the orthogonal multiplicity of g is the cardinality of* $\ker T$.

We may now prove Result 3.13 for the case x does not divide g.

Proof: Suppose that $g\in\mathbb{F}_2[x]$ with g not divisible by x. From Proposition 3.16, we know that the orthogonal multiplicity of g is either 0 or $2^{\dim\ker T}$. It therefore remains to show that the $\dim\ker T$ is the number of non-linear irreducible factors of g.

Let $g=(x+1)^{e_1}\prod_{2\le i\le k+1}g_i^{e_i}$, where $g_i\,(2\le i\le k+1)$ are non-linear irreducible binary polynomials. Then from the Chinese Remainder Theorem for polynomials ([2, page 136]) we see that

$$R_g\cong\oplus_{i=1}^{k+1}R_{g_i^{e_i}}$$

where $g_1=x+1$. Here "$\cong$" denotes an isomorphism of rings. Thus we may write

$$\ker T\cong\oplus_{i=1}^{k+1}\ker T_{R_{g_i^{e_i}}},$$

where $T_{R_{g_i^{e_i}}}$ denotes the map from $R_{g_i^{e_i}}$ to $R_{g_i^{e_i}}$ given by

$$h\mapsto h^2(1+x)+h. \tag{3.5}$$

On $R_{g_1^{e_1}}=R_{(x+1)^{e_1}}$ this map is injective, as we now show: It is easily seen that the only divisors of zero in $R_{(x+1)^{e_1}}$ are the non-zero elements of the form $z(x+1)^i$ where $1\le i\le e_1-1$ and $z\in R_{(x+1)^{e_1}}$. Also, since $1+x$ is a divisor of zero there are no h in $R_{(x+1)^{e_1}}$ with $h(1+x)+1=0$. So the only possible elements of the kernel of the map (3.5) on $R_{(x+1)^{e_1}}$ are $h=0$, and those elements h such that $h\ne0$ and $h(1+x)+1\ne0$ but $h(h(1+x)+1)=0$. Thus an $h\ne0$ is in the kernel of this map only if both h and $h(1+x)+1$ are zero divisors. But in this case $1+x$ divides both h and $h(1+x)+1$, which clearly cannot happen. Thus $\ker T_{R_{(x+1)^{e_1}}}=\{0\}$.

Finally, we observe that $\dim\ker T_{R_{g_i^{e_i}}}=1$ for $2\le i\le k+1$: following similar arguments to those in the preceding paragraph, it is easily seen that the kernel of the map $T_{R_{g_i^{e_i}}}$ consists of the elements 0 and $(1+x)^{-1}$. The latter element existing since $\gcd(1+x,g_i)=1$ for $2\le i\le k+1$. Thus $\dim\ker T=k$, as required.

□

We may now prove that the orthogonal multiplicity of a non-linear irreducible binary polynomial is 2. In fact, we prove a slight generalisation of this result

Proposition 3.17 *The orthogonal multiplicity of a power of a non-linear irreducible binary polynomial is* 2.

Proof: Let $g = r^t$ where r is a non-linear irreducible polynomial over $\mathbb{F}_2$. Thus x does not divide g, and so Proposition 3.16 applies. The kernel of the map $T : R_{r^t} \to R_{r^t}$ is the set of all $h \in R_{r^t}$ such that

$$h^2(1+x) + h = 0. \tag{3.6}$$

One may argue as in the proof of Result 3.13 that there are no solutions to equation (3.6) which arise from zero divisors. Hence the kernel of T consists solely of the elements 0 and $(1+x)^{-1}$, this latter element existing since $\gcd(1+x, g) = 1$. We need to show that both of these elements lie in U. Certainly $0 \in U$. Writing $g = \sum_{i=0}^{n} g_i x^i$, we see that

$$(1+x)^{-1} = \sum_{k=1}^{n-1} \left(\sum_{i=1}^{k} g_i \right) x^k$$

This may be verified by multiplying both sides of the equation by $1+x$ and using the fact that $g_0 = 1$. Thus $(1+x)^{-1} \in U$. Hence the orthogonal multiplicity of $g = r^t$ is the cardinality of $\ker T$ which is 2.

□

This proof demonstrates the techniques used by Blackburn to obtain results over the binary field. We shall return to this in Chapter 7 in which we discuss efficient algorithms for computing the orthogonal multiplicity of a binary polynomial.

Finally, Blackburn also proves the following result. We give a simpler and more revealing proof of this result in Chapter 4 (Corollary 4.8).

Result 3.18 *Let $g \in \mathbb{F}_2[x]$. Then g has orthogonal multiplicity* 1 *if and only if $g = x^{m_1}(x+1)^{m_2}$ where $\binom{m_1+m_2}{m_1} \equiv 0 \bmod 2$.*

We finish with an example which illustrates the methods we have employed in this section.

Example 3.19 In this example, we show how one may compute by hand the orthogonal multiplicity of a binary polynomial, provided the factorisation is known. Note that we present a more practical method for doing this in Example 7.2 of Chapter 7, and this example is intended only to illustrate some of the ideas we have used. Consider the polynomial

$$\begin{aligned} g &= (x+1)(x^2+x+1)^2(x^3+x^2+1) \\ &= x^8+x^5+x^4+x^3+x+1. \end{aligned}$$

Adopting the above notation, we must compute the kernel of the map T on R_g. Now

$$R_g \cong \oplus_{i=1}^{3} R_{g_i^{e_i}},$$

where $g_1^{e_1} = (x+1), g_2^{e_2} = (x^2+x+1)^2$ and $g_3^{e_3} = (x^3+x^2+1)$. From the proof of Result 3.13 we see that the kernel of this map is the vector space spanned by the set

$$\{(0,a,0),(0,0,b)\} \subseteq \oplus_{i=1}^{3} R_{g_i^{e_i}},$$

where a is the inverse of $(1+x)$ in $R_{(x^2+x+1)^2}$, and b is the inverse of $(1+x)$ in $R_{x^3+x^2+1}$. Using the Euclidean Algorithm, we find that $a = x^3+x^2$ and $b = x^2$. We now must write the elements $(0,a,0)$ and $(0,0,b)$ of $\oplus_{i=1}^{3} R_{g_i^{e_i}}$ in terms of the basis $1, x, x^2, \ldots, x^7$ of R_g. This may be done using the Chinese Remainder Theorem, and we have

$$\begin{aligned} (0,a,0) &= x^6+x^5+x^4+x \\ (0,0,b) &= x^7+x^6+x+1 \end{aligned}$$

Thus $\ker T$ is not contained in the subspace U of R_g generated by $x, x^2, \ldots, x^7$, and Proposition 3.16 tells us that the orthogonal multiplicity of $g = x^8+x^5+x^4+x^3+x+1$ is zero. We shall return to this example at the end of Section 7.2.1 in Chapter 7.

3.4 Motivation

Mathematicians working in this area appear to have approached it from one or more of the following three directions.

- The study of the Euclidean Algorithm for polynomials.
- The study of the linear complexity profiles of sequences over finite fields.
- The study of the statistical properties of a specific pseudorandom number generator.

We discuss all three in the following sections.

3.4.1 The Euclidean Algorithm for Polynomials

The work of Mesirov and Sweet ([28]) on the continued fraction expansions of rational functions over the binary field is presented in terms of the Euclidean Algorithm. This connection is undoubtedly the most transparent of the three. We discuss how this relates to computing inverses in polynomial rings.

Recall that one may use the "Extended Euclidean Algorithm" to compute the inverse of a polynomial f modulo a coprime polynomial g. Let $f/g = [\,a_0; a_1, a_2, \ldots, a_m\,]$ and f_k/g_k denote the kth convergent to f/g. We may assume that $\deg f < \deg g$ since we are thinking of f as an element of $\mathbb{F}_q[x]/g\mathbb{F}_q[x]$. We know that $f_m g_{m-1} - f_{m-1} g_m = (-1)^{m-1}$. Now $f/g = f_m/g_m$ and so $f = l f_m$ and $g = l g_m$ for some $l \in {\mathbb{F}_q}^*$. Hence $f(l^{-1} g_{m-1}) \equiv (-1)^{m-1} \bmod g$. Thus

$$f^{-1} \bmod g = \begin{cases} l^{-1} g_{m-1} \bmod g & \text{if } m \text{ is odd,} \\ -l^{-1} g_{m-1} \bmod g & \text{if } m \text{ is even.} \end{cases}$$

Once we have computed the continued fraction expansion of f/g, which takes m polynomial divisions, we can recover g_{m-1} and hence $f^{-1} \bmod g$ using recurrences (2.14) which involves m polynomial multiplications. We shall call this the **EEA-method** for computing inverses in polynomial factor rings. Thus the EEA-method for computing the inverse of f modulo g, where $\gcd(f, g) = 1$ and $f/g = [\,0; a_1, a_2, \ldots, a_m\,]$, takes m polynomial divisions and m multiplications. Now $m \le \deg g = n$ and thus m is maximal when f/g has n partial quotients (excluding the 0th one), which forces $K(f/g) = 1$. Thus our first question (following Definition 3.8) can be rephrased as

> For any polynomial g of degree n can we find an element in $\mathbb{F}_q[x]/g\mathbb{F}_q[x]$ for which it takes n polynomial divisions and n multiplications to compute its inverse using the EEA-method?

This question is of particular interest when g is irreducible and $\mathbb{F}_q$ is a prime field. In this case we are working in $\mathbb{F}_p[x]/g\mathbb{F}_p[x] \cong \mathbb{F}_q$, where $q = p^n$. Here the question relates to the worst case running time of the EEA-method for computing inverses in a non-prime field using polynomial arithmetic over the underlying prime field. Thus Result 3.14 tells us that for any non-prime finite field $\mathbb{F}_{2^n}$ of characteristic 2, we can find exactly two elements whose inversion takes as long as theoretically possible using the EEA-method. It should be mentioned, however, that there are faster algorithms for computing inverses in such polynomial rings and finite fields, and so these observations are only of theoretical interest ([2, page 150]).

3.4.2 The Linear Complexity Profiles of Sequences

We have already discussed in some detail in Section 2.4 of Chapter 2 the relation between linear complexity and continued fractions. To express concisely how the notion of orthogonal multiplicity fits into this picture we need one last definition.

Definition 3.20 *[16, page 101] Let $S = \{s_i\}_{i\geq 1}$ be an eventually periodic sequence whose minimal polynomial has degree n, and which has jumps sequence*

$$\underbrace{111\ldots 11}_{n}.$$

*We say that S has a **perfect staircase profile**.*

The notion of a perfect staircase profile is closely related to that of a **perfect linear complexity profile**. We say that a sequence has a perfect linear complexity profile if its generating function is irrational and has partial quotients all of degree 1 (excluding the 0th, which is just 0).

Result 2.38 tells us that S has a perfect staircase profile if and only if $K(s) = 1$. In this context, our first question (following Definition 3.8) can be paraphrased as

> Is any polynomial the minimal polynomial of a sequence with a perfect staircase profile?

3.4.3 Pseudorandom Number Generation

Niederreiter's interest in continued fractions with partial quotients of small degree appears to have arisen from a connection with a pseudorandom number generator proposed by Tausworthe. In this section, we briefly discuss this connection, closely following Niederreiter's own exposition on this topic in [30, Page 270].

Let p be a prime and let $y_0, y_1, y_2, \ldots$ be a sequence of integers in the least residue system mod$p$ generated by the recursion

$$y_{n+k} \equiv a_{k-1}y_{n+k-1} + \ldots + a_0 y_n \bmod p \text{ for } n \geq 0,$$

where $a_0, \ldots, a_{k-1}$ are fixed integer coefficients, with $a_0 \not\equiv 0 \bmod p$ and the initial values $y_0, \ldots, y_{k-1}$ are not all 0. Then pseudorandom numbers simulating the interval $[0, 1]$ are defined by

$$x_n = \sum_{j=1}^{k} y_{kn+j-1}p^{-j} \in [0,1] \text{ for } n \geq 0.$$

An important role in the theoretical analysis of these pseudorandom numbers is played by the characteristic polynomial

$$f(x) := x^k - a_{k-1}x^{k-1} - \ldots - a_0,$$

of the recursion, which is viewed as a polynomial over the finite field $\mathbb{F}_p$ with p elements. Define $L(f) = K(f/x^k)$. Niederreiter shows that a connection with $L(f)$ arises when one considers the statistical independence of the pairs x_n and x_{n+1} of consecutive random numbers. In particular, the polynomial f should be chosen so that $L(f)$ is small. We refer the reader to [30] for further information on this connection as we shall not pursue it in this thesis.

Chapter 4

Polynomials with Odd Orthogonal Multiplicity

4.1 Introduction

We begin by recalling the definitions and notation we shall need in this chapter. If f and g are polynomials over a finite field $\mathbb{F}_q$ with $\gcd(f, g) = 1$ and $\deg g \geq 1$, then the rational function f/g has a unique continued fraction expansion

$$a_0 + 1/(a_1 + 1/(a_2 + \ldots + 1/a_m))$$

where $a_j \in \mathbb{F}[x]$ for $0 \leq j \leq m$ and $\deg a_j \geq 1$ for $1 \leq j \leq m$. We write the above continued fraction as $[\, a_0\, ; a_1, a_2, \ldots, a_m\,]$ and define

$$K\left(\frac{f}{g}\right) = \max_{1 \leq j \leq m} \deg a_j.$$

For a monic $g \in \mathbb{F}_q[x]$ with $\deg g = n \geq 1$, we denote by $m(g)$ the number of $f \in \mathbb{F}_q[x]$ with $\deg f < n$, such that $\gcd(f, g) = 1$ and $K(f/g) = 1$. So $m(g)$ is the cardinality of the set

$$M_g := \{f/g \in \mathbb{F}(x) \mid \deg f < n, \gcd(f, g) = 1, \text{ and } K(f/g) = 1\}.$$

We call $m(g)$ the orthogonal multiplicity of g, or when there is no possibility of confusion, simply the multiplicity of g.

We will be concerned primarily with polynomials over finite fields which have positive orthogonal multiplicity; as we observed in the preceding chapter, they arise in stream cipher theory, a sub-discipline of cryptography, as the minimal polynomials of sequences over finite fields with perfect staircase profiles. More recently, Blackburn, and Cattell and Muzio have applied such polynomials to cellular automata theory ([7, 9]).

For a given finite field $\mathbb{F}_q$, it is of interest to ask exactly which polynomials over $\mathbb{F}_q$ have positive orthogonal multiplicity, and what can be said about their multiplicities. Some results in this direction, and in related areas ([30, 32]), have already been established, as we described in some detail in Chapter 3. In [6] Blackburn shows that if $g \in \mathbb{F}_q[x]$ with $\deg g = n$, then g has positive multiplicity provided $\frac{1}{2}n(n+1) \leq q$. Blackburn conjectures that if $q \neq 2$ then every polynomial over $\mathbb{F}_q$ has positive multiplicity. The situation over $\mathbb{F}_2$ is somewhat different; in particular, there exist polynomials over $\mathbb{F}_2$ with multiplicity zero. However, Mesirov and Sweet ([28])

prove that all non-linear irreducible polynomials over $\mathbb{F}_2$ have multiplicity 2, and one may further show ([6, 28]) that if a polynomial g over $\mathbb{F}_2$ has positive multiplicity then it has multiplicity 2^k, where k is the number of distinct non-linear irreducible factors of g.

In Section 4.3 of this chapter we characterize polynomials which have odd orthogonal multiplicity and give a lower bound on the multiplicity of such polynomials. This bound is used in Section 4.4 to prove that if the characteristic of $\mathbb{F}_q$ is 2 and $q \neq 2$, then a polynomial over $\mathbb{F}_q$ has multiplicity $q-1$ if and only if it has degree 1; and an alternative characterization to that in Blackburn's paper ([6]) is given in Section 4.4 of polynomials over $\mathbb{F}_2$ of multiplicity 1. Section 4.4 also contains a proof of the following result: if $g \in \mathbb{F}_2[x]$ splits into linear factors then there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f,g) = 1$ such that $K(f/g) \leq 2$. This establishes a special case of a conjecture made by Mesirov and Sweet ([28]). Section 4.5 contains a discussion of odd characteristic fields, as well as three examples. All of these results depend upon lemmas which are contained in Section 4.2.

4.2 Preliminaries

If $f/g = [\,0\,; a_1, a_2, \ldots, a_m\,]$ where f and g are polynomials over $\mathbb{F}_q$ and $\deg g \geq 1$, then $kf/g = [\,0\,; k^{-1}a_1, ka_2, \ldots, k^{(-1)^m}a_m\,]$ for any $k \in {\mathbb{F}_q}^*$. Hence if $f/g \in M_g$ then $kf/g \in M_g$ for any $k \in {\mathbb{F}_q}^*$, and so the orthogonal multiplicity of a polynomial over a field $\mathbb{F}_q$ is a multiple of $|{\mathbb{F}_q}^*| = q-1$. Since we are interested in this chapter mainly in polynomials with odd multiplicity, we shall primarily be concerned with finite fields of characteristic 2. Throughout this section and Sections 4.2.2, 4.3 and 4.4, $\mathbb{F}_q$ will be a finite field of characteristic 2.

4.2.1 Continued Fractions

Let f/g be a rational function over the field $\mathbb{F}_q$ with $\gcd(f,g) = 1$ and $f/g = [\,a_0\,; a_1, a_2, \ldots, a_m\,]$. Recall that the rational functions f_j/g_j $(0 \leq j \leq m)$ defined by

$$\begin{array}{ll} f_{-1} = 1,\ f_0 = a_0, & f_j = a_j f_{j-1} + f_{j-2}\,, \text{ for } 1 \leq j \leq m, \\ g_{-1} = 0,\ g_0 = 1, & g_j = a_j g_{j-1} + g_{j-2}\,, \text{ for } 1 \leq j \leq m. \end{array} \tag{4.1}$$

are called the convergents of f/g, and the polynomials a_j the partial quotients of f/g. It is easily shown that $f_j/g_j = [\,a_0\,; a_1, \ldots, a_j\,]$. One may write the above recurrences conveniently for $1 \leq j \leq m$ as

$$\begin{pmatrix} f_{j-1} & f_{j-2} \\ g_{j-1} & g_{j-2} \end{pmatrix} \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_j & f_{j-1} \\ g_j & g_{j-1} \end{pmatrix},$$

and so

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_j & f_{j-1} \\ g_j & g_{j-1} \end{pmatrix}. \tag{4.2}$$

Following [35], we write

$$\begin{pmatrix} f_j & f_{j-1} \\ g_j & g_{j-1} \end{pmatrix} \leftrightarrow [\,a_0\,; a_1, a_2, \ldots, a_j\,],$$

to indicate the correspondence between continued fractions and matrices of a particular form.

The above approach allows one to prove simple continued fraction identities with great ease. For example, taking the determinant of both sides of (4.2) gives us the identity $f_j g_{j-1} - g_j f_{j-1} = (-1)^{j+1}$ (Result 2.15 Part 2), or, as we are working in characteristic 2, $f_j g_{j-1} + g_j f_{j-1} = 1$. This implies that $\gcd(f_j, g_j) = 1$ and so the convergents are in reduced form.

The following lemma is central to the methods in this chapter.

Lemma 4.1 *Let* $\operatorname{char} \mathbb{F}_q = 2$ *and* $a \in \mathbb{F}_q[x]$. *For* $0 \le j \le m$, *let* f_j/g_j *denote the* j*th convergent of the continued fraction* $[\,0\,; a_1, a_2, \ldots, a_m\,]$. *So* $f_m/g_m = [\,0\,; a_1, a_2, \ldots, a_m\,]$. *Then*

1. $g_{m-1}/g_m = [\,0\,; a_m, a_{m-1}, \ldots, a_1\,]$.
2. $(f_m g_m + 1)/g_m^2 = [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m + 1, a_m + 1, a_{m-1}, \ldots, a_2, a_1\,]$.
3. $(a f_m g_m + 1)/a g_m^2 = [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m, a, a_m, a_{m-1}, \ldots, a_2, a_1\,]$.

The lemma may be deduced from results proved by Niederreiter in [30]; however, we give a simple proof which follows the approach taken by van der Poorten and Shallit in [35].

Proof: To prove Part 1, take the transpose of each side of (4.2). Putting $a_0 = 0$ and post-multiplying each side of the resulting identity by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gives us

$$\begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{j-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} g_j & f_j \\ g_{j-1} & f_{j-1} \end{pmatrix}. \tag{4.3}$$

Setting $j = m$ we get $g_m/g_{m-1} = [\,a_m\,; a_{m-1}, a_{m-2}, \ldots, a_1\,]$, and so $g_{m-1}/g_m = [\,0\,; a_m, a_{m-1}, \ldots, a_1\,]$.

We prove Part 2 by considering the matrix product

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_m + 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_m + 1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\leftrightarrow [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m + 1, a_m + 1, a_{m-1}, \ldots, a_2, a_1\,].$$

Multiplying the first m and the last $m-1$ matrices together using identities (4.2) and (4.3), with $j = m-1$, gives us

$$\begin{pmatrix} f_{m-1} & f_{m-2} \\ g_{m-1} & g_{m-2} \end{pmatrix} \begin{pmatrix} a_m + 1 & 1 \\ 1 & 0 \end{pmatrix}^2 \begin{pmatrix} g_{m-1} & f_{m-1} \\ g_{m-2} & f_{m-2} \end{pmatrix}.$$

We multiply these matrices using the fact that $f_{m-1} g_{m-2} + g_{m-1} f_{m-2} = 1$ to get

$$\begin{pmatrix} f_m g_m + 1 & f_m^2 \\ g_m^2 & f_m g_m + 1 \end{pmatrix},$$

and so $(f_m g_m + 1)/g_m^2 = [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m + 1, a_m + 1, a_{m-1}, \ldots, a_2, a_1\,]$.

The steps in the proof of Part 3 are outlined below; in this case the identity $f_m g_{m-1} + g_m f_{m-1} = 1$ is used.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} f_m & f_{m-1} \\ g_m & g_{m-1} \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} g_m & f_m \\ g_{m-1} & f_{m-1} \end{pmatrix} = \begin{pmatrix} af_mg_m + 1 & af_m^2 \\ ag_m^2 & af_mg_m + 1 \end{pmatrix}$$
$$\leftrightarrow [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m, a, a_m, a_{m-1}, \ldots, a_2, a_1\,].$$

□

Now, to facilitate the exposition, we introduce some new definitions and notation. Let $w = a_1a_2\ldots a_m$ be a word over the alphabet $\{a \in \mathbb{F}_q[x] \,|\, \deg a \geq 1\}$. We let $\overrightarrow{w} = w$ and $\overleftarrow{w} = a_ma_{m-1}\ldots a_1$ and write $[\,w\,]$ to mean $[\,0\,; a_1, a_2, \ldots, a_m\,]$. If $\overrightarrow{w} = \overleftarrow{w}$ then we call $[\,w\,]$ a **symmetric** continued fraction. Define the mapping ϕ on the set of all words by $\phi : a_1a_2\ldots a_m \mapsto a_1a_2\ldots a_{m-1}(a_m+1)$. Since $\operatorname{char} \mathbb{F}_q = 2$, the map ϕ is an involution.

Let g be a monic polynomial and suppose that $[\,w\,] \in M_g$, so each letter in the word w is a polynomial of degree 1. It is easily seen, by considering the recurrence relations (4.1) that generate the convergents of $[\,w\,]$, that $m = deg\, g$. The following observation will be of use in the proof of Theorem 4.5.

