

A type of hyperelliptic continued fraction.

T.G. Berry*

Abstract

Based on hints of Tschebychev, a continued fraction is described which gives an effective algorithm for calculating the torsion, if finite, of divisors $D - D^-$ on a hyperelliptic curve of genus ≥ 2 , where D is an effective divisor of degree 2 and D^- denotes the image of D under the hyperelliptic involution. The difficulties involved in extending the algorithm to divisors of degree ≥ 3 are briefly discussed.

AMS 2000 subject classification: 14Q05, 11Y55. Keywords: hyperelliptic curve, torsion divisor, continued fraction.

1 Introduction

This paper describes a type of continued fraction expansion associated with a general effective divisor of degree 2 on a hyperelliptic curve of genus $g \geq 2$. This generalizes a continued fraction introduced by Halphen [12], using elliptic function theory, which is associated with one point on a curve of genus 1. However, the principal motivation for this paper is an attempt to understand the remarks of Tschebychev in the introduction to [8], reproduced here as Fig 1. In [7], Tschebychev developed a theory of integration in finite terms of algebraic functions on curves $y^n = F(x)$ which anticipates for these curves the general theory later developed by Risch. In particular, Tschebychev showed (though not in this language), that the determination of possible logarithmic terms in the integral, which is conceptually the most difficult part of the theory, reduces to the study of torsion of certain divisors on the curve. In [6] he further showed that when the curve is hyperelliptic the

*Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela

divisors whose torsion is to be determined can be reduced to the form $D - D^-$ where D is an effective divisor of degree $\leq g$ and D^- denotes the image of D under the hyperelliptic involution. If $g = 1$ then $D = P$, a point, and the torsion of $P - P^-$ is to be determined. After transforming P off to infinity, this is equivalent to solving the polynomial Pell equation $A^2 - B^2F = 1$, a problem solved by Abel by means of a continued fraction expansion, analogous to the classical method used to solve the integer Pell equation. (We henceforth refer to this as the classical CFE. See [1], Tschebychev (loc. cit.), [12], and for more recent accounts [2, 3, 4, 18]). Tchebychev worked out the genus 1 case explicitly in [6], but it seems his only mention of the higher genus hyperelliptic cases is that shown in Fig 1. The present paper is an attempt to understand this: specifically, to define the “fraction continue de la forme plus générale”. For $\deg D = 2$ we have a satisfactory answer: we define a continued fraction, of the required form, with all the good properties of the classical CFE. The fraction detects the torsion, when finite, of $D - D^-$ and $D - W$, where W is any divisor in the class $P + P^-$ (P a point). The asymptotic complexity of the algorithm is equal to that of Cantor’s algorithm which manipulates directly in the Jacobian (c.f.[5]) when this is applicable, but in many cases, because of symmetries analogous to those of the classical CFE, it can be expected to run about twice as fast-though of course there are also refinements to the straightforward Jacobian algorithm. (See [13] for an analogous discussion for the classical CFE). This is worked out in §§2-4 below. Unfortunately the situation for $\deg D \geq 3$ is different. The continued fraction exists, but both theoretically and algorithmically leaves much to be desired, and in fact does not seem to lead to a practical algorithm. The difficulties are briefly described in §5. Of course it is entirely probable that Tchebychev had a much better idea.

Notation

We denote by K an arbitrary base field. In particular, K may have char. 2. The treatment we give is independent of the characteristic (a similar treatment is possible for the classical continued fraction). Everything we define (curves, morphisms between curves, rational functions and divisors on curves etc...) is assumed to be defined over K , unless otherwise stated. C will denote a non-singular projective curve of genus $g \geq 2$; to keep matters straight it will not be assumed that C is hyperelliptic until §3.

We use standard notation of algebraic geometry-for linear equivalence,

Dans le mémoire sous le titre *Sur l'intégration des différentielles irrationnelles* j'ai montré comment on trouve, dans l'intégration sous forme finie des différentielles contenant une racine quelconque, le terme algébrique ainsi que les équations qui déterminent séparément chaque terme logarithmique. Pour résoudre complètement la question sur l'intégration sous forme finie de ces différentielles il reste à donner le procédé pour calculer les termes logarithmiques d'après les équations qui les déterminent. Jusqu'à présent un tel procédé n'a été donné que pour les cas les plus simples.

Dans le mémoire connu d'Abel sur l'intégration de la différentielle $\frac{\rho dx}{\sqrt{R}}$ (Oeuvres compl., t.I, p. 65) nous trouvons un tel procédé pour le cas du radical carré, ρ étant une fonction entière et R une fonction sans facteurs multiples. Dans le mémoire sous le titre *Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynôme du troisième ou quatrième degré* j'ai montré que par le même procédé on peut déterminer les termes logarithmiques de l'intégrale $\int \frac{\rho dx}{\sqrt{R}}$ dans le cas même de ρ fractionnaire, pourvu que le degré du polynôme R ne dépasse 4. Ce procédé de la détermination des termes logarithmiques dans l'expression de l'intégrale $\int \frac{\rho dx}{\sqrt{R}}$ consiste, comme on le sait, dans le développement du radical \sqrt{R} en fraction continue de la forme

$$r_0 + \frac{1}{r_1 + \frac{1}{r_2 + \frac{1}{\dots}}}$$

les fractions *réduites* que l'on obtient en développant l'expression \sqrt{R} , donnent les deux fonctions inconnues qui figurent dans le terme logarithmique de l'intégrale $\int \frac{\rho dx}{\sqrt{R}}$ pour les cas considérés. On peut démontrer que ce procédé de la détermination des termes logarithmiques s'étend à tous les autres cas d'intégration des différentielles contenant une racine *carrée* et qu'il ne faut pour cela que prendre le développement du radical \sqrt{R} en fraction continue de la forme plus général, savoir

$$r_0 + \frac{s_1}{r_1 + \frac{s_2}{r_2 + \frac{s_3}{r_3 + \dots}}}$$

ou s_1, s_2, s_3, \dots sont certaines fonctions de x, \dots

Figure 1: Tschebychev's remarks

linear systems, etc. A brief reminder: $K(C)$ denotes the function field of C . If $f \in K(C)$ then its divisor is denoted by (f) . If D is a divisor on C then $\mathcal{L}(D) = \{f \in K(C) : (f) + D \geq 0\}$ and $\ell(D) = \dim_K \mathcal{L}(D)$. Linear equivalence is denoted by \equiv .

2 Approximants

Let \mathcal{E} be a divisor, (in practice, not effective), of degree g on C . Then by the Riemann-Roch theorem, $\ell(\mathcal{E}) \geq 1$.

