AN ABSTRACT OF THE THESIS OF

Katthaleeya Daowsud for the degree of Doctor of Philosophy in Mathematics presented on April 25, 2013.

Title: Continued Fractions and the Divisor at Infinity on a Hyperelliptic Curve: Examples and Order Bounds

Abstract approved: _____

Thomas A. Schmidt

We use the theory of continued fractions over function fields in the setting of hyperelliptic curves of equation $y^2 = f(x)$, with $\deg(f) = 2g+2$. By introducing a new sequence of polynomials defined in terms of the partial quotients of the continued fraction expansion of y, we are able to bound the sum of the degrees of consecutive partial quotients. This allows us both (1) to improve the known naive upper bound for the order N of the divisor at infinity on a hyperelliptic curve; and, (2) to apply a naive method to search for hyperelliptic curves of given genus g and order N. In particular, we present new families defined over $\mathbb{Q}$ with $N = 11$ and $2 \leq g \leq 10$.

Continued Fractions and the Divisor at Infinity on a Hyperelliptic Curve: Examples and Order Bounds

by

Katthaleeya Daowsud

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented April 25, 2013
Commencement June 2013

Doctor of Philosophy thesis of Katthaleeya Daowsud presented on April 25, 2013

APPROVED:

Major Professor, representing Mathematics

Chair of the Department of Mathematics

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Katthaleeya Daowsud, Author

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my advisor, Dr. Thomas A. Schmidt, for his valuable guidance and support through the years. I would also like to thank my committee members for their help in making this dissertation possible.

Secondly, I would like to give special thanks to all of my teachers in the mathematics department at Oregon State University and Kasetsart University in Thailand, for uncountable knowledge. Also, thanks to Oregon State University for providing me with a good environment and facilities to complete this dissertation. Additionally, I would like to thank the Royal Thai Government and the Department of Mathematics at Oregon State University for their financial support.

Lastly, I wish to express my heartfelt thanks to my beloved mother, and my wonderful sister, Jef, for their understanding and endless love. I am thankful for my father who is my inspiration to study mathematics. I am grateful to all my friends and their friendship that made me feel so at home in Corvallis. Thank you Au, Nij, Huang, Liw, Yod, Mon, Sombat, Don, Dojin, Nick, John, JB, Boris and Patty. You guys have meant so much to me. Thank you.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1. A Brief History 1

1.2. Statement of the Problem 3

1.3. Organization of this Thesis 4

2. MATHEMATICAL BACKGROUND 6

2.1. Function Fields of Curves 6

2.2. The Divisor at Infinity for a Hyperelliptic Curve 10

2.3. Continued Fractions in the Rational Function Field 12

2.4. Continued Fractions in the Hyperelliptic Function Field 14

3. RESULTS AND EXAMPLES 21

3.1. Naive Method for Determining Hyperelliptic Curves of Given Genus and Order of Divisor at Infinity 21

3.1.1 N=g+2 23
3.1.2 N=2g+1 28

3.2. Restrictions on Partial Quotients 31

3.2.1 The Polynomials f_j−Definition and Initial Results 31
3.2.2 The Polynomials f_j−Equivalent Formulation and Results 36
3.2.3 The Polynomials h_j 43
3.2.4 Upper Bound on N in terms of Genus and Quasi-Period Length . 47
3.2.5 Application when $g = 1$ 49
3.2.6 Application: Order N in Convergent Sequences 52

3.3. New Infinite Families with $\text{ord}(D_\infty) = 11$ 58

3.3.1 Genus 2 59
3.3.2 Genus Greater than 2 62

4. CONCLUSIONS AND FUTURE DIRECTIONS 67

TABLE OF CONTENTS (Continued)

Page

4.1. Conclusions 67

4.2. Future directions 68

BIBLIOGRAPHY 70

CONTINUED FRACTIONS AND THE DIVISOR AT INFINITY ON A HYPERELLIPTIC CURVE: EXAMPLES AND ORDER BOUNDS

1. INTRODUCTION

1.1. A Brief History

That finiteness of the order of points on elliptic curves, and more generally of divisors at infinity on hyperelliptic curves is related to periodicity of continued fractions, is a notion that can be traced back to Abel [1] and Chebychev [8]. We first learned of this history, and the relationship itself, from the paper of Adams and Razar [2]. Other authors who have discussed these notions include Berry[5] and van der Poorten, with various coauthors, see for example [28], [25].

The study of the arithmetic of function fields over finite fields goes back at least to E. Artin [3]. Much more recently, Friesen in particular has studied the structure of class groups using continued fractions, refer to [13] - [16]. Our approach is a variant of that used by Friesen; whereas he solves for the initial partial quotient in terms of the remaining terms of a given (quasi)-period, for small genus we find it more practical to solve for a (quasi)-period satisfying small sets of constraints.

As Cassels and Flynn express in the introduction to their text [7], there is still a need for interesting examples of curves of low genus over number fields. Here, we show that the decidedly "low brow" method of continued fractions over function fields continues to have much to offer.

We show that with a fixed base field, and given (low) genus and desired (small) order,

one can search fairly easily for hyperelliptic curves of the given genus over the field whose divisor at infinity is of the given order. We know that the divisor at infinity has finite order if and only if a corresponding continued fraction expansion, in polynomials, is periodic; the order itself is given in terms of the degrees of the initial partial quotients. Given a genus g and order N, there are then finitely many possible partitions for the degrees of these initial partial quotients; by making appropriate choices relating the coefficients of these partial quotients, it is often possible to determine a curve with the desired genus and order.

It has been known since 1940 [6] for which there is no elliptic curve over $\mathbb{Q}$ with a point of order 11. (Later Mazur [22] determined the exact list of possible orders of a point on an elliptic curve over $\mathbb{Q}$.) Thus, our continued fraction approach must certainly fail with $k = \mathbb{Q}$, and $N = 11$, $g = 1$. Fixing $k = \mathbb{Q}$, it is natural to ask about $N = 11$ and higher genus. Indeed, Flynn [11], [12] gave a one-dimensional family of hyperelliptic curves with $g = 2$ and $N = 11$. Much more recently, Bernard *et al* [4] found 18 additional individual curves with $(g, N) = (2, 11)$. (They state that they have found 19, but their table of results lists one curve twice.) They explicitly state that they sought new infinite families of such curves. We exhibit new infinite families of this type, in Section 3.3.

1.2. Statement of the Problem

This dissertation attempts to respond to the following questions:

1. How can we find hyperelliptic curves over a field of characteristic zero of given genus and given order of divisor at infinity?

2. In particular, how can we find infinite families of hyperelliptic curves over $\mathbb{Q}$ of the divisor at infinity of order 11 for a given genus $g \geq 2$? (Recall that there is no divisor at infinity of order 11 for any elliptic curve over $\mathbb{Q}$.)

3. A naive bound, found in [27], states that a hyperelliptic curve defined by $y^2 = f(x)$ with genus g and divisor at infinity of order N satisfies the following bounds:

$$g + m \leq N \leq g\,m + 1,$$

where m is the quasi-period length for the continued fraction expansion of y. The obvious question to ask is

"Can these bounds for the order of the divisor at infinity of a hyperelliptic curves be improved?"

This leads to the more technical question: How do we control the leading coefficient of each partial quotient of the continued fraction expansion of y?

1.3. Organization of this Thesis

Chapter 2 of this dissertation presents the mathematical background. We divide this chapter into four sections. The first section briefly discusses function fields and divisors. The goal of Section 2.2 is to define hyperelliptic curves over a field k, and divisors at infinity. In Section 2.3, we discuss continued fractions in function fields and their properties. Divisors at infinity for hyperelliptic curves given by $y^2 = f(x)$ and their relationship to the continued fraction expansion of y are topics of Section 2.4.

Chapter 3 presents our results and new examples. We divide this chapter into three sections. Section 3.1 begins with the form of a hyperelliptic curve in terms of certain convergents. This gives a number of consequences: Explicit equations for hyperelliptic curves where the corresponding y has continued fraction expansion of short period; the classification all hyperelliptic curves of genus g whose divisor at infinity has order $N = g+2$; and the determination of hyperelliptic curves of shortest possible period length with genus g and $N = 2g + 1$. We give examples relating to these.

Section 3.2 presents the main technical results of this dissertation. We introduce a sequence of polynomials h_j, which is our main tool to bound sums of degrees of consecutive partial quotients. Given g and N, the sequence of these degree is constrained due to this bound. Thus, the h_j leads to both (1) an improvement of the naive method in Section 3.3 of searching for hyperelliptic curves of given g, and N, and (2) an improvement on the upper bound on N in terms of g and the quasi-period length. In the very end of this section, we present a number of consequences in the case of genus 1.

Section 3.3 discusses the simplest ways to find new families of hyperelliptic curves over $\mathbb{Q}$ of divisors at infinity of order 11 for a given genus $g \geq 2$. In Subsection 3.2.1, we focus on $g = 2$ and improve upon work of Bernard *et al* [4] by presenting a new infinite family of curves defined over $\mathbb{Q}$ with $g = 2$ and $N = 11$. (Note that Flynn [7],[11] gave one

such family.) Subsection 3.2.2 presents new families when the genus g is greater than 2.

Chapter 4 presents conclusions and future directions.

2. MATHEMATICAL BACKGROUND

Our main object of study is a certain type of divisor on a hyperelliptic curve whose equation is of appropriate form. In Subsections 2.1 and 2.2., we briefly review vocabulary of elementary algebraic geometry so as to define these terms. Our main tool in this dissertation is continued fraction expansions of formal Laurent series in x^{-1}; we introduce these in Subsection 2.3 and review known results in the setting related to divisors on hyperelliptic curves in Subsection 2.4.

2.1. Function Fields of Curves

We tersely recall some basic definitions; we have borrowed material from the textbooks by Hulek[18] and Fulton [19].

Definition 2.1.0.1 *Let k be a field and $\mathbb{A}^n = \{(a_1, \ldots, a_n) : a_i \in k\}$. Let $f : \mathbb{A}^n \to k$ be a polynomial in $k[x_1, \ldots, x_n]$ mapping $(a_1, \ldots, a_n)$ in to $f(a_1, \ldots, a_n)$. Then a point $P = (a_1, \ldots, a_n)$ in $\mathbb{A}^n$ is called a* **zero** *of f if $f(P) = 0$. The* **zero locus** *of T is the set*

$$V(T) = \{P \in \mathbb{A}^n | f(P) = 0 \, for \, all \, f \in T\}.$$

Definition 2.1.0.2 *Let k be a field and $\mathbb{A}^n = \{(a_1, \ldots, a_n) : a_i \in k\}$. A subset $Y \subset \mathbb{A}^n$ is called an* **(affine) algebraic set** *in $\mathbb{A}^n$ if there is a subset $T \subset k[x_1, \ldots, x_n]$ such that $Y = V(T)$. An algebraic subset X is called* **irreducible** *if there is no decomposition X into proper algebraic subsets X_1, X_2. That is,*

$$X = X_1 \cup X_2$$

where X_1, X_2 are both proper algebraic subsets of X. An **affine variety** *is an affine algebraic set.*

Definition 2.1.0.3 *Let X be a subset of $\mathbb{A}^n$. The* **ideal** *of X is an ideal in $k[x_1, \ldots, x_n]$ consisting of all polynomials which vanish on X, denoted by $I(X)$. That is,*

$$I(X) = \{f \in k[x_1, \ldots, x_n] | f(P) = 0 \, for \; all \, P \in X\}.$$

The **coordinate ring** *of a affine variety V, denoted by $k[V]$ is defined by*

$$k[V] = k[x_1, \ldots, x_n]/I(V).$$

Now, let $\mathcal{C}$ be a smooth projective curve over a field k, f a rational function on $\mathcal{C}$, and P a point in $\mathcal{C}$.

Definition 2.1.0.4 *The rational function f is called* **regular** *at P if there exist polynomials g and h in $k[\mathcal{C}]$ such that $h(P) \neq 0$. The* **local ring** *of $\mathcal{C}$ at a point $P \in \mathcal{C}$ is the ring*

$$\mathcal{O}_{\mathcal{C},P} = \{f \in k(\mathcal{C}) | f \text{ is regular at } P\}.$$

Since $\mathcal{O}_{\mathcal{C},P}$ has a unique maximal ideal, say

$$m_P := \Big\{ \frac{f}{g} \in k(\mathcal{C}) | f, g \in k[\mathcal{C}], f(P) = 0, g(P) \neq 0 \Big\},$$

we obtain that $\mathcal{O}_{\mathcal{C},P}$ is in fact a local ring (it has a unique maximal ideal). And for an integer n,

$$m_P^n := \{f^n | f \in m_P\}.$$

Definition 2.1.0.5 *Let $f \in \mathcal{O}_{\mathcal{C},P}$ be regular at P. Then we define the* **multiplicity** *of f at P, denoted by $\nu_P(f)$ by*

$$\nu_P(f) = \max\{n | f \in m_P^n\}.$$

A function f vanishes at P if and only if $\nu_P(f) \geq 1$. If f has a multiplicity n at P, then we can express

$$f = g \, t^n$$

where $g \in \mathcal{O}_{\mathcal{C},P}$ so that $h(P) \neq 0$ and $t \in m_P$.

Definition 2.1.0.6 *The* **multiplicity** *of a rational function* $0 \neq f \in k(\mathcal{C})$ *is defined by*

$$\nu_P(f) = \nu_P(g) - \nu_P(h)$$

where $g, h \in \mathcal{O}_{\mathcal{C},P}$. *We say that* f *has a* **pole** *of order* $-\nu_P(f)$ *in* P *if* $\nu_P(f) < 0$, *and* f *has a* **zero** *of order* $\nu_P(f)$ *in* P *if* $\nu_P(f) > 0$.

Definition 2.1.0.7 *A* **divisor** D *on a curve* $\mathcal{C}$ *is a finite formal sum of points on* $\mathcal{C}$. *That is,*

$$D = \sum_{i=1}^{l} n_i P_i, \quad n_i \in \mathbb{Z}, P_i \in \mathcal{C},$$

where the **degree** *of* D *is defined by*

$$\deg(D) = \sum_{i=1}^{l} n_i.$$

The **divisor group** *of* $\mathcal{C}$ *is defined by*

$$\mathrm{Div}(\mathcal{C}) = \{D | D \text{ is a divisor on } \mathcal{C}\}.$$

The function $\deg : \mathrm{Div}(\mathcal{C}) \longrightarrow \mathbb{Z}$ is a group homomorphism and hence its kernel is the subgroup $\mathbf{Div}_0(\mathcal{C})$ containing all divisors of degree 0.

Definition 2.1.0.8 *The* **divisor** *of a* **rational function** f *is defined by*

$$(f) = \sum_{P \in \mathcal{C}} \nu_P(f) P.$$

A divisor D *is called a* **principal divisor** *if there exists a rational function* $f \neq 0$ *in* $k(\mathcal{C})$ *such that* $D = (f)$. *That is,*

$$(f) = \sum_{P \in \mathcal{C}} \nu_P(f)\, P \in \mathrm{Div}(\mathcal{C}).$$

The set of principal divisors is defined by

$$\mathrm{Prin}(\mathcal{C}) = \{D : D \text{ is a principal divisor}\}.$$

Since $(fg) = (f) + (g)$, and $(\frac{1}{f}) = -(f)$, we obtain a group homomorphism from the multiplicative group $k(\mathcal{C})^*$ to the additive group $Div(\mathcal{C})$ mapping f to (f). Note that (f) has a degree 0.

Example 2.1.1: Principle Divisor. Consider $\Sigma = \mathbb{C} \cup \{\infty\}$ and

$$f(z) = c \prod_{k=1}^{n} (z - \lambda_k)^{l_k}$$

for some integers c, and l_k. Then

$$\operatorname{div}(f) = \sum_{k=1}^{n} l_k \cdot \lambda_k - \big(\sum_{k=1}^{n} l_k\big) \cdot \infty,$$

and

$$\deg(\operatorname{div}(f)) = \sum_{k=1}^{n} l_k - \big(\sum_{k=1}^{n} l_k\big) = 0.$$

□

2.2. The Divisor at Infinity for a Hyperelliptic Curve

We recall the definition of a main object of study of this dissertation.

Definition 2.2.0.9 *Let k be a field of characteristic zero. A* **hyperelliptic curve** $\mathcal{C}$ *of genus $g > 0$ over k is given by an equation of the form*

$$y^2 = f(x)$$

where $f(x)$ is a monic polynomial in $k[x]$ such that $\deg(f(x)) = 2g+2$ and f has distinct roots over $\overline{k}$.

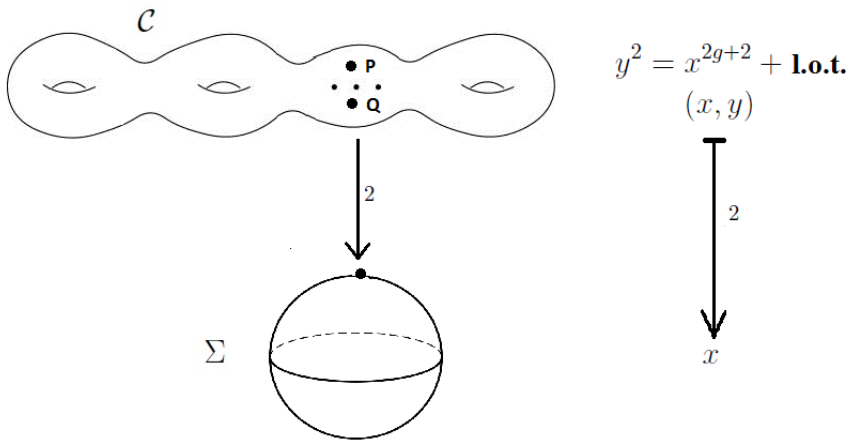

FIGURE 2.1: A hyperelliptic curve

The curve $\mathcal{C}$ can be completed to a projective curve (which we also denote by $\mathcal{C}$). The completion of $\mathcal{C}$ leads to two points at infinity, say P, Q. Then the divisor $D_\infty = P - Q \in \mathrm{Div}(\mathcal{C})$ is called the **divisor at infinity**. The hyperelliptic involution $(x, y) \mapsto (x, -y)$ interchanges P and Q.