Observation 4.2 If $[\,w\,] \in M_g$ is a symmetric continued fraction and $\deg g$ is even then $w = \overrightarrow{v}\,\overleftarrow{v}$ for some word v, and if $\deg g$ is odd then $w = \overrightarrow{v}\ a\ \overleftarrow{v}$ for some word v and polynomial a of degree 1.

We restate the results in Lemma 4.1 which are of greatest relevance to us in the following way.

Lemma 4.3 *Let $\mathbb{F}_q$ be a finite field of characteristic 2.*

1. *If g is a monic polynomial and $[\,\overrightarrow{w}\,] \in M_g$, then $[\,\overleftarrow{w}\,] \in M_g$.*
2. *(i) If g is a monic polynomial and $[\,\overrightarrow{w}\,\overleftarrow{w}\,] \in M_g$, then $g = h^2$ for some monic polynomial h and $[\,\overrightarrow{\phi(w)}\,] \in M_h$.*

   (ii) If h is a monic polynomial, $[\,\overrightarrow{w}\,] \in M_h$ and $g = h^2$, then $[\,\overrightarrow{\phi(w)}\ \overleftarrow{\phi(w)}\,] \in M_g$.
3. *(i) If g is a monic polynomial and $[\,\overrightarrow{w}\ a\ \overleftarrow{w}\,] \in M_g$ with $a = kb$, b a monic polynomial of degree 1 and $k \in \mathbb{F}_q^*$, then $g = bh^2$ for some monic polynomial h and $[\,\overrightarrow{w}\,] \in M_h$.*

   (ii) If h is a monic polynomial, $[\,\overrightarrow{w}\,] \in M_h$, and $g = bh^2$ where b is a monic polynomial of degree 1, then $[\,\overrightarrow{w}\ a\ \overleftarrow{w}\,] \in M_g$ for any $a = kb$ where $k \in \mathbb{F}_q^*$.

Proof: The lemma is essentially a rewording of the special case of Lemma 4.1 in which all the partial quotients $a_j\,(1 \leq j \leq m)$ of f/g and the polynomial a are of degree 1. We prove Part 3; the other parts are proved in a similar way.

3(i) Let $[\,\overrightarrow{w}\ a\ \overleftarrow{w}\,] \in M_g$ where $a = kb$ with b a monic polynomial of degree 1 and $k \in \mathbb{F}_q^*$. Then there exists $f \in \mathbb{F}_q[x]$ with $f/g = [\,\overrightarrow{w}\ a\ \overleftarrow{w}\,]$. If we write $w = a_1a_2\ldots a_m$ where $\deg a_j = 1\,(1 \leq j \leq m)$, and let r_m/s_m denote the m^{th} convergent of the continued fraction $[\,w\,]$, then by Lemma 4.1 Part 3, $(ar_ms_m+1)/as_m^2 = [\,\overrightarrow{w}\ a\ \overleftarrow{w}\,]$. Hence $(ar_ms_m+1)/as_m^2 = f/g$. Let $as_m^2 = lbh^2$ where h is monic and $l \in \mathbb{F}_q^*$. Then $l^{-1}(ar_ms_m+1)/bh^2 = f/g$ with $\gcd\,(l^{-1}(ar_ms_m+1), bh^2) = \gcd\,(ar_ms_m+1, as_m^2) = 1$. Since $\gcd\,(f,g) = 1$ and both bh^2 and g are monic, we have that $g = bh^2$. Finally, $[\,\overrightarrow{w}\,] \in M_h$ since $\sqrt{kl^{-1}}r_m/h = [\,\overrightarrow{w}\,]$ and each letter in the word w is a polynomial of degree 1.

3(ii) Let $[\overrightarrow{w}] \in M_h$ where h is monic, and let $g = bh^2$ where b is monic of degree 1. Let $a = kb$ for some $k \in \mathbb{F}_q^*$. If we write $w = a_1a_2 \ldots a_m$ where $\deg a_j = 1\,(1 \le j \le m)$, and let r_m/s_m denote the m^{th} convergent of the continued fraction $[\overrightarrow{w}]$, then by Lemma 4.1 Part 3, $(ar_ms_m + 1)/as_m^2 = [\overrightarrow{w}\ a\ \overleftarrow{w}]$. Now $s_m = lh$ for some $l \in \mathbb{F}_q^*$, and so $as_m^2 = kl^2bh^2$. Thus $k^{-1}l^{-2}(ar_ms_m + 1)/bh^2 = (ar_ms_m + 1)/as_m^2$ and, moreover, $\gcd(k^{-1}l^{-2}(ar_ms_m + 1), bh^2) = \gcd(ar_ms_m + 1, as_m^2) = 1$. Since $g = bh^2$ and all the letters in the word $\overrightarrow{w}\ a\ \overleftarrow{w}$ are polynomials of degree 1, we have that $[\overrightarrow{w}\ a\ \overleftarrow{w}] \in M_g$.

□

4.2.2 Folded Polynomials

We define the set of all **folded polynomials** in $\mathbb{F}_q[x]$ recursively as follows.

1. If r is a monic polynomial of degree 1 then r is folded.

2. If r is folded then r^2 and ar^2 are folded, where a is a monic polynomial of degree 1.

The motivation for this definition comes from [35] in which a class of continued fractions dubbed "folded continued fractions" is studied by van der Poorten and Shallit; the denominators of certain types of "folded continued fractions" are folded polynomials, as we define them.

It is easily seen that folded polynomials are monic and split into linear factors. In fact, it is a simple matter to classify which polynomials of this form are folded. (We write $n = (\alpha_0\alpha_1\alpha_2\ldots)_2$ to indicate that $n = \sum_{i\ge 0}\alpha_i 2^i$ where $\alpha_i = 0$ or 1 for $i \ge 0$.)

Proposition 4.4 *Let $g \in \mathbb{F}_q[x]$, $\operatorname{char}\mathbb{F}_q = 2$, with $g = a_1^{m_1}a_2^{m_2}\ldots a_k^{m_k}$ where a_j is monic of degree 1 and $m_j = (\alpha_0^j\alpha_1^j\alpha_2^j\ldots)_2$ for $1 \le j \le k$. Then g is folded if and only if $\alpha_i^{j_1}\alpha_i^{j_2} = 0$ for all $1 \le j_1 \ne j_2 \le k$ and $i \ge 0$.*

Proof: For the sake of clarity we only consider the case $q = 2$; the general case is proved in an analogous fashion.

Let g be a folded polynomial over $\mathbb{F}_2$. Then g splits into linear factors and we may write $g = x^{m_1}(x+1)^{m_2}$ where $m_1 = (\alpha_0\alpha_1\alpha_2\ldots)_2$ and $m_2 = (\beta_0\beta_1\beta_2\ldots)_2$. If $\deg g = 1$ then $\alpha_i\beta_i = 0$ for $i \ge 0$. Let $\deg g > 1$. Observe that since g is folded at most one of m_1 and m_2 can be odd. Firstly, suppose that m_1 and m_2 are even, so $\alpha_0 = \beta_0 = 0$. Then $g = h^2$ where $h = x^{l_1}(x+1)^{l_2}$ is a folded polynomial with $l_1 = (\alpha_1\alpha_2\ldots)_2$ and $l_2 = (\beta_1\beta_2\ldots)_2$. We may assume by induction that $\alpha_i\beta_i = 0$ for $i \ge 1$. Hence $\alpha_i\beta_i = 0$ for $i \ge 0$. Suppose now that m_1 is odd and m_2 is even, so $\alpha_0 = 1$ and $\beta_0 = 0$. Then $g = xh^2$ where $h = x^{l_1}(x+1)^{l_2}$ is a folded polynomial with $l_1 = (\alpha_1\alpha_2\ldots)_2$ and $l_2 = (\beta_1\beta_2\ldots)_2$. Once again, we may assume by induction that $\alpha_i\beta_i = 0$ for $i \ge 1$. So $\alpha_i\beta_i = 0$ for $i \ge 0$, as required. The remaining case, m_0 even and m_1 odd, follows in the same way.

Conversely, let $\alpha_i\beta_i = 0$ for $i \ge 0$. If $\deg g = 1$ then g is folded. Let $\deg g > 1$. We have that $\alpha_0\beta_0 = 0$ and so there are three possibilities for the pair α_0, β_0: either $\alpha_0 = \beta_0 = 0$; $\alpha_0 = 1$ and $\beta_0 = 0$; or $\alpha_0 = 0$ and $\beta_0 = 1$. If $\alpha_0 = \beta_0 = 0$ then $g = h^2$ for some polynomial h. Now $h = x^{l_1}(x+1)^{l_2}$ where $l_1 = (\alpha_1\alpha_2\ldots)_2$ and $l_2 = (\beta_1\beta_2\ldots)_2$. Since $\alpha_i\beta_i = 0$ for $i \ge 1$ we may assume by induction that h is folded. Hence g is folded. The remaining two cases are proved in a similar way.

□

4.3 Theorems

The main theorem of this chapter reveals the intimate connection between polynomials with certain orthogonal multiplicities and the folded polynomials we have described.

Theorem 4.5 *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and let g be a monic polynomial over $\mathbb{F}_q$. Then g has odd orthogonal multiplicity if and only if g is folded.*

Proof: Let g be a monic polynomial. We first prove that if g has odd multiplicity then g is folded. To be more precise, we show that if g has odd multiplicity and $\deg g > 1$ then $g = ah^2$ where $a = 1$ or a is monic of degree 1, and where h is monic and has odd multiplicity. The result then follows by induction from the fact that all monic polynomials of degree 1 are folded.

Let g have odd multiplicity with $\deg g > 1$. Let θ denote the map that acts on the set $\{r/s \in \mathbb{F}_q(x) \mid \deg r < \deg s\}$ and sends the continued fraction $[\,\overrightarrow{w}\,]$ to the continued fraction $[\,\overleftarrow{w}\,]$. Then the set M_g is invariant under θ by Lemma 4.3 Part 1, and θ is an involution. Since $\#(M_g)$ is odd, there must exist an element of M_g which is fixed by θ. The involution θ fixes a continued fraction if and only if it is symmetric. So there exists a symmetric continued fraction $[\,v\,]$ in M_g. There are two cases to consider.

Firstly, suppose that $\deg g$ is odd. Then by Observation 4.2, $v = \overrightarrow{w}\ a\ \overleftarrow{w}$ for some word w and polynomial a of degree 1, and we have that $[\,\overrightarrow{w}\ a\ \overleftarrow{w}\,] \in M_g$. Let $a = kb$ where $k \in \mathbb{F}_q^*$ and b is monic. Then by Lemma 4.3 Part 3(i), $g = bh^2$ where h is monic and $[\,\overrightarrow{w}\,] \in M_h$. We need to show that h has odd multiplicity. Suppose then that $m(h)$ is even. Let $U = \{[\,\overrightarrow{w}\ c\ \overleftarrow{w}\,] \mid [\,\overrightarrow{w}\,] \in M_h,\, c = lb,\, l \in \mathbb{F}_q^*\}$. Since every continued fraction in U is symmetric, U is invariant under the involution θ, and by Lemma 4.3 Part 3(ii), we have that $U \subseteq M_g$. Hence $M_g - U$ is invariant under θ. Now $\#(U) = (q-1)\#(M_h) = (q-1)m(h)$, an even number. Therefore $\#(M_g - U)$ is odd, and so there must be a symmetric continued fraction $[\,\overrightarrow{u}\ d\ \overleftarrow{u}\,]$ in $M_g - U$ where u is a word and d is a polynomial of degree 1. Now $[\,\overrightarrow{u}\,] \in M_r$ for some unique monic r, and $d = le$ where e is monic and $l \in \mathbb{F}_q^*$. By Lemma 4.3 Part 3(i), $g = er^2$, and so $er^2 = bh^2$. If $e \neq b$ then e would occur as a factor an odd number of times on the left-hand side of this equation and an even number of times on the right-hand side. Therefore $e = b$ and so $r = h$, since $\operatorname{char} \mathbb{F}_q = 2$. But then $[\,\overrightarrow{u}\,] \in M_h$, and so $[\,\overrightarrow{u}\ d\ \overleftarrow{u}\,] \in U$. This is a contradiction and so $m(h)$ must be odd.

Suppose now that $\deg g$ is even. Then by Observation 4.2, $v = \overrightarrow{w}\overleftarrow{w}$ for some word w, and so $[\,\overrightarrow{w}\overleftarrow{w}\,] \in M_g$. Let h be the unique monic polynomial such that $[\,\overrightarrow{\phi(w)}\,] \in M_h$. Then by Lemma 4.3 Part 2(i), we have that $g = h^2$. We argue by contradiction to prove that $m(h)$ is odd. Suppose $m(h)$ is even. Let $U = \{[\,\overrightarrow{\phi(w)}\ \overleftarrow{\phi(w)}\,] \mid [\,\overrightarrow{w}\,] \in M_h\}$. Then by Lemma 4.3 Part 2(ii), $U \subseteq M_g$ and we further have that $M_g - U$ is invariant under the involution θ. Now $\#(U) = \#(M_h)$ is even and so $\#(M_g - U)$ is odd, and there must be a symmetric continued fraction, $[\,\overrightarrow{u}\,\overleftarrow{u}\,]$ say, in $M_g - U$. Letting r be the unique monic polynomial such that $[\,\overrightarrow{\phi(u)}\,] \in M_r$, we find by Lemma 2 Part 2(ii) that $r^2 = g = h^2$, and so $r = h$, as $\operatorname{char} \mathbb{F}_q = 2$. Hence $[\,\overrightarrow{\phi(u)}\,] \in M_h$ and so, since ϕ is an involution, $[\,\overrightarrow{u}\,\overleftarrow{u}\,] \in U$, which is a contradiction. Therefore $m(h)$ is odd.

We now show by induction on $\deg g$ that if g is a folded polynomial then the multiplicity of g is odd. Let g be a folded polynomial. If $\deg g = 1$ then $K(k/g) = 1$

for all $k \in \mathbb{F}_q^*$ and so g has multiplicity $q-1$. Let $\deg g > 1$. We must consider two cases.

Firstly, suppose $\deg g$ is odd. Then $g = bh^2$ where h is folded and b is monic of degree 1. We may assume by induction that $m(h)$ is odd. We argue by contradiction to prove that $m(g)$ is odd. Suppose that $m(g)$ is even. Let $U = \{[\overrightarrow{w}\ c\ \overleftarrow{w}] \mid [\overrightarrow{w}] \in M_h,\ c = lb, l \in \mathbb{F}_q^*\}$. Then $U \subseteq M_g$ by Lemma 4.3 Part 3(ii), and $M_g - U$ is invariant under the involution θ. Now $\#(U) = (q-1)\#(M_h) = (q-1)m(h)$, an odd number, and so $\#(M_g - U)$ is also odd. Therefore $M_g - U$ contains a symmetric continued fraction $[\overrightarrow{u}\ d\ \overleftarrow{u}]$ where u is a word and d is a polynomial of degree 1. If we let r be the unique monic polynomial such that $[\overrightarrow{u}] \in M_r$, and let $d = le$ where e is monic and $l \in \mathbb{F}_q^*$, we have that $er^2 = bh^2$. As before, we conclude that $r = h$ and so $[\overrightarrow{u}\ d\ \overleftarrow{u}] \in U$, which is a contradiction. Therefore $m(g)$ is odd.

Suppose now that $\deg g$ is even. Then $g = h^2$ where h is folded. We may assume by induction that $m(h)$ is odd. Suppose that $m(g)$ is even. Let $U = \{[\overrightarrow{\phi(w)}\ \overleftarrow{\phi(w)}] \mid [\overrightarrow{w}] \in M_h\}$. Once again, $U \subseteq M_g$ by Lemma 4.3 Part 2(ii), and $\#(U) = \#(M_h)$ is odd. So $\#(M_g - U)$ is odd and $M_g - U$ must contain a symmetric continued fraction $[\overrightarrow{u}\ \overleftarrow{u}]$. If we let r be the unique monic polynomial such that $[\overrightarrow{\phi(u)}] \in M_r$, then $r^2 = g = h^2$ and so $r = h$. We then have that $[\overrightarrow{u}\ \overleftarrow{u}] \in U$, which is a contradiction. So $m(g)$ is odd. This completes the proof.

□

As we observed in the remarks preceding Proposition 3.9 in Section 3.3, the expected value for the orthogonal multiplicity of a polynomial of degree n over $\mathbb{F}_q$ is $(q-1)^n$. Proposition 3.9 also tells us that the orthogonal multiplicity of such a polynomial is no greater than $(q-1)^{\lceil n/2 \rceil} q^{\lfloor n/2 \rfloor}$. There are, however, no known non-trivial lower bounds on the multiplicity of an arbitrary polynomial. Theorem 4.6 gives us a lower bound on the multiplicity of a folded polynomial.

Theorem 4.6 *Let $g \in \mathbb{F}_q[x]$, $\operatorname{char} \mathbb{F}_q = 2$, be a folded polynomial of degree n. Let $wt(n)_2$ denote the weight of the binary representation of n. Then $m(g) \geq (q-1)^{wt(n)_2}$.*

Proof: We prove by induction on $\deg g$ that if g is folded then $m(g) \geq (q-1)^{wt(n)_2}$, where $n = \deg g$ and $wt(n)_2$ denotes the weight of the binary representation of n. Let $g \in \mathbb{F}_q[x]$, $\operatorname{char} \mathbb{F}_q = 2$, be a folded polynomial. If $\deg g = 1$ then $K(k/g) = 1$ for all $k \in \mathbb{F}_q^*$ and so $m(g) = (q-1) = (q-1)^{wt(1)_2}$. So let $\deg g > 1$.

Suppose that $\deg g = n$ is even. Then $g = h^2$ where h is folded of degree $n/2$. We may assume by induction that $m(h) \geq (q-1)^{wt(n/2)_2}$. From the proof of the even case of the second part of Theorem 4.5, it is clear that $m(g) \geq m(h)$. Now $wt(n)_2 = wt(n/2)_2$ and so we have that $m(g) \geq m(h) \geq (q-1)^{wt(n/2)_2} = (q-1)^{wt(n)_2}$.

Suppose now that $\deg g = n$ is odd. Then $g = bh^2$ where h is folded of degree $(n-1)/2$ and b is a monic polynomial of degree 1. We may assume by induction that $m(h) \geq (q-1)^{wt((n-1)/2)_2} = (q-1)^{wt(n)_2 - 1}$. Define the set U as in the odd case of the second part of Theorem 4.5. Then $m(g) = \#(M_g) \geq \#(U) = (q-1)\#(M_h) = (q-1)m(h)$. Since $m(h) \geq (q-1)^{wt(n)_2 - 1}$ we have $m(g) \geq (q-1)m(h) \geq (q-1)^{wt(n)_2}$ as required.

□

4.4 Further Results

As we have mentioned before, the orthogonal multiplicity of a polynomial over a finite field $\mathbb{F}_q$ is a multiple of $q-1$ and so a polynomial over $\mathbb{F}_q$ with positive multiplicity must have multiplicity at least $q-1$. If a polynomial g over $\mathbb{F}_q$ has multiplicity exactly $q-1$ then this means that there exists a unique monic f, of degree less than that of g and coprime to g, such that $K(f/g) = 1$. Theorem 4.6 has as a corollary a classification of all polynomials with multiplicity $q-1$ over finite fields of even order $q \neq 2$.

Corollary 4.7 *Let g be a monic polynomial in $\mathbb{F}_q[x]$, $\operatorname{char}\mathbb{F}_q = 2$, with $q \neq 2$. Then $m(g) = q-1$ if and only if g has degree 1.*

Proof: If g is a monic polynomial of degree 1 then $K(k/g) = 1$ for all $k \in \mathbb{F}_q^*$ and so $m(g) = q-1$. Conversely, let $g \in \mathbb{F}_q[x]$, $\operatorname{char}\mathbb{F}_q = 2$, have multiplicity $q-1$. By Theorem 4.5, g is a folded polynomial. If $\deg g = n$ then we must have by Theorem 4.6 that $wt(n)_2 = 1$, that is to say, $n = 2^m$ for some m. We claim that the only folded polynomials of degree 2^m for some $m \geq 0$ are those of the form a^{2^m}, where a is a monic polynomial of degree 1. This is easily proved by observing that if s is folded of degree 2^m then $s = t^2$ for some folded polynomial of degree 2^{m-1}. We may assume by induction that $t = a^{2^{m-1}}$ for some monic polynomial a of degree 1. Thus $s = a^{2^m}$. Therefore we must have that $g = a^{2^m}$ for some monic polynomial a of degree 1. We now prove by induction on $m \geq 1$ that $m(a^{2^m}) \geq m(a^2)$. Certainly $m(a^{2^1}) \geq m(a^2)$. Assume now that $m(a^{2^{m-1}}) \geq m(a^2)$ for some $m \geq 2$. It is clear from the proof of the even case of the second part of Theorem 4.5 that $m(a^{2^m}) = m((a^{2^{m-1}})^2) \geq m(a^{2^{m-1}})$. So $m(a^{2^m}) \geq m(a^2)$ as required. Finally, observe that if $\deg b = 1$ and $b \neq la$, $l \in \mathbb{F}_q^*$, then $\gcd(b, a^2) = 1$ and $K(b/a^2) = 1$. So $m(a^2) = (q-1)^2 > q-1$, since $q \neq 2$. Hence $m(a^{2^m}) > q-1$ for $m \geq 1$. We must therefore have that $g = a$ where a is a monic polynomial of degree 1.

□

In [6] Blackburn shows that a polynomial g over $\mathbb{F}_2$ has orthogonal multiplicity 1 if and only if it is of the form $x^{m_1}(x+1)^{m_2}$ where $\binom{m_1+m_2}{m_2} \equiv 1 \bmod 2$ (Result 3.18). It is of interest that Theorem 4.5 can also be used to obtain an alternative, but of course equivalent, classification of polynomials of multiplicity 1 over $\mathbb{F}_2$. (This equivalence can be seen directly from the Lucas congruence for binomial coefficients ([26]).)

Corollary 4.8 *Let $g \in \mathbb{F}_2[x]$. Then g has orthogonal multiplicity 1 if and only if $g = x^{m_1}(x+1)^{m_2}$ where $m_1 = (\alpha_0\alpha_1\alpha_2\ldots)_2$, $m_2 = (\beta_0\beta_1\beta_2\ldots)_2$ and $\alpha_i\beta_i = 0$ for $i \geq 0$.*

Proof: Let $g \in \mathbb{F}_2[x]$. We claim that g has multiplicity 1 if and only if g is folded. By Theorem 4.5, if g has multiplicity 1 then g is folded. Conversely, if g is folded then it must have odd multiplicity. From Result 3.13, we know that if a polynomial g over $\mathbb{F}_2$ has positive multiplicity then it must have multiplicity 2^k, where k is the number of distinct non-linear irreducible factors of g. Therefore a polynomial over $\mathbb{F}_2$ which has odd multiplicity must have multiplicity 1. This proves the claim. The result now follows from the characterization of folded polynomials given in Proposition 4.4.