Definition 2.1. *An \mathcal{E} -approximant is a non-zero function $f \in \mathcal{L}(\mathcal{E})$. If \mathcal{E} is non-special, then f is called quasi-extremal.*

By Riemann-Roch, if \mathcal{E} is non-special, then $\ell(\mathcal{E}) = 1$, so that a quasi-extremal \mathcal{E} -approximant is unique up to constant multiples.

Let f be an \mathcal{E} -approximant. Then, by definition,

$$(f) + \mathcal{E} = Z_f \tag{1}$$

where Z_f is an effective divisor of degree g . By definition $Z_f \equiv \mathcal{E}$, whence the following proposition, which is useful, since, in concrete cases, there are good criteria for deciding if an effective divisor is special, and no such criteria for non-effective divisors.

Proposition 2.2. *f is quasi-extremal iff Z_f is non-special*

2.1 Multiplicative structure

Let $\mathcal{E}, \mathcal{E}'$ be divisors of degree g , and let f, f' be $\mathcal{E}, \mathcal{E}'$ -approximants, respectively. Then (notation of (1))

$$(ff') + \mathcal{E} + \mathcal{E}' = Z_f + Z_{f'}$$

Let \mathcal{E}'' be any divisor of degree g . Then $Z_f + Z_{f'} - \mathcal{E}''$ has degree g , so let ϕ be an approximant. We have

$$(ff'\phi) + \mathcal{E} + \mathcal{E}' - \mathcal{E}'' = Z_\phi$$

so that $ff'\phi$ is an $(\mathcal{E} + \mathcal{E}' - \mathcal{E}'')$ -approximant, (not necessarily quasi-extremal even when f, f', ϕ are).

In applications, we shall be given a sequence $\{\mathcal{E}_n\}$ of divisors of degree g and want to generate, by some iterative procedure, the \mathcal{E}_n -approximants or some subset of them. In good cases, for a suitable choice of \mathcal{E}'' , one gets $\mathcal{E}_n + \mathcal{E}_{n'} - \mathcal{E}'' = \mathcal{E}_k$, where $k \approx n + n'$.

Suppose given a sequence $\{\mathcal{E}_n\}$ as above, and an inclusion $K[x] \subseteq K(C)$ (corresponding to a cover $C \rightarrow \mathbb{P}^1 = \mathbb{A}^1 \cup \infty$).

Definition 2.3. *An \mathcal{E}_n -approximant f_n is extremal if it is not of the form $u(x)f_m$ where $m < n$, f_m is an \mathcal{E}_m -approximant and $u \in K[x]$.*

Generally speaking, we seek algorithms which generate iteratively only the successive extremal approximants.

2.2 Examples

1. Suppose C hyperelliptic, with two points at infinity, denoted ∞^+ , ∞^- . Let $B \geq 0$ be an effective divisor on C of degree b , $0 \leq b \leq g$; assume $\text{Supp}(B)$ consists of finite points and contains no hyperelliptic pair. (A *hyperelliptic pair* is a pair $\{R, R^-\}$ consisting of a point R of a hyperelliptic curve and its image R^- under the hyperelliptic involution. This terminology will be used frequently). Define $\mathcal{E}_n = B - n\infty^+ + (n + g - b)\infty^-$. If $\infty^+ - \infty^-$ is torsion of order N and $h \in K(C)$, $(h) = N(\infty^+ - \infty^-)$, then

$$(h) + \mathcal{E}_n = D + (N - n)\infty^+ + (n - N + g - b)\infty^-$$

The right-hand side is an effective divisor iff $N - g + b \leq n \leq N$, so h is an \mathcal{E}_n -approximant for all n in this range. Using a variant of Prop. 4.1 below, it is easy to see that h is a quasi-extremal \mathcal{E}_{N-g+b} and \mathcal{E}_N -approximant. By definition (2.3) it is an extremal \mathcal{E}_{N-g+b} approximant, but not an extremal \mathcal{E}_N -approximant. (Take $u = 1$ in def. 2.3). Thus h can be found by generating successive extremal approximants. The classical CFE of a suitable function in $K(C)$ does this, i.e. the approximants of the expansion are the successive extremal \mathcal{E}_i approximants. This is the origin of our terminology. The multiplicative method 2.1, when $B = 0$, reduces to Shanks' infrastructure method for finding the regulator of a quadratic extension (c.f. [10]), generally with $\mathcal{E}'' = g\infty^-$. These considerations lead to simple proofs of known results on classical hyperelliptic continued fractions.

2. Suppose P_1, P_2, P_3 are points on an arbitrary C , and suppose $P_1 + P_2 - 2P_3$ is N -torsion. Let $h \in K(C)$, $(h) = N(P_1 + P_2) - 2NP_3$. Then, generalizing the previous example, we can define $\mathcal{E}_n = -n(P_1 + P_2) + (2n+g)P_3$. h is a quasi-extremal \mathcal{E}_N -approximant, provided gP_3 is non-special. If g is even, then h is a quasi-extremal \mathcal{E}_R -approximant with $R = N - g/2$, provided $g(P_1 + P_2)/2$ is non-special. Thus again, h can be found by generating a sequence of quasi-extremal \mathcal{E}_i -approximants for appropriate \mathcal{E}_i . This appears to be the underlying philosophy of [14].

3 Hyperelliptic curves

We now assume C hyperelliptic with hyperelliptic double cover $\pi : C \rightarrow \mathbb{P}^1$. The hyperelliptic involution $C \rightarrow C$ is denoted $U \mapsto U^-$, for any object on which it acts. Choose an affine coordinate x on \mathbb{P}^1 , i.e. a function $x \in K(\mathbb{P}^1)$ with just one simple pole which we denote ∞ . Then $\mathbb{P}^1 = \mathbb{A}^1 \cup \infty$ and $K(\mathbb{P}^1) = K(\mathbb{A}^1) = K(x)$. Via π , $K(x) \subset K(C)$, and Nm and Tr are the norm and trace of this extension. For $f \in K(C)$, $P \in C$, $\text{ord}_P(f)$ denotes the value of f in the discrete valuation defined by P .

If $\pi^{-1}(\infty)$ consists of a single point of C , this is also denoted ∞ ; if it consists of two points we call them ∞^+ and ∞^- . (Note that ∞^+ and ∞^- may not be defined over K , though the divisor $\infty^+ + \infty^-$ is.) Set $D_\infty = \infty^+ + \infty^-$ or 2∞ according as C has one or two points at infinity. If $u(x) \in K[x] \subset K(C)$ then (u) always means the divisor of u considered as function on C , so $(u) = (u)_0 - (\deg u)D_\infty$, where $(u)_0$ denotes the divisor of zeros of u , a divisor consisting entirely of hyperelliptic pairs.

