

Continued fractions in hyperelliptic function fields.

T.G. Berry

Departamento de Matematicas Puras y Aplicadas

Universidad Simón Bolívar

Caracas

Venezuela

Abstract

Known results on hyperelliptic continued fractions, and in particular the Baby-Step Giant-Step algorithm, are obtained using algebro-geometric techniques. The methods used are valid in all characteristics and the proofs are simpler than those based on analogies with real quadratic number fields.

1 Introduction

This article contains virtually no new results. Its purpose is to show how the known properties of hyperelliptic continued fraction expansions, in particular the Baby-Step Giant-Step algorithm, can be derived very easily by algebro-geometric methods. In the published literature hyperelliptic continued fractions are mainly studied by adapting techniques from the theory of real quadratic number fields. The resulting proofs, while not extraordinarily difficult, can be quite intricate, and need slightly different arguments for even and odd characteristic. The geometric arguments work in all characteristics and are (to this author anyway) more transparent than their number-theoretic counterparts.

Notation and Conventions

Let K be an arbitrary field. Everything we define (curves, morphisms between curves, rational functions and divisors on curves etc...) is assumed to be defined over K . Let C be a non-singular hyperelliptic curve of genus p with hyperelliptic double cover $\pi : C \rightarrow \mathbf{P}^1$ (so π is a separable degree 2 map). The hyperelliptic involution $C \rightarrow C$ is denoted $U \mapsto U^-$, for any object on which it acts. Choose a point ∞ on \mathbf{P}^1 , and a function $x \in K(\mathbf{P}^1)$ with a simple pole at ∞ , and identify $K(\mathbf{P}^1)$ with $K(x)$. Then $K(x) \subset K(C)$ via π . *Norm* refer to norm of this extension. Assume that the pullback under π of the point at infinity on \mathbf{P}^1 consists of two distinct points, necessarily unramified, which we call, varying the notation slightly, ∞^+ and ∞^- ; without serious loss of generality, we assume that these points are defined over K . (If not, replace K by an appropriate quadratic extension). The discrete valuations of $K(C)$ corresponding to ∞^+ and ∞^- are denoted v_+, v_- respectively.

2 Continued fraction expansions

We recall the theory very briefly. For details and algorithms see [3, 6, 8].

Since ∞^+ is unramified, $1/x$ is a uniformising parameter, and defines an embedding $K(C) \rightarrow K((1/x))$ -we call the image of f *the Laurent series* of f (at ∞^+ , understood). Let $f \in K(C)$. The *polynomial part* of f , denoted $\lfloor f \rfloor$ is the principal part of the Laurent series of f , together with the constant term. Thus $\lfloor f \rfloor$ is a polynomial in x , and as such a well-defined rational function on C . The continued fraction expansion (henceforth abbreviated ‘‘CFE’’) of $f \in K(C) \setminus K(x)$ consists of sequences $\{a_i\}, \{p_i\}, \{q_i\} \in K[x], \{g_i\}, \{f_i\} \in K(C)$, defined iteratively by:

$$\begin{aligned} g_0 &= f; a_i = \lfloor g_i \rfloor; g_i = a_i + \frac{1}{g_{i+1}} \\ \frac{p_i}{q_i} &= [a_0, \dots, a_{i-1}] \text{ (in a standard notation for continued fractions. Note the indices!)} \\ f_0 &= 1; f_i = q_i f - p_i, i \geq 1 \end{aligned}$$

The a_i are the *partial quotients*, the p_i, q_i the *convergents*, and the g_i, f_i the *reducts* and the *approximants*, respectively, of f .

Let $y \in K(C) \setminus K(x)$ be a function with no finite poles, poles of order $p+1$ at both points at infinity, and whose zero set contains no pair of points twinned in the hyperelliptic involution. Then $K(C) = K(x)(y)$. We assume the affine plane curve defined by the minimal polynomial of y over $K(x)$ is non-singular.