□

By Result 3.13, if a polynomial over $\mathbb{F}_2$ which splits into linear factors has positive orthogonal multiplicity then it must have multiplicity $2^0 = 1$. Therefore by the above corollary, there exist polynomials over $\mathbb{F}_2$ which split into linear factors which have multiplicity zero. We show, however, that if g is a polynomial over $\mathbb{F}_2$ which splits into linear factors then there exists a polynomial f over $\mathbb{F}_2$ with $\gcd(f, g) = 1$ such that $K(f/g) \leq 2$. This proves a special case of Conjecture 3.6 from Chapter 3 which claims: If $g \in \mathbb{F}_2[x]$ then there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f, g) = 1$ such that $K(f/g) \leq 2$.

Proposition 4.9 *If $g \in \mathbb{F}_2[x]$ splits into linear factors then there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f, g) = 1$ such that $K(f/g) \leq 2$.*

Proof: Let $g \in \mathbb{F}_2[x]$ with $g = x^{m_1}(x+1)^{m_2}$. We prove by induction on $\deg g$ that there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f, g) = 1$ such that $K(f/g) \leq 2$.

If $\deg g = 1$ then we have that $K(1/g) = 1$. Let $\deg g > 1$. If m_1 and m_2 are even then we may write $g = s^2$ where s splits into linear factors. We may assume by induction that there exists $r \in \mathbb{F}_2[x]$ with $\gcd(r, s) = 1$ and $K(r/s) \leq 2$. Without loss of generality, we may further assume that $\deg r < \deg s$, and so $r/s = [\,w\,]$ for some $w = a_1 a_2 \ldots a_m$ with $\deg a_j \leq 2\,(1 \leq j \leq m)$. Let r_m/s_m denote the m^{th} convergent of $[\,w\,]$. Then $r_m/s_m = [\,w\,] = r/s$ and $\gcd(r_m, s_m) = 1$. Hence, since we are working over $\mathbb{F}_2$, $r = r_m$ and $s = s_m$. By Lemma 4.1 Part 2, $(rs+1)/g = (rs+1)/s^2 = [\,\overrightarrow{\phi(w)}\;\overleftarrow{\phi(w)}\,]$, and we also have that $\gcd(rs+1, g) = \gcd(rs+1, s^2) = 1$. Finally, since $\deg a_j \leq 2$ for $1 \leq j \leq m$, we have that $K((rs+1)/g) \leq 2$.

If at least one of m_1 and m_2 is odd then we may write $g = as^2$ where $1 \leq \deg a \leq 2$ and s splits into linear factors. We may assume by induction that there exists $r \in \mathbb{F}_2[x]$ with $\gcd(r, s) = 1$ and $K(r/s) \leq 2$. We may further assume that $\deg r < \deg s$, and so $r/s = [\,w\,]$ for some $w = a_1 a_2 \ldots a_m$ with $\deg a_j \leq 2\,(1 \leq j \leq m)$. Let r_m/s_m denote the m^{th} convergent of r/s. We have that $r = r_m$ and $s = s_m$, and so by Lemma 4.1 Part 3, $(ars+1)/g = (ars+1)/as^2 = [\,\overrightarrow{w}\;\;a\;\;\overleftarrow{w}\,]$. Certainly, $\gcd(ars+1, g) = \gcd(ars+1, as^2) = 1$. By assumption $\deg a_j \leq 2$ for $1 \leq j \leq m$, and we further have that $\deg a \leq 2$. Hence $K((ars+1)/g) \leq 2$, which completes the proof.

□

4.5 Comments and Examples

One may define folded polynomials over finite fields $\mathbb{F}_q$ of odd characteristic in an obvious way; however, few of the results which hold for folded polynomials in characteristic 2 are still true. A plausible analogue of Theorem 4.5, that a polynomial has orthogonal multiplicity $k(q-1)$ where k is odd if and only if it is folded, is, in general, false. For example, over $\mathbb{F}_3$ the folded polynomial x^3 has multiplicity 8, and the polynomial $x^3 + x = x(x^2+1)$ has multiplicity 6. One may show, however, that if g is a folded polynomial over $\mathbb{F}_q$ with $\deg g = n$ then $m(g) \geq (q-1)^{wt(n)_2}$, and, of course, an odd characteristic analogue of Proposition 4.4 is still true. It also seems reasonable to conjecture that over a finite field $\mathbb{F}_q$ of odd characteristic a polynomial has multiplicity $q-1$ if and only if it is linear.

We now present two examples which illustrate the ideas introduced in this chapter.

Example 4.10 (Folded polynomials over $\mathbb{F}_3$.) Recall that in Example 3.12 in Chapter 3 we illustrated the proof of Result 3.11 by computing the orthogonal multiplicity of the polynomial $g = x^3 + 2x^2 + x = x(x+1)^2$ over $\mathbb{F}_3$. We found that $m(g) = 6$. Now g is easily seen to be a folded polynomial. The lower bound on the multiplicity of folded

Mult.	Freq.	Mult.	Freq.	Mult.	Freq.
114	24	186	72	282	24
126	4	210	24	294	72
138	12	222	60	306	48
144	12	234	216	318	72
162	60	246	108	330	72
174	48	258	24	342	36
177	12	261	4		
180	12	270	8		

Table 4.1: Frequencies of Orthogonal Multiplicities for Polynomials of Degree 5 over $\mathbb{F}_4$.

polynomials in odd characteristic which we mentioned in the preceding paragraph tells us that $m(g) \geq (3-1)^{wt_2(3)} = 4$. We may immediately write down 4 continued fractions in M_g; namely

$$[\,0; a(x+1), bx, -a(x+1)\,],$$

where a and b are non-zero elements of $\mathbb{F}_3$. The remaining two continued fractions in M_g must be symmetric. They are in fact

$$[\,0; ax, a(2x+1), ax\,],$$

where a is a non-zero element of $\mathbb{F}_3$.

Example 4.11 (The orthogonal multiplicity of polynomials over $\mathbb{F}_4$.) Consider the field $\mathbb{F}_4$ with four elements $0, 1, \gamma, 1+\gamma$ where $\gamma^2 = 1+\gamma$. Let $g = x^3 + \gamma x = x(x+(1+\gamma))^2$. Then g is certainly a folded polynomial and so by Theorem 4.6 it must have orthogonal multiplicity at least $(4-1)^{wt(3)_2} = 9$. The 9 badly approximable rational functions in reduced form whose denominators are g which we know exist from Theorem 4.6 are those of the form

$$[\,0; a(x+(1+\gamma)), bx, a(x+(1+\gamma))\,],$$

where a, b are non-zero elements of $\mathbb{F}_4$. The average value of the orthogonal multiplicity of a polynomial of degree 3 over $\mathbb{F}_4$ is $(4-1)^3 = 27$ and the upper bound is $(4-1)^2 4 = 36$. In fact, the orthogonal multiplicity of g is 21.

For polynomials of degree 5 over $\mathbb{F}_4$ the expected value for the orthogonal multiplicity is $3^5 = 243$ and the upper bound is $3^3 4^2 = 432$. Computation reveals (see Table 4.1) that the lowest multiplicity occurring amongst such polynomials is 114 and the highest is 342. Exactly 216 polynomials have multiplicity 234 and 108 polynomials have multiplicity 246, these being the closest values to the average which occur. Thus 324 polynomials out of all 1024 monic polynomials of degree 5 over $\mathbb{F}_4$ have orthogonal multiplicity very near to the average. There are 16 folded polynomials of degree 5 over $\mathbb{F}_4$. Twelve of those have multiplicity 177 and the remaining 4 have multiplicity 261. The lower bound given by Theorem 4.6 is $3^2 = 9$ in this case. Thus there is certainly considerable room for improvement to this bound.

We conclude this chapter by returning to an earlier theme. The next example unravels the puzzle of the missing convergents in Example 2.29.

Example 4.12 Recall that in Examples 2.13, 2.29 and 2.39 we studied the algebraic element $z = \sum_{i\geq 0} x^{-p^i}$ in L_q, where $\operatorname{char}\mathbb{F}_q = p$. In Example 2.39 we gave the explicit continued fraction of z in the case $p = 2$, and in Example 2.29 we were able to find a subsequence of the sequence of convergents to z when $p > 2$. We now give the explicit continued fraction expansion of z in the case $p > 2$. In fact, we shall do much more.

Let t be any integer greater than 2 and consider the element $y = \sum_{i\geq 0} x^{-t^i}$ over the finite field $\mathbb{F}_q$. So the element z in which we are most interested is just the case $t = \operatorname{char}\mathbb{F}_q = p$. Then it may be shown using a generalisation of Lemma 4.1 Part 3 to arbitrary characteristic (called the "folding lemma" in [36]) that the continued fraction expansion of y is

$$\begin{gathered}[\,0; x, -x^{t^0(t-2)}, -x, -x^{t^1(t-2)}, x, x^{t^0(t-2)}, -x, -x^{t^2(t-2)},\\ x, -x^{t^0(t-2)}, -x, x^{t^1(t-2)}, x, x^{t^0(t-2)}, -x, -x^{t^3(t-2)}, \ldots\,]\end{gathered}$$

To explain the pattern into which the partial quotients fall, we need to borrow some notation from [35, page 242-243]: As in Section 4.2.1 let $w = a_1 a_2 \ldots a_m$ denote a word over the alphabet $\{a \in \mathbb{F}_q[x] \mid \deg a \geq 1\}$, and let $\overrightarrow{w} = w$. Write $[\,w\,]$ for the continued fraction $[\,0; a_1, \ldots, a_m\,]$. Further, let $-\overleftarrow{w} = (-a_m)(-a_{m-1})\ldots(-a_1)$. For any element a in this alphabet, let the map $\mathcal{F}_a$ send a word w to the word $\overrightarrow{w}\ a -\overleftarrow{w}$. Denote by $\prod_{1\leq i\leq n}\mathcal{F}_{a_i}$ the composition of maps $\mathcal{F}_{a_n} \circ \ldots \circ \mathcal{F}_{a_1}$. Given an infinite sequence of maps $\mathcal{F}_{a_i}$, write $\prod_{i=1}^{\infty}\mathcal{F}_{a_i}(w)$ to be the limit of the sequence of words $\prod_{l\leq i\leq n}\mathcal{F}_{a_i}(w)$ as $n \to \infty$. The limit is with respect to the natural topology on words where two words are considered close together if they agree initially in many places.

With this notation, the continued fraction expansion of y is

$$[\,\prod_{i=0}^{\infty}\mathcal{F}_{-x^{t^i(t-2)}}(x)\,].$$

Putting $t = p$ and $\operatorname{char}\mathbb{F}_q = p$ gives us the continued fraction of z. So

$$z = [\,\prod_{i=0}^{\infty}\mathcal{F}_{-x^{p^i(p-2)}}(x)\,].$$

The convergent a_n/b_n of z, for $n \geq 0$, defined in Example 2.29 is just the finite continued fraction obtained by truncating the above expansion before the first appearance of $-x^{p^n(p-2)}$. For $n \geq 1$ we can write this as

$$a_n/b_n = [\,\prod_{i=0}^{n-1}\mathcal{F}_{-x^{p^i(p-2)}}(x)\,].$$

Thus the convergents a_n/b_n are rather special ones, as they are the only convergents of z whose continued fractions are symmetric.

Finally it is of interest to note that the continued fraction expansion of the Laurent series $y = \sum_{i\geq 0} x^{-t^i}$ is the same when y is viewed as a member of the field of Laurent series over $\mathbb{Q}$. Using the method of "specialisation" described in [36], this enables us to present the continued fraction expansions of the (transcendental) real numbers

$$\sum_{i\geq 0} s^{-t^i},$$

where s is some integer at least 2. However, pursuing this fascinating connection would lead us too far astray, and the reader is referred to [36] for more details.

Chapter 5

Continued Fractions of Algebraic Laurent Series

5.1 Introduction

In this short chapter, we turn our attention to the continued fraction expansions of algebraic Laurent series. As before, we begin by considering an area of classical number theory, the study of continued fraction expansions of algebraic numbers. In his delightful book on continued fractions penned in the 1930s ([17]), A.Ya. Khinchin comments

> It is interesting to note that we do not, at the present time, know the continued-fraction expansion of a single algebraic number of degree higher than 2. We do not know, for example, whether the sets of elements in such expansions [partial quotients] are bounded or unbounded. In general, questions connected with the continued-fraction expansion of algebraic numbers of higher degree than the second are extremely difficult and have hardly been studied.

In the intervening years, many significant papers have been published in this area, but none have shed light on the open questions laid before us by Khinchin in this quotation. This failure was bluntly expressed in a recent paper of Van der Poorten and Shallit ([35]), which opened

> It is notorious that it is damnably difficult to explicitly compute the continued fraction of a quantity expressed in some other form.

However, when one recasts Khinchin's problems in terms of Laurent series over finite fields rather than real numbers, much more progress can be made. Since interest in continued fraction expansions of Laurent series was rekindled in the 1970s by the work of Baum and Sweet, a number of papers have answered analogues of the problems of Khinchin. Two essential differences between Laurent series over finite fields and real numbers, the positive characteristic and non-Archimedean norm, have made this possible. In the next chapter we will present a new result on continued fraction expansions of algebraic Laurent series, but we first lay in place the background to this new work by discussing the progress which has been made in this area in recent years.

5.2 The Contribution of Baum and Sweet

After Artin's thesis in the 1920s in which the continued fraction algorithm for Laurent series over finite fields was apparently introduced ([2, page 149]), other than a few scattered results, scant attention was paid to this area. However, since the work of Baum and Sweet in the 1970s there has been a steady trickle of papers on the subject, a tributary to a larger flow of new results on the algebraic and combinatorial properties of formal Laurent series. Baum and Sweet wrote two papers on this topic. The first ([4]) is a mélange of constructions of Laurent series in characteristic 2 whose continued fractions have partial quotients of both bounded and unbounded degrees. In the second ([5]) they present a simple characterisation of "badly approximable" Laurent series over the binary field, and this forms the starting point for our new work in Chapter 6. We begin by describing some of the highlights of the first paper.

Baum and Sweet present a cubic equation whose root in L_2 has a continued fraction with partial quotients of bounded degree.

Result 5.1 *[4, Theorem 2] Let $\alpha \in L_2$ satisfy*

$$\alpha^3 + x^{-1}\alpha + 1 = 0.$$

Then all the partial quotients of α have degree ≤ 2.

One may see from Hensel's Lemma (Result 2.11) that the polynomial $T^3+x^{-1}T+1$ indeed has a unique root in L_2. The explicit continued fraction expansion of this root, known as the Baum-Sweet cubic, is not given in [4] but is presented in [29].

Result 5.1 cannot be generalised in a straightforward way to higher degree elements, as shown by the next result.

Result 5.2 *[4, Theorem 5] Let $n > 1$. If $\alpha \in L_2$ satisfies*

$$\alpha^{2^n+1} + u^{-1}\alpha + 1,$$

where $u \in \mathbb{F}_2[x]$ has degree ≥ 1, then α has unbounded partial quotients.

It is also worth noting that one may use linear fractional transformations to obtain other elements with bounded/unbounded partial quotients from existing ones with bounded/unbounded partial quotients.

Result 5.3 *[4, Lemma 4] Let $g_1, g_2, h_1, h_2 \in \mathbb{F}_2(x)$ with $g_1h_2+h_1g_2 \neq 0$. Then $\alpha \in L_2$ has bounded partial quotients if and only if $(g_1\alpha + h_1)/(g_2\alpha + h_2)$ has bounded partial quotients.*

It is of interest to consider a related result: We say that two Laurent series α and $\alpha^\star$ in L_2 are equivalent if

$$\alpha^\star = \frac{g_1\alpha + h_1}{g_2\alpha + h_2},$$

where $g_1h_2 + g_2h_1 = 1$ and $g_1, g_2, h_2, h_2 \in \mathbb{F}_2[x]$. As is observed in [4, Page 601], one may show that α and $\alpha^\star$ are equivalent if and only if the there exists m and n such that $a_{m+i} = b_{n+i}$ for all $i \geq 0$, where $\alpha = [\,a_0; a_1, a_2, \dots]$ and $\alpha^\star = [\,b_0; b_1, b_2, \dots]$.

In fact, these ideas are used in [8, 29] to compute the continued fractions expansions of certain elements $\alpha \in L_p$, where p is a prime, such that α and α^p are related by a linear fractional transformation. For example, if we let α denote the Baum-Sweet cubic, then $x\alpha^3 + \alpha + x = 0$. One may verify that the first two partial quotients of α are 1 and x and so $\alpha = [1; x, \beta]$ for some $\beta \in L_2$. A calculation reveals that

$$\beta = \frac{(x^2 + x)\beta^2 + 1}{x\beta^2 + 1},$$

and so β and β^2 are related by a linear fractional transformation. This allows Mills and Robbins ([29]) to explicitly exhibit the continued fraction expansion of β and therefore α, which contains symmetries similar to those explored in Chapter 4.

Baum and Sweet also consider questions relating to the rational approximation of Laurent series. Recall that Liouville's theorem for real numbers states that if α is an algebraic real number of degree D then there is a constant c depending only on α such that

$$|\alpha - (m/n)|_\infty \geq c/n^D$$

for any rational number m/n. Here $|\,|_\infty$ denotes the absolute value norm on $\mathbb{R}$. This is easily proved. A far more profound result was obtained by Roth ([38]), following on from work of Thue, Seigel and Dyson: Suppose that the inequality

$$|\alpha - (m/n)|_\infty < 1/n^\kappa,$$

has an infinite number of rational solutions m/n. Roth proved that $\kappa \leq 2$. This exponent for n is best possible, for the sequence of convergents $\{m_i/n_i\}_{i\geq 0}$ to α gives an infinite number of solutions m/n to

$$|\alpha - (m/n)|_\infty < 1/n^2.$$

It is observed in [27] that an analogue of Liouville's theorem holds for Laurent series.

Result 5.4 *[27, Theorem 1] Let $\alpha \in L_q$ be algebraic of degree $D > 1$ over $\mathbb{F}_q(x)$. Suppose that $h(\alpha) = 0$ where $h := \sum_{0\leq j\leq D} h_j T^j$ is an irreducible polynomial with coefficients in $\mathbb{F}_q[x]$. Define $c_1 = \max\{1, |\alpha|\}$ and $c_2 = \max_{0\leq j\leq D}\{|h_j|\}$. Then for $c := \min\{c_2, 1/c_1 c_2^{D-1}\}$ we have that*

$$|\alpha - (f/g)| \geq c/|g|^D,$$

for all $f, g \in \mathbb{F}_q[x]$.

Mahler further observes that the rational number z in L_q which satisfies

$$z^p - z + x^{-1} = 0$$

shows that the above result is sharp, as we now explain. Recall from Example 2.29 in Chapter 2 we saw that there is a subsequence $\{a_n/b_n\}_{n\geq 1}$ to the sequence of convergents $\{f_i/g_i\}_{i\geq 0}$ of z such that

$$|z - (a_n/b_n)| = 1/|b_n|^p.$$

We also proved in Example 2.13 that z has exact degree p over $\mathbb{F}_q(x)$, with minimal polynomial $T^p - T + x^{-1}$. Applying Result 5.4 we see that

$$|z - (f/g)| \geq 1/|g|^p,$$

for all rational functions f/g in $\mathbb{F}_q(x)$. The infinite subsequence of convergents $\{a_n/b_n\}_{n\geq 1}$ meets this bound. Thus no Roth type improvement to Result 5.4 can be made without putting some restriction on α. It is claimed in [1] that an analogue of Roth's theorem is true for elements which do not lie in power of p cyclic extensions of $\mathbb{F}_q(x)$, but this is shown to be false in characteristic 2 in [4]. Explicitly, Baum and Sweet show [4, Corollary 7] that if α is the unique element in L_2 which satisfies

$$\alpha^{2^n+1} + x\alpha + 1 = 0$$

then

$$|\alpha - (f/g)| = 2^{-1}/|g|^{2^n+1}$$

has infinitely many solutions $f/g \in \mathbb{F}_2(x)$. However, one may prove an analogue of Thue's theorem, a weaker and earlier version of Roth's theorem, for elements $\alpha \in L_q$ such that α and α^{p^f}, where char $L_q = p$ and for any $f \geq 1$, are not related by a linear fractional transformation ([21, Theorem 1]).

We now turn our attention to the second paper of Baum and Sweet ([5]). Recall that P_2 denotes the set of all Laurent series in L_2 with a zero polynomial part, and write $CF(\{x, x+1\})$ for the set of continued fractions in P_2 which have partial quotients a_j $(j \geq 1)$ all of degree 1. The main result of [5] states

Result 5.5 *[5, Theorem 1] An element $\alpha \in P_2$ lies in $CF(\{x, x+1\})$ if and only if α satisfies*

$$\alpha^2 + (x+1)\alpha + 1 = x\beta^2,$$

for some $\beta \in P_2$.

One significant corollary of this result is that the coefficients of the Laurent series expansions of badly approximable rational functions over $\mathbb{F}_2$ satisfy a simple linear recurrence. This was discussed in Chapter 3 Section 3.3.2.

We conclude by presenting a modest generalisation of this result due to Baum and Sweet which we greatly extend in the next chapter.

Result 5.6 *[5, Theorem 6]*

1. *If the partial quotients of $\alpha \in P_2$ satisfy $a_j = u, v,$ or $u+v$ for all $j \geq 1$, then*

$$\alpha^2 + u\alpha + 1 = v(u+v)\beta^2,$$

   for some $\beta \in P_2$

2. *Conversely, when $\deg u = \deg v = 2$ and $\deg(u+v) = 1$, then for any $\beta \in P_2$, there is an element $\alpha \in P_2$ with*

$$\alpha^2 + u\alpha + 1 = v(u+v)\beta^2,$$

   and all its partial quotients equal to u, v or $u+v$.

This result is used in [16, pages 112-117] to study sequences with specific linear complexity profiles. We discuss similar applications of our more general theorem in Section 6.5.2 of the next chapter.

Chapter 6

Continued Fractions of Laurent Series with Partial Quotients from a Given Set

6.1 Introduction

In this chapter we consider families of continued fractions of Laurent series whose partial quotients all lie in a given set. Following ideas of Baum and Sweet ([5]), we show that one may describe the zeros of certain collections of equations in terms of such families. The two paragraphs which follow recall the notation and definitions necessary to give a fuller description of our results.

Let $\mathbb{F}_q$ be the finite field with q elements and L_q denote the field of formal Laurent series in x^{-1} over $\mathbb{F}_q$ given by

$$L_q = \left\{ \sum_{i=n}^{\infty} \alpha_i x^{-i} \,|\, n \in \mathbb{Z}, \alpha_i \in \mathbb{F}_q \right\}.$$

We have the inclusions $\mathbb{F}_q[x] \subseteq \mathbb{F}_q(x) \subseteq L_q$. Elements in $\mathbb{F}_q(x)$ are called rational, and those which lie in L_q but not in $\mathbb{F}_q(x)$ are called irrational. We define the norm $|\,|$ on L_q as follows: If $\alpha \in L_q$ is non-zero then we may write $\alpha = \sum_{i \geq n} \alpha_i x^{-i}$ where $\alpha_n \neq 0$. In this case we define $|\alpha| = q^{-n}$. If $\alpha = 0$ we define $|\alpha| = 0$. Observe that if $\alpha = s/t$ is a rational Laurent series with s, $t \in \mathbb{F}_q[x]$ then $|\alpha| = q^{\deg s - \deg t}$. We define P_q to be the ring of all $\alpha \in L_q$ with $|\alpha| < 1$, and we will frequently abbreviate L_q and P_q to L and P.