To make explicit calculations, choose a function $y \in K(C)$ integral over $K[x]$, with poles at infinity of order $g+1$ or $2g+1$ according as there are two points or one point at infinity. Let the minimal polynomial of y be $Y^2 + \beta Y - \phi = 0$, where $\beta(x), \phi(x) \in K[x]$, and the affine curve defined by the minimal polynomial is non-singular. Then $y^- = -y - \beta$, $\text{Tr}(y) = -\beta$ and $\text{Nm}(y) = -\phi$. Finally, if D is an effective divisor on C , supported on finite points and without hyperelliptic pairs, then a *pole descriptor* for D is any $f_D \in \mathcal{L}(D + (g+1 - \deg D)D_\infty)$, of the form $(\ell+y)/d(x)$, where $\ell(x), d(x) \in K[x]$ and $d(x)$ is zero on D . (This implies $d(x)$ divides $\text{Nm}(\ell(x) + y)$ and $\deg d(x) = \deg D$. Aficionados of the ideal-theoretic approach to algebraic curves will recognise $(d(x), \ell(x) + y)$ as a basis of the ideal corresponding to

D). Thus for example if $D = 0$ a pole descriptor is any function $y + \ell(x)$ where $\deg \ell \leq g + 1$. If P is a point of C with affine coordinates $(a, b) \in k^2$ and $D = P$, then a pole descriptor for D is any function $(y + \ell(x))/(x - a)$ where $\ell(a) = b$, $\deg \ell(x) \leq g + 1$. A pole descriptor $y + \ell(x)/d(x)$ can be normalised by requiring $d(x)$ monic and $\deg \ell(x) < \deg d(x)$. Such a normalised descriptor is uniquely determined by the divisor D ; however, in our continued fraction algorithm (and in the classical CFE) non-normalised descriptors appear naturally, so we shall not insist on normalisation.

4 Approximants on C

Let $D = P + Q$ where P, Q are finite points and $P \neq Q^-$. Fix a non-special divisor $B \geq 0$, whose support does not contain P^-, Q^- , and such that $\deg B \leq g$ and $g \equiv \deg B \pmod{2}$. Set $\epsilon = (g - \deg B)/2$.

For $n \in \mathbf{N}$ set

$$\mathcal{E}_n = \mathcal{E}_n(B) = -nD + B + (n + \epsilon)D_\infty$$

Then \mathcal{E}_n has degree g and we look for \mathcal{E}_n -approximants, which we henceforth abbreviate as n -approximants. We also write Z_n instead of Z_f , when f is an n -approximant. We note that our approximants are a type of two-point Padé approximant, and no doubt some of the results of this section are special cases of known results in Padé theory.

Lemma 4.1. *An n -approximant is quasi-extremal iff Z_n has no hyperelliptic pairs in its support. An n -approximant is extremal iff $Z_n + D$ has no hyperelliptic pairs in its support. Thus an extremal approximant is quasi-extremal.*

Proof. An effective divisor of degree g on C is special iff its support contains a hyperelliptic pair, from which, and Prop. 2.2, the first affirmation follows. For the second, Let f_n be an n -approximant. Suppose f_n not extremal. Then $f_n = uf_m$ for some polynomial $u(x)$ and m -approximant f_m , $m < n$. If u isn't constant, then the divisor of zeros of uf contains the hyperelliptic pairs which are the divisors of zeros of u ; if u is constant, then f_m is also an n approximant, so must have zeros of order $\geq n$ at D . Since $\mathcal{E}_n = \mathcal{E}_m - (n - m)D + (n - m)D_\infty$, we have $Z_n = (f_n) + \mathcal{E}_n = (f_m) + \mathcal{E}_n = Z^* + (n - m)D_\infty$ where Z^* is effective, and $\text{Supp}(Z_n)$ contains the hyperelliptic pair D_∞ . Thus sufficiency of the second condition follows. For necessity, suppose that $Z_n + D$

contains a hyperelliptic pair, say $R + R^-$, where R may or may not coincide with one of P, Q or be at infinity. If R is at infinity then as in the first part of the argument f_n is also an f_{n-1} approximant, so f_n isn't extremal. If R is a finite point then let $v \in K[x]$ have divisor $R + R^- - D_\infty$. One sees immediately that f_n/v is an $(n-1)$ -approximant, no matter if R coincides with one of P, Q or not, so again $f_n = v \cdot f_n/v$ isn't extremal. \square

Proposition 4.2. *Suppose $D - D_\infty$ is torsion of order N , and let $h \in K(C)$, $(h) = N(D - D_\infty)$. Then h is an extremal $N - \epsilon$ -approximant.*

Proof. From the definitions

$$(h) + \mathcal{E}_{N-\epsilon} = \epsilon D + B$$

Thus h is an $N - \epsilon$ -approximant. It is extremal by Lemma 4.1, since, again by the definitions of D and B , $\epsilon D + B$ contains no hyperelliptic pairs. \square

Prop. 4.2 shows that h and N can be found by generating successive extremal n -approximants.

Let f be an n -approximant. It may have zeros of order greater than n at P, Q and it is often convenient to make this explicit. Therefore we introduce the divisor \hat{Z}_n defined by

$$Z_n = aP + bQ + \hat{Z}_n \tag{2}$$

where $a, b \geq 0$ and $\text{Supp}(\hat{Z}_n)$ is disjoint from P, Q . In this notation, if f is an n -approximant, then

$$(f) = nD + aP + bQ + \hat{Z}_n - B - (n + \epsilon)D_\infty \tag{3}$$

Proposition 4.3. *Let f be an extremal n -approximant. With the notation just introduced, for $n < m \leq n + a + b$ there is no extremal m -approximant, but there is an extremal $m = n + a + b + 1$ -approximant.*

Proof. It is straightforward to see that there exist polynomials $u_k \in K[x]$ such that the functions $u_k f_n$ are (non-extremal) $n + k$ -approximants iff $k \leq a + b$. Since an extremal approximant is unique up to constant multiples, there can be no extremal m -approximants where non-extremal m -approximants exist. This proves the first affirmation. For the second, set $m = n + a + b + 1$.