Definition 2.2.0.10 *The divisor D_∞ is of* **order** *n if nD_∞ is principal and n is the least such positive integer.*

The following discussion appears from in Adams and Razar [2]. Let $\mathcal{C}$ be a hyperelliptic curve of genus g given by $y^2 = f(x)$ and $K = k(x, y)$. Then the units of R are of the form:

$$u = p(x) + yq(x),$$

where $p(x), q(x)$ are polynomial in $k[x]$, satisfying Pell's equation:

$$uu^* = p^2(x) + f(x)q^2(x) \in k^\times. \tag{2.1}$$

Lemma 2.2.0.1 (Adams and Razar) *The following are equivalent:*

1. *For some positive integer n, there is a rational function f in K such that*

$$(f) = nD_\infty,$$

2. *the ring R contains a non-constant unit,*
3. *Pell's equation* (2.1) *has a non-trivial solution,*
4. *the continued fraction expansion of y is periodic.*

We will discuss the continued fraction expansion of y in Section 2.4.

Remark 2.2.0.1 *The order of a divisor could be defined as the order of the corresponding point on the "Jacobian variety" of the curve $\mathcal{C}$. Our divisors at infinity give $k-$rational points, see Cassels and Flynn [7].*

2.3. Continued Fractions in the Rational Function Field

Given any field k, the order of vanishing of a polynomial $f \in k[x]$ at the origin $x = 0$ extends to define a valuation on the quotient field, the field of rational functions $k(x)$. The valuation is simply given by writing any non-zero rational function as an integral power of x times a rational function with neither zero nor pole at $x = 0$; the exponent of x is then the valuation of the initial rational function. One defines a metric on $k(x)$ in the usual manner; the completion of this field with respect to the metric is the ring of formal Laurent series, $k((x))$.

The point at infinity on the projective line over the field k can be viewed as corresponding to the vanishing of x^{-1}. We obtain once again a valuation on $k(x)$, this time leading to a completion that is $k((x^{-1}))$. For $\alpha \in k((x^{-1}))$, say

$$\alpha = c_{-n}x^n + c_{-n+1}x^{n-1} + \cdots + c_{-1}x + c_0 + c_1x^{-1} + c_2x^{-2} + \cdots ,$$

we define the **polynomial part** of α as

$$\lfloor\, \alpha \,\rfloor = c_{-n}x^n + c_{-n+1}x^{n-1} + \cdots + c_{-1}x + c_0 \,.$$

We then define a continued fraction algorithm by way of the following sequences. Let $\alpha_0 = \alpha$; for $i \geq 0$ let $a_i = \lfloor\, \alpha_i \,\rfloor$ and while $\alpha_i - a_i \neq 0$, let $\alpha_{i+1} = (\alpha_i - a_i)^{-1}$. We then find an expansion of the form

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} =: [a_0; a_1, a_2, \ldots,] \,,$$

where we have defined the flat notation for typographic ease. The a_i are called the **partial quotients** of the expansion and each α_j is called **a complete quotient**. The continued fraction $[a_0; a_1, \ldots, a_i]$ is called a **convergent** of α.

It is not hard to see that this process terminates if and only if $\alpha_j \in k[x]$ for some j. Also, the convergent

$$[a_0; a_1, \ldots, a_i] = \frac{p_j}{q_j}$$

where p_j, q_j can be defined recursively by setting $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$, and

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_0 a_1 + 1, & q_1 &= a_1, \text{ and} \\ p_j &= a_j p_{j-1} + p_{j-2}, & q_j &= a_j q_{j-1} + q_{j-2}. \end{aligned}$$

For $j = 2, 3, \ldots,$

$$\alpha_j = [a_j; a_{j-1}, a_{j-2}, a_{j-3} \ldots],$$

and

$$\alpha = [a_0, a_1, \ldots, a_{j-1}, \alpha_j] = \frac{p_{j-1}\alpha_j + p_{j-2}}{q_{j-1}\alpha_j + q_{j-2}}.$$

2.4. Continued Fractions in the Hyperelliptic Function Field

The local ring of regular functions at a non-singular point of a projective curve is a discrete valuation ring. In particular, its maximal ideal, defined by vanishing at the point is principal. Any generator of this maximal ideal is called a local uniformizer. For the point at infinity of $\mathbb{P}^1$ we can take x^{-1} as a local uniformizer, thus giving the valuation on $k(x)$ leading to the continued fractions above.

Our insistence on affine equations of the equation $y^2 = x^{2g+2} + \text{lower order terms}$ is so that the degree two map from $\mathcal{C}$ to $\mathbb{P}^1$ defined by $(x, y) \mapsto x$ is such that the point at infinity of $\mathbb{P}^1$ has two pre-images. The local rings at these points are then isomorphic to the local ring uniformized by x^{-1}. From this, it follows that there is a square root of $y^2 = f(x)$ in $k((x^{-1}))$. Indeed, the completion of the "rational field" $k(x)$ with respect to the metric from our valuation is analogous to the completion of $\mathbb{Q}$ with respect to the usual metric. Our $y = \sqrt{f(x)}$ is of the type that Artin [3] called "real quadratic" — exactly because it is a value in the completed field.

In the number field setting, see [26] the continued fraction expansion of $\sqrt{d}$ is

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_{n-1}, 2a_0}\,]$$

satisfying the following properties:

- $\alpha_0 = \alpha$, and $\alpha_{i+1} = \frac{1}{\alpha_i - \lfloor \alpha_i \rfloor}$,
- $a_i = \lfloor \alpha_i \rfloor$,
- $a_{n-1} = a_1, a_{n-2} = a_2, \ldots$ (palindromic property), and
- $a_i < a_0$ for all $i < n$.

Analogous properties holds in the function field case, see Adams and Razar [2] and van der Poorten and Tran [28]. Let k be a field of characteristic zero and let $\mathcal{C}$ be a

hyperelliptic curve over k given by $y^2 = f(x)$ with genus g. Then , when periodic, the continued fraction expansion of

$$\alpha = y = \sqrt{f(x)} = [a_0; \overline{a_1, \ldots, a_{n-1}, 2a_0}\,]$$

satisfies the following properties:

- $\alpha_0 = \alpha$, and $\alpha_{i+1} = \frac{1}{\alpha_i - \lfloor \alpha_i \rfloor}$,
- $\lfloor a_i \rfloor$ is the polynomial part of α_i,
- $a_{n-1} = a_1, a_{n-2} = a_2, \ldots$ (palindromic property), and
- $\deg(a_i) \leq \deg(a_0)$ for all $i < n$.

A new phenomenon occurs in the function field setting.

Definition 2.4.0.11 *We call an even length sequence of* $(a_1, \ldots, a_{2\ell})$ **skew symmetric** *of* skew value γ *if*

$$a_{2(\ell-i)} = \gamma\, a_{2i+1} \quad \forall\, 0 \leq i < \ell\,,$$

with nonzero $\gamma \in k$.

Proofs of the following are given in [14] when k is a finite field, and in [28] in general; see also [2], [27] and [25]. We use an overline to denote a repetition of a sequence of partial quotients.

Theorem 2.4.0.1 (Friesen; vander Poorten and Tran) *Suppose that a non-square* $f(x) \in k[x]$ *is of even degree, with leading coefficient a square in* k. *If the continued fraction expansion of the Laurent series of* $\sqrt{f(x)}$ *is periodic, then it is of the form*

$$\sqrt{f(x)} = [\, a_0; \overline{a_1, \ldots, a_{m-1}, 2\kappa a_0, a_{m-1}, \ldots, a_1, 2a_0}]\,, \tag{2.2}$$

where $(a_1, \ldots, a_{m-1})$ *is skew symmetric of skew value* κ^{-1}.

From the previous theorem, we see that

1. If $\kappa = 1$, then $n = m$ and $a_{m-1} = a_1, a_{m-2} = a_2, \ldots$.

2. If $\kappa \neq \pm 1$, then $n = 2m, a_m = 2\kappa\, a_0$ and

   (a) if $\frac{m-1}{2}$ is odd, then $a_{m-1} = \kappa^{-1}a_1, a_{m-2} = \kappa\, a_2, \ldots, a_{\frac{m-1}{2}} = \kappa^{-1}a_{\frac{m-1}{2}-1}$,

   (b) otherwise, we have $a_{m-1} = \kappa^{-1}a_1, a_{m-2} = \kappa\, a_2, \ldots, a_{\frac{m-1}{2}} = \kappa\, a_{\frac{m-1}{2}-1}$.

Definition 2.4.0.12 *In the setting of Theorem 2.4.0.1, we call (the minimal) m the* **quasi-period** *length. Thus, exactly when $\kappa = 1$, we have equality of the (minimal) period length with the quasi-period length.*

The proper quasi-period can occur only in the function field case. Similar to the number field case, set $P_0 = 0$ and $Q_0 = 1$. Define polynomials P_j and Q_j recursively by

$$P_{j+1} = a_j Q_j - P_j \quad \text{and} \quad Q_{j+1} = \frac{f(x) - P_j^2}{Q_j},$$

where Q_j divides $f(x) - P_j^2$. Then the complete quotient α_j is of the form

$$\alpha_j = \frac{\sqrt{f(x)} + P_j}{Q_j} = a_j - \frac{\sqrt{f(x)} - P_j}{Q_j}.$$

The proof of following theorem is the same as the corresponding theorem for number fields.

Theorem 2.4.0.2 *Let $\mathcal{C}$ be a hyperelliptic curve of genus g over a field k given by $y^2 = f(x)$ where $f(x)$ is monic and has a degree $2g+2$. Define α_j, P_j, and Q_j as above. Let $\frac{p_j}{q_j}$ be the convergent of the continued fraction expansion of α. Then*

$$p_j^2 - f(x)q_j^2 = (-1)^{j-1}Q_{j+1}$$

for all $j = 0, 1, 2, \ldots$.

The following theorems and propositions appears in [28].

Proposition 2.4.0.1 (van der Poorten and Tran) *Let $f(x)$ be a monic polynomial in $k[x]$ which is not a perfect square, $\deg(f(x)) = 2g+2$ and $\alpha = \sqrt{f(x)}$ where g is a positive integer. If $x^2 - f(x)y^2 = z$ and $\deg(z) \leq g$, then $\frac{x}{y}$ is a convergent of the continued fraction expansion of α.*

Proposition 2.4.0.2 (van der Poorten and Tran) *The polynomials P_j and Q_j satisfy*

$$\deg(P_j) = g+1 \quad \text{and} \quad 0 \leq \deg(Q_j) \leq g.$$

Furthermore, if m is a quasi-period length, then

$$\deg(a_0) = g+1 \quad \text{and} \quad 0 < \deg a_j \leq g,$$

for all $j = 1, \ldots, m-1$.

Theorem 2.4.0.3 (van der Poorten and Tran) *Suppose that $\mathcal{C}$ is a hyperelliptic curve of genus g over a field k of equation*

$$y^2 = f(x)$$

where $\deg(f) = 2g+2$ and f is monic, $m < \infty$ is the quasi-period length of the continued fraction of y and n is the period length of the continued fraction of y. Then

$$p_{m-1}^2 - d(x)q_{m-1}^2 = (-1)^m \kappa^{-1}$$

if and only if the continued fraction expansion of y is

$$y = [a_0; \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}]$$

where $(a_1, a_2, \ldots, a_{m-1})$ is a skew-symmetric sequence.

The following is given by Adams and Razar [2] in the genus $g = 1$ case. The general case is proven in [28], see also [25]. W. Schmidt [27] presents a large portion of this result in his Lemma 7.

Theorem 2.4.0.4 (Adams and Razar, van der Poorten and Tran) *Suppose that $\mathcal{C}$ is a hyperelliptic curve of genus g over a field k of affine equation*

$$y^2 = f(x)$$

where f is a monic polynomial of degree $2g+2$. Then the divisor at infinity D_∞ is of finite order N if and only if the continued fraction expansion of y is periodic, say with quasi-period length m and the sum of the degrees of the partial quotients $a_0, a_1, \ldots, a_m$ is N; that is

$$ord(D_\infty) = \sum_{j=0}^{m-1} \deg(a_j).$$

Example 2.4.2: Quasi-period 3 and the divisor at infinity of order 5. Consider

$$y = x(x^2-2) + \cfrac{1}{\boldsymbol{\frac{x}{2}} + \cfrac{1}{\boldsymbol{2x} + \cfrac{1}{\boldsymbol{\frac{1}{2}x(x^2-2)} + \cfrac{1}{2x + \cfrac{1}{\frac{x}{2} + \cfrac{1}{2x(x^2-2) + \ddots}}}}}}$$

Here, $a_0 = x(x^2-2), a_1 = \frac{x}{2}, a_2 = \mathbf{4}a_1$, and $a_3 = 2(\frac{\mathbf{1}}{\mathbf{4}})a_0$. This implies the continued fraction expansion of y has a period length $n = 6$ and a quasi-period length $\boldsymbol{m} = 3$ with $\boldsymbol{\kappa} = \frac{1}{4}$.

This continued fraction corresponds to the hyperelliptic curve of genus 2 over $\mathbb{Q}$ defined by

$$y^2 = x^6 - 4x^4 + 8x^2 - 4 = (x(x^2-2))^2 + 4(x^2-1).$$

By Theorem 2.4.0.4, we compute the order of D_∞,

$$N = \delta_0 + \delta_1 + \delta_2 = 3 + 1 + 1 = 5.$$

□

Remark 2.4.0.2 *Since* $\deg(a_0) = g + 1$ *and* $0 < \deg a_j \leq g$, *for all* $j = 1, \ldots, m-1$, *we conclude that*

$$\text{ord}(D_\infty) = g + 1 + \sum_{j=1}^{m-1} a_j \quad \text{and hence} \quad g + m \leq \text{ord}(D_\infty) \leq g\ m + 1.$$

We improve the above result in two ways. Firstly, we show that not all $\deg(a_j) = g$ *for* $1 \geq j \geq m-1$. . *Secondly, under a certain condition, see Lemma 3.2.4.1 states that*

$$\text{ord}(D_\infty) \leq \begin{cases} \Big(\lfloor \frac{m}{2} \rfloor + 1 \Big) g + \lfloor \frac{m+1}{2} \rfloor & \text{if } r = m, \\ \Big(\frac{m}{2} + \lceil \frac{m}{4} \rceil \Big) g + \frac{m}{2} - \lceil \frac{m}{4} \rceil & \text{if } r < m \text{ and } m \text{ is even}, \\ \Big(\lfloor \frac{m}{2} \rfloor + \lceil \frac{m}{4} \rceil + 1 \Big) g + \lfloor \frac{m}{2} \rfloor - \lceil \frac{m}{4} \rceil & \text{if } r < m, \text{ and } m \text{ is odd}. \end{cases}$$

Example 2.4.3: Suppose that $\mathcal{C}$ is an elliptic curve, thus of genus $g = 1$, given by $y^2 = f(x)$. That is, $\deg(f(x)) = 4$. Then $\deg(a_0) = 2$ and $\deg(a_j) = 1$ for all $j = 1, \ldots, m-1$. Assume that the period length of the continued fraction expansion of y is $n > 1$ and m is the quasi-period length of the continued fraction expansion of y. Applying the above remark, we have

Case I: $\kappa = 1$. Then $n = m$, and

$$\text{ord}(D_\infty) = g + 1 + \sum_{j=1}^{m-1} a_j = 2 + (m-1) = m + 1 = n + 1$$

Case II: $\kappa \neq \pm 1$. Then $n = 2m$,

$$\text{ord}(D_\infty) = g + 1 + \sum_{j=1}^{m-1} a_j = 2 + (m-1) = m + 1 = \frac{n}{2} + 1.$$

□

In the finite field setting, Friesen [14] gives a method for solving for $f(x)$ when given the initial $m-1$ terms of its (quasi-)period. Just as for Theorem 2.4.0.3, it is easily seen that his result holds in general.

Theorem 2.4.0.5 (Friesen) *Suppose that* $(a_1, \ldots, a_{m-1})$ *is a skew symmetric sequence of elements of* $k[x]$*, with skew value* $\kappa \in k^*$*. Let*

$$\begin{pmatrix} P & R \\ Q & S \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & 1 \\ 1 & 0 \end{pmatrix} .$$

Then a monic $f(x) \in k[x]$ *has continued fraction expansion* (3.1)*, with* $a_0 = \lfloor f(x) \rfloor$*, if and only if*

$$f = P^2 X^2 + (2Q + (-1)^{m-1} PQS) X + (Q^2/4 + (-1)^{m-1} \kappa) S ,$$

for any $X \in k[x]$ *such that* $XP + (-1)^{m-1} QS/2$ *is monic.*

3. RESULTS AND EXAMPLES

3.1. Naive Method for Determining Hyperelliptic Curves of Given Genus and Order of Divisor at Infinity

Let k be a field of characteristic zero and let $\mathcal{C}$ be a hyperelliptic curve given by

$$y^2 = f(x)$$

where $f(x) \in k[x]$ is monic and has degree $2g+2$ where $g > 0$. Suppose the continued fraction of y, as defined in the previous chapter, is periodic of quasi-period length m, and of period length n. We know that the period has a palindromic symmetry, so we have

$$y = [a_0; \overline{a_1, a_2, \ldots, a_{m-1}, a_m, a_{m-1} \ldots, a_{2m-1}, 2a_0}\,] \tag{3.1}$$

where

$$a_m = 2\kappa a_0, a_{m-1} = \kappa^{-1} a_1, a_{m-2} = \kappa a_2, \ldots, \quad \text{with } \kappa \in k,\ \kappa \notin \{1, 0, -1\}.$$

If $\kappa = 1$, then the period length n is equal to the quasi-period length m.

Let $z = [\overline{a_1; a_2, \ldots, a_{2m-1}, 2a_0}\,]$ and let p'_j/q'_j denote the convergents to the purely periodic $z = 1/(\sqrt{f(x)} - a_0)$. Set $p'_{-2} = 0, p'_{-1} = 1, q'_{-2} = 1$, and $q'_{-1} = 0$. Then

$$\begin{aligned} p'_0 &= a_1, & q'_0 &= 1, \\ p'_1 &= a_2 a_1 + 1, & q'_1 &= a_2 \\ p'_j &= a_{j+1} p'_{j-1} + p'_{j-2}, & q'_j &= a_{j+1} q'_{j-1} + q'_{j-2}. \end{aligned} \tag{3.2}$$

We denote the leading coefficient of $f(x)$ by $\mathrm{lc}(f(x))$.