We saw in Chapter 2 Section 2.3 that a continued fraction theory exists for the field L_q. In particular, any irrational Laurent series α in L has a unique infinite continued fraction expansion

$$\alpha = a_0 + 1/(a_1 + 1/(a_2 + 1/(\dots)))$$

where $a_j \in \mathbb{F}_q[x]$ with $\deg a_j \geq 1$ for $j \geq 1$. We write $\alpha = [\,a_0; a_1, a_2, \dots]$. We call the polynomials a_j $(j \geq 0)$ the partial quotients of α, and a_0 is also referred to as the polynomial part of α. Any irrational Laurent series in P will have a zero polynomial part. It is these elements of L with which we shall be primarily concerned. The significance of the continued fraction expansion of a Laurent series is that one may use it to define a sequence of rational functions which are best approximations to the original Laurent series, as we saw in Chapter 2 Section 2.3.4. Laurent series whose continued fractions have partial quotients of "small degree" are of particular interest as these may be thought of as being difficult to approximate. This was justified for rational Laurent series in Chapter 3 Section 3.2; it is equally true for irrational Laurent series, as is readily seen.

We need one new definition before we may present the results of this chapter: Let A be a finite subset of $\mathbb{F}_q[x]$, and $CF(A) \subseteq P$ be given by

$$CF(A) = \{[\,0; a_1, a_2, \dots\,] \,|\, a_j \in A,\ \deg a_j \geq 1\}\,.$$

So $CF(A)$ is the set of all infinite continued fractions which have a zero polynomial part and whose remaining partial quotients lie in A.

We begin with a result for arbitrary finite fields which describes the number of expressions $\alpha_1 x^{-1} + \dots \alpha_m x^{-m}$ which occur as the initial segment of a Laurent series in $CF(A)$ in terms of a generating function. This result, Proposition 6.4, is not only of some independent interest, but is a vital ingredient in the sections which follow. We now describe the main theorem. For a fixed $u \in \mathbb{F}_q[x]$ where $\operatorname{char} \mathbb{F}_q = 2$, let I_u denote the set of all $\alpha \in P$ for which there exists a $\beta \in L$ with

$$\alpha^2 + u\alpha + (1 + x\beta^2) = 0.$$

We first show, Lemma 6.6, that one may construct non-empty sets A such that $CF(A) \subseteq I_u$. Moreover, an application of Proposition 6.4 allows us to prove that for certain u there exists associated sets A such that $CF(A) = I_u$; this is Theorem 6.13, the main result of the chapter. We determine all u for which this is true in Propositions 6.14, 6.15, 6.17 and Table 6.1. The case $u = x + 1$ over $\mathbb{F}_2$ is a well-known result due to Baum and Sweet ([5]) which has an application in the study of binary sequences. Our new results have similar applications which we discuss in Section 6.5.2. We also show in Corollary 6.19 that for "many" values of d, there exist Laurent series in L_4 which are algebraic over $\mathbb{F}_4(x)$ of degree d, and which have partial quotients of bounded degree in their continued fraction expansion.

The remainder of this chapter is organised in the following way. We gather some technical lemmas and a definition in Section 6.2. The first two lemmas will be used in Section 6.3 to determine the cardinality of sets of the form $CF(A)$ up to a given rational approximation. The final one is used in the proof of the main theorem. Section 6.4 contains a statement and proof of the main theorem of the chapter as well as several related propositions. Finally, we present two different applications of our theorem in Section 6.5.

6.2 Preliminaries

In this chapter, we shall assume a familiarity with the basic notions from the theory of continued fractions of Laurent series, as presented in Chapter 2 Section 2.3.

6.2.1 Lemmas

This section does not contain any essential definitions, and the reader may move directly onto Section 6.2.2 and refer back when required. We begin with a technical lemma which shall be used in the proof of the first part of Proposition 6.4.

Lemma 6.1 *Let $\alpha = [\,0; a_1, a_2, \ldots]$ and $\alpha' = [\,0; a'_1, a'_2, \ldots]$ where $a_j, a'_j \in \mathbb{F}_q[x]\,(j \geq 1)$. Suppose that $a_j = a'_j$ for $1 \leq j \leq s-1$ and $a_s \neq a'_s$. Let $\sum_{1 \leq j \leq s-1} \deg a_j = \sigma$. Then*

$$|\alpha - \alpha'| = \frac{|a_s - a'_s|}{q^{2\sigma}|a_s||a'_s|}.$$

Proof: For $j \geq 1$, let f_j/g_j denote the j^{th} convergent to $[\,0; a_1, a_2, \ldots]$. So $f_j/g_j = [\,0; a_1, a_2, \ldots, a_j]$ with $\gcd(f_j, g_j) = 1$.
Let $\beta = [\,a_s; a_{s+1}, a_{s+2}, \ldots]$ and $\beta' = [\,a'_s; a'_{s+1}, a'_{s+2}, \ldots]$. Then by recurrences (2.14) in Chapter 2

$$\alpha = \frac{\beta f_{s-1} + f_{s-2}}{\beta g_{s-1} + g_{s-2}},\ \alpha' = \frac{\beta' f_{s-1} + f_{s-2}}{\beta' g_{s-1} + g_{s-2}}.$$

Hence

$$\alpha - \alpha' = \frac{(-1)^{s-2}(\beta - \beta')}{(\beta g_{s-1} + g_{s-2})(\beta' g_{s-1} + g_{s-2})},$$

where we use the relation $f_{s-1}g_{s-2} - g_{s-1}f_{s-2} = (-1)^{s-2}$ (Chapter 2 Result 2.15 Part 2). The lemma now follows since $|\beta| = |a_s|$, $|\beta'| = |a'_s|$ and $|g_{s-1}| = q^{\sigma}$.

□

For any complex function $h(z)$ which is analytic in some region, let $[z^n]h(z)$ denote the coefficient of z^n in the power series expansion of $h(z)$. The next result is from [33, Theorem 10.2], and shall be useful in the proof of the second part of Proposition 6.4.

Lemma 6.2 *Let $h(z)$ be a complex function which is analytic in the disk $\|z\| < R$, where $\|\,\|$ denotes the complex modulus and $R \in \mathbb{R}$. Then for any $r \in \mathbb{R}$ with $0 < r < R$ and any $n \in \mathbb{Z}$ with $n \geq 0$ we have*

$$\|[z^n]h(z)\| \leq r^{-n} \max_{\|z\|=r} \|h(z)\|.$$

Proof: From the Cauchy integral formula we have that $[z^n]h(z) = \dfrac{1}{2\pi i}\displaystyle\int_\Gamma \frac{h(z)}{z^{n+1}}\,dz$ where Γ is any closed contour in the disk $\{z \in \mathbb{C} \mid \|z\| < R\}$ that contains the origin inside it and is positively orientated (traversed in a counter-clockwise direction). Taking Γ to be the circle centre the origin radius r gives us the result.

□

We conclude with a result which we shall appeal to in the proof of Lemma 6.10. For a polynomial $f \in \mathbb{F}_q[x]$ the coefficient of x^n in f is denoted $[x^n]f$.

Lemma 6.3 *Let $W \subseteq \mathbb{F}_q[x]$ and let a be an odd positive integer and b an arbitrary integer with $b \geq a$. Denote by $n_b(W)$ the number of elements $c \in \mathbb{F}_q$ such that $c = [x^b]f$ for some $f \in W$. Suppose that*

1. *Each polynomial in W has degree not greater than b.*

2. *If $v, v' \in W$ with $v \neq v'$ then the degree of $v - v'$ is an odd number at least a.*

Then $\#(W) \leq n_b(W)q^{\lceil (b-a)/2 \rceil}$.

Proof: For each $c \in \mathbb{F}_q$, let $W(c)$ denote the set of all polynomials f in W with $[x^b]f = c$. If $W(c) \neq \emptyset$ then we may choose $f_c \in W(c)$. Let $V(c) = f_c - W(c)$. Then by property *2* of W, any two polynomials in $V(c)$ differ in some coefficient x^d where d is odd and $a \leq d$. Furthermore $d < b$ by property *1*. There are $\lceil (b-a)/2 \rceil$ such odd numbers d. So the cardinality of $V(c)$ is not greater than $q^{\lceil (b-a)/2 \rceil}$. Thus $\#(W(c)) = \#(V(c)) \leq q^{\lceil (b-a)/2 \rceil}$. Hence $\#(W) = \sum_c \#(W(c)) \leq n_b(W)q^{\lceil (b-a)/2 \rceil}$ as required.

□

6.2.2 An Equivalence Relation on Sets of Polynomials

We define the following equivalence relation on finite subsets of $\mathbb{F}_q[x]$: We say that A and B are **equivalent** if $\{a \in A \mid \deg a \geq 1\} = \{a \in B \mid \deg a \geq 1\}$. So if A and B are equivalent, then $CF(A) = CF(B)$. (The converse is also true.) It will be convenient for us to consider sets $CF(A)$ where A contains polynomials of degree zero and zero itself. Any set B which is equivalent to such a set A will give us the same collection of continued fractions $CF(B)\,(= CF(A))$, and we will make frequent use of this simple equivalence relation in the statements of the results which follow.

6.3 The Cardinality of $CF(A)$ up to a Given Rational Approximation

Let A be a finite set of polynomials in $\mathbb{F}_q[x]$. We wish to count the number of elements in $CF(A)$ up to a given rational approximation. To be more precise, for each $m \in \mathbb{N}$ we define an equivalence relation $\sim_m$ on L by

$$\alpha \sim_m \alpha' \Leftrightarrow |\alpha - \alpha'| < q^{-m}.$$

We consider the equivalence relation $\sim_m$ restricted to $CF(A)$ and denote the set of equivalence classes by $CF(A)/\sim_m$. So if $\alpha,\ \alpha' \in CF(A)$ then $\alpha \sim_m \alpha'$ if and only if the first m coefficients in the Laurent series expansions of α and α' agree. Proposition 6.4 describes the number of equivalence classes mod$\sim_m$ $(m \geq 1)$ in terms of a generating function which we construct in the paragraphs which follow. This result is not only of some interest in its own right, but is also a crucial ingredient in the proof of Theorem 6.13.

We make the following definitions: for $i \geq 1$ let v_i denote the number of polynomials in A of degree i and let the **degree enumerator** $f_A(z)$ of A be given by

$$f_A(z) = \sum_{i \geq 1} v_i z^i \in \mathbb{C}[z].$$

For $i \geq 1$, define the equivalence relation $\approx_i$ on A in the following way. Let $v, v' \in A$. Define $v \approx_i v'$ if

$$(1/v) \sim_{2i-1} (1/v').$$

Let w_i be the number of $\approx_i$-equivalence classes of polynomials of degree greater than i in A. Thus w_i is the cardinality of the largest subset of polynomials of degree greater than i in A which lie in distinct $\approx_i$-equivalence classes. Defining $w_0 = 1$ we let the **deficiency polynomial** $g_A(z)$ of A be given by

$$g_A(z) = \sum_{i \geq 0} w_i z^i \in \mathbb{C}[z].$$

Observe that if A and B are equivalent sets (according to Section 6.2.2) then $f_A(z) = f_B(z)$ and $g_A(z) = g_B(z)$. Also note that we shall write $f(z)$ and $g(z)$ for $f_A(z)$ and $g_A(z)$ when there is no risk of confusion.

Recall that the coefficient of z^n in $g(z)/(1 - f(z))$ is denoted $[z^n]g(z)/(1 - f(z))$. Also, let $\lceil m/2 \rceil$ denote the least integer which is not less than $m/2$; so $\lceil m/2 \rceil = (m+1)/2$ when m is odd, and $m/2$ when m is even. We may now state the main result of this section.

Proposition 6.4 *Let m be an odd positive integer. Then the cardinality of $CF(A)/\sim_m$ is $[z^{\lceil m/2\rceil}]g(z)/(1-f(z))$. If the root [roots] of $1-f(z)$ with the smallest complex modulus has [have] modulus R, then for any $\varepsilon>0$ there exists a constant $c\in\mathbb{R}$ such that the cardinality of $CF(A)/\sim_m$ is bounded above by $c(1/(R-\varepsilon))^{\lceil m/2\rceil}$*

Proof: We begin by proving the first statement of the proposition. Let m be an odd positive integer. For any $\alpha=[0;a_1,a_2,\dots]$ define the ***mth*-deficiency** of α to be the unique integer k such that $\lceil m/2\rceil-k=\sum_{1\le j\le l}\deg a_j\le\lceil m/2\rceil<\sum_{1\le j\le l+1}\deg a_j$. We first claim that any two elements α, α' in $CF(A)$ with mth-deficiencies k and k' respectively, where $k\ne k'$, must lie in different equivalence classes mod $\sim_m$. For suppose $\alpha=[0;a_1,a_2,\dots]$ and $\alpha'=[0;a_1',a_2',\dots]$ lie in $CF(A)$, with $\sum_{1\le j\le l}\deg a_j=\lceil m/2\rceil-k$, $\sum_{1\le j\le l'}\deg a_j{}'=\lceil m/2\rceil-k'$ where $\deg a_{l+1}>k$, $\deg a_{l'+1}'>k'$ and $k\ne k'$. Let $j=s$ be the minimum integer for which $a_j\ne a_j'$. Then certainly $s\le\min\{l,l'\}+1$, and by Lemma 6.1 we have that $|\alpha-\alpha'|=\dfrac{|a_s-a_s'|}{q^{2\sigma}|a_s||a_s'|}$ where $\sigma=\sum_{1\le j\le s-1}\deg a_j$. Since α and α' have different mth-deficiencies, at least one of $\deg a_s$ and $\deg a_s'$ is strictly less than $\lceil m/2\rceil-\sigma$. So suppose $\deg a_s\le\deg a_s'$ with $\deg a_s<\lceil m/2\rceil-\sigma$. If $\deg a_s=\deg a_s'$ then both are less than $\lceil m/2\rceil-\sigma$ and so $|\alpha-\alpha'|>q^{-2\lceil m/2\rceil}\ge q^{-m-1}$. Otherwise $\deg a_s<\deg a_s'$ and $|\alpha-\alpha'|=q^{-2\sigma-\deg a_s}>q^{-\sigma-\lceil m/2\rceil}$. But certainly $\sigma<\lceil m/2\rceil$ and so $|\alpha-\alpha'|>q^{-2\lceil m/2\rceil}\ge q^{-m-1}$. This proves the claim.

Let $CF_k(A)\,(0\le k\le\lceil m/2\rceil)$ be the set of all elements in $CF(A)$ with mth-deficiency k. We have shown that the number of equivalence classes of $CF(A)/\sim_m$ is equal to the summation over $k\,(0\le k\le\lceil m/2\rceil)$ of the number of classes of $CF_k(A)/\sim_m$.

Consider now the set of continued fractions $CF_k(A)$ for some $0\le k\le\lceil m/2\rceil$. Let α, $\alpha'\in CF_k(S)$ with $\alpha=[0;a_1,a_2,\dots]$ and $\alpha'=[0;a_1',a_2',\dots]$ where $\sum_{1\le j\le l}\deg a_j=\sum_{1\le j\le l'}\deg a_j'=\lceil m/2\rceil-k$ and $\deg a_{l+1}$, $\deg a_{l'+1}'>k$. If $a_j\ne a_j'$ for some $j\,(1\le j\le\min\{l,l'\})$ then a similar argument to the one in the preceding paragraph shows that $\alpha\not\sim_m\alpha'$. Otherwise $l=l'$ and $a_j=a_j'\,(1\le j\le l)$. In this case by Lemma 6.1, α and α' are in different $\sim_m$-classes if and only if $\dfrac{|a_{l+1}-a_{l+1}'|}{|a_{l+1}||a_{l+1}'|}\ge q^{-2k+1}$. But this latter condition is equivalent to $|(1/a_{l+1})-(1/a_{l+1}')|\ge q^{-2k+1}$, that is to say, $a_{l+1}\not\approx_k a_{l+1}'$. (Here we need the fact that m is odd. We refer the reader to the paragraphs following this proof for a brief discussion of slight modification we need to make in the case m even.) So the cardinality of $CF_k(A)/\sim_m$ is the number of ways of selecting polynomials a_j in A of degree at least 1 whose degrees sum to $\lceil m/2\rceil-k$, multiplied by the number of $\approx_k$-equivalence classes in A of polynomials of degree greater than k. (There are two exceptions to this: in the case $k=0$ we actually "multiply" the number of ways of selecting non-constant polynomials in A whose degrees sum to $\lceil m/2\rceil$ by 1; when $k=\lceil m/2\rceil$ we take the number of ways of selecting no polynomials whose degrees sum to zero to be 1.) The latter is simply w_k, the coefficient of z^k in $g(z)$. The former is the coefficient of $z^{\lceil m/2\rceil-k}$ in $\sum_{i\ge0}f(z)^i=1/(1-f(z))$. Thus the cardinality of $CF(A)/\sim_m$ is the summation of this product over k, which is the coefficient of $z^{\lceil m/2\rceil}$ in $g(z)/(1-f(z))$. (See [46, page 36] for a description of the "arithmetic" of generating functions.) This proves the first part of the proposition.

To prove the second part, let $h(z)=g(z)/(1-f(z))$. Then h is certainly analytic in the disk centre the origin of radius R, where R is the modulus of the "smallest" root [roots] of $1-f(z)$. By Lemma 6.2, we have $\|[z^{\lceil m/2\rceil}](g(z)/(1-f(z)))\|=[z^{\lceil m/2\rceil}](g(z)/(1-f(z)))\le c(1/(R-\varepsilon))^{\lceil m/2\rceil}$ where $\varepsilon>0$ and $c=\max_{\|z\|=R-\varepsilon}h(z)$.

□

To determine the cardinality of $CF(A)/\sim_m$ where m is even we must work with a slightly different generating function $\hat{g}(z)/(1-f(z))$. The polynomial $\hat{g}(z)(=\hat{g}_A(z)) = \sum_{i\geq 0} \hat{w}_i z^i$, which we call the **new deficiency polynomial**, is defined as follows. Let $\hat{w}_0 = 1$. For $i \geq 1$ and $v, v' \in A$ let $v \simeq_i v'$ if

$$(1/v) \sim_{2i} (1/v').$$

Let $\hat{w}_i$ denote the number of $\simeq_i$-equivalence classes of polynomials of degree greater than i in A. One may show that $\#(CF(A)/\sim_m)$ for m even is the coefficient of $z^{m/2}$ in $\hat{g}(z)/(1-f(z))$. Thus the statement of Proposition 6.4 remains true if we replace "m an odd positive integer" by "m an even positive integer" and $g(z)$ by $\hat{g}(z)$. The proof in the even case is almost identical to that given for the odd case, except we must replace $g(z)$ by $\hat{g}(z)$ wherever it occurs, and make other appropriate minor changes. We shall only need the case m odd in the proof of the case of Theorem 6.13 which we explicitly give in Section 6.4.2, but in the outlined proof of the other case in Section 6.4.3 we use the new deficiency polynomial $\hat{g}(z)$.

6.4 The Main Theorem

6.4.1 Preliminary Results

Let char $\mathbb{F}_q = 2$ and $u \in \mathbb{F}_q[x]$. Abbreviate L_q to L and P_q to P. We shall be concerned with the set of roots which lie in P of equations of the form

$$T^2 + uT + (1 + x\beta^2)$$

where β is a suitably chosen element in L. Let $\deg u = t$. Suppose that for some β there exists an α in P with $\alpha^2 + u\alpha + 1 = x\beta^2$. Then taking the norm of both sides we have $|\beta|^2 \leq q^{t-2}$. Conversely

Lemma 6.5 *For any $\beta \in L$ with $|\beta|^2 \leq q^{t-2}$ where $\deg u = t$ there exists a unique $\alpha \in P$ with $\alpha^2 + u\alpha + (1 + x\beta^2) = 0$.*

Proof: Let $\beta \in L$ with $|\beta|^2 \leq q^{t-2}$. Let $u = \sum_{0\leq j\leq t} u_j x^j$ and $x\beta^2 = \sum_{i\geq -(t-1)} h_i x^{-i}$. Observe that $h_i = 0$ for i even. We wish to show that there exists a unique $\alpha = \sum_{i\geq 1} f_i x^{-i} \in P$ with $\alpha^2 + u\alpha + (1 + x\beta^2) = 0$. Consider the Laurent series $\sum_i \alpha_i x^{-i}$ defined in the following way. Let $\alpha_i = 0$ for $i \leq 0$ and determine α_i for $i \geq 1$ from the following recurrences (here $s \geq -(t-1)$).

$$\begin{cases} \sum_{0\leq j\leq t} u_j \alpha_{s+j} + \alpha_{s/2}^2 = 0 & \text{for } s \text{ even, } s \neq 0 \\ \sum_{0\leq j\leq t} u_j \alpha_{s+j} + 1 = 0 & \text{for } s = 0 \\ \sum_{0\leq j\leq t} u_i \alpha_{s+j} + h_s = 0 & \text{for } s \text{ odd} \end{cases}$$

(The sequence $\{\alpha_i\}$ is consistently and uniquely defined because for each $s \geq -(t-1)$ the associated recurrence relation defines α_{s+t} uniquely in terms of the α_i with $i < s+t$.) The Laurent series $\alpha := \sum_{i\geq 1} \alpha_i x^{-i}$ then satisfies $\alpha^2 + u\alpha + (1 + x\beta^2) = 0$ by construction, and the properties of the Frobenius map (Chapter 2 Section 2.2.3). This proves existence. Uniqueness follows from the observation that the sequence of coefficients of any Laurent series $\alpha \in P$ for which $\alpha^2 + u\alpha + (1 + x\beta^2) = 0$ must satisfy the above recurrences. (Alternatively, observe that if $\alpha \in P$ is a root of $T^2 + uT + (1 + x\beta^2)$ then the other root is $\alpha + u$. This root does not lie in P if $u \neq 0$, and is not distinct from α if $u = 0$.)

□

Define $D_u = \{\beta \in L \,|\, |\beta|^2 \leq q^{t-2}\} = \{\beta \in L \,|\, |\beta| \leq q^{\lfloor t/2 \rfloor - 1}\}$. Let the map $\phi : D_u \to P$ be defined as follows: for $\beta \in D_u$ let $\phi : \beta \mapsto \alpha$ where α is the unique Laurent series in P with $\alpha^2 + u\alpha + (1 + x\beta^2) = 0$. Denote the image of the map ϕ by I_u. Observe that the map ϕ is an injection since $\operatorname{char} \mathbb{F}_q = 2$ and so ϕ is a bijection from D_u to I_u. An equivalent description of I_u is the set of all $\alpha \in P$ for which there exists $\beta \in L$ with $\alpha^2 + u\alpha + 1 = x\beta^2$.

The proof of the implication ($\Leftarrow$) in the following lemma is based upon the proof of the first part of Theorem 1 in Baum and Sweet ([5]).

Lemma 6.6 *Let $u \in \mathbb{F}_q[x]$ with $\operatorname{char} \mathbb{F}_q = 2$. Let A be a finite set of polynomials in $\mathbb{F}_q[x]$. Then $CF(A) \subseteq I_u$ if and only if for each polynomial $v \in A$ of degree at least 1 there exists $w \in \mathbb{F}_q[x]$ with $v^2 + uv = xw^2$.*

Proof: In this proof we use the equivalent description of I_u as the set of $\alpha \in P$ for which there exists a $\beta \in L$ such that $\alpha^2 + u\alpha + 1 = x\beta^2$.