Observe that an m -approximant cannot be of the form uf_n with $u \in K[x]$ -this would require $\deg u \geq a + b + 1$. Moreover, if u is a polynomial of degree $a + b$ with zeros of order b, a at P, Q respectively, then

$$(uf_n) + \mathcal{E}_{m-1} = \hat{Z}_n + bP^- + aQ^-$$

hence by Lemma 4.1 and the definition of \hat{Z}_n , uf_n is a quasi-extremal $(m - 1)$ -approximant. Thus up to constant multiples, uf_n is the only $(m - 1)$ -approximant. Now let f^* be an m -approximant, with $(f^*) + m\mathcal{E} = Z^*$. If f^* is not extremal then $\text{Supp}(Z^* + D)$ contains a pair $R + R^-$ for some point $R \in C$. If R is at infinity then $(f^*)_\infty \leq (\epsilon + m - 1)D_\infty$, so that f^* is an $(m - 1)$ -approximant. (Here $(f^*)_\infty$ denotes the divisor of poles of f^* .) But any $(m - 1)$ -approximant is a constant multiple of uf and we have observed that f^* cannot be a polynomial multiple of f . Similarly, if R is a finite point then dividing by $v(x)$ where $(v) = R + R^- - D_\infty$ leaves f/v as an $m - 1$ -approximant (even where $R = P$ or $R = Q$), and again we would have f^* a polynomial multiple of f . Thus no pair $R + R^-$ can occur in $\text{Supp}(Z^* + D)$ and f^* is extremal. \square

4.1 The continued fraction expansion

We continue with the notation of the previous section. We shall describe the continued fraction for the case that either $B = 0$, or B is supported on finite points. The modifications for other cases are left to the reader.

For $f \in K(C)$ regular at P, Q , and $m, n \geq 0$ integers, let $r(f, m, n) \in K[x]$ be the polynomial of least degree such that $f - r(f, m, n)$ has zeros of order $\geq m, n$ at P, Q respectively. We write $r(m, n)$ instead of $r(0, m, n)$, so $r(m, n) = (x - x(P))^m(x - x(Q))^n$ and $\deg r(m, n) = m + n$. Note that if f is non-zero at at least one of P, Q then $\deg r(f, m, n) \leq m + n - 1$. Finally, let f_B be a pole descriptor of B .

Initialise: $\gamma_0 := f_B; M_0 := \text{ord}_P \gamma_0; N_0 := \text{ord}_Q \gamma_0$
Iterate: for $i = 1, 2, 3 \dots$

1. If $i = 1$ then $\alpha_i := \epsilon + 1$ else $\alpha_i := \alpha_{i-1} + 1 + (M_{i-1} - \alpha_{i-1}) + (N_{i-1} - \alpha_{i-1})$
2. $u := \alpha_i - M_{i-1}; v = \alpha_i - N_{i-1}$.
3. $r_{i-1}(x) := r(\gamma_{i-1}, u, v)$
4. $m := \text{ord}_P(\gamma_{i-1} - r_{i-1}); n := \text{ord}_Q(\gamma_{i-1} - r_{i-1})$
5. $s_i(x) := r(m, n)$
6. $\gamma_i = \frac{s_i}{\gamma_{i-1} - r_{i-1}}$
7. $M_i := M_{i-1} + m; N_i := N_{i-1} + n$

The basic continued fraction algorithm
Table 1A.

The iteration described in Table 1A defines a continued fraction

$$\gamma_0 = r_0 + \frac{s_1}{r_1 + \frac{s_2}{r_2 + \dots}} \quad (4)$$

with polynomial r_i, s_i , together with functions $\gamma_i, i \geq 0 \in K(C)$ regular and non-zero at P and at Q , and sequences $\{(M_i, N_i)\}, \{\alpha_i\}$. The *convergents* of (4) are defined to be:

$$\left. \begin{aligned} p_1 &= r_0; q_1 = 1 \\ p_2 &= r_1 p_1 + s_1; q_2 = r_1 \\ p_{i+1} &= r_i p_i + s_i p_{i-1} \\ q_{i+1} &= r_i q_i + s_i q_{i-1} \end{aligned} \right\} i \geq 2$$

We now make a change in notation: we set $f_0 = 1, f_i = q_i f_B - p_i$ so that

henceforth f_i denotes the i th approximant of the continued fraction and not, as it has up to now, an \mathcal{E}_i -approximant.

Theorem 4.4. *The approximants $f_i = q_i\gamma_0 - p_i$, $i = 1, 2, \dots$ of the continued fraction expansion (4) are extremal α_i -approximants, with $(\text{ord}_P f_i, \text{ord}_Q f_i) = (M_i, N_i)$, and any extremal approximant is an α_i -approximant for some i . Moreover the γ_i are pole descriptors of the finite parts of the divisors \hat{Z}_{α_i} defined by eqn. (2).*

Proof. The proof goes by induction on i . A standard fact of continued fractions (cf. [9]) is

$$f_i = q_i\gamma_0 - p_i = \frac{(-1)^i s_1 \dots s_{i-1}}{\gamma_1 \dots \gamma_{i-1}} \quad (5)$$

Equivalently, using Table 1A(4)

$$f_i = -f_{i-1} \cdot (\gamma_{i-1} - r_{i-1}) \quad (6)$$

If $i = 1$, then by inspection $f_1 = \gamma_B - r_0$ is an extremal $\alpha_1 = \epsilon + 1$ approximant. (In fact it is not hard to see that $\epsilon + 1$ is the least α such that there exists an extremal α -approximant), and by definition $(M_1, N_1) = (\text{ord}_P f_1, \text{ord}_Q f_1)$. Thus the theorem is true for $i = 1$. Now assume $i \geq 2$ and that the theorem is true up to level $i - 1$. Then by the induction hypothesis f_{i-1} is an extremal α_{i-1} approximant and

$$(f_{i-1}) = \alpha_{i-1}D + (M_{i-1} - \alpha_{i-1})P + (N_{i-1} - \alpha_{i-1})Q + \hat{Z}_{\alpha_{i-1}} - (\alpha_{i-1} + \epsilon)D_\infty$$

By Prop. 4.3, the next extremal approximant is an α_i approximant, where α_i is as given Table 1A(1). Now, using equation (6)

$$\text{ord}_P f_i = \text{ord}_P f_{i-1} + \text{ord}_P(\gamma_{i-1} - r_{i-1})$$