Remark 3.1.0.3 *The following lemma is key to our results, and lays the foundation for almost all results in Chapter 3. Friesen [14] has this result but he only considers a finite field k and he did use this directly to find hyperelliptic curves. Many arguments about*

continued fractions are by way of formal algebraic manipulations; in particular, we can and do use the following, which is proven in [14],

$$p'_{m-3} = \kappa\, q'_{m-2}.$$

Lemma 3.1.0.2 *Suppose that* $\sqrt{f(x)}$ *has a continued fraction expansion as in* (3.1)*, with quasi-period length* $m < \infty$*. Let* p'_j/q'_j *denote the convergents to the purely periodic* $1/(\sqrt{f(x)} - a_0)$*. Then*

$$f(x) - a_0^2 = \frac{q'_{m-1}}{\kappa p'_{m-2}},$$

$$\deg(f(x) - a_0^2) = \deg(a_0) - \deg(a_1),$$

and the leading coefficient of $f(x) - a_0^2$ *is*

$$\mathrm{lc}(\, f(x) - a_0^2\,) = \frac{2}{\mathrm{lc}(a_1)}.$$

Proof. Let $z = 1/(\sqrt{f(x)} - a_0)$. From Section 2.3, since z has purely periodic expansion with period length m, we have

$$\frac{1}{\kappa} q'_{m-1} z^2 + (q'_{m-2} - \frac{1}{\kappa} p'_{m-1}) z - p'_{m-2} = 0\,. \tag{3.3}$$

Now, due to the palindromic nature of the period, from the above definition both

$$p'_{m-1} = 2\kappa a_0 p'_{m-2} + p'_{m-3}\,,$$

and

$$q'_{m-2} = \frac{1}{\kappa} p'_{m-3}\,.$$

Thus, (3.3) becomes

$$\frac{1}{\kappa} q'_{m-1} z^2 - (2a_0 z + 1) p'_{m-2} = 0.$$

Since

$$f(x) - a_0^2 = (\sqrt{f(x)} + a_0)(\sqrt{f(x)} - a_0) = \frac{2a_0 + \frac{1}{z}}{z} = \frac{2a_0 z + 1}{z^2}\,,$$

the equality holds. Since

$$f(x) - a_0^2 = \frac{q'_{m-1}}{\kappa p'_{m-2}}, \quad q'_{m-1} = 2a_0 a_{m-1} \cdots a_2 + \text{lower order terms},$$

and $p'_{m-2} = a_{m-1} \cdots a_1 +$ lower order terms, both the degree and leading term are as claimed. □

Corollary 3.1.0.1 *When* $m = 1$,

$$y = [a_0; \overline{2a_0}\,] \quad \textit{if and only if} \quad f(x) = a_0^2 + 1.$$

When $m = 2$,

$$y = [a_0; \overline{a_1, 2a_0}\,] \quad \textit{if and only if} \quad f(x) = a_0^2 + \frac{2a_0}{a_1}.$$

When $m = 3$ *and the period length* $n = 3$,

$$y = [a_0; \overline{a_1, a_1, 2a_0}\,] \quad \textit{if and only if} \quad f(x) = a_0^2 + \frac{2a_0a_1 + 1}{a_1^2 + 1}.$$

When $m = 3$, *and the period length* $n = 6$,

$$y = [a_0; \overline{a_1, \kappa^{-1}a_1, 2\kappa a_0, \kappa^{-1}a_1, a_1, 2a_0}\,] \quad \textit{if and only if} \quad f(x) = a_0^2 + \frac{2a_0a_1 + 1}{a_1^2 + \kappa}.$$

3.1.1 N=g+2

The case of $N = g + 1$ is trivially resolved; a hyperelliptic curve with a divisor at infinity of order $g + 1$ has equation

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

where $g(x)$ is a monic polynomial of degree $g+1$ in $k[x]$ such that $g(x)^2+1$ has no repeated roots over $\overline{k}$.

When a divisor at infinity has order $N > 2$, we write $\text{ord}(D_\infty) = N$. We seek all corresponding hyperelliptic curves $\mathcal{C}$ with genus g over the field k which have the divisor at infinity of order $N = g + 2$.

Theorem 3.1.1.1 *Suppose that k is a field of characteristic zero. A hyperelliptic curve $\mathcal{C} : y^2 = f(x)$ of genus g over k has a divisor at infinity of order $N = g + 2$ if and only if $f(x)$ is of one of the following two forms:*

$$f(x) = (x-\alpha)h(x)\underbrace{\left((x-\alpha)^3 h(x) + \frac{2}{c}\right)}_{g(x)}$$

or

$$f(x) = h(x)\underbrace{\left((x-\alpha)^2 h(x) + \frac{2}{c}\right)}_{g(x)}$$

where $\alpha, c \in k$ and $h(x), g(x)$ are polynomials over an algebraic closure $\overline{k}$ of the field k such that $h(x)$ is monic, $\deg(h(x)) = g$, and both $h(x)$ and $g(x)$ have no repeated roots in $\overline{k}$.

Proof. ($\Longrightarrow$) Suppose that a hyperelliptic curve $\mathcal{C} : y^2 = f(x)$ of genus g over k has a divisor at infinity of order $N = g + 2$. By Theorem 2.4.0.4, we have

$$N = \operatorname{ord}(D_\infty) = \deg(a_0) + \sum_{j=1}^{m-1} \deg(a_j) = g + 2$$

where m is the quasi-period length of the continued fraction of y. Here, $\deg(a_0) = g + 1$. That gives $\deg(a_1) = 1$ and $N = g + 2 = \deg(a_0) + \deg(a_1)$. It follows that the period length of the continued fraction of y must be 2. Let $a_1 = c\,x - e \in k[x]$. We can rewrite a_1 as $a_1 = c(x - \alpha)$ where $\alpha = \frac{e}{c}$. By Corollary 3.1.0.1 when $m = 2$, we have either

$$a_0 = (x-\alpha)^2 h(x) \in k[x]$$

or

$$a_0 = (x-\alpha)h(x) \in k[x].$$

Since a_0 is monic, we have $h(x)$ is also monic, and then $f(x)$ is monic and

$$f(x) = (x-\alpha)h(x)\underbrace{\left((x-\alpha)^3 h(x) + \frac{2}{c}\right)}_{g(x)}$$

or

$$f(x) = h(x)\underbrace{\Big((x-\alpha)^2 h(x) + \frac{2}{c}\Big)}_{g(x)}.$$

Since $\mathcal{C}$ is a hyperelliptic curve over k, both $g(x)$ and $h(x)$ must have distinct roots in $\overline{k}$.

($\Longleftarrow$) Assume that

$$f(x) = (x-\alpha)h(x)\Big((x-\alpha)^3 h(x) + \frac{2}{c}\Big) = ((x-\alpha)^2 h(x))^2 + \frac{2}{c}(x-\alpha)h(x).$$

We see that $a_0 = (x-\alpha)^2 h(x)$ and

$$\frac{2}{c}(x-\alpha) = \frac{2a_0}{c\,(x-\alpha)}$$

Applying Corollary 3.1.0.1 when $m = 2$, we have the period length of the continued fraction expansion of y is $n = 2$ and partial quotients

$$a_0 = (x-\alpha)^2 h(x) \quad \text{and} \quad a_1 = c(x-\alpha). \tag{3.4}$$

By Theorem 2.4.0.4, we have

$$N = \operatorname{ord}(D_\infty) = \deg(a_0) + \deg(a_1) = g + 1 + 1 = g + 2.$$

The second case is analogous to the first case. □

Remark 3.1.1.1 *One easily finds $f(x)$ as above. Indeed, for both of the forms of $f(x)$ above, if $h(x)$ has no repeated roots, then for each α there is only a finite number of c such that $g(x)$ has repeated roots over $\overline{k}$.*

We sketch this, where for simplicity we consider only $\alpha = 0$ and we set $b = 2/c$. Let $h(x)$ be a monic polynomial of degree n in $k[x]$. Then there are only a finite number of b in k such that $g(x) = x^3\,h(x) + b$ has repeated roots over $\overline{k}$; we sketch this by using the

resultant *of* $g(x)$ *and* $g'(x)$*. The resultant of* $g(x)$ *and* $g'(x)$*,*

$$R(g(x), g'(x)) = R(x^3h(x) + b, (x^3h(x))')$$

$$= \det \begin{pmatrix} 1 & -s_1 & \cdots & (-1)^n s_n & 0 & 0 & b & \cdots & 0 \\ 0 & 1 & \cdots & (-1)^{n-1} s_{n-1} & (-1)^n s_n & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & -s_1 & s_2 & -s_3 & \cdots & b \\ n+3 & -(n+2)s_1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & n+3 & \cdots & 3(-1)^n s_n & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & n+3 & -(n+2)s_1 & (n+1)s_2 & \cdots & 0 \end{pmatrix}$$

is a polynomial of degree $n+2$ *in the variable* b *(as can be shown by induction) where the* **the elementary symmetric functions** $s_1, s_2, \ldots$ *are defined by*

$$h(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n,$$

see Dummit and Foote [10]. But the resultant of $g(x)$ *and* $g'(x)$ *equals to 0 if and only if* g *has repeated roots. Hence, the result holds.*

Similarly, there is only a finite number of c *such that* $g(x) = x^2\, h(x) + \frac{2}{c}$ *has repeated roots over* $\overline{k}$*.*

Example 3.1.1.1: $k = \mathbb{Q}$ **and** $N = g + 2$. We give a hyperelliptic curve such that the divisor at infinity has order $g + 2$. Let $h(x) = \prod_{i=0}^{n-1}(x - i)$. We show that $\mathcal{C} : y^2 = f(x)$ where

$$f(x) = h(x)\big(x^2 h(x) + 2\big)$$

is a hyperelliptic curve which has genus g, and $\mathrm{ord}(D_\infty) = g + 2$.

By the argument in the proof of Theorem 3.1.1.1 see equation (3.4), we conclude

that partial quotients are

$$a_0 = x^2 h(x) = x^3 \prod_{i=1}^{n-1}(x-i), \qquad a_1 = x,$$

and the divisor at infinity has order $g+2$. Let $g(x) = x^2 h(x) + 2$. It suffices to show that $g(x)$ has no repeated roots over $\mathbb{C}$. We will show that $g_j(x) = x^3 \prod_{i=1}^{j}(x-i) + 2$ has distinct roots over $\mathbb{C}$ for all j. For $j < 6$, we found that $g_j(x)$ has no repeated roots in $\mathbb{C}$, by direct computation (using, say, Maple).

Now, we use Rouché's Theorem, to show that for all $i \geq 5, g_j$ has only three zeros in the disk with radius $\frac{1}{2}$ and centered at 0, denoted by $D(0, \frac{1}{2})$. Let $h_j(x) = x^3 \prod_{i=1}^{j}(x-i)$ and $z \in \partial D(0, \frac{1}{2})$, consider

$$\begin{aligned} |h_j(z)| &\geq |z|^3 \prod_{i=n}^{n+j} \big|i - |z|\big| \\ &\geq |z|^3 \big|1-|z|\big|\big|2-|z|\big| \ldots \big|6-|z|\big| = 2.25 \\ &> 2 = |g_j(z) - h_j(z)|. \end{aligned}$$

Applying Rouché's Theorem, we have the number of zeros of g_j in $D(0, \frac{1}{2})$ counting multiplicities is equal to the number of zeros of h_j in $D(0, \frac{1}{2})$ counting multiplicities; thus, the number equals 3. Similarly we can use Rouché's Theorem to show that there is only one zero in each of the annuli $\{z \in \mathbb{C} : \frac{2s-1}{2} < |z| < \frac{2s+1}{2}\}$ for all $s = 1, ..., j$. Therefore the rest of the zeros of g_j are distinct. Notice that the graph of $g_j(x)$ is the graph of $h_j(x)$ shifted up by 2 units. But h_j has only $j-1$ turning points in $\mathbb{R}$. It follows that the number of roots of g_j in $\mathbb{R}$ is less than or equal to $j+1$. Since there are j distinct real roots outside the disk $D(0, \frac{1}{2})$, there is only one real root of g_j in $D(0, \frac{1}{2})$. Thus, in this disk g_j has one real root with multiplicity 3 or one real root and two complex roots. Since $g_j' = h_j'$, and this clearly has a root of multiplicity higher than 1 only at $x = 0$ whereas $g_j = h_j + 2$ does not has a root at $x = 0$. We now obtain that g_j has one real root and two complex roots in this disk. Hence, we conclude that g_j has no repeated roots over $\mathbb{C}$. $\square$

In fact, the above can be extended to any $h(x) = x\prod_{i=n}^{g+n-1}(x-i)$.

3.1.2 N=2g+1

We seek hyperelliptic curves $\mathcal{C}$ with genus g over the field k whose divisor at infinity is of order $N = 2g+1$.

Theorem 3.1.2.1 *Let $\mathcal{C}$ be a hyperelliptic curve with genus g over a field k, $char(k) = 0$ defined by*

$$y^2 = f(x).$$

Then $\mathcal{C}$ has a divisor at infinity of order $2g+1$ and the continued fraction expansion of y has period length 2 if and only if $f(x)$ is of the form

$$f(x) = (x-\alpha)\underbrace{\left((x-\alpha)h^2(x) + \frac{2}{c}\right)}_{g(x)}$$

where $c, \alpha \in k$, and $h(x), g(x)$ are polynomials in $k[x]$ such that $h(x)$ is monic and $g(x)$ has no repeated roots in $\overline{k}$.

Proof. ($\Longleftarrow$) Since $g(x)$ has no repeated root in $\overline{k}$ and clearly $x = \alpha$ is not a root of g, $f(x)$ has no repeated root in $\overline{k}$. It follows that the curve $\mathcal{C}$ is a hyperelliptic curve over k. It is not hard to see that the first and second partial quotients of the continued fraction of y are

$$a_0 = (x-\alpha)h(x), \text{ and } a_1 = c\,h(x).$$

where $h(x)$ is a monic polynomial in $k[x]$ with $\deg(h(x)) = g$ and c is a constant. It follows that

$$f(x) = a_0^2 + \frac{2a_0}{a_1}.$$

By Corollary 3.1.0.1, we obtain that the period length of the continued fraction of y is 2. By Theorem 2.4.0.4, we have

$$\text{ord}(D_\infty) = \deg(a_0) + \sum_{j=1}^{m}\deg(a_j)$$

where m is the quasi-period length of the continued fraction of y, and hence

$$\mathrm{ord}(D_\infty) = \deg(a_0) + \deg(a_1) = g + 1 + g = 2g + 1.$$

($\Longrightarrow$) Conversely, suppose $\mathcal{C}$ has a divisor at infinity of order $2g+1$ and the continued fraction expansion of y has period length 2. By Remark 2.4.0.2, we have

$$2g + 1 = \mathrm{ord}(D_\infty) = \deg(a_0) + \deg(a_1).$$

But $\deg(a_0) = g+1$. It follows that $\deg(a_1) = g$. By Corollary 3.1.0.1, there exist elements c, α in k and a monic polynomial $h(x)$ over k such that

$$a_0 = (x - \alpha)h(x), \qquad a_1 = c\,h(x),$$

and thus

$$f(x) = a_0^2 + \frac{2a_0}{a_1} = (x - \alpha)\Big((x - \alpha)h^2(x) + \frac{2}{c}\Big)$$

□

Remark 3.1.2.1 *In Theorem 3.1.2.1, since* $\sum_{j=0}^{m-1} \deg(a_i) = \mathrm{ord}(D_\infty) = N$ *and* $\deg(a_0) = g + 1 = \frac{N-1}{2} + 1 = \frac{N+1}{2}$, *we have*

$$\sum_{j=1}^{m-1} \deg(a_i) = \frac{N-1}{2}.$$

where m is the quasi-period length of the continued fraction of y. However, there are a number of different ways to partition $\frac{N-1}{2}$. In the above Theorem we choose the trivial partition, that is the partition of $\frac{N-1}{2}$ is $\frac{N-1}{2}$. There may be hyperelliptic curves with $\mathrm{ord}(D_\infty) = N = 2g + 1$ *corresponding to other partitions of $\frac{N-1}{2}$.*

Example 3.1.2.1: $k = \mathbb{Q}$ **and** $N = 2g + 2$. Let N be an odd positive integer. Let $k = \mathbb{Q}, \alpha \in k$. Claim: the curve $\mathcal{C} : y^2 = (x - \alpha)[(x - \alpha)^{2g+1} - 1]$ is a hyperelliptic curve with genus g and $\mathrm{ord}(D_\infty) = N = 2g + 1$.

Since $x^{2g+1} - 1$ has no repeated root in $\mathbb{C}$, we also have $g(x) = (x-\alpha)^{2g+1} - 1$ has no repeated roots in $\mathbb{C}$. And $x - \alpha$ is not a root of $g(x)$. Using Theorem 3.1.2.1, with $c = -2, h(x) = (x-\alpha)^{g-1}$ and $a_0 = (x-\alpha)^g$, we conclude that $\mathcal{C}$ is a hyperelliptic curve, as required. □

Knowledge of the order of D_∞ can be significant; indeed, McMullen [24] uses this order as a key, if simple, tool in his proof that the only "primitive Teichmüller curve" coming from an "abelian 1-form" with simple zeros on a genus 2 curve is generated by his "decagon form." (We will not delve into the background of this.) Here, we simply verify one of his calculations.

Example 3.1.2.2 [**McMullen's decagon family**] Consider the family of hyperelliptic curves over $\mathbb{C}$ given by

$$\begin{aligned} X_t : y^2 &= q_t(x) \\ &= x(-1 - 2t^5 - t^{10} + 25t^4x - 50t^3x^2 + 35t^2x^3 - 10t^2x^3 - 10tx^4 + x^5) \end{aligned}$$

We verify McMullen's Theorem 5.2: Each X_t has $\mathrm{ord}(D_\infty) = 5$. Fix t; since

$$f(x) = q_t(x) = x(x(x^2 - 5tx + 5t^2)^2 - (1 + t^5)^2)$$

using Theorem 3.1.2.1 with $\alpha = 0, c = \frac{-2}{(1+t^5)^2}$ and $h(x) = x^2 - 5tx + 5t^2$, we conclude that the divisor at infinity has the order 5 and the continued fraction expansion of $\sqrt{q_t(x)}$ is of period length 2, with partial quotients

$$a_0 = x(x^2 - 5tx + 5t^2) \quad \text{then} \quad a_1 = \frac{-2}{(1+t^5)^2}(x^2 - 5tx + 5t^2).$$

□

3.2. Restrictions on Partial Quotients

The purpose of this Section is to find bound on the degrees of consecutive pairs of the partial quotients a_j and improve the upper bound on the order N of divisor at infinity. Our main tool is the use of certain polynomial sequences. (We discovered these sequences by focusing on the leading coefficient of the partial quotients.)

3.2.1 The Polynomials f_j−Definition and Initial Results

The case of $m = n = 1$ is of the form $y^2 = a_0^2 + 1$, see Corollary 3.1.0.1. Hence in this Subsection, we always assume $m > 1$.