($\Leftarrow$) Let $\alpha = [\,0; a_1, a_2, \ldots]$ where $a_j \in A\,(j \geq 1)$ with $\deg a_j \geq 1$. For each $l \geq 0$ define $\alpha^{(l)} = [\,0; a_1, a_2, \ldots, a_l, u, u, \ldots]$ where we use the obvious convention for $l = 0$. We prove by induction on l that there exists $\beta^{(l)} \in L$ with $(\alpha^{(l)})^2 + u\alpha^{(l)} + 1 = x(\beta^{(l)})^2$. If $l = 0$ then $\alpha^{(0)} = [\,0; u, u, \ldots]$ and so $(1/\alpha^{(0)}) + u = \alpha^{(0)}$ and $(\alpha^{(0)})^2 + u\alpha^{(0)} + 1 = 0$. We may therefore take $\beta^{(0)} = 0$. Now suppose that $l = n > 0$. Then $(1/\alpha^{(n)}) + a_1 = [\,0; a_2, \ldots, a_n, u, u, \ldots]$. So by induction, there exists $\beta' \in L$ such that

$$\{(1/\alpha^{(n)}) + a_1\}^2 + u\{(1/\alpha^{(n)}) + a_1\} + 1 = x(\beta')^2.$$

Hence

$$(\alpha^{(n)})^2 + u\alpha^{(n)} + 1 = x\{\alpha^{(n)}(\beta' + w)\}^2$$

where $a_1^2 + ua_1 = xw^2$.

Now $\alpha = [\,0; a_1, a_2, \ldots]$. So $\alpha = \lim_{l \to \infty} \alpha^{(l)}$ where $\alpha^{(l)} = [\,0; a_1, \ldots, a_l, u, u, \ldots]$. To each $\alpha^{(l)}$ there corresponds a unique $\beta^{(l)}$ with $(\alpha^{(l)})^2 + u\alpha^{(l)} + 1 = x(\beta^{(l)})^2$. Taking limits we find that $\alpha^2 + u\alpha + 1 = x\beta^2$ where $\beta = \lim_{l \to \infty} \beta^{(l)}$. By Result 2.8, the field L is complete with respect to $|\,|$ and so $\beta \in L$ as required.

($\Rightarrow$) To prove the converse suppose that $\alpha = [\,0; a_1, a_2, \ldots]$ where $a_j \in A\,(j \geq 1)$ with $\deg a_j \geq 1$ and $\alpha^2 + u\alpha + 1 = x\beta^2$ for some $\beta \in L$. Since $CF(A) \subseteq I_u$ there exists a $\beta' \in L$ such that $\alpha' := [\,0; a_2, a_3, \ldots]$ satisfies $(\alpha')^2 + u\alpha' + 1 = x(\beta')^2$. Now $\alpha' = (1/\alpha) + a_1$ and so $(a_1^2 + ua_1) = x(\beta' + (\beta/\alpha))^2$. The righthand side contains only odd powers of x and so there must exist $w \in \mathbb{F}_q[x]$ with $a_1^2 + ua_1 = xw^2$. Since a_1 was a arbitrary non-constant polynomial of A this completes the proof.

□

(Observe that if $\deg u = 0$ or $u = 0$ then if $v^2 + uv$ contains no even powers of x we must have that $\deg v = 0$ or $v = 0$. But if A is a set which does not contain any polynomials of degree greater than zero then $CF(A) = \emptyset$. Thus the cases $\deg u = 0$ and $u = 0$ are of no interest and we assume for the remainder of the chapter that $\deg u \geq 1$.)

Lemma 6.6 motivates Section 6.4.2 in which we study the pairs of polynomials v and w in $\mathbb{F}_q[x]$ which satisfy $v^2 + uv = xw^2$ for some fixed $u \in \mathbb{F}_q[x]$. We show that there is a bound on the number of pairs that can occur, and when and only when this bound is met we have that $CF(A) = I_u$ for some suitably chosen $A \subseteq \mathbb{F}_q[x]$. We prove this by considering the cardinality of the set of equivalence classes $CF(A)/\sim_m$ (where A is the appropriate set) and so must first determine the forms of $f_A(z)$ and $g_A(z)$ to make use of Proposition 6.4.

We finish this section with an example which illustrates the proof of Lemma 6.6.

Example 6.7 Let $u = x^2+x+1 \in \mathbb{F}_2[x]$ and $A = \{x, x^2+1, u\}$. Then one may verify that for every $v \in A$ there exists a corresponding $w \in \mathbb{F}_2[x]$ such that $v^2 + uv = xw^2$. For instance, $(x^2+1)^2+(x^2+x+1)(x^2+1) = x^3+x = x(x+1)^2$. Thus Lemma 6.6 tells us that $CF(A) \subseteq I_u$. As an example, consider the element $\alpha = [\,0; x, x^2+1, u, u, u, \dots\,] \in CF(A)$. Then

$$\begin{aligned}\alpha' : &= \frac{1}{(1/\alpha) - x} - (x^2+1)\\ &= [\,0; u, u, u, \dots\,].\end{aligned}$$

We know that $(\alpha')^2+u\alpha'+1 = 0$. Hence $\alpha^2+u\alpha+1 = x\beta^2$ where $\beta = (1+x^2)\alpha+(1+x)$.

6.4.2 The Case $\deg u$ Even

It is easier to treat the cases $\deg u$ even and $\deg u$ odd separately, although the analysis in each case is essentially the same. In this section, we consider the former case, and briefly discuss the latter in the next.

Let $\deg u = t$ be a positive even number. We are interested in determining the solutions in $\mathbb{F}_q[x] \times \mathbb{F}_q[x]$ of the equation $T^2 + uT + xY^2 = 0$ where $\operatorname{char} \mathbb{F}_q = 2$. Observe that if (v, w) is such a solution, then w is uniquely determined by v (since squaring is an automorphism in $\mathbb{F}_q$). We therefore define the set $G(u)$ to be the set of all $v \in \mathbb{F}_q[x]$ for which there exists $w \in \mathbb{F}_q[x]$ with $v^2 + uv = xw^2$. (It is convenient to include polynomials of degree zero and zero itself in $G(u)$, although these polynomials do not occur as partial quotients of continued fractions in $CF(G(u))$.) For the sake of notational simplicity, we occasionally abbreviate $G(u)$ to G. For $m \geq 0$, let G_m denote the set of all polynomials in G of degree less than or equal to m, and V_m the set of polynomials in G with degree exactly m. Define $G_{-1} = \{0\}$.

Lemma 6.8 *The set G is an elementary abelian 2-group under addition and the sets G_m are subgroups with $G = G_t$. Furthermore, $\#(G_m/G_{m-2}) \leq q$ for $1 \leq m \leq t-1$ and $\#(G_t/G_{t-1}) = 2$.*

Proof: It is easy to see that the set G is an elementary abelian 2-group with the sets G_m as subgroups. We claim that G does not contain any elements of even degree except those elements of degree t. For if v has even degree not equal to t then the leading term of $v^2 + uv$ has even degree, and so no polynomial w can exist with $v^2 + uv = xw^2$. Thus $G_m = G_{m-1}$ for m even. Similarly G does not contain any polynomials of odd degree greater than t. Thus $G = G_t$. To prove the remaining remarks, it suffices to consider the case m odd with m less than t. Suppose that $\#(G_m/G_{m-2}) > q$ where m is odd with $1 \leq m \leq t-1$. Then G_m/G_{m-2} must contain elements of the form $\gamma x^m + \gamma' x^{m-1} + G_{m-2}$ and $\gamma x^m + \gamma'' x^{m-1} + G_{m-2}$ where $\gamma, \gamma', \gamma'' \in \mathbb{F}_q$ with $\gamma' \neq \gamma''$. But then $(\gamma' - \gamma'')x^{m-1} + G_{m-2} \in G_m/G_{m-2}$ and so G_m contains a polynomial of even degree. This is a contradiction since $m \leq t-1$. To prove the final claim, we first observe that 0, $u \in G$ and so $\#(G_t/G_{t-1}) \geq 2$. Suppose that $\#(G_t/G_{t-1}) > 2$. Then G_t contains an element v whose leading coefficient $l(v)$ differs from the leading coefficient $l(u)$ of u. But since $v^2 + uv$ contains only odd powers of x, we have that $l(u)^2 + l(u)l(v) = 0$, which implies $l(u) = l(v)$. This contradiction establishes the final claim and completes the proof.

□

We call the set $G = G(u)$ the **full solution group** for u, and a subset of G a **solution set** for u. If G meets the bounds imposed by the above lemma then we say that G is a **maximal solution group**.

Lemma 6.9 *Let $u \in \mathbb{F}_q[x]$ have even degree $t \geq 2$ where $\operatorname{char} \mathbb{F}_q = 2$, and suppose that $G(u)$ is a maximal solution group for u. Then the degree enumerator $f(z)$ of $G(u)$ is given by*

$$f(z) = \sum_{\substack{1 \leq i \leq t-1 \\ i\, odd}} (q-1)q^{(i-1)/2} z^i + q^{t/2} z^t$$

and we have the factorisation

$$1 - f(z) = (1 - qz) \sum_{\substack{0 \leq i \leq t-2 \\ i\, even}} q^{i/2}(z^i + z^{i+1}).$$

Proof: Recall that $V_m = \{v \in G \mid \deg v = m\}$. So the mth coefficient $(m \geq 1)$ of $f(z)$ is $v_m = \#(V_m)$. As we observed in the proof of the preceding lemma, for m even and not equal to t, and for m odd and greater than t, we have $\#(V_m) = 0$. For m odd and less than t, $\#(V_m) = \#(G_m) - \#(G_{m-1}) = \#(G_m) - \#(G_{m-2})$ since $\#(G_{m-1}) = \#(G_{m-2})$. Now $\#(G_{-1}) = 1$ and since G meets the bounds imposed by the previous lemma we have that $\#(G_m/G_{m-2}) = q$ for m odd with $1 \leq m \leq t-1$. An easy induction argument establishes that $\#(G_m) = q^{(m+1)/2}$ and furthermore since $\#(G_t/G_{t-1}) = 2$ we have that $\#(G_t) = 2q^{t/2}$. So $\#(V_m) = (q-1)q^{(m-1)/2}$ for m odd and less than t. Similarly $\#(V_t) = \#(G_t) - \#(G_{t-1}) = 2q^{t/2} - q^{t/2} = q^{t/2}$. The factorisation is easy to verify.

□

(We in fact have the fuller factorisation

$$1 - f(z) = (1 - qz)(1 + z) \prod_{1 \leq s \leq (t/2)-1} (qz^2 - \exp 2\pi i s/(t/2)).$$

It is somewhat curious that the roots of $1 - f$ have complex modulus $1/q, 1/\sqrt{q}$ and 1, although this observation plays little part in what follows.)

Having determined the form of the degree enumerator polynomial $f(z)$ in the case that G is a maximal solution group, we now wish to find that of the deficiency polynomial $g(z)$. We show in Lemma 6.10 that $g(z)$ is actually equal to the cofactor of $1 - qz$ in the factorisation of $1 - f(z)$, and so $g(z)/(1 - f(z)) = (1 - qz)^{-1}$. Using Proposition 6.4 we then see in Lemma 6.11 that the cardinality of $CF(G)/\sim_{2n-1}$ when G is a maximal solution group is q^n. This allows us to prove Lemma 6.12, which is the main result of Section 6.4.2.

Lemma 6.10 *Let $u \in \mathbb{F}_q[x]$ have positive even degree t where $\operatorname{char} \mathbb{F}_q = 2$, and suppose that $G(u)$ is maximal. Then the deficiency polynomial $g(z)$ of $G(u)$ is given by*

$$g(z) = \sum_{\substack{0 \leq i \leq t-2 \\ i\, even}} q^{i/2}(z^i + z^{i+1})$$

Proof: Let $g(z)$ denote the deficiency polynomial of $G = G(u)$ and w_i ($i \geq 0$) the coefficient of z^i in $g(z)$. Certainly $w_i = 0$ for $i \geq t$ and by definition $w_0 = 1$. For $1 \leq i \leq t-1$ we must establish that

$$w_i = \begin{cases} q^{i/2} & \text{when } i \text{ is even,} \\ q^{(i-1)/2} & \text{when } i \text{ is odd.} \end{cases}$$

We first show that $w_i \leq q^{\lfloor i/2 \rfloor}$ $(1 \leq i \leq t-1)$ by considering the number of polynomials of each degree in a subset $W^{(i)} \subseteq G$ of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes. We then argue that this bound can be met by considering the structure of the maximal solution group G.

Suppose that $W^{(i)} \subseteq G$ is a set of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes. Let $W_s^{(i)}$ denote the subset of polynomials in $W^{(i)}$ which have degree s. Then $\#(W^{(i)}) = \sum_{s>i} \#(W_s^{(i)})$. Since $W^{(i)} \subseteq G$, $\#(W_s^{(i)}) = 0$ if $s > t$, or $s < t$ with s even. It remains to bound the cardinality of $W_s^{(i)}$ for $s = t$ or $i < s < t$ with s odd.

We consider two cases: Suppose first that $2i \leq t$. Let $i < s < 2i$ with s odd (and so $s < t$). Let $v, v' \in W_s^{(i)}$ with $v \neq v'$. Since $v \not\approx_i v'$ we have that $|(1/v) - (1/v')| \geq q^{-2i+1}$ and so $|v - v'| \geq q^{2(s-i)+1}$. Furthermore, since $v, v' \in G$ and G is a group which contains only polynomials of odd degree (excluding those of degree t) we have that $\deg(v - v')$ is odd. We now apply Lemma 6.3 with $b = s$ and $a = 2(s-i)+1$ to deduce that $\#(W_s^{(i)}) \leq (q-1)q^{(2i-s-1)/2}$. Writing $W_{\geq 2i}$ for $\cup_{s \geq 2i} W_s^{(i)}$ we see that if $W_{\geq 2i}$ contains two distinct members v and v' of degrees m and n respectively with $m \geq n \geq 2i$ then $q^m \geq |v - v'| \geq q^{-2i+m+n+1} \geq q^{m+1}$ which is a contradiction. Thus $\#(W_{\geq 2i}) \leq 1$. It is a simple exercise in summing geometric series to then show that $\#(W^{(i)}) = \sum_{s>i} \#(W_s^{(i)}) = \sum_{i<s<2i, s\ odd} \#(W_s^{(i)}) + \#(W_{\geq 2i}) \leq \sum_{i<s<2i, s\ odd} (q-1)q^{(2i-s-1)/2} + 1 = q^{\lfloor i/2 \rfloor}$

Suppose now that $2i > t$. For $i < s \leq t-1 < 2i$ and s odd one may show as before that $\#(W_s^{(i)}) \leq (q-1)q^{(2i-s-1)/2}$. Similarly we may appeal to Lemma 6.3 to show that $\#(W_t^{(i)}) \leq q^{(2i-t)/2}$. (Recall that $\#(G_t/G_{t-1}) = 2$ and so $n_t(W_t^{(i)}) = 1$ in Lemma 6.3 in this case.) Once again summing over s one concludes that $\#(W^{(i)}) = \sum_{i<s\leq t-1} \#(W_s^{(i)}) + \#(W_t^{(i)}) \leq \sum_{i<s\leq t-1, s\ odd} (q-1)q^{(2i-s-1)/2} + q^{(2i-t)/2} = q^{\lfloor i/2 \rfloor}$.

To show that $w_i = q^{\lfloor i/2 \rfloor}$ one must first prove that the bounds on the cardinalities of the sets $W_s^{(i)}$ discussed above can actually be met. For each i $(1 \leq i \leq t-1)$ and each suitable s we show that one may construct a set $W_s^{(i)}$, of polynomials of degree s in G which lie in distinct $\approx_i$-equivalence classes, whose cardinality meets the appropriate bound. (For each i, we also define a set $W_{\geq 2i}$ which we need in the case $2i \leq t$.) We then take suitable unions of these sets to give, for each required i, a set $W^{(i)}$, of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes, such that $\#(W^{(i)}) = q^{\lfloor i/2 \rfloor}$.

If s is even or s is greater than t, then we define $W_s^{(i)} = \emptyset$. In the case $2i \leq t$ we define $W_{\geq 2i} = \{f\}$ where f is any polynomial in G with degree at least $2i$. The main cases to consider are s odd with $i < s < t$, and $s = t$. In the former case, one must show that for each i $(1 \leq i \leq t-1)$ there exist a set $W_s^{(i)}$ $(i < s \leq \min\{2i-1, t\}$, s odd$)$ of $(q-1)q^{(2i-s-1)/2}$ polynomials of G which have degree s such that distinct elements lie in different $\approx_i$-equivalence classes. That is to say: $v, v' \in W_s^{(i)}$ with $v \neq v' \Rightarrow |v - v'| \geq q^{2(s-i)+1}$. We construct such a set as follows: For each positive m which is odd and less than t, choose polynomials $f_{m_0}, f_{m_1}, \ldots, f_{m_{q-1}}$ such that the images of the f_{m_i} under the natural homomorphism $G_m \to G_m/G_{m-2}$ are distinct. (One may do this since G is a maximal solution group.) We may assume that $\deg f_{m_i} = m$ for

$1 \leq i \leq q-1$. Let the set $W_s^{(i)}$ be given by

$$W_s^{(i)} = \{f_{s_i} + \sum_{\substack{2(s-i)+1 \leq m \leq s-2 \\ m\ odd}} f_{m_{j_m}} \mid 1 \leq i \leq q-1; \text{ for each } m, 0 \leq j_m \leq q-1\}.$$

It is easy to verify that $W_s^{(i)}$ meets our requirements.

The case $s = t$ is similar. It is easily verified that for each $i\,(1 \leq i \leq t-1)$ the set $W_t^{(i)}$ constructed as follows has cardinality $q^{(2i-t)/2}$, and if $v, v' \in W_t^{(i)}$ with $v \neq v'$ then $|v - v'| \geq q^{2(t-i)+1}$, and so distinct members lie in different $\approx_i$-equivalence classes: Let f_{t_0} and f_{t_1} be elements in G_t with distinct images under the natural homomorphism $G_t \to G_t/G_{t-1}$, and $f_{m_0}, f_{m_1}, \ldots, f_{m_{q-1}}$ (m odd and less than t) be as in the preceding paragraph. (Such elements exist since G is maximal.) We may assume $\deg f_{t_1} = t$. Let $W_t^{(i)}$ be given by

$$W_t^{(i)} = \{f_{t_1} + \sum_{\substack{2(t-i)+1 \leq m \leq t-1 \\ m\ odd}} f_{m_{j_m}} \mid \text{For each } m,\ 0 \leq j_m \leq q-1\}.$$

Finally, for each $i\,(1 \leq i \leq t-1)$ we define a set $W^{(i)}$ of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes, with $\#(W^{(i)}) = q^{\lfloor i/2 \rfloor}$ as follows: For $2i \leq t$ let $W^{(i)} = \cup_{i<s<2i} W_s^{(i)} \cup W_{\geq 2i}$ and for $2i > t$ let $W^{(i)} = \cup_{i<s\leq t-1} W_s^{(i)} \cup W_t^{(i)}$. From the construction of the sets $W_s^{(i)}$ we know that $W^{(i)}$ will in both cases have the appropriate cardinality. We need to show that distinct polynomials in $W^{(i)}$ lie in different $\approx_i$-equivalence classes. Let $v, v' \in W^{(i)}$ with $\deg v = s$ and $\deg v' = s'$ and $v \neq v'$. Now $W^{(i)}$ can contain at most one polynomial of degree greater than $2i$. So $s, s' \leq 2i$ and $v \in W_s^{(i)}$, $v' \in W_{s'}^{(i)}$. If $s = s'$ then $v \not\approx_i v'$ by our previous observations on the set $W_s^{(i)} (= W_{s'}^{(i)})$. If $s \neq s'$ then $|(1/v) - (1/v')| = q^{-\min\{s,s'\}} \geq q^{-2i+1}$ since $\min\{s, s'\}$ is odd. Hence $v \not\approx_i v'$ in this case. Thus $w_i = \#(W^{(i)}) = q^{\lfloor i/2 \rfloor}$ which completes the proof.

□

Recall that we say that two sets of polynomials are equivalent if any polynomial of degree at least 1 which lies in one, lies in the other.

Lemma 6.11 *Let $u \in \mathbb{F}_q[x]$ have positive even degree and* $\operatorname{char} \mathbb{F}_q = 2$. *If H is a solution set for u which is equivalent to a maximal solution group for u then the cardinality of $CF(H)/\sim_{2n-1}$ is q^n. If H is a solution set for u which is not equivalent to a maximal solution group then the cardinality of $CF(H)/\sim_{2n-1}$ is strictly less than q^n for sufficiently large n.*

Proof: Let $G = G(u)$ denote the full solution group for u and let H be a solution set for u. Denote the degree enumerator and deficiency polynomials for G and H by $f_G(z)$, $g_G(z)$ and $f_H(z)$, $g_H(z)$ respectively. Suppose that H is equivalent to a maximal solution group for u. Then in this case G must be maximal and from Lemmas 6.9 and 6.10, the rational function $g_G(z)/(1 - f_G(z))$ is $(1 - qz)^{-1}$. But H is equivalent to G and so $g_H(z)/(1 - f_H(z)) = g_G(z)/(1 - f_G(z))$. So by Proposition 6.4, the cardinality of $CF(H)/\sim_{2n-1}$ is q^n.

We now consider the second case in which H is not equivalent to a maximal solution group. The coefficients of $f_H(z)$ are positive real numbers and are bounded by those of $f_G(z)$; thus $f_H(z) \leq f_G(z)$ for all positive real z. We claim that $f_H(1/q) < 1$: In the case that G is maximal we have that $f_G(1/q) = 1$ and so $f_H(1/q) < 1$ since at least one coefficient of $f_H(z)$ is strictly smaller than the corresponding coefficient of

$f_G(z)$ (here H is not equivalent to G). If G is not maximal then it is not difficult to see that $f_G(1/q) < 1$. Since $f_H(1/q) \leq f_G(1/q)$ our claim is also true in this case.

Now let $\gamma \in \mathbb{C}$ be the root of $1 - f_H(z)$ with smallest complex modulus. If $\|\gamma\| \leq 1/q$ then $\|1 - f_H(\gamma)\| \geq 1 - f_H(\|\gamma\|) \geq 1 - f_H(1/q) > 0$ (the penultimate inequality holds because f_H is an increasing function on the positive reals). Hence $\|\gamma\| > 1/q$. Letting $A = H$ in Proposition 6.4 and choosing ε in the second part of the proposition so that $\|\gamma\| - \varepsilon > 1/q$ yields the second statement.

□

We may now state the main result of this section.

Lemma 6.12 *Let $u \in \mathbb{F}_q[x]$ have positive even degree and* $\operatorname{char} \mathbb{F}_q = 2$*. Then $I_u = CF(A)$ if and only if A is equivalent to a maximal solution group for u.*

Proof: ($\Leftarrow$) Suppose that A is equivalent to a maximal solution group for u. Let $\beta, \beta' \in D_u$ with $\phi(\beta) = \alpha$ and $\phi(\beta') = \alpha'$ where $\alpha, \alpha' \in I_u$. Subtracting the relevant equations we find that

$$(\alpha - \alpha')^2 + u(\alpha - \alpha') = x(\beta - \beta')^2$$

and so $|\beta - \beta'|^2 = q^{t-1}|\alpha - \alpha'|$. From this it follows that

$$\beta \sim_{n-(t/2)} \beta' \Leftrightarrow \alpha \sim_{2n-1} \alpha' \tag{6.1}$$

where $\deg u = t$.