We consider CFE's of functions $f \in K(C)$ of the form $(L+y)/M$, where $L, M \in K[x]$, L is monic, and M divides $\text{Norm}(L+y)$. We call these *standard functions*. (Zuccherato calls them *quadratic irrationalities*, but this seems a bit hard on the other functions in $K(C) \setminus K(x)$). The needed facts on CFE's are summarized in the following proposition.

Proposition 2.1. *Let $f \in K(C) \setminus K(x)$, and consider the CFE of f . For all $i \geq 0$:*

1. $\deg a_i > 0$ for $i > 0$.
2. If f is a standard function then so are its reducts, the g_i .
3. $\deg q_1 = 0$, and for $i \geq 2$, $\deg q_i = \sum_{j=1}^{i-1} \deg a_j$. Hence $\deg q_{i+1} = \deg q_i + \deg a_i$ and $\{\deg q_i\}$ is a strictly increasing sequence.
4. $f_i = \left(\prod_{j=0}^i g_j \right)^{-1}$.
5. (Diophantine approximation property.) For $i \geq 1$, the f_i satisfy $v_+(f_i) = \deg q_{i+1}$.

The divisor D of finite poles (i.e poles excluding ∞^+ and ∞^-) of a standard function is what is termed in [7] a *standard finite divisor*, that is, D is an effective divisor, no two points in the support of D are paired in the hyperelliptic involution, and branch points occur with multiplicity at most 1. Conversely, associated to such a divisor D there is a nearly canonical standard function called the *pole function* of D (cf [7]): it is the function $(L+y)/M$ with divisor of finite poles D , with L monic and $\deg L < \deg M$.

A basic theorem is

Theorem 2.2. *Let f_D be the pole function of a standard finite divisor D , and let $b \in \mathbf{Z}, b \geq 0$. Consider the CFE of f_D . Let k be the index for which $\deg q_k \leq \deg D + b - (g+1) < \deg q_{k+1}$. Then a K -basis of $\mathcal{L}(D + b\infty^-)$ is given by the functions $f_i, 0 \leq i \leq k$, together with functions $x^\alpha f_i$, where $1 \leq \alpha \leq \deg q_{i+1} - \deg q_i - 1$, if $i < k$, and $1 \leq \alpha \leq \deg D + b - (p+1) - \deg q_k$, if $i = k$.*

The proof is not difficult. The dimension $l(D+b\infty^-)$ is given by Riemann-Roch. One checks that the given functions are in $\mathcal{L}(D+b\infty^-)$, that they are linearly independent, and one counts them. For details see [7].

Observations:

1. In general one expects $\deg a_i = 1$, i.e. $\deg q_{i+1} = \deg q_i + 1$, so that the terms $x^\alpha f_i$ can be thought of as correction terms, which occur rarely.
2. The members of the basis have pairwise distinct zero orders at ∞^+ and pairwise distinct pole orders at ∞^- .
3. If $v_-(f_k) < 0$ then (c.f.[7])

$$v_-(f_k) = -(\deg q_k + p + 1 - \deg D) \quad (1)$$

The significance of the index k in the theorem is that it is the index for which $|v_-(f_k)| \leq b < |v_-(f_{k+1})|$.

We shall make considerable use of equation (1), often without explicit reference.

Consider f_k in the CFE of f_D . For some b , $f_k \in \mathcal{L}(D+b\infty^-)$, so

$$(f_k) = -D' + Z'_k + \text{components at infinity}$$

where $0 \leq D' \leq D$ and Z'_k is the divisor of finite zeros of f_k . It may well happen that $D' < D$, but by adding $D - D'$ to D' and to Z'_k , we can always write

$$(f_k) = -D + Z_k + \text{components at infinity} \quad (2)$$

where $Z_k = Z'_k + D - D'$. In particular, if $v_-(f_k) < 0$, then by Prop.2.1(4) and (5), and equation(1) we can write

$$(f_k) = -D + Z_k + \deg q_{i+1}\infty^+ - (\deg q_i + p + 1 - \deg D)\infty^- \quad (3)$$

We shall always write (f_k) in the form (2) or (3). The principal advantage is that, as is easily seen, using Prop.2.1(4) (c.f. [6]) Z_k is the divisor of finite poles of the function g_k . It is this that makes the CFE useful. Usually in curve theory the objects of basic interest are the spaces $\mathcal{L}(D)$; however, the functions in $\mathcal{L}(D)$ can be difficult to handle. In our case, for example, when k is large p_k, q_k are polynomials of high degree. For many (not all) purposes,

it is enough to know the Z_k , and these can be obtained from the g_k , which remain manageable for all $k \gg 0$, and which constitute, together with the a_i , the primary data of the CFE.