$\text{ord}_P f_{i-1} = M_{i-1} \geq \alpha_{i-1}$ by the induction hypothesis and $\text{ord}_P(\gamma_{i-1} - r_{i-1}) = m \geq u$ by definition (Table 1A (2) and (3)). Thus $\text{ord}_P f_i \geq \alpha_{i-1} + u = \alpha_i$ (Table 1 (4)). Similarly $\text{ord}_Q f_i \geq \alpha_i$. Thus to show f_{i+1} is an α_{i+1} -approximant it only remains to show that $(f_i)_\infty \leq (\alpha_i + \epsilon)D_\infty$, where $(f_i)_\infty$ denotes that part of (f) supported at infinity. The recurrences on p_i, q_i and the definition of f_i yield,

$$f_i = r_{i-1}f_{i-1} + s_{i-1}f_{i-2} \quad (7)$$

for $i \geq 2$. Thus $(f_i)_\infty \leq \max((r_{i-1}f_{i-1})_\infty, (s_{i-1}f_{i-2})_\infty)$. Since, by definition of the polynomial $r(f, a, b)$, $\deg r_{i-1} \leq u+v-1$, and by the inductive hypothesis $(f_{i-1})_\infty \leq (\alpha_{i-1} + \epsilon)D_\infty$ we have $(r_{i-1}f_{i-1})_\infty \leq (u+v-1 + \alpha_{i-1} + \epsilon)D_\infty = (\alpha_i + \epsilon D_\infty)$. Similarly, using the induction hypothesis for f_{i-2} and (by an easy manipulation of the the formulae of Table 1A), $\alpha_{i+1} = \alpha_{i-1} + \deg s_i$, we find that $(s_{i-1}f_{i-2})_\infty \leq (\alpha_i + \epsilon D_\infty)$. We conclude $(f_{i+1})_\infty \leq (\alpha_{i+1} + \epsilon)D_\infty$, so that f_{i+1} is an extremal α_{i+1} -approximant. For the final assertion of the Theorem, note that, since the f_i have finite poles only on B , then in view of equation (6), the divisor of finite zeros of f_i is \geq the divisor of finite poles of γ_i , (since this is also the divisor of finite poles of $\gamma_i - r_i$). If the divisors are not equal then f_i and f_{i+1} have a finite zero in common, not P or Q . But then equation (7) shows that this finite zero is common to all the f_i , $i \geq 1$. But $f_2 = r_1f_1 - s_1$ so f_2 and f_1 cannot have a finite zero in common except P, Q . This contradiction establishes the final affirmation of the theorem. \square

The algorithm in Table 1A is inefficient. A more efficient, though more obscure, version is given in Table 1B. An example is given in Fig. 2 (where the notation comes from Table 1B and Prop.4.7). The example comes from [11], with a change of coordinates.

Initialise: $u_0 := v_0 := \epsilon + 1$; $\gamma_0 := f_B$; $M_0 := N_0 := 0$
Iterate: for $i = 1, 2, 3 \dots$

1. $r_{i-1}(x) := r(\gamma_{i-1}, u_{i-1}, v_{i-1})$
2. $m_i := \text{ord}_P(\gamma_{i-1} - r_{i-1})$; $n_i := \text{ord}_Q(\gamma_{i-1} - r_{i-1})$
3. $s_i(x) := r(m_i, n_i)$
4. $\gamma_i = \frac{s_i}{\gamma_{i-1} - r_{i-1}}$
5. $u_i := 1 + n_i - v_{i-1}$; $v_i = 1 + m_i - u_{i-1}$
6. $M_i := M_{i-1} + m_i$; $N_i := N_{i-1} + n_i$
7. $\alpha_i = M_{i-1} + u_{i-1}$

A somewhat more efficient version of the continued fraction algorithm.
Table 1B.

4.2 Properties of the continued fraction

In this section we show that our CFE has most of the properties associated with the classical CFE, up to minor modifications. A sequence of functions u_i is *quasi-periodic* of quasi-period k if there are constants c_i such that $u_{i+k} = c_i u_i$ for all $i \geq 1$. We say our continued fraction expansion is quasi-periodic of quasi-period k if $\{r_i\}$ and $\{s_i\}$ are quasi-periodic sequences of quasi-period k . Then, since the s_i are monic, they form a periodic sequence, and it is easy to see that the γ_i also form a quasi-periodic sequence of the same quasi-period.

Theorem 4.5. *The continued fraction expansion is quasi-periodic iff $D - D_\infty$ is torsion. If the torsion is N then the quasi-period $k \leq N - \epsilon$.*

Proof. Suppose $D - D_\infty$ has torsion N and that $h \in K(C)$ exhibits the torsion, i.e. $(h) = N(D - D_\infty)$. As we have already observed, h is an extremal $N - \epsilon$ -approximant, and so by Thm. 4.4, $h = f_k$ for some $k \leq N - \epsilon$. By

Prop. 4.3, the next extremal approximant, which is f_{k+1} , is an $N + \epsilon + 1$ -approximant. But, inspecting its divisor, hf_1 is an $N + \epsilon + 1$ -approximant. Therefore, by uniqueness of extremal approximants, there is a constant c_1 such that $f_{k+1} = c_1hf_1$. Then, by induction and a similar argument about divisors, for all j there are constants c_j such that $f_{j+k} = c_jhf_j$. It then follows from (5) and the fact that the s_j are zero on P, Q while the γ_j are non-zero, that the s_j form a periodic sequence of period k and the γ_j a quasi-periodic sequence of quasi-period k , whence the r_j also form a quasi-period sequence of quasi-period k , as was to be proved. The converse can be proved by reversing the steps in this argument. \square

Henceforth, unless otherwise stated, we assume that $D - D_\infty$ is torsion of order N and that $h \in K(C)$ exhibits the torsion. By the previous theorem the CFE is quasi-periodic of quasi-period $k \leq N$.

Assume $B = B^-$. This means either $B = 0$ or B is supported on branch points. $B = \infty$ is not excluded. We show that under this hypothesis our CFE enjoys a symmetry analogous to that enjoyed by the classical CFE under a similar hypothesis.

Theorem 4.6. *If $1 \leq i, j$ and $i + j = k$ then, with the notation of Table 1(A or B) and Lemma 2, $M_i + M_j = N_i + N_j = N$ and $\hat{Z}_i = \hat{Z}_j^-$. Conversely, if in the CFE for some pair i, j $M_i + M_j = N_i + N_j = M$ and $\hat{Z}_i = \hat{Z}_j^-$ then N divides M and $N = M$ if i, j are less than the pseudoperiod.*

Proof. For given i , f_i is an extremal α_i -approximant where $i \leq \alpha_i$ so

$$(f_i) = M_iP + N_iQ + \hat{Z}_i - B - (\epsilon + \alpha_i)D_\infty$$

conjugating and multiplying by $h = f_k$

$$\begin{aligned} hf_i^- &= M_iP^- + N_iQ_i^- + N(P + Q) - B^- + \hat{Z}_i^- - (\epsilon + \alpha_i + N)D_\infty \\ &= M_i(P + P^-) + N_i(Q + Q^-) + (N - M_i)P - B^- \\ &\quad + (N - N_i)Q + \hat{Z}_i^- - (\epsilon + \alpha_i + N)D_\infty \end{aligned}$$