Thus $\#(I_u/\sim_{2n-1}) = \#(D_u/\sim_{n-(t/2)}) = q^n$ (the first equality holds because of (6.1) and the final one comes directly from the definition of D_u). From Lemma 6.11, $\#(CF(A)/\sim_{2n-1}) = q^n$ since A is a equivalent to a maximal solution group, and so $\#(CF(A)/\sim_{2n-1}) = \#(I_u/\sim_{2n-1})$ for each n. Furthermore $CF(A) \subseteq I_u$ by Lemma 6.6. Suppose that $CF(A) \neq I_u$. Let $\alpha \in I_u$ with $\alpha \notin CF(A)$. In particular, for some m we have that $\alpha \not\sim_{2m-1} \alpha'$ for all $\alpha' \in CF(A)$. Since $CF(A) \subseteq I_u$ it follows that $\#(I_u/\sim_{2m-1}) > \#(CF(A)/\sim_{2m-1})$, which is a contradiction. Thus $CF(A) = I_u$.

($\Rightarrow$) Suppose that A is not equivalent to a maximal solution group for u. If A is not equivalent to a solution set for u then the contrapositive of ($\Rightarrow$) in Lemma 6.6 shows that $CF(A) \not\subseteq I_u$. So suppose that A is equivalent to a solution set for u but is not equivalent to a maximal solution group. Then by Lemma 6.11 the cardinality of $CF(A)/\sim_{2n-1}$ is strictly less than q^n for sufficiently large n. But if $CF(A) = I_u$ then we must have that $\#(CF(A)/\sim_{2n-1}) = \#(I_u/\sim_{2n-1}) = q^n$ for all n. Therefore $CF(A) \neq I_u$ as required.

□

6.4.3 The Case $\deg u$ Odd

The case $\deg u$ odd can be treated in a similar way to $\deg u$ even, modulo a few changes which we describe in this section.

The full solution group $G(u)$ of a polynomial u of odd degree t is defined in exactly the same way and any subset of this group is called a solution set for u. The full solution group $G(u)$ is said to be maximal if its degree enumerator $f(z)$ is of the form

$$f(z) \quad = \quad \sum_{\substack{1 \leq i \leq t-1 \\ i\ even}} (q-1)q^{i/2}z^i + q^{(t+1)/2}z^t.$$

In this case we have the factorisation

$$1 - f(z) \quad = \quad (1 - qz)(1 + \sum_{\substack{1 \le i \le t-2 \\ i\,odd}} q^{(i+1)/2}(z^i + z^{i+1})).$$

For any finite subset A of $\mathbb{F}_q[x]$, recall (from the discussion following Proposition 6.4) that one may define the new deficiency polynomial $\hat{g}_A(z) = \sum_{i \ge 0} \hat{w}_i z^i$. We then have that the cardinality of $CF(A)/\sim_{2n}$ equals the coefficient of z^n in $\hat{g}_A(z)/(1 - f_A(z))$, where $f_A(z)$ is the degree enumerator of A. Examining the proof of Lemma 6.12, we see that to establish an odd case version of the lemma we need to show the following: if $G(u)$ is a maximal solution group for u then $\#(CF(G(u))/\sim_{2n}) = q^n$, and if H is any solution set which is not equivalent to a maximal solution group then $\#(CF(H)/\sim_{2n}) < q^n$ for sufficiently large n. Once again, the latter is straightforward and follows from the fact that the complex modulus of the smallest root of $1 - f_H(z)$ in the case that H is a solution set for u which is not equivalent to a maximal solution group is strictly greater than $1/q$. To prove the former we must establish the form of the new deficiency polynomial $\hat{g}(z)$ of a maximal solution group $G(u)$. We must show that it is equal to the cofactor of $1 - qz$ in the above factorisation of $1 - f(z)$. Fortunately, we can use Lemma 6.10 to do this: Observe first that if $G(u)$ is a maximal solution group for u where $\deg u$ is odd, then $xG(u)$ is a maximal solution group for xu, which has even degree. Now suppose that $W \subseteq G(u)$ is a set of polynomials of degree greater than i which lie in distinct $\simeq_i$-equivalence classes. Then it is easily seen that $xW \subseteq xG(u)$ is a set of polynomials of degree greater than $i+1$ which lie in distinct $\approx_{i+1}$-equivalence classes. One may deduce (with a little work) from this observation and Lemma 6.10 that for i with $1 \le i \le t-1$ the coefficient of z^i in $\hat{g}(z)$ is $q^{(i+1)/2}$ if i is odd, and $q^{i/2}$ if i is even. Thus $\hat{g}(z)$ has the required form.

Lemma 6.12 together with the odd case version of the lemma whose proof we have just outlined together establish Theorem 6.13, which we present in the next section.

6.4.4 A Statement of the Main Theorem

We have now proved the following theorem, which is the central result of this chapter. For ease of reference, we include all necessary definitions in the statement of the theorem.

Theorem 6.13 *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $u \in \mathbb{F}_q[x]$. Let I_u denote the set of all $\alpha \in P_q$ for which there exists a $\beta \in L_q$ with*

$$\alpha^2 + u\alpha + (1 + x\beta^2) = 0.$$

For a finite set of polynomials A, let $CF(A)$ be given by

$$CF(A) = \{[0; a_1, a_2, \dots] \,|\, a_j \in A,\, \deg a_j \ge 1\}.$$

Then $I_u = CF(A)$ if and only if A is equivalent to a maximal solution group for u. That is to say, $\deg u \ge 1$ and A is a set of polynomials which satisfies the following criteria

1. *For each $v \in A$ of degree at least 1 there exists $w \in \mathbb{F}_q[x]$ with $v^2 + uv = xw^2$.*

2. *The number n_m of polynomials of degree $m \geq 1$ in A is:*
   For $\deg u$ *even*

$$n_m = \begin{cases} (q-1)q^{(m-1)/2} & \text{for } m \text{ odd and less than } \deg u \\ 0 & \text{for } m \text{ even or } m \text{ greater than } \deg u \\ q^{m/2} & \text{for } m = \deg u \end{cases}$$

   For $\deg u$ *odd*

$$n_m = \begin{cases} (q-1)q^{m/2} & \text{for } m \text{ even and less than } \deg u \\ 0 & \text{for } m \text{ odd or } m \text{ greater than } \deg u \\ q^{(m+1)/2} & \text{for } m = \deg u. \end{cases}$$

In the remaining parts of Section 6.4 we will be concerned with finding all polynomials whose full solution groups are maximal. We shall see that they do not exist for fields with more than 4 elements; however, we are able to give a complete description in the case that the field has 2 or 4 elements.

6.4.5 Polynomials with Maximal Solution Groups

We begin with a result which implies that in the search for polynomials with maximal solution groups we may restrict our attention to the fields with two elements and four elements.

Proposition 6.14 *Let $u \in \mathbb{F}_q[x]$ and $\deg u \geq 1$, where $\operatorname{char} \mathbb{F}_q = 2$ and $q \neq 2$ or 4. The full solution group for u is not maximal.*

Proof: Let $u \in \mathbb{F}_q[x]$ with $\deg u \geq 1$ and $\operatorname{char} \mathbb{F}_q = 2$. Observe that if $G(u)$ is a maximal solution group for u where $\deg u$ is odd, then $xG(u) = \{xv \mid v \in G(u)\}$ is a maximal solution group for xu. We may therefore assume that u has even degree at least 2. Suppose that $G(u)$ is maximal; so it meets the bounds imposed by Lemma 6.8. In particular $\#(V_1) = \#(G_1) - \#(G_{-1}) = q - 1$. Let $u = \sum_{0 \leq i \leq t} u_i x^i$ and $v = a + bx \in V_1$. Then the polynomial $v^2 + uv$ contains only odd powers of x. Thus the coefficients of x^0 and x^2 in $v^2 + uv$, which are $a^2 + au_0$ and $b^2 + bu_1 + au_2$ respectively, are both 0. We conclude that $a = 0$ or u_0. If $a = 0$ then $b = u_1$, since we must assume that $b \neq 0$. When $a = u_0$, b can take at most 2 values. Hence $\#(V_1) \leq 3$. Thus $q - 1 = \#(V_1) \leq 3$, which completes the proof.

□

We now determine all polynomials over the field with four elements which have maximal solution groups.

Proposition 6.15 *Let $u \in \mathbb{F}_4[x]$ with $\deg u \geq 1$. Then the full solution group for u is maximal if and only if $u = u_0 + u_1x + u_2x^2$ where $u_0u_2 = u_1^2 \neq 0$.*

Proof: We first consider the case $\deg u = 2$. So $u = u_0 + u_1x + u_2x^2$. Then $G(u)$ is maximal if and only if $\#(V_1) = 4 - 1 = 3$ and $\#(V_2) = 4$. If $\#(V_1) = 3$ then since $u \in V_2$ and $u + V_1 \subseteq V_2$ we have that $\#(V_2) = 4$. Thus $G(u)$ is maximal if and only if $\#(V_1) = 3$. We have seen from the proof of Proposition 6.14 that this is true precisely when $u_0 \neq 0$ (this ensures that the a in Proposition 6.14 can take two distinct values) and there are two elements b_1 and b_2 in $\mathbb{F}_4$ such that $b_i^2 + u_1b_i + u_0u_2 = 0\,(i = 1, 2)$ (this ensures the non-zero value of a will yield two distinct choices for b). Observe that $u_1 \neq 0$ in this case. Making the substitution $b_i = u_1 c_i \in \mathbb{F}_4$ and dividing by u_1^2 we see that $\mathrm{Tr}(c_i) := c_i^2 + c_i = u_0 u_2 / u_1^2$. If $u_0 u_2 / u_1^2 \in \mathbb{F}_2$ there are two distinct such c_i, and otherwise there are none. We have therefore shown that any polynomial of degree 2 with a maximal solution group must be of the form described in the proposition. If $\deg u = 1$ and $G(u)$ is maximal then xu has a maximal solution group $G(xu) = xG(u)$. But xu has a zero constant term. This contradicts our description of polynomials of degree 2 with maximal solution groups. Thus there are no polynomials of degree 1 with maximal solution groups.

Suppose now that $\deg u > 2$ with $u = \sum_{0 \leq i \leq t} u_i x^i$. Once again, we may assume that $\deg u$ is even. Let $G(u)$ be a maximal solution group for u. Then $G(u)$ must contain $(q-1)q = 12$ polynomials of degree 3. Let $v_0 + v_1 x + v_2 x^2 + v_3 x^3 \in V_3$. So $v_3 \neq 0$. Then the coefficients of x^0, x^2, x^4, x^6 in $v^2 + uv$ are 0. Therefore

$$\begin{aligned} v_0^2 + u_0 v_0 &= 0 \\ v_1^2 + u_0 v_2 + u_1 v_1 + u_2 v_0 &= 0 \\ v_2^2 + u_1 v_3 + u_2 v_2 + u_3 v_1 + u_4 v_0 &= 0 \\ v_3^2 + u_3 v_3 + u_4 v_2 &= 0 \end{aligned}$$

One may use ad hoc arguments to show that the above system of equations has at most 8 solutions (v_0, v_1, v_2, v_3) with $v_3 \neq 0$, for any choice of u_i $(0 \leq i \leq 4)$. Therefore $G(u)$ cannot be maximal. This contradiction completes the proof.

□

The above lemma gives a family of 9 polynomials u of degree 2 over $\mathbb{F}_4$ with $I_u = CF(G(u))$. More explicitly, if $u = u_0 + u_1 x + u_2 x^2 \in \mathbb{F}_4[x]$ where $u_0 u_2 = u_1^2 \neq 0$, then $G(u)$ is the additive group generated by the polynomials $u_1 x, u_0 + \gamma u_1 x$ and u. Here $\gamma \in \mathbb{F}_4$ with $\gamma \neq 0, 1$.

Example 6.16 (A maximal solution group in $\mathbb{F}_4[x]$.) Letting $u = 1 + x + x^2$ we have that $G(u) = \{0, x, 1 + \gamma x, 1 + (1 + \gamma)x, 1 + x + x^2, 1 + x^2, (1 + \gamma)x + x^2, \gamma x + x^2\}$. Any continued fraction $\alpha \in P$ whose partial quotients lies in $G(u)$ must satisfy an equation of the form $\alpha^2 + u\alpha + 1 = x\beta^2$ for some $\beta \in L$. We shall see in Corollary 6.22 that this implies the sequence of coefficients of such an α satisfies an "$\mathbb{F}_2$-linear" recurrence.

We conclude by considering the $\mathbb{F}_2$ case.

Proposition 6.17 *Let $u \in \mathbb{F}_2[x]$ with $\deg u > 6$. The full solution group of u is not maximal.*

Proof: Once again it is enough to prove the proposition for u a polynomial of even degree t with $t \geq 8$. So suppose that u is such a polynomial and $G(u)$ is maximal. Then either x or $x+1$ lies in $G(u)$ and also one of x^3, x^3+1, x^3+x^2 or x^3+x^2+1 must lie in $G(u)$.

Suppose that $x \in G(u)$. Then $u = x + \sum_{i \in M} x^i + x^t$ where $M \subseteq \{2, 4, \ldots, t-2\}$. Now $x^3 \notin G(u)$ as $x^6 + ux^3$ contains the even power x^4. Also $x^3 + 1 \notin G(u)$ as $x^6 + 1 + (x^3+1)u$ contains the term x^t (since $t > 6$). Similarly, if $v = x^3 + x^2$ or $x^3 + x^2 + 1$ then $v \notin G(u)$ since $v^2 + uv$ contains the even power x^{t+2} (since $t + 2 > 6$).

Hence $x + 1 \in G(u)$. So u must include the term x^{t-1}. Also observe that $(x+1)u$ consists of 1, x^2 and odd powers of x. If $v = x^3$ or $x^3 + 1$ then $v \notin G(u)$ since $v^2 + uv$ contains the even power x^{t+2}. If $v = x^3 + x^2$ then $x^6 + x^4 + x^2(x+1)u$ contains the term x^6 by our previous observation and so $v \notin G(u)$. Finally, $x^3 + x^2 + 1 \notin G(u)$ as $x^6 + x^4 + 1 + x^2(x+1)u + u$ contains the even power x^t (since $t > 6$). This contradiction

The polynomial u	The maximal solution group $G(u)$
$x+1$	$\langle 1, u\rangle$
x^2+x	$\langle x, u\rangle$
x^2+1	$\langle x+1, u\rangle$
x^2+x+1	$\langle x, u\rangle$
x^3+1	$\langle 1, x^2+x+1, u\rangle$
x^4+x	$\langle x, x^3+x^2+x, u\rangle$
x^4+x^3+x+1	$\langle x+1, x^3+1, u\rangle$
$x^4+x^3+x^2+1$	$\langle x+1, x^3+x+1, u\rangle$
x^4+x^2+x+1	$\langle x, x^3+x^2+1, u\rangle$
$x^6+x^5+x^2+1$	$\langle x+1, x^3+x^2+1, x^5+x+1, u\rangle$
x^6+x^4+x+1	$\langle x, x^3+1, x^5+x^4+1, u\rangle$

Table 6.1: Polynomials with Maximal Full Solution Groups in $\mathbb{F}_2[x]$

completes the proof.

□

We list all polynomials $u \in \mathbb{F}_2[x]$ whose full solution groups are maximal in Table 6.1 along with (the generators of) their full solution groups.

Example 6.18 (A maximal solution group in $\mathbb{F}_2[x]$.) Recall in Example 6.7 we considered the polynomial $u = x^2+x+1$ over $\mathbb{F}_2$. From Table 6.1 we see that u has a full solution group and so $CF(G(u)) = I_u$. Thus if we choose any $\beta \in L$ with $|\beta| \leq 1$ then we may find an $\alpha \in CF(G(u))$ such that $\alpha^2 + u\alpha + 1 = x\beta^2$. For example, if we take an appropriate $\beta \in \mathbb{F}_q(x)$, then the corresponding $\alpha \in CF(G(u))$ must be either an element of $\mathbb{F}_q(x)$, or have degree 2 over $\mathbb{F}_q(x)$. But all elements in $CF(G(u))$ have infinite continued fraction expansions and are therefore irrational. Hence α is a quadratic element in this case and so has an eventually periodic continued fraction expansion (see Example 2.22 in Chapter 2).

6.5 Corollaries to the Main Theorem

In this section, we discuss some applications of Theorem 6.13 and the results which follow it. The first is to the problem of constructing algebraic Laurent series with partial quotients of bounded degree, and the second to the study of sequences over finite fields.

6.5.1 Algebraic Laurent Series with Bounded Partial Quotients

There is a well-known conjecture in number theory which asserts that the partial quotients of the continued fraction expansion of an algebraic real number of degree at least 3 are unbounded ([35, page 238]); however, almost nothing is known about the continued fractions of such numbers, as we explained at the beginning of Chapter 5. The situation over fields of Laurent series in positive characteristic is somewhat different; in particular, in recent years several explicit expansions of algebraic Laurent series which have bounded partial quotients have been given (see Chapter 5 Section 5.2). The first and simplest result along these lines is that over the binary field, there exist algebraic Laurent series of every even degree, whose partial quotients are all linear polynomials ([5, Proposition 3]). We prove a similar result for the field of four elements.

Corollary 6.19 *Let $d \in \mathbb{N}$ be such that there exists an element of L_4 algebraic of degree d over $\mathbb{F}_4(x)$. Then there exists an element of L_4 with partial quotients of degree not greater than 2 which is algebraic of degree d or $2d$ over $\mathbb{F}_4(x)$.*

Proof: Consider the polynomial $u = 1 + x + x^2 \in \mathbb{F}_2[x] \subseteq \mathbb{F}_4[x]$. Then u has a maximal solution group $G(u)$, by Proposition 6.15. From Theorem 6.13 we know that $CF(G(u)) = I_u$. Let $\beta \in L_4$ be algebraic of degree d over $\mathbb{F}_4(x)$. By multiplying by a suitable power of x, we may assume that $|\beta| \leq 1 = q^{\lfloor 2/2 \rfloor - 1}$. Now β^2 has either degree d or possibly, if d is even, degree $d/2$ over $\mathbb{F}_4(x)$. We show that the latter cannot occur. For suppose that β^2 has degree $d/2$ with minimum polynomial $h(T)$ where $\deg_T h = d/2$. Then β is a repeated root of $h(T^2)$ and $\deg_T h(T^2) = d$. Since β has degree d, $h(T^2)$ must be the minimum polynomial of β, and so β is not separable. This contradicts Result 2.10 of Chapter 2. Thus β^2 is algebraic of degree d and therefore the unique element $\alpha \in CF(G(u)) \subseteq P_4$ for which $\alpha^2 + u\alpha + (1 + x\beta^2) = 0$ has degree d or $2d$. The partial quotients of the continued fraction of α belong to $G(u)$ and so have degree 1 or 2. This completes the proof.

□

6.5.2 An Application to Sequences

Let $S = \{s_i\}_{i \geq 1}$ be a sequence over the field $\mathbb{F}_q$. One measure of the predictability of a sequence which is of interest in stream cipher theory, a part of cryptography, is its linear complexity profile (see Chapter 2 Section 2.4). In this section, we discuss sequences which have prescribed linear complexity profiles, and mention how this relates to rational functions whose continued fractions have partial quotients of prescribed degrees.

Recall that the linear complexity profile of a sequence $S = \{s_i\}_{i \geq 1}$ over $\mathbb{F}_q$ may be described as follows (Definition 2.35). For $n \geq 1$ let $l_n(S)$ denote the length of the shortest linear recurrence satisfied by a sequence of the form $\{r_i\}_{i \geq 1}$ where $r_i = s_i$ $(1 \leq i \leq n)$. The linear complexity profile of S is the positive integer sequence $\{l_n(S)\}_{n \geq 1}$. The jumps profile of S (Definition 2.37) is the subsequence of non-zero terms in the (non-negative) sequence $l_1(S), l_2(S) - l_1(S), l_3(S) - l_2(S), \ldots$. The positive integers which appear in the jumps profile are called the **jumps** of S, and a linear complexity profile with jumps of size 1 is called perfect. Result 2.38 tells us that the jumps profile of a sequence $S = \{s_i\}_{i \geq 1}$ is $\{\deg a_j\}_{j \geq 1}$ where $s = \sum_{i \geq 1} s_i x^{-i} = [0; a_1, a_2, \ldots]$.

Each polynomial in Table 6.1 gives us a different family of binary sequences with particular linear complexity profiles which satisfy simple linear recurrences.

Example 6.20 (Binary sequences with perfect linear complexity profiles.) Consider the case $u = x + 1$. Let $S = \{s_i\}_{i \geq 1}$ and $s = \sum_{i \geq 1} s_i x^{-i}$. Then S has a perfect linear complexity profile if and only if all the partial quotients in the continued fraction expansion of s have degree 1, in other words, s lies in $CF(\{x, x+1\})$. Now $G(x+1) = \{0, 1, x, x+1\}$ and we have see from Table 6.1 that $CF(G(x+1)) = I_{x+1}$. Thus S has a perfect profile if and only if there exists an element $\beta \in L_2$ such that

$$s^2 + (x+1)s + 1 = x\beta^2.$$

Equating coefficients of x^i on each side of this equation we see that S has a perfect linear complexity profile if and only if

$$\begin{aligned} s_1 &= 1 \\ s_i + s_{2i} + s_{2i+1} &= 0 \quad \text{for } i \geq 1. \end{aligned}$$

This is a well-known result which we discussed in Chapter 3 Section 3.3.2.

Example 6.21 (Binary sequences with bounded jumps.) For $u = x^3 + 1$ we get that a binary sequence which satisfies

$$\begin{aligned} s_1 &= 0 \\ s_3 &= 1 \\ s_i + s_{2i} + s_{2i+3} &= 0 \quad \text{for } i \geq 1, \end{aligned}$$

has a linear complexity profile with jumps of sizes 2 and 3. The converse is not true in that there exist sequences whose linear complexity profiles have jumps of size 2 and 3 but which do not satisfy the above recurrence. However, it is easy to classify exactly which sequences do (namely those whose associated continued fractions have partial quotients which belong to the full solution group of $x^3 + 1$).

We do not get such neat linear recurrences for sequences over $\mathbb{F}_4$; however, we have the following "$\mathbb{F}_2$-linear" result.

Corollary 6.22 *Let $u_0, u_1, u_2 \in \mathbb{F}_4$ with $u_0 u_2 = u_1^2 \neq 0$. Then a sequence $\{s_i\}_{i \geq 1}$ over $\mathbb{F}_4$ which satisfies*

$$\begin{aligned} u_2 s_2 + u_1 s_1 + 1 &= 0, \\ u_2 s_{2i+2} + u_1 s_{2i+1} + u_0 s_{2i} + s_i^2 &= 0 \quad \textit{for } i \geq 1, \end{aligned}$$

has a linear complexity profile with jumps of sizes 1 *and* 2.