The following corollary of Theorem 2.2 is the principal tool used in the study of continued fractions. We continue with the premises and notation of Theorem 2.2.

Corollary 2.3. *Suppose there exists a standard finite divisor Z with degree $\leq p$ and and $h \in K(C)$, $h \neq \text{constant}$ such that*

$$(h) = -D + Z + a\infty^+ - b\infty^-$$

where $a, b \geq 0$. (Here, we allow D and Z to have points in common.) Then $\exists k$ such that h is a constant multiple of f_k , whence $Z = Z_k$.

Proof. The hypotheses imply that $h \in \mathcal{L}(D + b\infty^-)$. By theorem 2.2 a basis for this space is given by functions $x^\alpha f_i$ for appropriate indices α and $0 \leq i \leq k$ where k is the index such that $|v_-(f_k)| \leq b < |v_-(f_{k+1})|$. Observe that $a \leq a_k = v_+(f_k)$; indeed the orders of zero of our basis elements at ∞^+ are mutually distinct, so any linear combination, such as h , has order of zero the minimum of the orders of zero of functions occurring in the combination, while a_k is the highest order of zero of basis elements. Also $b_k = |v_-(f_k)| \leq b$ by choice. Thus

$$\left(\frac{f_k}{h}\right) = Z_k - Z + (a_k - a)\infty^+ + (b - b_k)\infty^-$$

has non-negative degree at infinity, so $f_k/h \in \mathcal{L}(Z)$. But Z is a standard finite divisor of degree $\leq p$; by Riemann-Roch $\mathcal{L}(Z) = K$, so $f_k/h = \text{constant}$ as was to be proved. \square

3 Applications

3.1 Reduction Algorithms

The results of this section are the hyperelliptic analogues of the theory of reduction of real quadratic forms.

A further corollary of Theorem 2.2 is:

Corollary 3.1. *[Reduction]*

1. Suppose $\deg D > p$. Let k be the index for which $\deg q_k \leq \deg D - (p + 1) < \deg q_{k+1}$. Then $\deg Z_k \leq p$ and $f_k \in \mathcal{L}(D)$.
2. With k the integer defined above, for all $i > k$ we can write

$$(f_i) = -D + Z_i + \text{components at infinity}$$

and $\deg Z_i \leq p$.

3. If $\deg D \leq p$ then $\deg Z_i \leq p$ for all $i \geq 0$.

Proof. (1). By Theorem 2.2, the function $f_k \in \mathcal{L}(D)$, so it only remains to prove $\deg Z_k \leq p$. We have

$$f_k = -D + Z_k + \deg q_{k+1} \infty^+ + b \infty^-$$

with $b \geq 0$. Taking degrees, we find $\deg Z_k = \deg D - \deg q_{k+1} - b$. But, by choice, $\deg D - (p + 1) < \deg q_{k+1}$, from which $\deg Z_k < p + 1 - b$ and it follows that $\deg Z_k \leq p$.

(2) Using again Theorem 2.2, for $i > k$ the function $f_i \notin \mathcal{L}(D)$, hence must have a pole at ∞^- . By the observations following Theorem 2.2, this implies $|v_-(f_i)| = \deg q_i + p + 1 - \deg D$. Then, taking degrees in equation 2 gives

$$\deg D = \deg Z_i + \deg q_{i+1} - \deg q_i - (p + 1) + \deg D$$

whence $p + 1 = \deg Z_i + \deg q_{i+1} - \deg q_i$. Since the $\deg q_i$ form a strictly increasing sequence, it follows that $\deg Z_i \leq p$.