Definition 3.2.1.1 *Let $\mathcal{C}$ be a hyperelliptic curve defined by $y^2 = f(x)$ where $f(x)$ is a polynomial in $k[x]$ and $\deg(f(x)) = 2g+2$. Suppose that y has a periodic continued fraction expansion of a finite quasi-period length m. Define a sequence $\{f_j\}$ of polynomials in $k[x]$ as follows:*

$$f_1 = f(x) - a_0^2 \tag{3.5}$$

$$f_2 = 2a_0 - a_1 f_1 \tag{3.6}$$

$$f_3 = a_1 f_1 - a_1 a_2 f_2 - a_2 \tag{3.7}$$

$$f_4 = p'_1(p'_0 f_2 + q'_0 - a_3 f_3) - q'_2 \tag{3.8}$$

$$f_j = p'_{j-3}(p'_{j-4} f_{j-2} + p'_{-1} p'_0 \cdots p'_{j-6} q'_{j-4} - a_{j-1} f_{j-1}) - p'_{-1} p'_0 \cdots p'_{j-5} q'_{j-2} \tag{3.9}$$

for all $j = 5, \ldots, m$, where the p'_l and q'_l are as in (3.2).

Notice that the recursion for the various p'_l implies

$$p'_{l+1} \equiv p'_{l-1} \pmod{p'_l}$$

for all $l \in \mathbb{N}$.

Proposition 3.2.1.1 *The polynomial f_j is divisible by $p'_0 p'_1 \cdots p'_{j-4}$ for all $j = 4, \ldots, m$.*

Proof. By Equations (3.7) and (3.8), we have

$$f_4 = a_1\big[p'_1(q'_2 f_2 - a_3 f_1) + a_2 q'_2\big],$$

and hence f_4 is divisible by p'_0. Since p'_0 and p'_1 are relatively prime, it is enough to show that p'_0 and p'_1 divide f_5. Since $p'_0 = a_1$ divides f_4, and by Equations (3.7)-(3.9), we have

$$\begin{aligned} f_5 &\equiv p'_2(p'_1 f_3 + q'_1) \\ &\equiv p'_2(p'_1(-a_2) + q'_1) \\ &\equiv p'_2(-(a_2 a_1 + 1)a_2 + a_2) \\ &\equiv 0 \pmod{p'_0}, \end{aligned} \tag{3.10}$$

and

$$\begin{aligned} f_5 &\equiv p'_2(q'_1 - a_4 f_4) - p'_0 q'_3 \\ &\equiv p'_2(q'_1 - a_4(-q'_2)) - p'_0 q'_3 \\ &\equiv p'_2 q'_3 - p'_0 q'_3 \\ &\equiv 0 \pmod{p'_1}. \end{aligned} \tag{3.11}$$

If $f_3 = 0$, then by the definition of f_3, we obtain $p'_0 = a_1$ divides $q'_1 = a_2$ and so, (3.10) becomes

$$\begin{aligned} f_5 &\equiv p'_2(q'_1) \\ &\equiv 0 \pmod{p'_0}. \end{aligned}$$

Similarly, if $f_4 = 0$, then p'_1 divides q'_2 and hence (3.11) becomes

$$\begin{aligned} f_5 &\equiv p'_2 q'_1 - p'_0 q'_3 \\ &\equiv p'_0 q'_1 - p'_0 q'_3 \\ &\equiv p'_0(-a_4 q'_2) \\ &\equiv 0 \pmod{p'_1}. \end{aligned}$$

Now, we will show both that f_j is divisible by $p'_0p'_1\cdots p'_{j-4}$ and that p'_{j-6} divides $p'_{n-5}\frac{f_{j-3}}{p'_0\cdots p'_{j-8}}+q'_{j-5}$ for all $j \geq 6$, by using strong induction on j. Since both f_4 and f_5 are divisible by p'_0, from its definition by recursion, so is f_6. Since p'_1 and p'_2 are relatively prime, it remains to show that p'_1 and p'_2 divide $\frac{f_6}{p'_0}$. Consider

$$\begin{aligned}\frac{f_6}{a_1} &= p'_3(p'_2\frac{f_4}{a_1}+q'_2-a_5\frac{f_5}{a_1})-p'_1q'_4\\ &\equiv p'_3(p'_2\frac{f_4}{a_1}+q'_2) \qquad (3.12)\\ &\equiv p'_3(p'_0\frac{f_4}{a_1}+q'_2)\\ &\equiv p'_3(f_4+q'_2)\\ &\equiv 0 \pmod{p'_1}.\end{aligned}$$

If $f_4 = 0$, we know that $p'_1|q'_2$ and hence (3.12) becomes

$$\begin{aligned}\frac{f_6}{a_1} &\equiv p'_3(q'_2)\\ &\equiv 0 \pmod{p'_1}.\end{aligned}$$

We claim that p'_0 divides $p'_1f_3+q'_1$. Consider

$$\begin{aligned}p'_1f_3+q'_1 &= (a_2a_1+1)(a_1f_1-a_1a_2f_2-a_2)+a_2\\ &= a_1(p'_1(f_1-a_2f_2)-a_2^2).\end{aligned}$$

But $a_1 = p'_0$. We have the claim. This implies

$$\begin{aligned}\frac{f_5}{a_1}+q'_3 &= p'_2\Big(\frac{p'_1f_3+q'_1}{a_1}-a_4\frac{a_4f_4}{a_1}\Big)\\ &\equiv 0 \pmod{p'_2}. \qquad (3.13)\end{aligned}$$

Hence,

$$\begin{aligned}\frac{f_6}{a_1} &\equiv p'_3(q'_2 - a_5\frac{f_5}{a_1}) - p'_1q'_4\\ &\equiv p'_3(q'_2 + a_5q'_3) - p'_1q'_4\\ &\equiv q'_4(p'_3 - p'_1)\\ &\equiv 0 \pmod{p'_2}.\end{aligned}$$

By (3.13), we obtain that if $f_5 = 0$, then p'_2 divides q'_3 and hence

$$\begin{aligned}\frac{f_6}{a_1} &\equiv p'_3(q'_2) - p'_1q'_4\\ &\equiv p'_3q'_2 - p'_1q'_2\\ &\equiv q'_2(p'_3 - p'_1)\\ &\equiv 0 \pmod{p'_2}.\end{aligned}$$

Now, suppose that f_n is divisible by $p'_0p'_1\cdots p'_{n-4}$ and that p'_{n-6} divides $p'_{n-5}\frac{f_{n-3}}{p'_{-1}p'_0\cdots p'_{n-8}} + q'_{n-5}$ for all $n < j$. Accordingly, we set

$$h_n = \frac{f_n}{p'_0\cdots p'_{n-4}} \tag{3.14}$$

for all $n < j$. By Equation (3.9), it is not hard to see that $p'_0\cdots p'_{j-6}$ divides f_j. Since p'_{j-5} and p'_{j-4} are relatively prime, it suffices to show that p'_{j-4} and p'_{j-5} divide $\frac{f_j}{p'_1p'_0\cdots p'_{j-6}}$. Consider

$$\frac{f_j}{p'_0\cdots p'_{j-6}} = p'_{j-3}(p'_{j-4}h_{j-2} + q'_{j-4} - a_{j-1}p'_{j-5}h_{j-1}) - p'_{j-5}q'_{j-2} \tag{3.15}$$

To show that p'_{j-5} divides $\frac{f_j}{p'_0\cdots p'_{j-6}}$, we have

$$\begin{aligned}\frac{f_j}{p'_0\cdots p'_{j-6}} &\equiv p'_{j-3}(p'_{j-4}h_{j-2} + q'_{j-4})\\ &\equiv p'_{j-3}(p'_{j-6}h_{j-2} + q'_{j-4}) \pmod{p'_{j-5}}.\end{aligned}$$

Since p'_{j-7} divides $p'_{j-6}h_{j-4} + q'_{j-6}$, we obtain

$$\begin{aligned} p'_{j-6}h_{j-2} + q'_{j-4} &= \frac{1}{p'_{j-7}}\Big(p'_{j-5}\Big(p'_{j-6}h_{j-4} + q'_{j-6} - a_{j-3}p'_{j-7}h_{j-3}\Big) - p'_{j-7}q'_{j-4}\Big) + q'_{j-4} \\ &= \Big(p'_{j-5}\Big(\frac{p'_{j-6}h_{j-4} + q'_{j-6}}{p'_{j-7}} - a_{j-3}h_{j-3}\Big) - q'_{j-4}\Big) + q'_{j-4} \\ &\equiv 0 \pmod{p'_{j-5}}. \end{aligned}$$

We then conclude that p'_{j-5} divides $\frac{f_j}{p'_0 \cdots p'_{j-6}}$.

To show that p'_{j-4} divides f_j, we have

$$\begin{aligned} p'_{j-5}h_{j-3} + q'_{j-5} &= \frac{1}{p'_{j-8}}\Big(p'_{j-6}(p'_{j-7}h_{j-5} + q'_{j-7} - a_{j-4}p'_{j-8}h_{j-4}) - p'_{j-8}q'_{j-5}\Big) + q'_{j-5} \\ &= \Big(p'_{j-6}\Big(\frac{p'_{j-7}h_{j-5} + q'_{j-7}}{p'_{j-8}} - a_{j-4}h_{j-4}\Big) - q'_{j-5}\Big) + q'_{j-5} \\ &\equiv 0 \pmod{p'_{j-6}}. \end{aligned}$$

since $p'_{j-7}h_{j-5} + q'_{j-7}$ is divisible by p'_{j-8}. It follows that

$$\begin{aligned} p'_{j-5}h_{j-1} - q'_{j-3} &= \frac{1}{p'_{j-6}}\Big(p'_{j-4}(p'_{j-5}h_{j-3} + q'_{j-5} - a_{j-2}p'_{j-6}h_{j-2}) - p'_{j-6}q'_{j-3}\Big) + q'_{j-3} \\ &= \Big(p'_{j-4}\Big(\frac{p'_{j-5}h_{j-3} + q'_{j-5}}{p'_{j-6}} - a_{j-2}h_{j-2}\Big) - q'_{j-3}\Big) + q'_{j-3} \\ &\equiv 0 \pmod{p'_{j-4}}. \end{aligned} \tag{3.16}$$

By Equation (3.15),

$$\begin{aligned} \frac{f_j}{p'_{-1}p'_0 \cdots p'_{j-6}} &\equiv p'_{j-3}(q'_{j-4} - a_{j-1}p'_{j-5}h_{j-1}) - p'_{j-5}q'_{j-2} \\ &\equiv p'_{j-3}(q'_{j-4} + a_{j-1}q'_{j-3}) - p'_{j-5}q'_{j-2} \\ &\equiv q'_{j-2}(p'_{j-3} - p'_{j-5}) \\ &\equiv q'_{j-2}(a_{j-2}p'_{j-4}) \\ &\equiv 0 \pmod{p'_{j-4}}. \end{aligned}$$

If $h_{j-1} = 0$, then by (3.16), we have $p'_{j-4}|q'_{j-3}$ and therefore

$$\begin{aligned}\frac{f_j}{p'_{-1}p'_0\cdots p'_{j-6}} &\equiv p'_{j-3}q'_{j-4} - p'_{j-5}q'_{j-2}\\ &\equiv p'_{j-5}q'_{j-4} - p'_{j-5}q'_{j-2}\\ &\equiv p'_{j-5}(q'_{j-4} - q'_{j-2})\\ &\equiv p'_{j-5}(a_{j-1}q'_{j-3})\\ &\equiv 0 \pmod{p'_{j-4}}.\end{aligned}$$

□

3.2.2 The Polynomials f_j−Equivalent Formulation and Results

In this Subsection, we show that

$$\deg(a_j) + \deg(a_j - 1) \leq \deg(a_1) + g + 1$$

for all j.

Lemma 3.2.2.1 *We have*

$$f_1 = \frac{q'_{m-1}}{\kappa\, p'_{m-2}} \tag{3.17}$$

$$f_2 = \frac{\kappa\,(p'_{m-4})f_1 - q'_{m-3}}{p'_{m-3}} \tag{3.18}$$

$$f_3 = \frac{\kappa^{-1}(a_1f_2 + 1)p'_{m-5} - q'_{m-4}}{p'_{m-4}} \tag{3.19}$$

$$f_j = \frac{c_j(p'_{j-3}f_{j-1} + p'_{-1}p'_0\ldots p'_{j-5}q'_{j-3})p'_{m-(j+2)} - p'_{-1}p'_0\ldots p'_{j-4}q'_{m-(j+1)}}{p'_{m-(j+1)}}. \tag{3.20}$$

for all $j = 4, \ldots, m$, where $c_j = \kappa$ if j is even, and otherwise, $c_j = \kappa^{-1}$. We include $p'_{-1} = 1$ in our formulas for simplicity.

Proof. By Lemma 3.1.0.2, we have $y^2 = (a_0)^2 + \frac{q'_{m-1}}{p'_{m-2}}$. Then

$$f_1 = \frac{q'_{m-1}}{\kappa\, p'_{m-2}} \in k[x].$$

If $f_1 = 0$, then $f(x) = (a_0)^2$ is a square of complex polynomial which contradicts to the irreducibility of the curve $\mathcal{C}$. Then $f_1 \neq 0$. Since $q'_{m-1} = 2\kappa\, a_0 q'_{m-2} + q'_{m-3}$ and $p'_{m-2} = \kappa^{-1} a_1 p'_{m-2} + p'_{m-3}$, we have

$$2a_0 = \frac{(a_1 p'_{m-3} + \kappa\, p'_{m-4}) f_1 - q'_{m-3}}{\kappa\, q'_{m-2}}.$$

But $\kappa\, q'_{m-2} = p'_{m-3}$. Hence,

$$f_2 = \frac{\kappa\,(p'_{m-4}) f_1 - q'_{m-3}}{p'_{m-3}} \in k[x] \tag{3.21}$$

We rewrite the equation (3.21) as

$$\kappa\, p'_{m-4} f_1 = f_2 p'_{m-3} + q'_{m-3}$$

Since $p'_{m-3} = a_{m-2} p'_{m-4} + p'_{m-5} = \kappa\, a_2 p'_{m-4} + p'_{m-5}$ and $\kappa\, q'_{m-2} = p'_{m-3}$, we have

$$q'_{m-3} = \frac{q'_{m-2} - q'_{m-4}}{\kappa^{-1} a_1} = \frac{p'_{m-3} - \kappa\, q'_{m-4}}{a_1} = \frac{\kappa\, a_2 p'_{m-4} + p'_{m-5} - \kappa\, q'_{m-4}}{a_1}.$$

It follows that

$$a_1 f_1 = a_1 a_2 f_2 + a_2 + \frac{\kappa^{-1}(a_1 f_2 + 1) p'_{m-5} - q'_{m-4}}{p'_{m-4}}.$$

Therefore,

$$f_3 = \frac{\kappa^{-1}(a_1 f_2 + 1) p'_{m-5} - q'_{m-4}}{p'_{m-4}} \in k[x]. \tag{3.22}$$

We rewrite the equation (3.22) as

$$f_3 p'_{m-4} = \kappa^{-1}(a_1 f_2 + 1) p'_{m-5} - q'_{m-4}.$$

But

$$q_{m-4} = \frac{(a_2 a_3 + 1) p'_{m-5} + \kappa\, a_2 p'_{m-6} - a_1 q'_{m-5}}{\kappa\,(a_1 a_2 + 1)}.$$

It follows that

$$(a_1 a_2 + 1)(a_1 f_2 + 1 - a_3 f_3) - (a_2 a_3 + 1) = \frac{\kappa((a_1 a_2 + 1) f_3 + a_2) p'_{m-6} - a_1 q'_{m-5}}{p'_{m-5}}.$$

Hence,

$$f_4 = \frac{\kappa((a_1a_2+1)f_3 + a_2)p'_{m-6} - a_1q'_{m-5}}{p'_{m-5}} = \frac{(p'_2f_3 + p'_{-1}q'_2)p'_{m-6} - p'_{-1}p'_0q'_{m-5}}{p'_{m-5}}. \tag{3.23}$$

By induction whose main step is completely analogous to the above, we have

$$f_j = \frac{c_j\,(p'_{j-3}f_{j-1} + p'_0\cdots p'_{j-5}q'_{j-3})p'_{m-(j+2)} - p'_0\cdots p'_{j-4}q'_{m-(j+1)}}{p'_{m-(j+1)}}.$$

where $j \le m$, and $c_j = \begin{cases} \kappa & \text{if } j \text{ is even,} \\ \kappa^{-1} & \text{otherwise.} \end{cases}$ □

Theorem 3.2.2.1 *For each* $j,\ 1 < j \le m$,

$$f_j = 0 \quad \textit{if and only if} \quad \deg(a_0) + \deg(a_1) = \deg(a_{j-1}) + \deg(a_j). \tag{3.24}$$

Furthermore, if $f_j \neq 0$, *then* $\deg(a_0) + \deg(a_1) > \deg(a_{j-1}) + \deg(a_j)$, *and*

$$\deg(f_j) = \deg(a_0) + (j-3)\deg(a_1) + (j-4)\deg(a_2) + \cdots + \deg(a_{j-3}) - \deg(a_{j-1}) - \deg(a_j) = \frac{(j-3)(j-2)}{2}$$

Proof. When $j = 2$, by Equation (3.18), we have

$$f_2 = \frac{\kappa\,(p'_{m-4})f_1 - q'_{m-3}}{p'_{m-3}}.$$

Suppose that $f_2 = 0$. Since $\deg(f_1) = \deg(a_0) - \deg(a_1), p'_{m-4} = a_{m-3}\cdots a_1 +$lower order terms, and $q'_{m-3} = a_{m-2}\cdots a_2 +$ lower order terms, we have

$$\deg(\kappa\,(p'_{m-4})f_1) = \deg(q'_{m-3})$$
$$\deg(a_{m-3}) + \cdots + \deg(a_1) + \deg(a_0) - \deg(a_1) = \deg(a_{m-2}) + \cdots + \deg(a_2)$$
$$\deg(a_0) = \deg(a_2).$$