Proof: It is easily seen that if $\{s_i\}_{i \geq 1}$ satisfies the recurrence relations then the Laurent series $s = \sum_{i \geq 1} s_i x^{-i}$ will satisfy $s^2 + us + (1 + x\beta^2)$ for some $\beta \in L_4$. Here $u = u_0 + u_1 x + u_2 x^2$. (Compare the recurrence relations with those in the proof of Lemma 6.5.) The conditions on the coefficients of u ensure that $I_u = CF(G(u))$ (by Theorem 6.13 and Proposition 6.15) and so $f \in CF(G(u))$. Thus the partial quotients in the continued fraction of f have degree 1 or 2 and so by Result 2.38 we know that the sequence $\{s_i\}_{i \geq 1}$ must have a jumps profile which consists solely of ones and twos.

□

It is conceivable that this corollary could be used to prove results for rational functions over the field $\mathbb{F}_4$ whose continued fractions have partial quotients of small degree.

Chapter 7

Algorithms for Continued Fractions

7.1 Introduction

In this short chapter, we discuss some algorithmic questions relating to badly approximable rational functions. The main two problems we shall attempt to tackle are

- Given $g \in \mathbb{F}_q[x]$ compute $m(g)$, the orthogonal multiplicity of g, efficiently.
- Given a polynomial over a finite field of characteristic 2, determine whether it has odd orthogonal multiplicity efficiently.

We deem an algorithm to be **efficient** if the number of $\mathbb{F}_q$-field operations it involves is bounded by a polynomial in the algorithm's input size. Thus an algorithm which takes as input a polynomial of degree n over $\mathbb{F}_q$ is considered efficient if its running time is bounded by a polynomial in n and $\ln q := 1 + \lfloor \log_2 q \rfloor$ (see [2, page 41] for this notation). We shall use "big O" notation to present bounds on the number of field operations involved in an algorithm: we write $f(n) = O(g(n))$ if there exist constants $c > 0$ and N such that $f(n) \leq cg(n)$ for all $n \geq N$. The algorithms we consider will be deterministic. A full account of the relevant ideas from complexity theory can be found in [2, Chapter 3].

This chapter is organised in the following way. In Section 7.2.1 we observe that one may efficiently compute the orthogonal multiplicity of a binary polynomial, and in Section 7.2.2 we discuss the more difficult case for general finite fields. The main theorem in Chapter 4 is used in Section 7.3 to show that one may check whether a polynomial in characteristic 2 has odd orthogonal multiplicity in time which is polynomial in its degree.

7.2 Computing the Orthogonal Multiplicity

7.2.1 The Binary Field

We first of all show that the orthogonal multiplicity of a binary polynomial may be computed efficiently.

Proposition 7.1 *Let $g \in \mathbb{F}_2[x]$ with $\deg g = n \geq 1$. The orthogonal multiplicity of g can be calculated using $O(n^3)$ binary field operations.*

Proof: We shall describe an algorithm for computing the orthogonal multiplicity of g. The algorithm falls into two parts. We first of all use row-reduction on a specific matrix to determine whether g has positive orthogonal multiplicity. By Proposition 3.13, it only then remains to calculate the number of distinct non-linear irreducible factors of g, which we show may easily be done.

Let $R_g = \mathbb{F}_2[x]/g\mathbb{F}_2[x]$. Recall from the discussion following Result 3.15 in Chapter 3 that g has positive orthogonal multiplicity if and only if the element $1 \in R_g$ is not in the subspace of R_g generated by the set $\{x^{i-1} + x^{2i-1} + x^{2i} \mid 1 \leq i \leq n-1\}$. For $1 \leq i \leq n-1$, let m_i denote the $n \times 1$ column vector which expresses the element $x^{i-1} + x^{2i-1} + x^{2i}$ in terms of the basis $1, x, \ldots, x^{n-1}$ of R_g. Let m_n denote the column vector expressing 1 in terms of the basis elements $1, x, \ldots, x^{n-1}$, which is just the transpose of $(1, 0, \ldots, 0)$. Let M denote the $n \times n$ matrix whose ith column is m_i. The column m_i $(1 \leq i \leq n-1)$ of M is computed by dividing g into $x^{i-1} + x^{2i-1} + x^{2i}$ which may be done using $O(n^2)$ binary field operations. Thus matrix M may be constructed in time $O(n^3)$. We may put M into "row-reduced echelon form", M' say, in $O(n^3)$ binary field operations. It is a standard result in linear algebra ([45, Result 28.2]) that m_n may be written as an $\mathbb{F}_2$-linear combination of the vectors m_i $(1 \leq i \leq n-1)$ if and only if M' does not contain any row of the form $(0, 0, \ldots, 0, 1)$. Thus we may determine whether 1 lies in the subspace generated by the set $\{x^{i-1} + x^{2i-1} + x^{2i} \mid 1 \leq i \leq n-1\}$ using $O(n^3)$ binary field operations.

We describe how to compute the number of non-linear irreducible factors of g. We first remove all linear factors from g by division to obtain a polynomial h such that $g = x^{e_1}(x+1)^{e_2}h$ where $\gcd(h, x(x+1)) = 1$. Let $\deg h = d \leq n$. We now wish to calculate the total number of distinct irreducible factors of h, as this equals the number of distinct non-linear irreducible factors of g. Let $F : R_h \to R_h$ be given by $r \mapsto r^2$. Let I denote the identity map on R_h and consider the map $F - I : r \mapsto r^2 - r$. As observed in [23, page 135], the number of distinct irreducible factors of g is the dimension of the kernel of the map $F - I$. (This may easily be proved by analysing the linear map $F - I$ in a similar way to the map T in the proof of Proposition 3.13.) The matrix for the map $F - I$ with respect to the basis $1, x, \ldots, x^{d-1}$ of R_h may be constructed in time $O(d^3)$. The dimension of the kernel of this matrix may then be computed in time $O(d^3)$ using elementary row operations ([2, Theorem 7.4.3]).

□

Observe that for polynomials which are not divisible by x, Proposition 3.16 may be used to construct an algorithm for computing the orthogonal multiplicity which has the same asymptotic running time as that in Proposition 7.1, but is more practical. One simply computes the kernel of the map T on R_g using [2, Theorem 7.4.3] and checks whether it lies in the subspace of R_g generated by $x, x^2, \ldots, x^{n-1}$.

Example 7.2 Consider the polynomial $g = x^8 + x^5 + x^4 + x^3 + x + 1$ whose orthogonal multiplicity we calculated to be zero in Example 3.19. In this example we recompute its orthogonal multiplicity using the method suggested in the paragraph following

Proposition 7.1. The matrix of the map T on R_g in this case is

$$\begin{pmatrix} 0&0&0&0&1&1&0&0 \\ 1&1&0&0&0&1&0&0 \\ 0&1&1&0&1&1&1&0 \\ 0&1&0&1&1&1&1&0 \\ 0&0&1&0&1&0&1&1 \\ 0&0&1&0&0&1&1&1 \\ 0&0&0&1&1&0&1&1 \\ 0&0&0&1&0&0&0&0 \end{pmatrix}$$

Reducing this matrix using elementary row operations we get

$$\begin{pmatrix} 1&1&0&0&0&1&0&0 \\ 0&1&1&0&1&1&1&0 \\ 0&0&1&1&0&0&0&0 \\ 0&0&0&1&1&0&1&1 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{pmatrix}$$

To construct elements $(v_0, v_1, \dots, v_7)$ in the kernel of T, we choose v_6 and v_7 arbitrarily, and the remaining v_i are determined from the relations defined by the top 6 rows of the above row-reduced matrix. A basis for the kernel of the linear map T is found to be $(0,1,0,0,1,1,1,0)$ and $(1,0,0,0,1,1,0,1)$. Hence by Proposition 3.16 we see that the orthogonal multiplicity of g is zero.

7.2.2 General Finite Fields

Without the apparatus of linear algebra which is available to us for the binary field, it is not clear that one may efficiently compute the orthogonal multiplicity of a polynomial. Given a monic polynomial g of degree n over $\mathbb{F}_q$, the naive method would be to compute the continued fraction expansion of f/g for all f with $\deg f < n$. This would take $O(q^n n^3)$ field operations. One may certainly refine this naive method by restricting the polynomials f which one considers, but the algorithm remains exponential in n. It is conceivable that one may be able to improve on this by exploiting the algebraic-geometric method of Blackburn presented in Section 3.3.1 of Chapter 3; however, there are significant obstacles to this, as we explain in the next paragraph, and the problem of efficiently computing $m(g)$ for g over arbitrary finite fields remains open.

Using the notation introduced in Section 3.3.1 of Chapter 3, the orthogonal multiplicity of a polynomial g is the cardinality of the complement of the zero set of the associated multivariate polynomial $h \in \mathbb{F}_q[X_1, X_2, \dots, X_n]$, where $\deg g = n$. The polynomial h has total degree not greater than $\frac{1}{2}n(n+1)$. One possible method for computing $m(g)$ would be to calculate the number of points on the variety defined by h. (Computing the number of points on a variety is a major area of research, and their exist non-trivial algorithms for varieties with extra structure, such as abelian varieties, although the general algorithmic problem remains intractable ([43]).) However, since h is the product of $i \times i$ determinants for $1 \le i \le n$, it may have as many as $\prod_{1 \le i \le n} i!$ terms, and so it does not even seem practical to construct h_g for large n. Therefore methods based upon point counting on algebraic varieties do not appear much help in tackling this problem. In the next chapter we shall discuss some algorithms for other problems involving multivariate polynomials over finite fields.

7.3 Polynomials with Odd Orthogonal Multiplicity

The main theorem of Chapter 4 gives a quick method for checking whether a polynomial over a field of characteristic 2 has odd multiplicity. The algorithm is not efficient in the strict sense, but is nevertheless practical for polynomials of large degree over fields of modest size.

Proposition 7.3 *Let* $\operatorname{char} \mathbb{F}_q = 2$ *and* g *be a monic polynomial over* $\mathbb{F}_q$ *of degree* $n \geq 1$. *One may determine whether the orthogonal multiplicity of* g *is odd using* $O(qn)$ $\mathbb{F}_q$*-field operations.*

Proof: By Theorem 4.5 of Chapter 4, g has odd multiplicity if and only if g is folded, and this latter condition may easily be checked, as we now explain.

We first describe an auxiliary algorithm A which we shall need. The algorithm A takes as input a monic polynomial g of degree n and outputs either a monic polynomial h or NOT FOLDED according to the following rules.

1. If n is even with $g = h^2$ then output h. If n is even and g is not a square then output NOT FOLDED.
2. If n is odd and there is a unique monic polynomial h such that $g = ah^2$ for some monic polynomial a, then output h. If n is odd and there is more than one monic polynomial h with $g = ah^2$ for some linear polynomial a, or there are no such polynomials, then output NOT FOLDED.

We now describe algorithm A: If n is even then check whether g is a square. If it is, then compute its square root, and if not output NOT FOLDED. This may be done in time $O(n \ln^3 q)$ since we are working in characteristic 2 ([2, page 155]). If n is odd then for each monic linear polynomial a in $\mathbb{F}_q[x]$ divide g by a. This takes $O(qn)$ field operations. In each case, if the remainder is zero, check whether the quotient is a square. If there is exactly one monic polynomial a such that a divides g and the quotient is a square, then compute the square root of g/a. If there are no such polynomials or more than one then output NOT FOLDED. The running time of A is $O(qn)$.

If g is folded then it is easily proved that there will be a *unique* monic polynomial h such that either ah^2 or h^2 equals g, for some monic linear polynomial a. Thus algorithm A will output h in this case. Observe that h is folded. We may then apply algorithm A to the output h, and continue in this way until a polynomial of degree 1 is obtained. If g is not folded then after successive iterative applications of algorithm A, the output NOT FOLDED will be given. In either case, by iterative use of algorithm A, we shall determine whether g is folded using $O(\sum_{1 \leq i < \log_2 n} q\lfloor n/2^i \rfloor) = O(qn)$ field operations.

$\square$

Chapter 8

Absolutely Irreducible Bivariate Polynomials

8.1 Introduction

In this chapter we present some new algorithms for multivariate polynomials over finite fields. We do not attempt to tackle the difficult problem of efficiently computing the number of points on an arbitrary algebraic variety mentioned in Section 7.2.2 of Chapter 7, but content ourselves by presenting some new ideas for more modest problems. Although the algorithms we describe in this chapter do not contribute in any direct way to this difficult problem, it is conceivable that the simple new ideas this chapter contains could lead to improved algorithms for important problems such as computing the zeta function of a variety ([43]). We begin by discussing some more direct applications of the work in this chapter.

The set of zeros of an absolutely irreducible bivariate polynomial form an irreducible algebraic curve, and a version of Weil's theorem gives bounds on the number of points of such curves over finite fields ([41, page 197]). These bounds have been applied in numerous areas including number theory, coding theory ([24]) and combinatorics ([41]). It is therefore of interest to create efficient algorithms for testing absolute irreducibility, to produce easily-checked criteria for absolute irreducibility, and to construct families of absolutely irreducible polynomials. In this chapter, following ideas of Gao ([12]), we present a simple algorithm which tests for the absolute irreducibility of a bivariate polynomial defined over an arbitrary field. The algorithm will not identify all absolutely irreducible polynomials, but it is widely applicable and very efficient. We also present some absolute irreducibility criteria for bivariate polynomials which complement those of Gao, and construct families of polynomials which satisfy these criteria.

The idea behind the results is simple: with each k-variate polynomial we associate a convex polytope in k-dimensional Euclidean space. If the polynomial reduces over any extension of the original field, then the associated polytope will decompose in a certain way into several other convex polytopes. Thus if the polytope does not "decompose", the polynomial must be absolutely irreducible. For a bivariate polynomial of total degree n, our algorithm determines whether the associated polytope is "indecomposable" in $O(n^3)$ steps. Our absolute irreducibility criteria for bivariate polynomials depend upon criteria for the "indecomposability" of a convex polygon.

The author is not aware of any other algorithms which check for absolute irreducibility, although efficient algorithms exist for testing the irreducibility of a bivariate polynomial over a finite field or an algebraic number field ([13]), and factoring such polynomials ([14, 22, 42]). There are other well-known simple criteria for the absolute irreducibility of bivariate polynomials (Stepanov-Schmidt and Eisenstein-Dumas (see [12])), but they are just special cases of the criteria presented in Gao ([12]). Some of the ideas presented in this chapter were prefigured in Lipkovski ([25]); however, Lipkovski is concerned with analytic reducibility and Newton polyhedra and does not obtain any new results on bivariate polynomials.

The remainder of this chapter is organised in the following way: in Section 8.2 the fundamental connection between multivariate polynomials and convex polytopes is explained, and we gather some preliminary results; Section 8.3 contains our absolute irreducibility testing algorithm; some simple absolute irreducibility criteria appear in Section 8.4; we conclude with a informal discussion of other results which it may be possible to obtain following the ideas in this chapter.

8.2 Preliminaries

8.2.1 The Newton Polytope of a Multivariate Polynomial

Before we can describe the connection between polynomials and polytopes, it is necessary to recall some terminology and results from the theory of convex polytopes ([15]). A **convex set** in Euclidean k-space is a set such that the points on the line segment joining any two points of the set lie in the set; the **convex hull** of a set of points is the smallest convex set which contains them; and the convex hull of a finite set of points is called a **convex polytope**. A point of a polytope is called a **vertex** (or **extreme point** ([15, page 17])) if it does not belong to the relative interior of any line segment contained in the polytope. A polytope is the convex hull of its vertices ([15, page 18]). A hyperspace **cuts** a polytope if both of the open half spaces determined by it contain points of the polytope. A hyperspace which does not cut a polytope, but has a non-empty intersection with it is called a **supporting hyperspace**. The intersection of a supporting hyperspace and a polytope is a **(proper) face**, and the union of all (proper) faces is the **boundary**. One may equivalently define a vertex to be a 0-dimensional face, and 1-dimensional faces are known as **edges**.

For two subsets A and B in Euclidean k-space, define their **Minkowski sum** to be $A + B = \{a + b \,|\, a \in A, b \in B\}$ ([15, page 316]). We call A and B the **summands** of $A + B$. It is easy to show that the Minkowski sum of two convex polytopes is a convex polytope ([15, page 32]).

Let $f \in K[X_1, X_2, \dots, X_k]$, where K is an arbitrary algebraically closed field. The polynomial f is called **absolutely irreducible** if it has no non-trivial factors over K. For a polynomial defined over a finite field, the case we are most interested in, we say that it is absolutely irreducible if it is absolutely irreducible over an algebraic closure of the finite field. Denote the coefficient of the multinomial $X_i^{i_1} X_2^{i_2} \dots X_k^{i_k}$ in f by $a_{i_1 i_2 \dots i_k}$, and associate with f the set of points in Euclidean k-space

$$Supp(f) = \{(i_1, i_2, \dots, i_k) \,|\, a_{i_1 i_2 \dots i_k} \neq 0\}.$$

The **total degree** of f, where $f \neq 0$, is the maximum value of $\sum_{1 \leq j \leq k} i_j$ over all $(i_1, \dots, i_k) \in Supp(f)$. The convex hull of the set $Supp(f)$, denoted P_f, is known as the **Newton polytope** of f.

The following lemma appears in Ostrowski ([34]); since this lemma is central to the chapter, we present a proof which follows the approach taken by Gao.

Lemma 8.1 *Let $f, g, h \in K[X_1, X_2, \ldots, X_k]$ with $f = gh$. Then $P_f = P_g + P_h$.*

Proof: [Gao] The inclusion $P_f \subseteq P_g + P_h$ is straight-forward. Observe that $P_g + P_h$ is a convex polytope; to prove the reverse inclusion it is therefore enough to show that every vertex of $P_g + P_h$ lies in P_f, as a polytope is the convex hull of its vertices. Let w be a vertex of $P_g + P_h$. So there exist points u and v of P_g and P_h respectively, with $w = u + v$. We wish to show that these points are unique, and are in fact vertices. The uniqueness follows from the observation that if $u + v = w = u' + v'$, with $u' \in P_g$ and $v' \in P_h$, then $w = \frac{1}{2}(u' + v) + \frac{1}{2}(u + v')$. Thus w is the midpoint of the line joining the points $u' + v$ and $u + v'$. But both these points lie in $P_g + P_h$ and so, since w is a vertex of $P_g + P_h$, all three points must coincide. It follows easily that $u = u'$ and $v = v'$. This proves uniqueness. Suppose now that u is not a vertex. Then u lies on a line segment which is strictly contained in P_g. One may show that this implies that w lies on a line segment which is strictly contained in $P_g + P_h$, which contradicts the fact that w is a vertex. Thus u is a vertex, as is v. Let a_u and a_v be the non-zero terms in g and h respectively, which correspond to the vertices u and v (such terms exist as both u and v must have integer coordinates). Then the term $a_u a_v$ is non-zero and corresponds to the point $u + v$ in $P_{gh} = P_f$. Hence $w = u + v$ lies in P_f, as required.

□

An **integral polytope** is a polytope whose vertices have integer coordinates, and we say that a polytope is **integrally [in]decomposable**, or more simply **[in]decomposable**, if it can[not] be written as the Minkowski sum of two integral polytopes, each of which has more than one point. Observe that the Newton polytope of a multinomial is a single integral point, and more generally, it is easy to see that Newton polytopes are integral. If a polynomial factors into two polynomials each of which has at least two terms, then by Lemma 8.1 its Newton polytope must be decomposable. Thus:

Corollary 8.2 *Let $f \in K[X_1, X_2, \ldots, X_k]$ with f containing no factor of the form X_l^i for $1 \leq l \leq k$. If the Newton polytope of f is integrally indecomposable, then f is absolutely irreducible.*

8.2.2 Convex Polygons

For the remainder of this section and the following section we will be concerned primarily with bivariate polynomials and polytopes in Euclidean 2-space. Such a polytope is called a **polygon**. (We refrain from using the term Newton polygon for a 2-dimensional Newton polytope as historically this term is used to referred to the boundary of the "Newton polyhedron".) Observe that hyperspaces in real Euclidean 2-spaces are just lines, and each edge has a unique supporting line.

The following lemma is an elaboration of the case $k = 2$ of a more general result which appears in Gao ([12, Lemma 3.2]); we sketch a proof, and refer the reader to [12] for more details.

Lemma 8.3 *Let P, Q and R be convex polygons in Euclidean 2-space with $P = Q + R$. Any edge of P decomposes uniquely as the sum of a face of Q and a face of R, at least one of which is an edge. Conversely, any edge of Q or R is a summand of exactly one edge of P.*

Proof: Let $\mathcal{F}$ be a edge of P, with l the supporting line and the suppose that the polytope lies in the lower half-plane defined by l. Let m and n be translates of the line l such that the line m intersects Q with Q lying in the lower half-plane defined by m, and n intersects R with R lying in the lower half-plane defined by n. Define the faces $\mathcal{G} = m \cap Q$ and $\mathcal{H} = n \cap R$ of Q and R respectively. One may show that $\mathcal{F} = \mathcal{G} + \mathcal{H}$. Uniqueness is proved by showing that any two faces that sum to $\mathcal{F}$ must have supporting lines which are parallel to l, with the polygons lying in the lower half-planes defined by these lines, and must therefore be $\mathcal{G}$ and $\mathcal{H}$. The observation that one of these faces must be an edge follows from the fact that the sum of two vertices is a single point. The converse is proved in a similar way: If $\mathcal{G}$ is any edge of Q, then one may consider the line m which supports it, and the appropriate translates of this line which support faces of P and R.

□

We now describe the input to our polygon decomposition algorithm; we partly follow the notation of Lipkovski ([19]). Given a convex polygon in 2-dimensional Euclidean space, one may form a finite sequence of vectors associated with it as follows: Let $v_0, v_1, \ldots, v_{m-1}$ be the vertices of the polygon, with v_0 chosen to be the lowest point among the left-most points on the boundary, and the remaining points taken in clockwise order from v_0 around the boundary. Let $v_i - v_{i-1} = (X_i, Y_i)$ for $1 \leq i \leq m$, where the indices are taken mod$m$. Let $n_i = \gcd(X_i, Y_i)$ and define $e_i = (x_i, y_i) = (X_i/n_i, Y_i/n_i)$. We call e_i a **primitive edge vector**, $n_i e_i$ an **edge vector** and the line segment joining v_{i-1} and v_i the i^{th} **edge** of P, denoted $\mathcal{E}_i$. Each edge $\mathcal{E}_i$ contains $n_i + 1$ integral points. The sequence of vectors $\{n_i e_i\}_{1 \leq i \leq m}$, which we call the **edge sequence**, uniquely identifies the polygon up to translation, and will be the input to our polygon decomposition algorithm. It will be convenient to identify sequences with those obtained by extending the sequence by inserting an arbitrary number of zero vectors. We may thus assume that the edge sequence of a summand of a polygon P is the same length as that of P. As the boundary of the polygon is a closed path, we have that $\sum_{1 \leq i \leq m} n_i e_i = (0, 0)$ and so $\sum_{1 \leq i \leq m} n_i x_i = \sum_{1 \leq i \leq m} n_i y_i = 0$. A suitable permutation of any sequence which satisfies the conditions in the preceding sentence will be the edge sequence of some polygon; we call such a sequence a **polygonal sequence**.

Lemma 8.4 *Let P be a polygon with edge sequence $\{n_i e_i\}_{1 \leq i \leq m}$. Let Q be a summand of P. Then the edge sequence of Q is of the form $\{k_i e_i\}_{1 \leq i \leq m}$ with $0 \leq k_i \leq n_i$. Furthermore, $\sum_{1 \leq i \leq m} k_i x_i = \sum_{1 \leq i \leq m} k_i y_i = 0$, where $e_i = (x_i, y_i)$ for $1 \leq i \leq m$. Conversely, any sequence of this form determines a summand of P.*

This Lemma is closely related to Lemma 2.11 in Lipkovski ([19]), although the latter contains a small error.