Let $u \in K[x]$ have divisor $(u) = M_i(P + P^-) + N_i(Q + Q^-) - (M_i + N_i)D_\infty$. Then (using $B = B^-$)

$$\begin{aligned} (hf_i^-/u) &= (N - M_i)P + (N - N_i)Q \\ &\quad - B + \hat{Z}_i^- - (\epsilon + \alpha_i + N - M_i - N_i)D_\infty \quad (8) \end{aligned}$$

Notice that $\alpha_i + N - M_i - N_i = N - \alpha_i - m_i - n_i$, in the notation of Table 1B. Thus (8) exhibits hf_i^-/u as an $N - \alpha_i - m_i - n_i$ -approximant, extremal by Lemma 4.3 (using f_i extremal). Thus, for some $j(i)$, hf_i^-/u is a constant multiple of $f_{j(i)}$, with $\alpha_{j(i)} = N - \alpha_i - m_i - n_i$. The $\alpha_i, i \geq 1$ form a strictly increasing sequence, the $\alpha_{j(i)}$ form a strictly decreasing sequence, from which $i + j(i) = k$ follows. The converse is left to the reader. \square

The results of the following proposition complete the basic continued fraction algorithm.

Proposition 4.7. *With the notation of the previous paragraph*

1. For all $i \geq 0$ $\gamma_i = \frac{\lambda_i + y}{\mu_i}$ where $\lambda_i, \mu_i \in K[x]$ and μ_i divides $Nm(\lambda_i + y)$.
2. $\lambda_{i+1} = r_i \mu_i - \lambda_i - \text{Tr}(y)$
3. $\mu_{i+1} = \frac{-Nm(\lambda_{i+1} + y)}{s_{i+1} \mu_i}$
4. For $i \geq 2$ $\mu_{i+1} = \frac{r_i(\lambda_i - \lambda_{i+1}) + s_i \mu_{i-1}}{s_{i+1}}$
5. $\hat{Z}_i = \hat{Z}_i^-$ if and only if $\lambda_i = \lambda_{i+1}$, and, if there are two points at infinity on C , $\deg \mu_i + (M_i - \alpha_i) + (N_i - \alpha_i) = g$. (This condition ensures that \hat{Z}_i is supported only on finite points.)
6. $\hat{Z}_i = \hat{Z}_{i+1}^-$ if and only if $\mu_i = c \mu_{i+1}$ for some constant c .

The Prop. can be established by arguments essentially the same as for the classical CFE; c.f. [3, 9].

In the light of theorems 4.5 and 4.6, the basic algorithm to find the torsion N of $D - D_\infty$ and $D - D^-$ is : develop the continued fraction until either $\hat{Z}_i = \hat{Z}_i^-$ and $M_i = N_i$, in which case $N = 2M_i$, (and the torsion of $D - D^-$ is M_i), or $\hat{Z}_i^- = \hat{Z}_{i+1}$ and $M_i + M_{i+1} = N_i + N_{i+1}$, in which case $N = M_i + M_{i+1}$ (and the torsion of $D - D^-$ is also N). Of course, this presupposes that the divisors in question are torsion. This will always be the case when everything is defined over a finite field. Over an infinite field, the divisors are unlikely to have finite order, and one would only run the algorithm in the presence of a bound for the possible torsion. (There are various methods of obtaining such bounds.). However, continued fractions in characteristic zero

are something of a delusion: the methods of Alf van der Poorten ([17]) apply also to our fraction, and show that, when say everything is defined over \mathbb{Q} , coefficient growth in the non-torsion case is doubly exponential, which makes the algorithm unusable.

In the example of Fig. 2, developing to $i = 9$ shows the divisor is 29-torsion, but (6) of Prop. 4.7 applies at $i = 4$ and thus it is only necessary to develop the fraction as far as $i = 5$ to determine the torsion.

It is not hard to see that the complexity, measured as the number of polynomial operations in one round of the continued fraction algorithm is $O(g^2)$, which is the same as the complexity of an addition in the Jacobian, using Cantor's algorithm [5].

4.3 Baby-step giant-step algorithms for the continued fraction

The basic baby-step giant step algorithm finds the order of an element t in a group, when the order is finite, as follows: for a suitably chosen integer b , compute t^i , $i = 1..b$ and keep a table of these values; these are the baby steps. Then compute t^{kb} , $k = 1, 2, \dots$; these are the giant steps. At each giant step compare t^{kb} with members of the table; if $t^{kb} = t^i$ for some $k, i \leq b$ then the order of t can be deduced, provided b is properly chosen. See [10] for details. Shanks extended this idea to give an algorithm (c.f.[10]) to find the regulator of a real quadratic number field. The baby steps of Shanks' algorithm are the iterations of the continued fraction expansion of a quadratic irrationality; the giant steps come from a type of multiplicative structure—the *infrastructure*, enjoyed by the approximants. Shanks' method was adapted by A. Stein to the case of the function field of a hyperelliptic curve over a finite field with two points at infinity, in which case the regulator is just the torsion of the divisor $\infty^+ - \infty^-$. The latest on Stein's algorithm can be found in [16]. Here, we adapt these ideas to the present situation. We continue with the notation of the previous sections.

Suppose $D - D_\infty$ is torsion of order N , and $(h) = N(D - D_\infty)$. We apply the technique, and use the notation, of §2.1. Recall $\{f_i\}$ denotes the sequence of *extremal* approximants, and that $h = f_k$ for some k , so that we can find h and N by computing the sequence $\{f_i\}$ from the convergents of the continued fraction expansion. Now suppose that f_i, f_j are extremal α_i, α_j

approximants respectively . Define s and a divisor $E \geq 0$, by

$$Z_i + Z_j = \hat{Z}_i + \hat{Z}_j + sD + E \quad (9)$$

where $s \geq 0$ and if $E \neq 0$ then E is supported on at most one of P, Q . Note that, in the generic case, $s = 0, E = 0$. Thus

$$(f_i f_j) = (\alpha_i + \alpha_j + s)D + E + \hat{Z}_i + \hat{Z}_j - 2B - ((\alpha_i + \alpha_j + 2\epsilon)D_\infty)$$