If $\deg(a_0) = \deg(a_2)$, then since $\deg(q'_{m-3}) < \deg(p'_{m-3})$, and $\deg((p'_{m-4})f_1) = \deg(q'_{m-3})$, we conclude that $f_2 = 0$, and $m = 2$. Similarly, if $f_2 \neq 0$, then

$$\deg(f_2) = \deg(a_0) - \deg(a_1) - \deg(a_2).$$

When $j = 3$, by Equation (3.19), we have

$$f_3 = \frac{\kappa^{-1}(a_1 f_2 + 1)p'_{m-5} - q'_{m-4}}{p'_{m-4}}.$$

Suppose that $f_3 = 0$. Since $\deg(f_2) = \deg(a_0) - \deg(a_1) - \deg(a_2)$, $p'_{m-5} = a_{m-4} \cdots a_1 +$ lower order terms, and $q'_{m-4} = a_{m-3} \cdots a_2 +$ lower order terms, we have

$$\begin{aligned}\deg(\kappa^{-1}(a_1 f_2 + 1)p'_{m-5}) &= \deg(a_1) + \deg(a_0) - \deg(a_1) - \deg(a_2) + \deg(a_{m-4}) + \cdots + \deg(a_1) \\ &= \deg a_0 + \deg(a_1) + \deg(a_{m-4}) + \cdots + \deg(a_3),\end{aligned}$$

and hence

$$\deg(a_0) + \deg(a_1) = \deg(a_2) + \deg(a_3).$$

If $\deg(a_0) + \deg(a_1) = \deg(a_2) + \deg(a_3)$, then since $\deg(q'_{m-4}) < \deg(p'_{m-4})$, and $\deg(\kappa^{-1}(a_1 f_2 + 1)p'_{m-5}) = \deg(q'_{m-4})$, we conclude that $f_3 = 0$. Similarly, if $f_3 \neq 0$, then we obtain

$$\deg(f_3) = \deg(a_0) - \deg(a_2) - \deg(a_3) \quad \text{and} \quad \deg(a_0) + \deg(a_1) > \deg(a_2) + \deg(a_3).$$

When $j = 4$, by Equation (3.20), we have

$$f_4 = \frac{\kappa((a_1 a_2 + 1)f_3 + a_2)p'_{m-6} - a_1 q'_{m-5}}{p'_{m-5}}.$$

Suppose that $f_4 = 0$. If $f_3 = 0$, then $\deg(a_0) + \deg(a_1) = \deg(a_2) + \deg(a_3), / a_2 p'_{m-6} = a_1 q'_{m-5}$, and so

$$\begin{aligned}0 &= \deg(a_2) + \deg(p'_{m-6}) - \deg(a_1) - \deg(q'_{m-5}) \\ &= \deg(a_2) - \deg(a_{m-4}) \\ &= \deg(a_0) + \deg(a_1) - \deg(a_3) - \deg(a_4),\end{aligned}$$

since $p'_{m-6} = a_{m-5}\cdots a_1 +$lower order terms, and $q'_{m-5} = a_{m-4}\cdots a_2 +$lower order terms, Suppose $f_3 \neq 0$. Then $\deg(f_3) = \deg(a_0) - \deg(a_2) - \deg(a_3)$. we have

$$\begin{aligned}\deg(\kappa((a_1a_2+1)f_3+a_2)p'_{m-6}) &= \deg((a_1a_2+1)f_3) + \deg(p'_{m-6})\\ &= \deg(a_1) + \deg(a_2) + \deg(a_0) - \deg(a_2) - \deg(a_3)\\ &+ \deg(a_{m-5}) + \cdots + \deg(a_1)\\ &= \deg a_0 + 2\deg(a_1) + \deg(a_2) + \deg(a_{m-5}) + \cdots + \deg(a_4),\end{aligned}$$

and

$$\deg(a_1q'_{m-5}) = \deg(a_1) + \deg(a_{m-4}) + \cdots + \deg(a_2).$$

It follows that

$$\deg(a_0) + \deg(a_1) = \deg(a_3) + \deg(a_4).$$

If $\deg(a_0) + \deg(a_1) = \deg(a_3) + \deg(a_4)$, then since $\deg(q'_{m-4}) < \deg(p'_{m-4})$, and $\deg(\kappa((a_1a_2+1)f_3+a_2)p'_{m-6}) = \deg(a_1q'_{m-5})$, we conclude that $f_4 = 0$. Similarly, if $f_4 \neq 0$, then we obtain

$$\deg(f_4) = \deg(a_0)+\deg(a_1)-\deg(a_3)-\deg(a_4) \quad \text{and} \quad \deg(a_0)+\deg(a_1) > \deg(a_3)+\deg(a_4).$$

Suppose that the statement (3.24) holds when $j = r-1$, and if $f_{r-1} \neq 0$, then

$$\begin{aligned}\deg(f_{r-1}) &= \deg(a_0) + (r-4)\deg(a_1) + (r-5)\deg(a_2)\\ &+ \cdots + \deg(a_{r-4}) - \deg(a_{r-2}) - \deg(a_{r-1})\end{aligned}$$

and

$$\deg(a_0) + \deg(a_1) \geq \deg(a_{r-2}) + \deg(a_{r-1}),$$

and the equality holds if and only if $f_{r-1} = 0$.

Now, suppose that $f_r = 0$. By Equation (3.20), we have

$$c_r(p'_{r-3}f_{r-1} + p'_0\ldots p'_{r-5}q'_{r-3})p'_{m-(r+2)} = p'_0\ldots p'_{r-4}q'_{m-(r+1)} \tag{3.25}$$

We see that

$$\begin{aligned}\deg(p'_{r-3}f_{r-1}) &= \deg(p'_{r-3}) + \deg(f_{r-1}) \\ &= \deg(a_{r-2}) + \cdots + \deg(a_1) + \deg(a_0) + (r-4)\deg(a_1) \\ &+ (r-3)\deg(a_2) + \cdots + \deg(a_{r-4}) - \deg(a_{r-2}) - \deg(a_{r-1}) \\ &= \deg(a_0) + (r-3)\deg(a_1) + \cdots + 2\deg(a_{r-4}) + \deg(a_{r-3}) \\ &- \deg(a_{r-1}),\end{aligned}$$

and

$$\begin{aligned}\deg(p'_0 \ldots p'_{r-5}q'_{r-3}) &= \deg(p'_0) + \deg(p'_1) + \cdots + \deg(p'_{r-5}) + \deg(q_{r-3}) \\ &= \deg(a_1) + \deg(a_2) + \deg(a_1) + \cdots + \deg(a_{r-4}) + \cdots + \deg(a_1) \\ &+ \deg(a_{r-2}) + \cdots + \deg(a_2) \\ &= \deg(a_{r-2}) + (r-4)\deg(a_1) + (r-4)\deg(a_2) + \cdots + \deg(a_{r-3}).\end{aligned}$$

But $\deg(a_0) + \deg(a_1) - \deg(a_{r-1}) \geq \deg(a_{r-2})$. It follows that

$$\deg(p'_{r-3}f_{r-1}) \geq \deg(p'_0 \ldots p'_{r-5}q'_{r-3}),$$

and the equality holds if and only if $f_{r-1} = 0$. Similarly,

$$\deg(p'_{m-(r+2)}) - \deg(q'_{m-(r+1)}) = \deg(a_1) - \deg(a_{m-r}),$$

and

$$\deg(p'_0 \ldots p'_{r-4}) = (r-3)\deg(a_1) + (r-4)\deg(a_2) + \cdots + \deg(a_{r+3})$$

Hence,

$$\deg(a_0) + \deg(a_1) = \deg(a_{r-1}) + \deg(a_r).$$

Now, suppose that $\deg(a_0)+\deg(a_1) = \deg(a_{r-1})+\deg(a_r)$. We know $\deg(q'_{m-(r+1)}) < \deg(p'_{m-(r+1)})$. This implies

$$c_r(p'_{r-3}f_{r-1} + p'_0 \ldots p'_{r-5}q'_{r-3})p'_{m-(r+2)} = p'_0 \ldots p'_{r-4}q'_{m-(r+1)}.$$

It follows that $f_r = 0$. By the same argument, if $f_r \neq 0$, then

$$\deg(f_r) = \deg(a_0) + (r-3)\deg(a_1) + (r-4)\deg(a_2)$$
$$+ \cdots + \deg(a_{r-3}) - \deg(a_{r-1}) - \deg(a_r)$$

and

$$\deg(a_0) + \deg(a_1) > \deg(a_{r-1}) + \deg(a_r).$$

□

When m is the quasi-period length, both $a_m = 2\kappa\, a_0$, and $a_{m-1} = \kappa^{-1} a_1$. Hence, the following corollary is immediate from Theorem 3.2.2.1.

Corollary 3.2.2.1 *If m is a quasi-period length of the continued fraction expansion of y, then $f_m = 0$.*

Remark 3.2.2.1 *The converse of Corollary 3.2.2.1 holds when genus $g = 1$ but does not hold in general. We show this with a counterexample, using a curve found by Franck Leprévost [21]. (He computed the order of the divisor at infinity without using continued fractions.)*

Example 3.2.2.1: Vanishing of f_j with $j < m$. Let $\mathcal{C}$ be a hyperelliptic curve over $k = \mathbb{Q}$ given by

$$y^2 = 4x^6 - 4x^5 + x^4 - 8x^3 + 20x^2 - 16x + 4.$$

Note that one could easily give a version of this example in the form $y^2 = f(x)$ where $f(x)$ is monic. This curve has the order of divisor at infinity 29 and the continued fraction of y has a quasi-period length 22. The following are partial quotients of this continued

fraction:

$$a_0 = 2x^3 - x^2 - 2 \qquad a_1 = \frac{1}{4}x + \frac{1}{8} \qquad a_2 = 8x + 8$$
$$a_3 = -\frac{1}{8}x^2 + \frac{1}{16}x \qquad a_4 = -8x^2 - 4x - 4 \qquad a_5 = \frac{1}{4}x + \frac{1}{4}$$
$$a_6 = 4x - 2 \qquad a_7 = -\frac{1}{4}x \qquad a_8 = -4x - 2$$
$$a_9 = \frac{1}{2}x - \frac{1}{2} \qquad a_{10} = x + \frac{3}{2} \qquad a_{11} = -2x^2$$
$$a_{12} = x + \frac{3}{2} \qquad a_{13} = \frac{1}{2}x - \frac{1}{2} \qquad a_{14} = -4x - 2$$
$$a_{15} = -\frac{1}{4}x \qquad a_{16} = 4x - 2 \qquad a_{17} = \frac{1}{4}x + \frac{1}{4}$$
$$a_{18} = -8x^2 - 4x - 4 \qquad a_{19} = -\frac{1}{8}x^2 + \frac{1}{16}x \qquad a_{20} = 8x + 8$$
$$a_{21} = \frac{1}{4}x + \frac{1}{8} \qquad a_{22} = 2(2x^3 - x^2 - 2)$$

Here, genus $g = 2$, and since

$$4 = 2 + 2 = \deg(a_{j-1}) + \deg(a_j) = \deg(a_0) + \deg(a_1) = 3 + 1 = 4,$$

we have $j = 4$. Applying Theorem 3.2.2.1, we have $f_4 = 0$. Notice that $\lfloor \frac{22}{4} \rfloor - 1 = 4$. □

3.2.3 The Polynomials h_j

We return to the h_j in the equation (3.14). In this Subsection, we improve our bound on degrees of consecutive partial quotients.

Definition 3.2.3.1 *Let $\mathcal{C}$ be a hyperelliptic curve defined by $y^2 = f(x)$ where $f(x)$ is a monic polynomial in $k[x]$ and $\deg(f(x)) = 2g+2$. Suppose that y has a periodic continued fraction expansion of finite quasi-period length m. Set $h_1 = f_1$, and $h_2 = f_2$. Define h_j as follows:*

$$\begin{aligned} h_j &= \frac{f_j}{p'_{-1}p'_0p'_1 \cdots p'_{j-4}} \\ &= \frac{c_j\left(a_{j-2}h_{j-1} + \frac{p'_{j-5}h_{j-1}+q'_{j-3}}{p'_{j-4}}\right)p'_{m-(j+2)} - q'_{m-(j+1)}}{p'_{m-(j+1)}} \end{aligned} \tag{3.26}$$

for $j = 3, \ldots, m$, where $c_j = \kappa$ if j is even, and otherwise, $c_j = \kappa^{-1}$. Then each h_j is a polynomial in $k[x]$, due to Proposition 3.2.1.1.

Lemma 3.2.3.1 *We have*

$$\deg(h_1) = \deg(a_0) - \deg(a_1),$$
$$\deg(h_2) = \deg(a_0) - \deg(a_1) - \deg(a_2)$$
$$\deg(h_j) = \deg(a_0) - \deg(a_{j-1}) - \deg(a_j),$$

for all $j = 3, \ldots, m-1$ whenever $h_j \neq 0$, and

$$\deg(a_j) + \deg(a_{j-1}) = \deg(a_1) + g + 1 \quad \textit{if and only if} \quad h_j = 0.$$

Furthermore, $h_m = 0$, and $h_{m-j+1} = h_j$, for all $j = 2, \ldots, m-1$.

Proof. One shows the palindromic property $h_{m-j+1} = h_j$, for all $j = 2, \ldots, m-1$ by using both $h_m = 0$ and the relationship of h_j to h_{j-1} given in Equation (3.26). We note that h_{m-2} is related to h_{m-3} as h_3 is to h_2 and that such a relationship holds for (h_{m+1-j}, h_{m-j}) to (h_{2+j}, h_{1+j}) for values of j until we find an equality at the midpoint (depending on parity). The rest of this Lemma follows from Theorem 3.2.2.1 and its Corollary. □

Remark 3.2.3.1 *This Lemma gives very interesting bounds on the degree of partial quotients:*

$$\deg(a_j) + \deg(a_j) \leq g + 1 \tag{3.27}$$

whenever $h_j \neq 0$. We use this in order to construct a hyperelliptic curve over k of given g and N and improve the upper bound on N.

Example 3.2.3.2: Impossible sequence of partial quotients Is it possible to have a periodic continued fraction expansion $[x^{g+1}; x^g, x^g, \ldots]$?

Solution. Here, $a_0 = x^{g+1}$ and $a_1 = x^g$. We see that a_1 divides a_0. In fact

$$h_2 = 2a_0 - a_1\, h_1.$$

We obtain that a_1 divides h_2. But

$$\deg(h_2) = \delta_0 - \delta_1 - \delta_2 \geq 0.$$

So $h_2 = 0$. Therefore, the answer is yes, only for $[x^{g+1}; \overline{x^g, 2\,x^{g+1}}]$. □

Corollary 3.2.3.1 to Lemma 3.2.3.1 *Let $\mathcal{C}$ be a hyperelliptic curve with genus g defined by $y^2 = f(x)$ where $f(x)$ is a monic polynomial in $k[x]$ and $\deg(f(x)) = 2g + 2$. Suppose the quasi-period length of the continued fraction of y is $m > 1$ and the degree of the second partial quotient a_1 is g. Then the sequence $\{h_j\}$ of polynomials in $k[x]$ satisfies*

$$\mathrm{lc}(h_1) = \frac{2}{\mathrm{lc}(a_1)}, \quad \mathrm{lc}(h_j) = \frac{2}{\mathrm{lc}(a_{j-1})\mathrm{lc}(a_j)}$$

for all $j = 2, \ldots, m-1$, and $h_m = 0$.

Although Example 3.2.2.1 shows that h_j can vanish for $j < m$, we can show that such vanishing is isolated in the sequence $\{h_j : j = 1, \ldots, m\}$.

(After this dissertation was defended, we noticed that the proof of the following result is flawed. Furthermore, if $n = m = 2(j-1)$ one always has $h_{j-1} = 0$ implies $h_j = 0$. We still conjecture with great optimism that the proposition holds when $j < \frac{m}{2}$.)

Proposition 3.2.3.1 *There are no consecutive zero polynomials in the sequence $\{h_j : j = 1, \ldots, m\}$.*

Proof. Since $\mathcal{C}$ is a hyperelliptic curve, h_1 does not vanish. When $m = 1$, we obtain $f_1 \neq 0$. When $m = 2$, we have $h_1 \neq 0$ and $h_2 = 0$ since $h_1 = f_1 \neq 0$ and $h_2 = f_2 = 0$ if and only if $m = 2$, When $m = 3$, we obtain $h_1 \neq 0, h_2 \neq 0$, and $h_3 = 0$ since $h_1 = f_1 \neq 0$ and $h_2 = f_2 = 0$ if and only if $m = 2$.

Assume that $m \geq 4, h_3 = 0$ and $h_4 = 0$. By definition of $\{h_j\}$, we have

$$p'_{m-5} = q'_{m-4} \tag{3.28}$$

$$\frac{\kappa a_2}{a_1} p'_{m-6} = q'_{m-5} \tag{3.29}$$

Also, by Theorem 3.2.2.1,

$$\deg(a_0) + \deg(a_1) = \deg(a_2) + \deg(a_3)$$

$$\deg(a_0) + \deg(a_1) = \deg(a_3) + \deg(a_4).$$

It follows that $\deg(a_2) = \deg(a_4)$. By Equation (3.28) and Equation (3.29), we have

$$a_4 p'_{m-6} + p'_{m-7} = a_3 q'_{m-5} + q'_{m-6}$$

$$\Big(a_4 - a_3 \frac{\kappa a_2}{a_1}\Big) p'_{m-6} = q'_{m-6} - p'_{m-7}.$$

But $\deg(p'_{m-6}) > \deg(q'_{m-6})$ and $\deg(p'_{m-6}) > \deg(p'_{m-7})$. This implies

$$a_4 = a_3 \frac{\kappa a_2}{a_1},$$

and so

$$\deg(a_4) = \deg(a_3) + \deg(a_2) - \deg(a_1) = \deg(a_0).$$

Also, $\deg(a_2) = \deg(a_4) = \deg(a_0)$. But $m \geq 4$, hence $\deg(a_2) < \deg(a_0)$. This gives a contradiction.