Proof: Let $\{e'_i\}_{1 \leq i \leq m}$ be the edge sequence of Q. By the final statement in Lemma 8.3, each edge of Q occurs as the summand of some edge of P, and it is easily seen that its corresponding edge vector must be of the form ke, with $0 \leq k \leq n$, where e is an edge vector of P whose related edge has $n + 1$ integral points. By considering supporting lines, one may show that if $\mathcal{E}'_j$ and $\mathcal{E}'_k$ are edges of Q with $j < k$ then they occur as summands of the edges $\mathcal{E}_p$ and $\mathcal{E}_q$ of P, with $p < q$. This proves the first assertion. The second assertion is simply the observation that the boundary of Q is a closed path. Conversely, any sequence of this form will determine a closed path. By considering supporting lines one may show it actually defines the boundary of a convex polygon. It will be a summand of P, with the other summand a polygon whose edge sequence is $\{(n_i - k_i)e_i\}_{1 \leq i \leq m}$.

□

Given as input a sequence of edge vectors $\{n_i e_i\}_{1 \leq i \leq m}$ of a polygon, our polygon decomposition algorithm will check for the existence of a sequence of the form $\{k_i e_i\}_{1 \leq i \leq m}$, where $0 \leq k_i \leq n_i$ for $1 \leq i \leq m$ and $k_m \neq n_m$, for which $\sum_{1 \leq i \leq m} k_i e_i = (0, 0)$. The "subset-sum" problem ([2, Page 63]), which is NP-complete, is polynomial-time reducible to this computational problem, and so one cannot reasonably expect to find a genuinely efficient algorithm for this. However, we are interested in finding an efficient algorithm for testing a bivariate polynomial for absolute irreducibility given as input its "dense representation", and we shall see that enough "information" about the polynomial is discarded when we consider only its Newton polytope, that the algorithm we construct for absolute irreducibility testing is efficient in terms of its input size. (In the **dense representation** of a multivariate polynomial f of total degree n, one explicitly gives the coefficient in f of each monomial $X_1^{i_i} \dots X_k^{i_k}$ with $\sum_{1 \leq j \leq k} i_j \leq n$. So for example, if f is defined over $\mathbb{F}_q$ then this will require $O(n^k \ln q)$ bits, regardless of how many non-zero terms there are in f.)

8.3 Algorithms

Our absolute irreducibility algorithm can be divided into two parts: one first computes the edge sequence of the Newton polytope corresponding to the bivariate polynomial which is inputed; this polygon is then tested for indecomposability. We begin by sketching a simple algorithm which performs the first part. We make two inessential assumptions which simplify the algorithm: we assume the input polynomial has no "trivial" factors, and that all its non-zero terms have the coefficient 1. The defining field of the polynomial plays no part in what follows, and the latter assumption obviates the need to consider how one encodes it.

Algorithm 8.5 (Construct Polygon)
Input: The dense representation of a bivariate polynomial $f(X_1, X_2) \in K[X_1, X_2]$. (We assume that X_1 and X_2 do not divide f and the non-zero terms in f have coefficient 1.)
Output: The edge sequence of P_f.

Step 1: Consider the set of points (i, j) for $0 \leq i \leq n$, where j is the highest or lowest power of X_2 that occurs in the coefficient of X_1^i in f. (This gives at most $2n$ points and it is easily seen that the convex hull of these points is the Newton polytope of f.) Compute the gradients of the line segments between pairs of these points, and trace out the boundary of the convex hull of these points by starting with the lowest point on the X_2-axis (such a point exists and must be a vertex) and picking out the line segment from that point which has the highest gradient. Repeat this with the point at the other end of that line segment, until the starting point is reached once more. This sequence of points may be used to determine the edge sequence.

Proof of timing: Computing the gradients involves $O(n^2)$ computations each of which can be done with division of numbers bounded by n. Tracing out the polygon simply involves ordering $O(n)$ lists of numbers, each of length $O(n)$. Thus the total time is certainly $O((n \ln n)^2)$.

□

We now describe the second algorithm, which checks whether a given polygonal sequence is that of an indecomposable polygon.

Algorithm 8.6 (Polygon Decomposition)
Input: The edge sequence $\{n_i e_i\}_{1\le i\le m} = \{(n_i x_i, n_i y_i)\}_{1\le i\le m}$ of a convex polygon P.
Output: YES if P is decomposable, and NO otherwise

Step 1: Define $X = \sum_{i:x_i\ge 0} n_i x_i$, $Y = \sum_{i:y_i\ge 0} n_i y_i$ and $\bar{Y} = \sum_{y_i:x_i\le 0, y_i\ge 0} n_i y_i$. Initialise a $(2X+1)\times(2Y+1)$ array A_0 in the following way. Index the cells as $[a,b]$ where $-X \le a \le X$ and $\bar{Y} - Y \le b \le \bar{Y} + Y$. Write NO in all cells, except the cell $[0,\bar{Y}]$ which is set to FIRST.

Step 2: For i from 1 up to $m-1$ define the array A_i as follows:

1. If the cell $A_{i-1}[a,b]$ is YES or FIRST, then set cells $A_i[a+kx_i, b+ky_i]$ to YES, where $0\le k\le n_i$ and $-X\le a+kx_i\le X$, $\bar{Y}-Y\le b+ky_i\le \bar{Y}+Y$.

2. Set $A_i[a,b] = A_{i-1}[a,b]$ for all remaining undefined cells.

Step 3: Define the array A as follows:

1. If the cell $A_{m-1}[a,b]$ is YES or FIRST, then set cells $A[a+kx_m, b+ky_m]$ to YES, where $0\le k< n_m$ and $-X\le a+kx_m\le X$, $\bar{Y}-Y\le b+ky_m\le \bar{Y}+Y$.

2. Set $A[a,b] = A_{m-1}[a,b]$ for all remaining undefined cells.

Step 3: Return YES if $A[0,\bar{Y}] =$ YES and NO otherwise.

Proof of correctness and timing: Observe first of all that if we take any sequence of the form $\{(k_j x_j, k_j y_j)\}_{1\le j\le i}$ with $0\le k_j\le n_j$, then

$$(0,\bar{Y}) + \sum_{1\le j\le i} (k_j x_j, k_j y_j) = (a,b)$$

where $-X\le a\le X$ and $\bar{Y}-Y\le b\le \bar{Y}+Y$. By construction the array A_i $(1\le i\le m-1)$ stores YES in all cells $A_i[a,b]$ such that there exists a sequence of the form $\{(k_j x_j, k_j y_j)\}_{1\le j\le i}$ where $0\le k_j\le n_j$ with $(0,\bar{Y}) + \sum_{1\le j\le i}(k_j x_j, k_j y_j) = (a,b)$. Similarly, the array A stores YES in all cells $A[a,b]$ such that the following is true: there exists a sequence of the form $\{(k_j x_j, k_j y_j)\}_{1\le j\le m}$ where $0\le k_j\le n_j$ for $1\le j\le m-1$ and $0\le k_m< n_m$, such that $(0,\bar{Y})+\sum_{1\le j\le m}(k_j x_j, k_j y_j) = (a,b)$. If the polygon is decomposable, then by Lemma 8.4 there exists a sequence $\{(k_j x_j, k_j y_j)\}_{1\le j\le m}$ where $(0,\bar{Y}) + \sum_{1\le j\le m}(k_j x_j, k_j y_j) = (0,\bar{Y})$ with $0\le k_j\le n_j$ for $1\le j\le m-1$ and $0\le k_m< n_m$. Thus in array A the cell $[0,\bar{Y}]$ will hold YES. Conversely, if the cell $A[0,\bar{Y}]$ holds YES, then we know that a sequence of the form in the preceding sentence exists, and so by Lemma 8.4 the polygon is decomposable.

Steps 2 and 3 take $O(\sum_{1\le i\le m} n_i XY)$ steps. (We need only hold two full arrays at any one time and so the space-complexity is just $O(XY)$.)

□

Combining these two algorithms gives our absolute irreducibility algorithm for bivariate polynomials.

Algorithm 8.7 (Absolute Irreducibility)
Input: The dense representation of a non-zero bivariate polynomial of total degree n.

Output: If the output is IRREDUCIBLE then the polynomial is absolutely irreducible. Otherwise the output will be FAILURE.

Step 1: Remove all factors of the form $X_1^i X_2^j$ and replace each non-zero coefficient in the new polynomial by 1. Input this polynomial to Algorithm 8.5. Apply Algorithm 8.6 to the output of Algorithm 8.5. Output IRREDUCIBLE if the output to Algorithm 8.6 is NO, and FAILURE otherwise.

Proof of correctness and timing: The correctness follows from Corollary 8.2. The running time is dominated by the time taken $(O(\sum_{1 \leq i \leq m} n_i XY))$ to perform Algorithm 2. Certainly $XY \leq n^2$ and $\sum_{1 \leq i \leq m} n_i \leq 3n$ and so the algorithm takes $O(n^3)$ steps.

□

Example 8.8 We finish this section with an example which illustrates the absolute irreducibility testing algorithm which we have presented. Consider the polynomial

$$f = X_2^6 + X_1 X_2^8 + X_1^2 X_2^3 + X_1^4 + X_1^5 X_2^9 + X_1^7 (X_2^2 + X_2^8) + X_1^9 X_2^7,$$

which lies over the finite field $\mathbb{F}_q$. The Newton polytope of f has edge sequence $(1,2),(4,1),2(2,-1),(-2,-5),(-3,-2),2(-2,3)$. Thus $X = Y = 9$, $\bar{Y} = 6$ and $m = 6$. We follow Algorithm 8.6 to test if P_f is integrally indecomposable; however, we make one simplification. It suffices to work with the smaller $(X+1) \times (Y+1)$ arrays $B_i\,(1 \leq i \leq m-1)$ and B defined as follows: initialise B_0 in exactly the same way as A_0, only B_0 is indexed by $[a,b]$ where $0 \leq a \leq X$ and $0 \leq b \leq Y$. Construct B_i from B_{i-1} and B from B_{m-1} following a similar rule to that given in Algorithm 8.6, adjusting the bounds appropriately (for example, require that $0 \leq a + kx_i \leq X$ rather than $-X \leq a + kx_i \leq X$). To prove that this modified algorithm works is slightly more involved, as one must show that no important information is compromised by working with a smaller array.

In the case of f, B_0 is a 10×10 array with NO in all cells, except the cell $[0,6]$ which is set to FIRST. Following our modified algorithm we find that B_5 is the following array (we replace NO by 0, YES by 1 and FIRST by F).

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
F & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0
\end{bmatrix}$$

Writing 1 in all cells which can be reached by adding the vector $(-2,3)$ to cells containing 1 in B_5, and copying remaining values across, we find that B is the array

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ F & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Cell $[0,6]$ in B holds FIRST rather than YES, and so P_f must be integrally indecomposable. Hence f is absolutely irreducible. Now the total degree of f is $d = 16$. From [41, page 197] we know that the number of $\mathbb{F}_q$-rational points, denoted $\#(V_q(f))$, on the curve defined by f satisfies

$$q + 1 - (d-1)(d-2)\sqrt{q} \le \#(V_q(f)) \le q + 1 + (d-1)(d-2)\sqrt{q}.$$

For q sufficiently large compared to d this gives non-trivial information.

8.4 Absolute Irreducibility Criteria

In [12] Gao presents absolute irreducibility criteria for k-variate polynomials ($k \ge 2$) based upon the irreducibility of their Newton polytopes. Lipkovski takes a similar approach, but instead considers polyhedra associated with multivariate formal power series. He obtains indecomposability criteria by considering 2-dimensional faces of the polyhedra. Lipkovski presents simple conditions ([25, Lemma 2.12]) which ensure that these polygons are indecomposable and uses these results to obtain analytic irreducibility criteria for k-variate formal power series ($k \ge 3$); however, more directly we get the following absolute irreducibility criterion for bivariate polynomials:

Proposition 8.9 *Let $f \in K[X_1, X_2]$ be a bivariate polynomial not divisible by X_1 or X_2 whose Newton polytope is a pentagon with 5 integral points on its boundary, including the vertices. Furthermore, suppose that the polytope does not have any parallel edges. Then f is absolutely irreducible*

Proof: The sequence of primitive edge vectors of the Newton polytope of f has five non-zero terms. Thus if P_f is decomposable, since each of these primitive edge vectors is indecomposable, there must be a subsequence of them which sums to zero. It is easily seen that this implies that two of the primitive edge vectors must sum to zero and so the Newton polytope has parallel edges.

□

Example 8.10 Any bivariate polynomial whose Newton polytope has vertices

$$(0,m), (m, m+n), (m+n+1, n), (n+2, 0), (1,1)$$

where $\gcd(m,n) = \gcd(m, n+1) = \gcd(m-1, n) = 1$ is absolutely irreducible. This example is of interest as all (2-dimensional) examples presented in Gao ([12]) have one indecomposable edge whose supporting angles sum to less than 2π; such polygons are indecomposable for a simple reason. If $n > m-1 \geq 1$ then all the interior angles in our Newton polytope are obtuse. For example, taking $m > 3$ an odd prime and n an odd number greater than $m-1$ with $n \not\equiv 0, 1 \bmod m$, gives us a new family of absolutely irreducible bivariate polynomials.

One may also construct simple absolute irreducibility criteria which depend upon conditions related to the lengths of the horizontal projections of the sides.

Proposition 8.11 *Let P be the Newton polytope of $f \in K[X_1, X_2]$, where f is not divisible by X_1 or X_2, with edge sequence $\{(x_i, y_i)\}_{1 \leq i \leq m}$. Suppose that $x_i \equiv 1 \bmod m$ for $1 \leq i \leq m$. Then f is absolutely irreducible.*

Proof: If J is a non-empty proper subset of $\{1, 2, \ldots, m\}$ then $\sum_{j \in J} x_j \equiv |J| \not\equiv 0 \bmod m$ and so $\sum_{j \in J} x_j \neq 0$.

□

Example 8.12 We give an example of a polygon which fulfils the criteria of the preceding proposition: Suppose that 4 divides m and let p be prime such that p does not divide $im + 1$ for $1 \leq i \leq m/4$. Let ϕ and θ denote reflections in the lines $x = (m/4) + (m^2(m+4)/32)$ and $y = pm/4$ respectively. Let l be the closed set from the vertex $(0, mp/4)$ along the sequence of vectors $\{(im+1, p)\}_{1 \leq i \leq m/4}$. If the Newton polytope of f has boundary the union of l, $\phi(l), \theta(l)$ and $\phi \circ \theta(l)$ then f is absolutely irreducible.

8.5 Comments

To construct a similar algorithm for k-variate polynomials where $k > 2$ one would need to construct an indecomposability testing algorithm for higher dimensional integral polytopes. This appears to be considerably more difficult, as the problem acquires a graph-theoretic flavour in higher dimensions. There are, however, some interesting combinatorial problems which remain in two dimensions. In analysing the running time of the algorithm, we gave the worst case running time, which corresponds to polygons with as many edges as possible. An answer to the following problem would allow one to estimate the average running time of the algorithm: how many integral point on average lie on the boundary of the Newton polytope of a bivariate polynomial of total degree not greater than n? The answer, of course, depends upon the cardinality of the finite field in question. Perhaps a more natural related question to ask is: how many sides does a "typical" polygon have? There are many ways in which one may formulate this problem. For example, consider the set $S(n)$ of integral points in Euclidean 2-space given by $S(n) = \{(a, b) \mid 0 \leq a, b \leq n\}$. Let $0 < m < 1$. For any $A \subseteq S(n)$ let $s(A)$ be the number of sides of the convex hull of A. If each point $(a, b) \in S(n)$ belongs to A with probability m what is the expected value for $s(A)$?

A different direction for further work is to try and use the ideas in this chapter to improve current factoring algorithms for bivariate polynomials over finite fields. For example, the author has been able to use such ideas to make heuristic improvements to a bivariate factoring algorithm due to Wan ([42]) which uses "Hensel lifting" and univariate factorisation. More generally, it may be possible to incorporate these simple geometrical ideas into other algorithms for multivariate polynomials and algebraic varieties over finite fields.

Bibliography

[1] J.V. Armitage, The Thue-Siegel-Roth theorem in characteristic p, J. Algebra **9**, (1968), 183-189.

[2] E. Bach and J. Shallit, Algorithmic Number Theory Vol.1: Efficient Algorithms, MIT Press, Cambridge Massachusetts, 1997.

[3] G. Bachman, Introduction to p-Adic Numbers and Valuation Theory, Academic Press, New York, 1964.

[4] L.E. Baum and M.M. Sweet, Continued fractions of algebraic power series in characteristic 2, *Ann. of Math.* **103**, (1976), 593-610.

[5] L.E. Baum and M.M. Sweet, Badly approximable power series in characteristic 2, *Ann. of Math.* **105**, (1977), 573-580.

[6] S.R. Blackburn, Orthogonal sequences of polynomials over arbitrary fields, *J. Number Theory* **68**, (1998), 99-111.

[7] S.R. Blackburn, Linear cellular automata as stream cipher components, preprint, University of London, (1997).

[8] M.W. Buck and D.P. Robbins, The continued fraction expansion of an algebraic power series satisfying a quartic equation, J. Number Theory **50**, (1995), 335-344.

[9] K. Cattell and J.C. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, *IEEE Trans. Comp. Aided Design of Integrated Systems* **15** No.3, (1996), 325-335.

[10] T.W. Cusick, Zaremba's conjecture and sums of the divisor function, *Math. Comp* **61**, (1993), 171-176.

[11] H. Davenport, The Higher Arithmetic, 5th edn, Cambridge University Press, 1982.

[12] S. Gao, Absolutely irreducibility of polynomials via Newton polytopes, pre-print, (1998).

[13] J. von zur Gathen, Irreducibility of multivariate polynomials, *J. Comp. and Systems Science* **31**, (1985), 225-264.

[14] J. von zur Gathen and E. Kaltofen, Factorisation of multivariate polynomials over finite fields, *Math. Comp.* **45** No. 171, (1985), 251-261.

[15] B. Grunbaum, Convex Polytopes, Pure and Applied Mathematics, John Wiley and Son, 1967.

[16] A.E.D. Houston, On binary sequences with specific linear complexity and correlation properties, Ph.D. Thesis, London University, 1995.

[17] A.Y. Khinchin, Continued Fractions, University of Chicago Press, Chicago and London, 1964.

[18] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, 2nd edn, Springer-Verlag, New York, 1984.

[19] A.G.B. Lauder, Polynomials with odd orthogonal multiplicity, *Finite Fields and Their Applications* **4** No.4, (1998), 453-464.

[20] A.G.B. Lauder, Continued fractions of Laurent series with partial quotients from a given set, to appear in *Acta Arithmetica.*

[21] A. Lasjaunias and B. de Mathan, Thue's theorem in positive characteristic, J. Reine Angew. Math. **473**, (1996), 195-206.

[22] A.K. Lenstra, Factoring multivariate polynomials over finite fields, *J. Comp. and Systems Science* **30**, (1985), 235-248.

[23] R. Lidl and H. Niederreiter, "Finite Fields", 2nd edn, Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

[24] J.H. van Lint and G. van der Greer, Introduction to Coding Theory and Algebraic Geometry, DMV Seminar, Band 12, Birkhauser Verlag, 1988.

[25] A. Lipkovski, Newton polyhedra and irreducibility, *Math. Z.* **199**, (1988), 119-127.

[26] E. Lucas, Sur les congruences des nombres Euleriennes, et des coefficients différentials des functions trigonométriques, suivant un-module premier, *Bull. Soc. Math. France* **6**, (1878), 49-54.

[27] K. Mahler, On a theorem of Liouville in fields of positive characteristic, *Can. J. Math* **1**, (1949), 397-400.

[28] J.P. Mesirov and M.M. Sweet, Continued fraction expansion of rational expressions with irreducible denominators in characteristic 2, *J. Number Theory* **27**, (1987), 144-148.

[29] W.H. Mills and D.P. Robbins, Continued fractions for certain algebraic power series, J. Number Theory **23**, (1986), 388-404.

[30] H. Niederreiter, Rational functions with partial quotients of small degree in their continued fraction expansion, *Monatsh. Math.* **103**, (1987), 269-288.

[31] H. Niederreiter, Sequences with almost perfect linear complexity profiles, in "Advances in Cryptology: Proc. Eurocrypt 87", D. Chaum and W.L. Price (Eds), Springer, Berlin, 37-51, 1988.

[32] H. Niederreiter, Continued fraction expansions of rational functions, in "Finite Fields, Coding Theory, and Advances in Comm. and Computing", G.L. Mullen and P.J.-S. Shuie (Eds), Lect. Notes in Pure and Appl. Math., Vol. 141. Marcel Dekker, New York, 433-434, 1993.

[33] A.M. Odlyzko, Asymptotic enumeration methods, in "Handbook of Combinatorics, Vol. 2", R.L. Graham, M. Groetschel, L. Lovasz (Eds), Elsevier Science, New York, 1063-1229, 1995.

[34] A.M. Ostrowski, On the multiplication and factorisation of polynomials 1. Lexicographic ordering and extreme aggregates of terms, *Aequationes Math.* **13**, (1975), 201-228.

[35] A.J. van der Poorten and J. Shallit, Folded continued fractions, *J. Number Theory* **40**, (1992), 237-250.

[36] A.J. van der Poorten and J. Shallit, A specialised continued fraction, *Can. J. Math.* **45** No.5, (1993), 1067-1079.

[37] A.M. Rockett and P. Szüsz, Continued Fractions, World Scientific Publishing, Singapore, 1992.

[38] K.F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2**, (1955), 1-20.

[39] J.O. Shallit, Simple continued fractions for some irrational numbers II, *J. Number Theory* **14**, (1982), 228-231.

[40] G. Szegő, "Orthogonal Polynomials", American Math. Soc., New York, 1959.

[41] T. Szönyi, Some applications of algebraic curves to finite geometry and combinatorics, in "Surveys in Combinatorics, 1997", R.A. Bailey (Ed), LMS Lecture Notes Series 241, Cambridge University Press, 197-236, 1997.

[42] D. Wan, Factoring multivariate polynomials over large finite fields, *Math. Comp.* **54**, No. 190, (1990), 755-770.

[43] D. Wan, Computing zeta functions over a finite field, in "Contemporary Mathematics", vol. 225, American Mathematical Society, 131-142, 1999.

[44] M. Wang, Linear complexity profiles and continued fractions, in "Advances in Cryptology - Eurocrypt '89", J-J. Quisquater and J. Vandewalle (Eds), Lecture Notes In Computer Science, vol. 434, Springer, Berlin, 1990.

[45] T.A. Whitelaw, An Introduction to Linear Algebra, 2nd edn, Blackie and Son Ltd, Glasgow, 1991.

[46] H.S. Wilf, Generatingfunctionology, 2nd edn, Academic Press, San Diego, 1994.

[47] S.K. Zaremba, La méthode des "bons treillis" pour le calcul des intégrales multiples, in "Applications of Number Theory to Numerical Analysis", S.K. Zaremba (Ed), Academic Press, New York, 39-119, 1972.

[48] S.K. Zaremba, Good lattice points modulo composite numbers, *Monatsh. Math.* **78**, (1974), 446-460.