We apply the theory of §2.1, and use notation of that section and §3. Set $\mathcal{E} = \mathcal{E}_i, \mathcal{E}' = \mathcal{E}_j$ and $\mathcal{E}'' = (\epsilon - s)D_\infty + sD + B$. (A little arithmetic shows that $\deg \mathcal{E}'' = g$). Then, from §2.1, if

$$\phi \in \mathcal{L}(Z_i + Z_j - \mathcal{E}'')$$

then $f_i f_j \phi$ is an $\mathcal{E} + \mathcal{E}' - \mathcal{E}''$ -approximant We have

$$\mathcal{E} + \mathcal{E}' - \mathcal{E}'' = -(\alpha_i + \alpha_j + s)D + B + (\alpha_i + \alpha_j + s - \epsilon)D_\infty$$

so that $f_i f_j \phi$ is an $\alpha = (\alpha_i + \alpha_j + s)$ approximant, in general neither extremal nor quasi-extremal. From this, an extremal approximant can be derived by dividing out by a suitable polynomial $u(x)$ and appropriately adjusting the value of α . Then $f_i f_j \phi / u$, being an extremal approximant, is a constant multiple of f_ℓ for some unknown index ℓ . By Lemma 4.3, $0 \leq \deg u \leq g + 1$, so $\alpha_i + \alpha_j + s - g - 1 \leq \alpha_\ell \leq \alpha_i + \alpha_k + s$. Since, generically, $\alpha_{i+1} = \alpha_i + 1$, we have that, in general ℓ is of the order of $i + j + s$. The passage from f_i, f_j to f_ℓ may be considered a giant step for the sequence $\{f_i\}$.

We note that $Z_i + Z_j - \mathcal{E}'' = \hat{Z}_i + \hat{Z}_j - (\epsilon - s)D_\infty + B - E$. Thus the calculation of ϕ uses only data directly available from the continued fraction algorithm. Indeed, in the giant step one only needs to handle the f_i explicitly if one needs h explicitly; if only N is needed all the data associated with f_ℓ can be calculated from the data provided by the continued fraction iterations-the baby steps. This is a great advantage since the f_i may be very large objects, while the functions generated explicitly by the CFE are of bounded size. The giant step takes as input data $\Delta_i = (\alpha_i, M_i, N_i, \gamma_i)$ as defined in Table 1A (or B), for two indices i, j . From these data, a set Δ_ℓ is generated, for some unknown index ℓ . Schematically, the giant step is as follows:

Input: $i, j \geq 1, \Delta_i, \Delta_j$ from the CFE of Table 1B.

Output: $\Delta = (\alpha, S, T, g)$ such that $\Delta = \Delta_k$ for some unknown k .

1. Find $s \geq 0$ and E as defined by (9).
2. $\alpha := \alpha_i + \alpha_j + s$; $S := M_i + M_j$; $T := N_i + N_j$.
3. $\mathcal{E} := \hat{Z}_i + \hat{Z}_j + E - B - (\epsilon - s)D_\infty$. Find $\phi \in \mathcal{L}(\mathcal{E})$
4. $Z := \mathcal{E} + (\phi)$. Remove hyperelliptic pairs from $\alpha D + Z$, modifying α, S, T, ϕ appropriately..
5. Return $\Delta := (\alpha, S, T, \phi)$.

The addition of divisors given by pole descriptors is done using the algorithm of [5]. The algorithm of [4] can be used in step 3 to compute ϕ .
 Example. We apply the algorithm to the example of Fig. 4.1 with input Δ_2, Δ_3 . Here

$$\Delta_2 = (4, 7, 5, \gamma_2), \Delta_3 = (9, 9, 9, \gamma_3)$$

where $\gamma_i = (\lambda_i + y)/\mu_i$, the λ_i, μ_i being given in Fig. 4.1. In what follows, if D is a finite divisor without hyperelliptic pairs then γ_D denotes a pole descriptor of D .

1. $s := \epsilon - s := 1$, $E := 2P$, $\alpha := 14$, $S := 16$, $T := 14$
2. $\gamma_P = \frac{y+2}{x}$ whence $\gamma_E = \frac{-10x+2+y}{x^2}$
3. Since μ_2 is constant $\hat{Z}_2 = 0$ and a pole descriptor of $\hat{Z}_3 + E$ is $\gamma := (\lambda+y)/\mu$ where $\lambda = 6x^5 - 2x^4 - 12x^3 + 18x^2 - 10x + 2$, $\mu = 80x^6 - 160x^5 + 160x^4 - 80x^3 + 16x^2$. In this simple case $\phi := \gamma$, since $\gamma \in \mathcal{L}(\hat{Z} - D_\infty)$.
4. The divisor $Z = \mathcal{E} + (\phi)$ is just the divisor of finite zeros of ϕ . Thus a pole descriptor is $\gamma_Z := (\lambda - y)/\mu^*$ where $\mu^* = \text{Nm}\gamma$. We find $\mu^* = (x-1)^4$.
5. Calculating, $L(1) = 2$. Thus γ_Z has finite pole divisor $4Q^-$. Remove $4(Q + Q^-)$ from $14D + Z$. This gives $\alpha := \alpha - 4$; $T := T - 4$; $Z = 0$.
6. Return($\Delta = (10, 14, 10, y)$). Thus Δ is equivalent to Δ_4 , an anti-climactic result, to be expected with these small indices.

Here is a brief description of the baby-step giant-step algorithm to find N , assuming the symmetries described in §4.2 hold: develop the continued fraction to a suitably chosen level i , keeping a table of the $\Delta_j, j \leq i$. Note that $i < k/2$ otherwise (Theorem 4.6) these baby steps would already find N . Then perform giant steps taking, e.g. Δ_i with itself. Because of periodicity and the symmetries, we can tell, comparing the output of each giant step with the table of initial values, when the output Δ is Δ_ℓ for $\ell \in [k-i, k+i]$. When this happens, N can be calculated. There are many technical details to be attended to; these can be deduced from those of the classical CFE given in [16].

5 General divisors

We briefly indicate the difficulties involved in extending the above to divisors D of degree > 2 .

Generalizing the situation of degree 2, let $D = \sum_{i=1}^d P_i$, $D_\infty = d\infty$ (we assume there is just one point at infinity) where P_1, \dots, P_d are (not necessarily distinct) finite points of C and $d \leq g$; assume there are no hyperelliptic pairs in $\text{Supp}D$. Define ϵ, b by $g = \epsilon d + b$, and $\mathcal{E}_n = -nD + B + (\epsilon + n)D_\infty$ where B is an effective divisor of degree b , satisfying the conditions described in §3. Then, if $D - D_\infty$ is N torsion and $h \in K(C)$ exhibits the torsion, h is an extremal $N - \epsilon$ -approximant, and any iterative method for generating extremal approximants will arrive at h, N . The analogue of Lemma 4.1 for extremality holds. However, Prop. 4.3 is no longer true—it only supplies a lower bound for the next extremal approximant. (The reader will have little difficulty verifying these and subsequent assertions). Worse, there does not appear to be any continued fraction whose convergents are exclusively the extremal \mathcal{E}_n -approximants. It seems necessary to define divisors $\mathcal{E}_{n,i,j} = -nD - P_i - P_j + (\epsilon + b)D_\infty + 2\infty$ and to move from an extremal \mathcal{E}_n to the next extremal \mathcal{E}_m via approximants of the $\mathcal{E}_{n,i,j}$, using the expansion of §3. This does not give an efficient algorithm.