Now, suppose that $2 < m \geq j$ $h_{j-1} = 0$ and $h_j = 0$. By definition of $\{h_j\}$, we have

$$\frac{c q'_{j-4}}{p'_{j-5}} p'_{m-(j+1)} = q'_{m-j} \tag{3.30}$$

$$\frac{c^{-1} q'_{j-3}}{p'_{j-4}} p'_{m-(j+2)} = q'_{m-(j+1)} \tag{3.31}$$

Also, by Theorem 3.2.2.1,

$$\deg(a_0) + \deg(a_1) = \deg(a_{j-2}) + \deg(a_{j-1})$$

$$\deg(a_0) + \deg(a_1) = \deg(a_{j-1}) + \deg(a_j),$$

and hence $\deg(a_{j-2}) = \deg(a_j)$. By Equation (3.30) and Equation (3.31), we have

$$\frac{c_j q'_{j-4}}{p'_{j-5}}(a_j\, p'_{m-(j+2)} + p'_{m-(j+3)}) = a_{m-(j-1)}q'_{m-(j+1)} + q'_{m-(j+2)}$$
$$\Big(\frac{c_j q'_{j-4}}{p'_{j-5}}a_j - \frac{c_j^{-1}q'_{j-3}}{p'_{j-4}}a_{j-1}\Big)p'_{m-(j+2)} = q'_{m-(j+2)} - \frac{c_j q'_{j-4}}{p'_{j-5}}p'_{m-(j+2)}.$$

But $\deg(LHS) > \deg(RHS)$. This implies

$$\deg\Big(\frac{c_j q'_{j-4}}{p'_{j-5}}a_j\Big) = \deg\Big(\frac{c_j^{-1}q'_{j-3}}{p'_{j-4}}a_{j-1}\Big)$$
$$\deg(a_{j-3}) + \deg(a_j) = \deg(a_{j-2}) + \deg(a_{j-1})$$
$$\deg(a_{j-3}) + \deg(a_j) = \deg(a_0) + \deg(a_1).$$

But $\deg(a_j) = \deg(a_{j-2})$. We then conclude that $h_{j-2} = 0$. By the same argument, we can show that $h_n = 0$ for all $n \le j \le m$, which contradict to $f_2 \neq 0$ if $m \neq 2$. □

3.2.4 Upper Bound on N in terms of Genus and Quasi-Period Length

We have bounds on degrees of consecutive partial quotients both when $h_j \neq 0$ and when $h_j = 0$; since also $h_j = 0$ implies $h_{j-1}h_{j+1} \neq 0$, a case-by-case analysis gives our improved upper bound on N.

Theorem 3.2.4.1 *Let m be a quasi-period of the continued fraction of y for the hyperelliptic curve $\mathcal{C}$ over a field k. Suppose r is the smallest number such that $h_r = 0$. Then*

$$\mathrm{ord}(D_\infty) \le \begin{cases} \Big(\lfloor \frac{m}{2} \rfloor + 1\Big)g + \lfloor \frac{m+1}{2} \rfloor & \text{if } r = m, \\ \Big(\frac{m}{2} + \lceil \frac{m}{4} \rceil\Big)g + \frac{m}{2} - \lceil \frac{m}{4} \rceil & \text{if } r < m \text{ and } m \text{ is even}, \\ \Big(\lfloor \frac{m}{2} \rfloor + \lceil \frac{m}{4} \rceil + 1\Big)g + \lfloor \frac{m}{2} \rfloor - \lceil \frac{m}{4} \rceil & \text{if } r < m, \text{ and } m \text{ is odd}. \end{cases}$$

Proof. If $m = 1$, then

$$N = \mathrm{ord}(D_\infty) = g + 1 = \Big(\Big\lfloor \frac{m}{2} \Big\rfloor + 1\Big)g + \Big\lfloor \frac{m+1}{2} \Big\rfloor.$$

Let δ_j denote $\deg(a_j)$ for all $j = 0, \ldots, m$ and $N = \mathrm{ord}(D_\infty)$. By Theorem 2.4.0.4, we have

$$N = g + 1 + 2\sum_{j=1}^{\lfloor \frac{m}{2} \rfloor} \delta_j, \tag{3.32}$$

if m is odd, and otherwise,

$$N = g + 1 + \delta_{\frac{m}{2}} + 2\sum_{j=1}^{\frac{m}{2}-1} \delta_j. \tag{3.33}$$

If $m = 2$, then

$$N = \deg(a_0) + \deg(a_1) \leq 2g + 1.$$

Since $h_2 = 0$ if and only if $m = 2$, suppose $m > 2$. If $s < \frac{m}{2}$ satisfies $h_s = 0$, then

$$\delta_s + \delta_{s+1} \leq g + 1$$

since $h_{s+1} \neq 0$; this follows from Proposition 3.2.3.1.

Now, suppose that $h_j = 0$ for all $j = j_1, \ldots, j_s$ and j_s is less than or equal to $\lfloor \frac{m}{2} \rfloor$. Since $\delta_{j-1} + \delta_j \leq g+1$ for all $j = 2, \ldots, m$ except $j = j_1, \ldots, j_s$, and $\delta_{j-1} + \delta_j = g+1+\delta_1$ for all $j = j_1, \ldots, j_s$, we have

$$\delta_1 + 2\sum_{j=2}^{\lfloor \frac{m}{2} \rfloor - 1} \delta_j + \delta_{\lfloor \frac{m}{2} \rfloor} \leq \Big(\Big\lfloor \frac{m}{2} \Big\rfloor - 1 \Big)\Big(g + 1\Big) + \delta_1 \tag{3.34}$$

Case 1: m is even. By Equation (3.33) and Equation (3.34), we obtain

$$\begin{aligned} N &= g + 1 + \delta_{\frac{m}{2}} + 2\sum_{j=1}^{\frac{m}{2}-1} \delta_j \\ &\leq \frac{m}{2}(g+1) + (s+1)\delta_1. \end{aligned}$$

If $s = 0$, then we conclude that

$$N \leq \Big(\frac{m}{2} + 1\Big)g + \frac{m}{2} = \Big(\Big\lfloor \frac{m}{2} \Big\rfloor + 1\Big)g + \left\lfloor \frac{m+1}{2} \right\rfloor.$$

If $s \neq 0$, then we conclude that

$$N \leq \Big(\frac{m}{2} + \Big\lceil \frac{m}{4} \Big\rceil \Big)g + \frac{m}{2} - \Big\lceil \frac{m}{4} \Big\rceil$$

since $\delta_1 \leq g-1$, and $s \leq \lceil \frac{m}{4} \rceil - 1$.

Case 2: m is odd. By Equation (3.33) and Equation (3.34), we obtain

$$\begin{aligned} N &= g+1+2\sum_{j=1}^{\lfloor \frac{m}{2} \rfloor} \delta_j \\ &\leq \left\lfloor \frac{m}{2} \right\rfloor (g+1) + (s+1)\delta_1 + \delta_{\lfloor \frac{m}{2} \rfloor}. \end{aligned}$$

If $s=0$, then we conclude that

$$N \leq \Big(\left\lfloor \frac{m}{2} \right\rfloor + 1 \Big) g + \left\lfloor \frac{m+1}{2} \right\rfloor$$

since $\delta_1 + \delta_{\frac{m}{2}} \leq g+1$. If $s \neq 0$, then we conclude that

$$N \leq \Big(\left\lfloor \frac{m}{2} \right\rfloor + \left\lceil \frac{m}{4} \right\rceil + 1 \Big) g + \left\lfloor \frac{m}{2} \right\rfloor - \left\lceil \frac{m}{4} \right\rceil$$

since $s \leq \lceil \frac{m}{4} \rceil - 1, \delta_{\lfloor \frac{m}{2} \rfloor} \leq g$, and $\delta_1 \leq g-1$. □

3.2.5 Application when $g = 1$

We show that the coefficients of a_0 and a_1 act as parameters when $g = 1$.

Corollary 3.2.5.1 to Lemma 3.2.3.1 *Let $\mathcal{C}$ be an elliptic curve defined by $y^2 = f(x)$ where $f(x)$ is a monic polynomial in $k[x]$ and $\deg(f(x)) = 4$. Suppose the quasi-period length of the continued fraction of y is $m > 1$. Then the sequence $\{h_j\}$ of polynomials in $k[x]$ such that*

$$\mathrm{lc}(h_1) = \frac{2}{\mathrm{lc}(a_1)} \neq 0, \quad h_j = \frac{2}{\mathrm{lc}(a_{j-1})\mathrm{lc}(a_j)} \neq 0$$

for all $j = 2, \ldots, m-1$, and $h_m = 0$.

Corollary 3.2.5.2 to Lemma 3.2.3.1 *Let $\mathcal{C}$ be an elliptic curve defined by $y^2 = f(x)$ where $f(x)$ is a monic polynomial in $k[x]$ and $\deg(f(x)) = 4$. Suppose the period length of the continued fraction of y is $n > 1$. Then for each $j \leq 2$, a_j can be expressed in the variables of the coefficients of a_0 and a_1, where*

$$y = [a_0, \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}\ ].$$

Proof: Let m be the quasi-period length of the continued fraction y. If $m = 2$, then $y = [a_0, \overline{a_1, 2a_0}\,]$, so we're done. If $m = 3$, then

$$y = [a_0, \overline{a_1, a_1, 2a_0}\,] \text{ or } \; y = [a_0, \overline{a_1, \kappa^{-1}a_1, 2\kappa a_0, \kappa^{-1}a_1, a_1, 2a_0}\,],$$

so we're done.

Assume $m > 3$. Let $a_0 = x^2 + \beta x + \gamma$, and $a_j = l_j x + k_j$ where $\alpha \neq 0$, $l_j \neq 0, \beta, \gamma, l_j, k_j \in \mathbb{C}$ for all $j = 1, \ldots, m-1$. By the definition of the sequence f_j, we have

$$2a_0 = a_1 f_1 + 2, \quad \text{and} \quad a_1 f_1 = a_2(a_1 f_2 + 1) + f_3,$$

so a_1 divides $a_2 + f_3$ in $k[x]$. But $\deg(a_1) = 1 = \deg(a_2)$. This gives

$$f_3 = s\, a_1 - a_2, \quad \text{where} \;\; s = \frac{l_2}{l_1}.$$

It follows that

$$f_1 = a_2 f_2 + s = \frac{2a_0 a_2 + s}{a_1 a_2 + 1} \tag{3.35}$$

and

$$f_2 = \frac{2a_0 - s\, a_1}{a_1 a_2 + 1} = \frac{2}{l_1 l_2}. \tag{3.36}$$

Now, we will show that f_1, f_2 and a_2 can be expressed in the variables of coefficients of a_0 and a_1. Since $\deg(f_2) = 0$, and by the equation (3.35) we see that $f_2 = \frac{2\alpha}{l_1 l_2}$, and so

$$\frac{2\alpha}{l_1 l_2}(k_1 l_2 + k_2 l_1) = 2\beta - l_2 \tag{3.37}$$

$$\frac{2\alpha}{l_1 l_2}(k_1 k_2 + 1) = 2\gamma - \frac{l_2 k_1}{l_1} \tag{3.38}$$

If $k_1 = 0$, then by the equations (3.37) and (3.38), we obtain

$$l_2 = \frac{1}{\gamma l_1}, \quad \text{and} \quad k_2 = \frac{l_2}{2}(2\beta - l_2) = \frac{\beta}{\gamma l_1} - \frac{1}{2\gamma^2 l_1^2},$$

and we also find that

$$f_1 = \frac{2}{l_1}x + \frac{2\beta}{l_1} \quad \text{and} \quad f_2 = \frac{2}{l_1 l_2} = 2\gamma.$$

Suppose $k_1 \neq 0$. By the equation (3.38), we have

$$k_2 = \frac{2\gamma l_1 l_2 - k_1 l_2^2 - 2}{2\alpha k_1}.$$

By equation (3.37), we have

$$l_2 = \frac{l_1}{\alpha k_1^2 - \beta l_1 k_1 + \gamma l_1^2},$$

so we also find that

$$f_1 = \frac{2}{l_1}x + \frac{2\beta}{l_1} - \frac{2k_1}{l_1^2}, f_2 = \frac{2}{l_1^2}(k_1^2 - \beta l_1 k_1 + \gamma l_1^2),$$

and

$$k_2 = \frac{4\beta l_1 k_1^2 + 2\gamma\beta l_1^3 - 2\gamma l_1^2 k_1 - 2\beta^2 l_1^2 k_1 - 2k_1^3 - \alpha l_1^2}{2(k_1^2 - \beta l_1 k_1 + \gamma l_1^2)^2}.$$

If $m = 4$, and $y = [a_0, \overline{a_1, a_2, a_1, 2a_0}\ ]$, and $f_4 = 0$, so we are done.

Suppose $m > 4$. We will show that f_4 and a_3 can be expressed in the variables of the coefficients of a_0 and a_1. By the definition of the sequence f_j, we have

$$(a_1 a_2 + 1)(a_1 f_2 + 1) = a_3(a_1 a_2 + 1)f_3 + (a_3 a_2 + 1) + f_4,$$

$f_4 \neq 0$, and $\deg(f_4) = 1$. Since a_1 divides f_4, we have $f_4 = r\, a_1$ where $r = 2a_0 - s\, a_1 - s\, a_1 a_2 a_3 - s\, a_3 + a_2^2 a_3 + a_2$ is a constant. But $\deg(a_1) = \deg(a_2) = \deg(a_3) = 1$. We then have

$$\frac{(a_2 a_3 + 1) + f_4}{a_1 a_2 + 1} = \frac{l_3}{l_1} = \frac{2}{f_3 l_1 l_2},$$

and hence

$$\frac{2}{l_2}x + \frac{2k_1 + 1}{l_1 l_2} = l_3(s\, k_1 - k_2)x + (s\, k_1 - k_2)k_3 + \frac{l_3}{l_1}.$$

It follows that

$$l_3 = \frac{2}{(s\, k_1 - k_2)l_2} = \frac{2}{f_3 l_2} = \frac{2}{(k_1 l_2 - k_2 l_1)s},$$

and

$$k_3 = \frac{1}{f_3}\Big(\frac{2}{l_1 l_2}k_1 + 1 - \frac{l_3}{l_1}\Big) = \frac{(2k_1 + l_1 l_2)f_3 - 2}{f_3^2 l_1 l_2}.$$

Suppose $m > 5$. We will show that f_5 and a_4 can be expressed in the variables of the coefficients of a_0 and a_1. By the definition of the sequence f_j, we have

$$p_1' f_3 + q_1' = a_4 f_4 + \frac{p_0' q_3' + f_5}{p_2'},$$

$f_5 \neq 0$, and $\deg(f_5) = 3$. But $\deg(\frac{p_0' q_3' + f_5}{p_2'}) = 1$. It follows that

$$l_4 = \frac{l_2 f_3}{r}, \quad \text{and} \quad k_4 = \frac{1}{\mathrm{lc}(f_4)}\Big(k_2 f_3 + \frac{l_2}{l_1} - \frac{l_4}{l_1}\Big),$$

and hence f_5 and a_4 can be expressed in the variables of the coefficients of a_0 and a_1.

Suppose $j < m$. Assume that $a_2, \ldots, a_{j-1}$, and $f_1, \ldots, f_j$ can be expressed in the variables of the coefficients of a_0 and a_1. By the definition of the sequence f_j, we have

$$p_{j-3}' f_{j-1} + p_0' \cdots p_{j-5}' q_{j-3}' = a_j f_j + \frac{p_0' \cdots p_{j-4}' q_{j-1}' + f_{j+1}}{p_{j-2}} \tag{3.39}$$

From the fact that $\deg(p_0' \cdots p_{j-3}') = \deg(f_{j+1})$ and $\deg(q_{j-1}') = \deg(p_{j-3}') + 1$, we have

$$\deg(\frac{p_0' \cdots p_{j-4}' q_{j-1}' + f_{j+1}}{p_{j-2}}) = \deg(f_j).$$

It follows that

$$l_j = \frac{l_1 l_2 \cdots l_{j-2} \mathrm{lc}(f_{j-1})}{\mathrm{lc}(f_j)},$$

and

$$k_j = \frac{l_1 c + l_1 \mathrm{lc}(p_0' \cdots p_{j-5}' q_{j-3}') - l_j \mathrm{lc}(p_0' \cdots p_{j-4}')}{l_1 \mathrm{lc}(f_j)}$$

where c is the coefficient $x^{\deg(f_j)}$ of $p_{j-3} f_{j-1}$. By the assumption, a_j can be express in the variables of coefficients of a_0 and a_1, and so, by the equation (3.39), is f_{j+1}. □

3.2.6 Application: Order N in Convergent Sequences

McMullen [24] showed that the order of the divisor at infinity does not increase at the limit of a converging sequence of hyperelliptic curves over $\mathbb{C}$ (with bounded order of these divisors). Here we show that when $g = 1$, the order is preserved. We first note that when $g = 2$ (at least) the period length can change.

Definition 3.2.6.1 *A sequence $d_j(x,y)$ is said to be* **converge** *to $d(x,y)$ in $\mathbb{C}[x,y]$ if the coefficients of the $d_j(x,y)$ converge to those of $d(x,y)$ in the standard topology of $\mathbb{C}$.*

Example 3.2.6.3: Example of changing period length. Let $\mathcal{C}_j$ be the hyperelliptic curve of genus 2 over $\mathbb{C}$ defined by

$$y^2 = d_j(x) = x^6 + (\frac{\kappa_j}{2} - \frac{2}{\kappa_j})x^4 + (\frac{\kappa_j^2}{16} - \frac{3}{2} + \frac{1}{\kappa_j^2})x^2 + \frac{1}{\kappa_j}$$

where

$$\kappa_j = \frac{j}{j+1},$$

and let $\mathcal{C}$ be the hyperelliptic curve of genus 2 over $\mathbb{C}$ defined by

$$y^2 = d(x) = x^6 - \frac{3}{2}x^4 - \frac{7}{16}x^2 + 1$$

We clearly see that $y^2 - d_j(x) \longrightarrow y^2 - d(x)$ as $j \longrightarrow \infty$.

We will show that the continued fraction of y for the curve $\mathcal{C}_j$ has period 6 with $\kappa_j = \frac{j}{j+1}$ but the continued fraction of y for the curve $\mathcal{C}$ has period 3. Compute the continued fraction of y for $\mathcal{C}_j$.

$$\begin{aligned} d_j(x) &= x^6 + (\frac{\kappa_j}{2} - \frac{2}{\kappa_j})x^4 + (\frac{\kappa_j^2}{16} - \frac{3}{2} + \frac{1}{\kappa_j^2})x^2 + \frac{1}{\kappa_j} \\ &= \big(x\big(x^2 + \frac{\kappa_j}{4} - \frac{1}{\kappa_j}\big)\big)^2 - x^2 + \frac{1}{\kappa_j}, \end{aligned}$$

so

$$
\begin{aligned}
a_0(j) &= x\big(x^2+\frac{\kappa_j}{4}-\frac{1}{\kappa_j}\big) = P_1(j) & Q_1(j) &= -x^2+\frac{1}{\kappa_j}\\
y_1(j) &= \frac{y+P_1(j)}{Q_1(j)} & a_1(j) &= \lfloor y_1(j)\rfloor = -2x\\
P_2(j) &= a_1(j)Q_1(j)-P_1(j) & Q_2(j) &= \frac{d_j(x)-P_2^2(j)}{Q_1(j)}\\
&= x\big(x^2-\frac{\kappa_j}{4}-\frac{1}{\kappa_j}\big) & &= -\kappa_j x^2+1\\
y_2(j) &= \frac{y+P_2(k)}{Q_2(k)} & a_2(j) &= \lfloor y_2(k)\rfloor = \frac{-2}{\kappa_j}x\\
P_3(j) &= a_2(j)Q_2(j)-P_2(j) & Q_3(j) &= \frac{d_j(x)-P_3^2(j)}{Q_2(j)}\\
&= x\big(x^2+\frac{\kappa_j}{4}-\frac{1}{\kappa_j}\big) & &= \frac{1}{\kappa_j}\\
y_2(j) &= \frac{y+P_3(j)}{Q_3(j)} & a_3(j) &= \lfloor y_3(j)\rfloor = \frac{1}{2}x\big(x^2+\frac{\kappa_j}{4}-\frac{1}{\kappa_j}\big)\\
& & &= 2\kappa_j a_0(j)
\end{aligned}
$$

This means the continued fraction of y for $\mathcal{C}_j$ has a period 6 with $\kappa_j = \frac{j}{j+1}$.

Now, we compute the continued fraction of y for $\mathcal{C}$ as follows: Since

$$d(x) = x^6-\frac{3}{2}x^4-\frac{7}{16}x^2+1 = \big(x\big(x^2-\frac{3}{4}\big)\big)^2-x^2+1,$$

we have

$$
\begin{aligned}
a_0 &= x\big(x^2-\frac{3}{4}\big) = P_1 & Q_1 &= -x^2+1\\
y_1 &= \frac{y+P_1}{Q_1} & a_1 &= \lfloor y_1\rfloor = -2x\\
P_2 =& a_1Q_1-P_1 = x^3-\frac{5}{4}x & Q_2 &= \frac{d(x)-P_2^2}{Q_1} = -x^2+1\\
y_2 &= \frac{y+P_2}{Q_2} & a_2 &= \lfloor y_2\rfloor = -2x\\
P_3 =& a_2Q_2-P_2 = x\big(x^2+\frac{3}{4}\big) = P_1 & Q_3 &= \frac{d(x)-P_3^2}{Q_2} = 1\\
y_2 &= \frac{y+P_3}{Q_3} & a_3 &= \lfloor y_3\rfloor = 2x^3-\frac{3}{2}x = 2a_0.
\end{aligned}
$$

This implies the continued fraction of y for $\mathcal{C}$ has a period 3. Hence, we conclude the order of the divisor at infinity $D_\infty(j)$ on the curve $\mathcal{C}_j$ is

$$\text{ord}(D_\infty(j)) = \deg(a_0(j)\, a_1(j)\, a_2(j)) = 3 + 1 + 1 = 5,$$

and the order of the divisor at infinity D_∞ on the curve $\mathcal{C}$ is

$$\text{ord}(D_\infty) = \deg(a_0 a_1 a_2) = 3 + 1 + 1 = 5.$$

□

Theorem 3.2.6.1 *Let k be a subfield of $\mathbb{C}$. Let $\mathcal{C}_j, \mathcal{C}$ be elliptic curves given by*

$$y^2 = d_j(x) \quad \textit{and} \quad y^2 = d(x),$$

respectively, where $d_j(x), d(x) \in k[x]$ such that $\deg(d_j(x)) = 4 = \deg(d(x))$. Suppose that

$$y^2 - d_j(x) \longrightarrow y^2 - d(x)$$

as $j \to \infty$ and for each j, ord$(D_\infty(j)) = N < \infty$ where $D_\infty(j), D_\infty$ are the divisors at infinity for $\mathcal{C}_j, \mathcal{C}$, respectively. Then the order of D_∞ is finite and equals N.

Proof. Since $\text{ord}(D_\infty(j)) = N < \infty$, there are complex polynomials b_j and c_j such that $\deg(b_k) = N$ and

$$b_j^2 - d_j(x)c_j^2 = 1.$$

It follows that $\text{ord}(D_\infty)$ is finite and hence a period-length of the continued fraction of y for the curve $\mathcal{C}$ is also finite.

Now, write

$$y = [a_{0,j}, a_{1,j}, a_{2,j}, \ldots] \text{ and } y = [a_0, a_1, a_2, \ldots]$$

are the continued fractions for the curves $\mathcal{C}_j, \mathcal{C}$, respectively. Since or each $j, \text{ord}(D_\infty(j)) = N, \deg(a_{i,j}) = 1$ for all $i = 1, \ldots, m_j - 1$ and $\text{ord}(D_\infty(j)) = \sum_{j=0}^{m_j-1}(\deg(a_i(j)))$, we have

$$m_k = N - 1$$

By Definition 3.2.3.1, we have sequences $h_{i,j}, h_i$ in $\mathbb{C}[x]$ satisfy the properties in the definition. Also, $h_{m,j} = 0$ for all j. Suppose m is a quasi-period length of the continued fraction of y for the curve $\mathcal{C}$. In order to show that $\text{ord}(D_\infty) = N$, it suffices to show that, for each $j = 1, \ldots, m-1, h_{j,k}$ converges to h_j, and $h_j \neq 0$ for all $j = 1, \ldots, m-1, h_m = 0$, and $m = N - 1$.

By Lemma 3.1.0.2, we have

$$d_j(x) = a_{0,j}^2 + h_{1,j}$$

Since $y^2 - d_j(x)$ converges to $y^2 - d_j$ as j goes to ∞, and $d(x) = a_0 + h_1$, we obtain $\{a_{0,j}\}, \{h_{1,j}\}$ converge to a_0, h_1, respectively. By Corollary 3.2.5.1,

$$2\text{lc}(a_{0,j}) = \text{lc}(a_{1,j})\text{lc}(h_{1,j}).$$

It follows that neither $\text{lc}(a_{1,j})$ nor $\text{lc}(f_{1,j})$ cannot tend to zero as j goes to ∞. This implies $h_1 \neq 0$.

Since $h_{2,j} = 2a_{0,j} - a_{1,j}h_{1,j}, h_2 = 2a_0 - a_1h_1$, and both $\{a_{0,j}\}, \{h_{1,j}\}$ converge a_0, h_1, respectively, we have both $\{a_{1,k}\}$ and $\{h_{2,k}\}$ converge to a_1 and h_2, respectively. By Corollary 3.2.5.1,

$$2\text{lc}(a_{0,j}) = \text{lc}(a_{1,j})\text{lc}(a_{2,j})h_{2,j}$$

and $h_{2,j} = 0$ if and only if $m = 2 = N - 1$. It follows that $h_2 = 0$ if and only if $N = 3$.

Suppose $m > 2$. Since $a_{1,j}f_{1,j} = a_{2,j}(a_{1,j}h_{2,j} + 1) + f_{3,j}$, $a_1f_1 = a_2(a_1h_2 + 1) + f_3$, and all $\{a_{0,j}\}, \{a_{1,j}\}, \{h_{1,j}\}$ and $\{h_{2,j}\}$ converge, we have both $a_{2,j}$ and $f_{3,j}$ converge to a_2 and f_3, respectively. This implies $\{h_{3,j}\}$ also converges to h_3. Similarly, by using Corollary 3.2.5.1, we conclude that $h_3 = 0$ if and only if $N = 4$.

Suppose $m > 3$. Suppose that $\{f_{i,j}\}$ converges to f_i for all $i = 0, 1, 2, \ldots, l-1 < n-1$ and $\{a_{i,j}\}$ converges to a_i for all $j = 0, 1, \ldots, l-1$. Consider

$$p'_{l-3,j}(p'_{l-4,j}f_{l-2,j} + p'_{-1,j}\cdots p'_{l-6,j}q'_{l-4,j}) = a_{l-1,j}p'_{l-3,j}f_{l-1,j} + p'_{-1,j}\cdots p'_{l-5,j}q'_{l-2,j} + f_{l,j}, \tag{3.40}$$

and

$$p'_{l-3}(p'_{l-4}f_{l-2} + p'_{-1}p'_0\cdots p'_{l-6}q'_{l-4}) = a_{l-1}p'_{l-3}f_{l-1} + p'_{-1}p'_0\cdots p'_{l-5}q'_{l-2} + f_l. \tag{3.41}$$

By the induction hypothesis, it is not hard to see that the left hand side of Equation (3.40) converges to the left hand side of Equation (3.41) in $k[x]$. It follows that the right hand side of Equation (3.40) must converge to the right of equation (3.41) in $k[x]$. Since $q'_{l-2,j} = a_{l-1,j}q'_{l-3,j} + q'_{l-4,j}, q'_{l-2} = a_{l-1}q'_{l-3} + q'_{l-4}$, and by the induction hypothesis, we obtain

$$(\lim_{j\to\infty} a_{l-1,j} - a_{l-1})(p'_{l-3}f_{l-1} + p'_{-1}p'_0\cdots p'_{l-5}q'_{l-3}) = \lim_{j\to\infty} f_{l,j} - f_l.$$

Since

$$f_l = \frac{(p'_{l-3}f_{l-1} + p'_0\ldots p'_{l-5}q'_{l-3})p'_{m-(l+2)} - p'_0\cdots p'_{j-4}q'_{m-(l+1)}}{p'_{m-(l+1)}}$$

where m is the period length of the continued fraction of y for the curve $\mathcal{C}$, we have

$$\deg(f_l) < \deg(p'_{l-3}f_{l-1}).$$

Also,

$$\deg(p'_{l-3}f_{l-1}) > \deg(p'_{-1}p'_0\cdots p'_{l-5}q'_{l-3}).$$

Hence, we conclude that $\{a_{l-1,j}\}$ converges to a_{l-1} and $\{f_{l,j}\}$ converges to f_l as $k \to \infty$. This implies $\{h_{l,j}\}$ converges to h_l as $k \to \infty$. By Corollary 3.2.5.1,

$$2\mathrm{lc}(a_{0,j}) = \mathrm{lc}(a_{1,j})\mathrm{lc}(a_{l,j})h_{l,j}$$

and $h_{l,j} = 0$ if and only if $l = N - 1$. □

3.3. New Infinite Families with ord$(D_\infty) = 11$

In this section, we will give new examples of infinitely many hyperelliptic curves with genus $g > 1$ over $k = \mathbb{Q}$ with divisors at infinity of order $N = 11$. Since $N \geq g + 1$, there are no divisors at infinity of order 11 when genus $g > 11$. In order to find such examples, we use Theorem 2.4.0.4, Lemma 3.1.0.2 and remark 3.2.3.1, in the form of the following conditions (3.42):

$$\begin{array}{lll} 1. \quad g+1+\deg(a_1) = \deg(a_{i-1}) + \deg(a_i) & \text{if and only if} & h_i = 0, \\ 2. \quad \deg(a_{i-1}) + \deg(a_i) \leq g+1 & \text{if and only if} & h_i \neq 0, \\ 3. \quad h_i h_{i+1} \neq 0 & \text{if} & h_i = 0. \end{array} \tag{3.42}$$

Note that $g + 1$ appears in the above becuase $\deg(a_0) = g + 1$. From now on, we denote by δ_i the degree of the partial quotient a_i for all i. The following method comes from Lemma 3.1.0.2 and works not only for $N = 11$ but also in general.

Definition 3.3.0.2 *Our **Naive Method** is the following. Given the field k, genus g and desired order N,*

- *choose m (satisfying the three conditions* (3.42)*)*
- *choose a partition (satisfying the three conditions* (3.42)*)*

$$N = g + 1 + \sum_{j=1}^{m-1} \delta_i \,,$$

  with each $1 \leq \delta_i \leq g$,

- *Assign a skew value variable $\kappa \notin \{-1\}$.*
- *Assign variable coefficients:*
  - $f_1(x) = \sum_{j=0}^{g+1-\delta_1} b_i x^i$,

- $a_0(x) = x^{g+1} + c_{0,g}x^g + \cdots + c_{0,1}x + c_{0,0}$, *and*
- $a_i(x) = \sum_{i=0}^{\delta_i} c_{i,j}x^j$ *for each* $1 \leq i \leq \left\lfloor \frac{m}{2} \right\rfloor$. *(Note that the* $c_{i,d_i} \neq 0$*.)*

- *Solve the equation* $f_1 = q'_{m-1}/(\kappa\, p'_{m-2})$ *in the form*

$$\kappa\, p'_{m-2} f_1 - q'_{m-3} = 2a_0 q'_{m-2}$$

for $b_i, c_{i,j} \in k$.

3.3.1 Genus 2

Flynn [11], [12] gave a one-dimensional family of curves with $g = 2$ and $N = 11$. Much more recently, Bernard *et al* [4] found 18 additional individual curves with $(g, N) = (2, 11)$. (They state that they have found 19, but their table of results lists one curve twice). They explicitly state that they sought new infinite families of such curves. We exhibit a new infinite family of this type. Flynn's family is given in terms of $t \in \mathbb{Q}$ by $\mathcal{F}_t : y^2 = f_t(x)$, where

$$f_t(x) = x^6 + 2x^5 + (2t+3)x^4 + 2x^3 + (t^2+1)x^2 + 2t(1-t)x + t^2. \tag{3.43}$$

Computing the continued fraction expansion of y for the Flynn family, one finds that each continued fraction expansion has a quasi-period length $m = 7$ and period length $n = 14$ with the partition

$$(\delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6) = (3, 2, 1, 1, 1, 1, 2).$$

Similarly computation reveals that all eighteen curves found by Bernard *et al* [4] have a quasi-period length $m = 9$ and period length $n = 18$.

The partions of $N = 11$ when $g = 2$ for which $\delta_0 = g + 1$ and $1 \leq \delta \leq g$ for

$1 \leq i \leq m-1$, are

$$\text{The quasi-period length } m=5 \ : \ (3,2,2,2,2) \tag{3.44}$$

$$\text{The quasi-period length } m=6 \ : \ (3,1,2,2,2,1) \tag{3.45}$$

$$\text{The quasi-period length } m=6 \ : \ (3,2,1,2,1,2) \tag{3.46}$$

$$\text{The quasi-period length } m=7 \ : \ (3,1,2,1,1,2,1) \tag{3.47}$$

$$\text{The quasi-period length } m=7 \ : \ (3,2,1,1,1,1,2) \tag{3.48}$$

$$\text{The quasi-period length } m=8 \ : \ (3,1,1,1,2,1,1,1) \tag{3.49}$$

$$\text{The quasi-period length } m=9 \ : \ (3,1,1,1,1,1,1,1,1) \tag{3.50}$$

Report of Results

The three conditions (3.42) further restrict the partitions. The partition in (3.44) is impossible since $\delta_1 = 2 = g$ and $\delta_1 + \delta_2 = 4 > 3 = g + 1$.

By using our Naive Method, we found that:

1. The partition in (3.45) and (3.46) are not realized over $\mathbb{Q}$ since the corresponding solutions must have that either the leading coefficient of a_2 or the leading coefficient of a_3 is equal to zero.

2. There exist at least four families when $m = 7$. One of the four is the Flynn family, up to a change of variables.

3. We found an infinite family over $\mathbb{Q}$ with the partition (3.49).

4. The partition in (3.50) gave the new family $\mathcal{K}_2(t)$ defined by $\mathcal{K}_2(t) : y^2 = g_t(x)$,

where

$$\begin{aligned} g_t(x) = x^6 - 2x^5 &- \frac{t^5+12t^4-11t^3-8t^2+20t-6}{(t-1)^2(t^3-2t^2+2)}x^4 + \frac{4(t^4+5t^3+2t^2-2t+2)}{(t-1)(t^3-2t^2+2)}x^3 \\ &- \frac{88t^7+65t^6-220t^5+40t^4+116t^3-96t^2+48t-12}{(t-1)^4(t^3-2t^2+2)^2}x^2 \\ &- \frac{2(1+t)(t^4+3t^3-14t^2+10t-2)(t^5+4t^4+5t^3-4t^2-2)}{(t-1)^4(t^3-2t^2+2)^2}x \\ &+ \frac{(1+t)(t^{12}+5t^{11}-11t^{10}-39t^9+32t^8+118t^7-30t^6-196t^5)}{(t^3-2t^2+2)^3(t-1)^4} \\ &+ \frac{(1+t)(228t^4-132t^3+32t^2-8t+8)}{(t^3-2t^2+2)^3(t-1)^4}. \end{aligned} \tag{3.51}$$

The partial quotients of this continued fraction expansion of y are the following:

$$\begin{aligned} a_0 &= x^3 - x^2 - \frac{4t^4-3t^3-4t^2+t^5-2+8t}{(t^3-2t^2+2)(t-1)^2}x + \frac{(1+c)(3t^3-6t^2-2+t^4+2t)}{(t^3-2t^2+2)(t-1)^2}, \\ a_1 &= -\frac{(t^3-2t^2+2)^2(t-1)}{32(1+t)t^3}((t-1)x+t+1), \\ a_2 &= \frac{8t}{(t^3-2t^2+2)(t-1)^2}((t-1)x-1-t), \\ a_3 &= t^2a_1,\ a_4 = \frac{8}{(t^3-2t^2+2)(t-1)^2}(x-1), \quad \text{and} \\ \kappa &= -\frac{(t-1)^6(t^3-2t^2+2)^3}{256\,t^3}. \end{aligned}$$

Isomorphism Classification

By computing the Igusa invariants, see our [9], one finds that all four familes with $m = 7$ give isomorphic curves. The family $\mathcal{K}_2(t)$ is distinct from Flynn's family (3.43), that is for all t, u, $\mathcal{K}_2(u)$ is not isomorphic over $\mathbb{Q}$ to $\mathcal{F}_t$, see our [9]. The family $\mathcal{K}_2(t)$ of genus 2 curves shares no isomorphism class with any of the curves of Flynn's family, $\mathcal{F}_t$, given by (3.43). This is verified by computation involving the Igusa invariants, which will be discussed in detail in our [9]. (We have yet to compute the Igusa invariants for the infinite family with partition (3.49).)

3.3.2 Genus Greater than 2

For each even $g > 2$ and integer $r, 0 \leq r \leq g$, Flynn [12] gives a 1-parameter family of hyperelliptic curves of genus g with a divisor of exact order $N = g^2 + 3g + 1 - r$:

$$\mathcal{T} : Y^2 + t(X-1)Y = (\psi(X))^2 - t(X^{g+2} + X^{r+1})$$

where $\psi(X) = \sum_{i=1}^{g-r+1} X^{r+1} = \frac{X^{g+2} - X^{r-1}}{X-1}$. If $g > 2$, then these are not divisors of order $N = 11$, because there is no positive integer r such that $0 \leq r \leq g$, and $r = g^2 + 3g - 10$. Now, we find families of hyperelliptic curves with genus g and $N = 11$ for all $g = 3, \ldots, 10$.