References

- [1] N.H. Abel, *Ueber die Integration der Differential-Formel $\frac{\rho dx}{\sqrt{r}}$ wenn ρ und r ganze Functionen sind.*, J. Reine und Angew. Math. **1** (1826),

185–221.

- [2] W. W. Adams and M.J. Razar, *Multiples of points on elliptic curves and continued fractions*, Proc. Lond. Math. Soc. **41** (1980), 481–498.
- [3] T.G. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Archiv der Mathematik **55** (1990), 259–266.
- [4] ———, *Construction of linear systems on hyperelliptic curves*, Jour. Sym. Comp. **26** (1998), 315–327.
- [5] David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101. MR 88f:11118
- [6] P.L. Chebychev, *Sur l'intégration des différentielles irrationnelles qui contiennent une racine carré d'un polinome du troisième ou du quatrième degré.*(1857), Oeuvres Complètes, Vol. 1, pp. 171–200.
- [7] ———, *Sur l'intégration des différentielles irrationnelles (1853)*, Oeuvres Complètes, Vol. 1, Acad. Nauk, St. Petersburg, 1901, Reprinted by Chelsea Publishing Company, NY (undated)., pp. 147–168.
- [8] ———, *Sur l'intégration des différentielles qui contiennent une racine cubique (1865)*, Oeuvres Complètes, Vol. 1, Acad. Nauk, St. Petersburg, 1901, Reprinted by Chelsea Publishing Company, NY (undated)., pp. 563–608.
- [9] G. Chrystal, *Algebra. vol 1. vol 2*, Chelsea Publishing company, New York, 1959.
- [10] Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105
- [11] E. V. Flynn, *Large rational torsion on abelian varieties*, J. Number Theory **36** (1990), no. 3, 257–265. MR 92b:11036
- [12] G. Halphen, *Traité des fonctions elliptiques et leurs applications. tome 2.*, Paris, 1886-1891.
- [13] Sachar Paulus and Hans-Georg Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comput. **68** (1999), 1233–1241.

- [14] R. Scheidler and A. Stein, *Voronoi's algorithm in purely cubic congruence function fields of unit rank 1.*, Math. Comput. **69** (2000), no. 231, 1245–1266.
- [15] A. Stein and H.C. Williams, *Baby Step Giant Step in real quadratic function fields*, to appear (1997).
- [16] Andreas Stein and Hugh C. Williams, *Some methods for evaluating the regulator of a real quadratic function field*, Experiment. Math. **8** (1999), no. 2, 119–133. MR 2000f:11152
- [17] Alfred J. van der Poorten, *Non-periodic continued fractions in hyperelliptic function fields.*, Bull. Aust. Math. Soc. **64** (2001), no. 2, 331–343 (English).
- [18] Alfred J. van der Poorten and Xuan Chuong Tran, *Quasi-elliptic integrals and periodic continued fractions.*, Monatsh. Math. **131** (2000), no. 2, 155–169 (English).

i	$[u_i, v_i]$	$[m_i, n_i]$	$[M_i, N_i]$	α_i	$\deg p_i$	$\deg q_i$
0	(3 3)	—	—	—	—	—
1	(1 1)	(3 3)	(3 3)	3	5	0
2	(2 4)	(4 2)	(7 5)	4	6	0
3	(1 1)	(2 4)	(9 9)	9	11	6
4	(1 5)	(5 1)	(14 10)	10	12	6
5	(5 1)	(1 9)	(15 19)	15	17	12
6	(1 1)	(5 1)	(20 20)	20	22	17
7	(4 2)	(2 4)	(22 24)	21	23	18
8	(1 1)	(4 2)	(26 26)	26	28	23
9	(3 3)	(3 3)	(29 29)	27	29	24

i	λ_i	μ_i
0	0	1
1	$2x^5 + 10x^4 - 24x^3 + 22x^2 - 10x + 2$	$112x^4 - 208x^3 + 176x^2 - 80x + 16$
2	$-2x^5 + 18x^4 - 28x^3 + 22x^2 - 10x + 2$	1
3	$6x^5 - 2x^4 - 12x^3 + 18x^2 - 10x + 2$	$80x^4 - 160x^3 + 160x^2 - 80x + 16$
4	$-6x^5 + 22x^4 - 28x^3 + 22x^2 - 10x + 2$	1
5	$10x^5 - 18x^4 + 12x^3 + 2x^2 - 6x + 2$	16
6	$-6x^5 + 22x^4 - 28x^3 + 22x^2 - 10x + 2$	$5x^4 - 10x^3 + 10x^2 - 5x + 1$
7	$6x^5 - 2x^4 - 12x^3 + 18x^2 - 10x + 2$	16
8	$-2x^5 + 18x^4 - 28x^3 + 22x^2 - 10x + 2$	$7x^4 - 13x^3 + 11x^2 - 5x + 1$
9	$2x^5 + 10x^4 - 24x^3 + 22x^2 - 10x + 2$	16

i	r_i
0	$2x^5 + 10x^4 - 24x^3 + 22x^2 - 10x + 2$
1	$\frac{1}{4}$
2	$4x^5 + 16x^4 - 40x^3 + 40x^2 - 20x + 4$
3	$\frac{1}{4}$
4	$4x^5 + 4x^4 - 16x^3 + 24x^2 - 16x + 4$
5	$\frac{1}{4}x^5 + \frac{1}{4}x^4 - x^3 + \frac{3}{2}x^2 - x + \frac{1}{4}$
6	$\frac{1}{4}$
7	$\frac{1}{4}x^5 + x^4 - \frac{5}{2}x^3 + \frac{5}{2}x^2 - \frac{5}{4}x + \frac{1}{4}$
8	$\frac{1}{4}$
9	$\frac{1}{4}x^5 + \frac{5}{4}x^4 - 3x^3 + \frac{11}{4}x^2 - \frac{5}{4}x + \frac{1}{4}$

Figure 2: Data from the continued fraction associated to $D = P + Q$, $P = (0, 2)$, $Q = (1, 2)$ on the genus 4 curve $Y^2 = 116x^{10} - 504x^9 + 1140x^8 - 1736x^7 + 1968x^6 - 1712x^5 + 1132x^4 - 552x^3 + 188x^2 - 40x + 4$