When $\boldsymbol{g = 3}$ the shortest possible partition in order to have the order of the divisor at infinity equal to 11 is

$$\text{The quasi-period length} \quad m = 6 \quad : \ (4, 2, 1, 1, 1, 2),$$

by using the same argument as in the case of genus 2. By applying our Naive Method, we found a family of hyperelliptic curves $\mathcal{K}_3(t)$ given by

$$\begin{aligned} y^2 = \frac{1}{4t^2}\Big[2x^3 + (t^2+t)x^2 - 2tx + 2\Big]\Big[2t^2x^5 + (6t^4 + 5t^3 + 4t)x^4 \\ + (6t^6 + 10t^5 + 4t^4 + 6t^3 + 10t^2 + 2)x^3 + (4t^6 + 5t + 8t^3 + 10t^4 + t^5 + 5t^7 + 2t^8)x^2 \\ + (2t^4 - 2t^7 + 4t^2 + 2t + 4t^5)x + 2 + 2t^6 + 5t^3\Big]. \end{aligned}$$

Each continued fraction expansion of y for the curves $\mathcal{K}_3(t)$ is

$$y = [a_0, \overline{a_1, a_2, a_3, a_2, a_1, 2a_0}\,]$$

where

$$a_0 = x^4 + (2t^2 + \frac{3}{2}t + \frac{1}{t})x^3 + (t^4 + \frac{3}{2}t^3 + \frac{1}{2}t^2 + \frac{3}{2}x^2 - \frac{1}{2}t(2t^2-1)x + (1 + \frac{1}{t})(t^2 - t + 1),$$
$$a_1 = \frac{2}{t}(x^2 + (t^2+t)x - t), \qquad a_2 = \frac{t}{2}x, \qquad \text{and} \quad a_3 = \frac{4}{t^2}(tx + t^3 + t^2 + 1).$$

Here; $\delta_0 = 4,\ \delta_1 = 2,\ $ and $\ \delta_2 = 1 = \delta_3$.

When $\boldsymbol{g = 4}$, the shortest possible partition in order to have the order of the divisor at infinity equal to 11 is

$$\text{The quasi-period length} \quad m = 4 \quad : \ (4, 3, 1, 3),$$

by using the same argument as in the case of genus 2. However in this case, we choose the partition $(4, 1, 2, 2, 1)$. When we use the Naive Method, in both partitions, we need to find a_0, a_1, and a_2; the latter partition is more effective because $\delta_1 + \delta_2$ are less than the former partition. We found the family of hyperelliptic curves $\mathcal{K}_4(t)$ given by

$$\begin{aligned} y^2 = \frac{1}{t^4(t-1)^2}\Big[&(t^4(t-1)^2)x^{10} + (4(t-1)^2t^3)x^9 + (2t^2(t-1)(t^3+3t-3))x^8 \\ &+ (4t(t-1)(t^2+1)(t^2+t-1))x^7 + (t^2-2t+8t^5-10t^4+3t^6+1)x^6 \\ &+ (2t^2(2-6t+3t^4+t^3+2t^2))x^5 + (2t(-2t+1+t^4-2t^3+5t^5))x^4 \\ &+ (2t^3(-1+3t^3-5t+6t^2))x^3 + (t^2(t^2+t+1)(9t^2-7t+1))x^2 \\ &+ (2t^4(3t+3t^2-1))x + 5t^6\Big]. \end{aligned}$$

Each continued fraction expansion of y for the curves $\mathcal{K}_4(t)$ is

$$y = [a_0, \overline{a_1, a_2, \kappa a_2, \kappa^{-1}a_1, 2\kappa a_0, \kappa^{-1}a_1, \kappa a_2, a_2, a_1, 2a_0}\,]$$

where $\kappa = \frac{1}{4}(1 - \frac{1}{t})^2$,

$$\begin{aligned} a_0 &= x^5 + \frac{2}{t}x^4 + \frac{t^3+t-1}{t^2(t-1)}x^3 + \frac{2t}{t-1}x^2 + \frac{t+t^2-1}{t(t-1)}x + \frac{t}{t-1}, \\ a_1 &= \frac{1}{2}(1-\frac{1}{t})x, \qquad \text{and} \quad a_2 = \frac{2}{1-\frac{1}{t}}(x^2 + \frac{1}{t}x). \end{aligned}$$

Here; $\delta_0 = 5$, $\delta_1 = 1$, and $\delta_2 = 2$.

When $\boldsymbol{g = 5}$, the shortest possible partition in order to have the order of the divisor at infinity equal to 11 is

$$\text{The quasi-period length} \quad m = 4 \quad : \ (6, 1, 3, 3, 1),$$

by using the same argument as in the case of genus 2. By applying our Naive Method, we found the family of hyperelliptic curves $\mathcal{K}_5(t)$ are given by

$$\begin{aligned} y^2 = \frac{1}{4}\Big[&(x^3+(2-t)x^2-x+1)(4x^9+(-4t+12)x^8+5x^7 \\ &+(-4t^2+9t+6)x^6-(t+7)(t-3)x^5+(-t^3+2t^2-6t+21)x^4 \\ &+(-3t^2+6t+3)x^3-(3t+4)(t-3)x^2-(6t-15)x+5)\Big]. \end{aligned}$$

Each continued fraction of y for the curves $\mathcal{K}_5(t)$ is

$$y = [a_0, \overline{a_1, a_2, a_1, 2a_0}\,]$$

where

$$\begin{aligned} a_0 &= x^6-(t-\frac{5}{2})x^5-(\frac{1}{2}t^2-t-1)x^3-(t-\frac{5}{2})x^2-\frac{1}{2}(t-3)x-\frac{1}{2}, \\ a_1 &= x, \qquad \text{and} \qquad a_2 = 2x^3+x^2+t\,x+1. \end{aligned}$$

Here; $\delta_0 = 6,\ \delta_1 = 1,$ and $\delta_2 = 3.$

When $\boldsymbol{g = 6}$, the shortest possible partition in order to have the divisor at infinity of order 11 is

$$\text{The quasi-period length} \quad m = 3 \quad : \ (7,2,2),$$

by using the same argument as in the case of genus 2. By applying our Naive Method, we found the family of hyperelliptic curves $\mathcal{K}_6(t)$ are given by

$$\begin{aligned} y^2 = {} & x^{14}+4(t+1)x^{13}+2(3t+5)(t+1)x^{12}+2(2t^3+12t^2+18t+11)x^{11} \\ &+(t^4+16t^3+48t^2+72t+37)x^{10}+(4t^4+28t^3+84t^2+108t+59)x^9 \\ &+(6t^4+40t^3+110t^2+147t+79)x^8+(6t^4+44t^3+119t^2+174t+92)x^7 \\ &+(5t^4+33t^3+120t^2+161t+103)x^6+(2t^4+26t^3+78t^2+155t+89)x^5 \\ &+(t^4+9t^3+61t^2+92t+\frac{349}{4})x^4+\frac{1}{2}(5t+4)(2t^2+6t+25)x^3 \\ &+(\frac{45}{4}t^2+22t+\frac{85}{2})x^2+(\frac{29}{2}t+12)x+\frac{37}{4}. \end{aligned}$$

Each continued fraction expansion of y for the curves $\mathcal{K}_6(t)$ is

$$y = [a_0, \overline{a_1, a_1, 2a_0}\,]$$

where

$$\begin{aligned} a_0 &= x^7 + 2(t+1)x^6 + (t+3)(t+1)x^5 + (2t^2+4t+5)x^4 + (t^2+6t+4)x^3 \\ &\quad + (t^2+2t+\frac{13}{2})x^2 + (\frac{5}{2}t+2)x + \frac{5}{2}, \quad \text{and} \\ a_1 &= x^2 + t\,x + 1. \end{aligned}$$

Here; $\delta_0 = 7$ and $\delta_1 = 2$.

When $\boldsymbol{g = 7}$, the shortest possible partition in order to have the divisor at infinity of order 11 is

$$\text{The quasi-period length} \quad m = 4 \quad : \ (8,1,1,1),$$

by using the same argument as in the case of genus 2. By applying our Naive Method, we found the family of hyperelliptic curves $\mathcal{K}_7(t)$ are given by

$$\begin{aligned} y^2 = \frac{1}{4}\Big[&(2x^7+4x^4+2x^3+x^2-t\,x+1)(2x^9+4tx^8+(2t^2+8)x^7 \\ &+ 4(2t+1)x^6 + 2(4t+5)x^5 + (4t^2+4t+17)x^4 + (t+8)(2t+1)x^3 \\ &- (t^2-8t-21)x^2 - (t^3-2t-8)x - 3t^2+8)\Big]. \end{aligned}$$

where t is a rational number. Each continued fraction of y for the curves $\mathcal{K}_7(t)$ is

$$y = [a_0, \overline{a_1, a_2, a_1, 2a_0}\,]$$

where

$$\begin{aligned} a_0 &= x^8 + t\,x^7 + 2x^6 + 2x^5 + (2t+1)x^4 + (t+\frac{9}{2})x^3 + 2x^2 - \frac{1}{2}(t^2-3)x - \frac{1}{2}t, \\ a_1 &= x, \qquad \text{and} \qquad a_2 = x + t. \end{aligned}$$

Here; $\delta_0 = 8,\ \delta_1 = 1,$ and $\delta_2 = 1$.

When $\boldsymbol{g = 8}$, the shortest possible partition in order to have the order of the divisor at infinity equal to 11 is

$$\text{The quasi-period length} \quad m = 2 \quad : \ (9, 2),$$

by using the same argument as in the case of genus 2. By applying our Naive Method, we found the family of hyperelliptic curves $\mathcal{K}_8(t)$ are given by

$$y^2 = x(x^{11} - t\,x^{10} - t^7x^4 + t^8x^3 + 2)(x^6 + t\,x^5 + t^2x^4 + t^3x^3 + t^4x^2 + t^5x + t^6).$$

Each continued fraction of y for the curves $\mathcal{K}_8(t)$ is

$$y = [a_0, \overline{a_1, 2a_0}\,]$$

where

$$a_0 = x^2(x^7 - t^7), \qquad \text{and} \qquad a_1 = x(x - t).$$

Here; $\delta_0 = 9$ and $\delta_1 = 2$.

When $\boldsymbol{g = 9}$, we have $\delta_0 = 10$, then the shortest possible partition is $(9, 2)$ and $m = 2$. Using Theorem 3.1.1.1, we have that the family of hyperelliptic curves $\mathcal{K}_9(t)$ are given by

$$y^2 = (x^9 - t)(x^{11} - tx^2 + 1).$$

Here; in the notation of Theorem 3.1.1.1

$$h(x) = x^9 - t, \ g(x) = x^{11} - tx^2 + 1, \ a_0 = x^{10} - t\,x,$$

and $a_1 = 2x$.

When $\boldsymbol{g = 10}$, due to Corollary 3.1.0.1, we have hyperelliptic curves with genus 10 and $N = 11$ defined by

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

where $h(x)$ is a monic polynomial over $\mathbb{Q}$ and $h(x)^2 + 1$ is no repeated roots over $\mathbb{C}$.

4. CONCLUSIONS AND FUTURE DIRECTIONS

4.1. Conclusions

We have shown that continued fractions over function fields can be used to give new examples of hyperelliptic curves over $\mathbb{Q}$ with low order of divisor at infinity. In particular:

1. For small N in terms of genus g, we determine all divisors at infinity on hyperelliptic curves with $N = \mathrm{ord}(D_\infty) = g + 2$, and similarly for $N = 2g + 1$ under the further condition that $y = \sqrt{f(x)}$ has (period) continued fraction of period length 2.

2. We improved the known bound on N in terms of genus and quasi-period length:

$$N \leq \begin{cases} \Big(\lfloor \frac{m}{2} \rfloor + 1 \Big) g + \lfloor \frac{m+1}{2} \rfloor & \text{if } r = m, \\ \Big(\frac{m}{2} + \lceil \frac{m}{4} \rceil \Big) g + \frac{m}{2} - \lceil \frac{m}{4} \rceil & \text{if } r < m \textit{ and } m \textit{ is even,} \\ \Big(\lfloor \frac{m}{2} \rfloor + \lceil \frac{m}{4} \rceil + 1 \Big) g + \lfloor \frac{m}{2} \rfloor - \lceil \frac{m}{4} \rceil & \text{if } r < m, \textit{ and } m \textit{ is odd.} \end{cases}$$

3. We give new families of hyperelliptic curves over $\mathbb{Q}$ with a divisor of order 11.

4. Key to the above is our introduction of the sequence of h_j; in particular we found for each $0 < j < m$,

- $\delta_{j-1} + \delta_j = g + 1 + \delta_1 \quad$ if and only if $\quad h_j = 0$;
- $\delta_{j-1} + \delta_j \leq g + 1 \qquad$ otherwise;
- and the first of these cannot occur for consecutive valves of the index j.

4.2. Future directions

The following are some directions for future research.

1. The original problem of this research was inspired by McMullen's Theorem 3.4 [**?**]: If $\{\mathcal{C}_k\}$ is a sequence of hyperelliptic curves of genus g with divisors at infinity of order less than or equal to N converging to an irreducible hyperelliptic curve $\mathcal{C}$ in $\mathbb{C}[x, y]$, then the order of the divisor for $\mathcal{C}$ is also less than or equal to N. This raises the question: When every element is of fixed order N, is the limit also of order N?

In Section 3.2, we showed that if $\{\mathcal{C}_k\}$ is a sequence of hyperelliptic curves of genus $g = 1$ with divisors at infinity of order N converging to a hyperelliptic curve $\mathcal{C}$ in $\mathbb{C}[x, y]$, then the order of the divisor for $\mathcal{C}$ is also N. We hope to answer this question in general or give a counterexample.

2. If we know how many zero polynomials are in the sequence $h_j; j = 1, \ldots, m$, we believe that we could improve our bound for the order of the divisor at infinity for a hyperelliptic curve. We would like to find more properties of the sequence h_j.

3. Related to the future direction (2), examples seem to hint of a correlation between the number of $j < m$ with $h_j = 0$ and the degree of a_1. We would like to determine if there is indeed such a relationship.

4. We ask if there is a simple proof using our h_j of the nonexistence of rational points of order 11 on an elliptic curve defined over $\mathbb{Q}$.

5. In Section 3.3, we notice that in genus 2, the quasi-period length of our new family and Flynn's family are different. We would like to know whether two hyperelliptic curves having different quasi-period length of the continued fraction expansion of y can be isomorphic.

6. It would be interesting to use our continued fraction techniques to obtain explicit

examples where N is at least quadratic in g.

BIBLIOGRAPHY

1. N. H. Abel, *Ueber die Integration der Differential-Formel* $\rho\,dx/\sqrt{R}$*, wenn* R *und* ρ *ganze Functionen sind*, J. Reine Angew. Math. I (1826), 185–221.

2. W. Adams and M. Razar, *Multiples of points on elliptic curves and continued fractions*, Proc. London Math. Soc. (3) 41 (1980), no. 3, 481–498

3. E. Artin, *Quadratische Körper im Gebiet der höheren Kongruenzen* I, II, Math. Zeitschrift, volume 19 (1924),153–246.

4. N. Bernard, F. Leprévost, and M. Pohst, *Jacobians of genus-2 curves with a rational point of order 11*, Experiment. Math. 18 (2009), no. 1, 65–70.

5. T. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math. (Basel) 55 (1990), no. 3, 259–266.

6. G. Billing and K. Mahler, *On exceptional points on cubic curves*, J. London Math. Soc. 15, (1940), 32–43.

7. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*. London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996.

8. P. L. Chebychev, *Sur l'int/'egration de la differential* $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma}}\,dx$, J. Math. Pures Appl. (2) 9 (1864), 225-46.

9. K. Daowsud and T. A. Schmidt, *Continued fraction for rational torsion*, in progress.

10. D. S. Dummit and R. M. Foote *Abstract Algebra*, John Wiley&Sons, Inc, 3rd, 2004.

11. E. V. Flynn, *Large rational torsion on abelian varieties*, J. Number Theory 36 (1990), no. 3, 257–265.

12. E. V. Flynn, *Sequences of rational torsions on abelian varieties*, Invent. Math. 106 (1991), no. 2, 433–442.

13. C. Friesen, *Continued Fractions and Real quadratic function fields*, doctoral thesis, Brown University, 1989.

14. C. Friesen, *Continued fraction characterization and generic ideals in real quadratic function fields*, In: The arithmetic of function fields (Columbus, OH, 1991), 465–474, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.

15. Friesen and P. van Wamelen, *Class numbers of real quadratic function fields*, Acta Arith. 81(1997), no. 1, 45–55.

16. C. Friesen, *Rational functions over finite fields having continued fraction expansions with linear partial quotients*, J. Number Theory 126 (2007), no. 2, 185–192.

17. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1979.

18. K. Hulek, *Elementary Algebraic Geometry*, SRML 20, AMS, 2003.

19. W. Fulton, *Algebraic Curves*, Mathematics Lecture Note series, The Benjamin/Cummings Publ., 1969.

20. J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) 72(1960), 612–649.

21. F. Leprévost, *Jacobiennes de certaines courbes de genre 2: torsion et simplicité*, Journal de Théorie des Nombres de Bordeaux 7 (1995), 283–306.

22. B. Mazur, *Rational Points of Modular Curves* in *Modular Functions of One Variable V*, Lecture Notes in Math. 601, Berlin-Heidelberg: Springer (1977), 107–148

23. J. F. Mestre, *Construction de courbes de genre 2 á partir de leurs modules.* In Effective methods in algebraic geometry (Castiglioncello, 1990), 313–334, Progr. Math., 94, Birkhäuser, Boston, Boston, MA, 1991.

24. C. McMullen, *Teichmüller curves in genus two: Torsion divisors and ratios of sines*, Invent. Math. 165 (2006), no. 3, 651–672.

25. F. Pappalardi and A. van der Poorten, *Pseudo-elliptic integrals, units, and torsion*, J. Aust. Math. Soc. 79 (2005), no. 3, 335–347.

26. K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley Publishing company, 3rd edition, 1993.

27. W. Schmidt, *On continued fractions and Diophantine approximation in power series fields*, Acta Arith. 95 (2000), no. 2, 139–166.

28. A. van der Poorten and X. Tran, *Quasi-elliptic integrals and periodic continued fraction*, Monatsh. Math. 131 (2000), no. 2, 155–169.