(3) Follows from (2). □

Note that the order of zero at ∞^+ of the function f_k used in part (1) is strictly positive, since it is $\deg q_{k+1} > \deg q_k \geq 0$.

Let A be an effective divisor supported only on finite points. We wish now to find a rational function $\sigma \in K(C)$, a standard finite divisor A_{red} of degree $\leq p$, and non-negative integers u, v , such that

$$(\sigma) = -A + A_{red} + u \infty^+ + v \infty^-$$

We call this process *total reduction* of the divisor A .

First, by pairing up all hyperelliptic twins (i.e. pairs $P + P^-$) that may occur in A , we can write $A = A_1 + B$ where $B = \pi^* B_1$ for some divisor B_1 on \mathbf{P}^1 , and A_1 is a standard finite divisor on C . Then let $G \in K[x]$ be such

that $(G) = B_1 - (\deg G)\infty$ on \mathbf{P}^1 , so that $B_1 = (G) + (\deg G)\infty$; pulling back to C and substituting, we obtain

$$A = (G) + A_1 + (\deg G)(\infty^+ + \infty^-)$$

If $\deg A_1 \leq p$ we are done. If not, then perform the reduction process described by Cor. 3.1, starting from the pole function of A_1 , (or any other standard function with A_1 as divisor of poles) to find a function $f \in K(C)$ and non-negative integers a, b such that

$$(f) = -A_1 + A_{red} + a\infty^+ + b\infty^-$$

where A_{red} is a standard finite divisor of degree $\leq p$, and $a, b, \geq 0$. Substituting for A_1 we obtain

$$A = -(f) + (G) + A_{red} + (\deg G + a)\infty^+ + (\deg G + b)\infty^- \quad (4)$$

whence the sought reduction, with $\sigma = f/G$. Note that we have $2 \deg G + a + b = \deg A - \deg A_{red} \leq \deg A$, whence, recalling that $a > 0$ as remarked after the proof of Cor. 3.1, we find

$$2 \deg G + b < \deg A \quad (5)$$

This will be used in the Baby Step-Giant Step algorithm.

The total reduction algorithm can be summarized as follows: Given a standard divisor A , first separate out the divisor B , and find the polynomial $G(x)$. This is usually straightforward. The residual divisor $A_1 = A - B$ will be described by a pole function $f = (L + y)/D$. If $\deg A_1 = \deg D \leq p$, there is no more to do. If not, then compute the CFE of f to level k , for which the inequality of Cor.3.1(1) holds. Then f_k/G is the reducing function, and $A_{red} = Z_k$.

The reduction algorithm is most often needed to reduce a divisor $A = D_1 + D_2$ where the D_i are standard finite divisors described by standard functions f_{D_i} which have the D_i as finite poles (e.g. they may be the pole functions of the D_i). An auxiliary algorithm, the hyperelliptic analogue of the algorithm for composition of quadratic forms, is needed to obtain, from the f_{D_i} , the polynomial G and a standard function $(L + y)/M$, whose pole divisor is A_1 . For this, see, e.g. [3, 4, 8].

3.2 Quasiperiodicity

When the ground field K is finite, hyperelliptic continued fraction expansions of standard functions are periodic (i.e the sequences of partial quotients and reducts are eventually periodic), as in the case of real quadratic irrationals, and the expansions can be studied by the same techniques as in the real case. Over an infinite field, the best one can hope for is quasiperiodicity, i.e. periodicity up to constant multiples. Over a finite field quasiperiodicity coexists with periodicity, and seems the more fundamental, or at least the more useful, phenomenon.

In the following theorem, the ground field K is arbitrary. The notation os, as always, that of §2.

Theorem 3.2. *Let D be a standard finite divisor of degree $\leq p$. Then the CFE of f_D is quasiperiodic iff $\infty^+ - \infty^-$ is a torsion divisor. If this is the case then the quasiperiod is bounded above by the order of torsion.*

Proof. (c.f. [6]) Suppose first that the expansion of a given $f = f_D$ is quasiperiodic, with quasiperiod l , so $g_{i+l} = c_i g_i, i \geq 1$. It follows that $Z_{i+l} = Z_i$. Then (c.f. equation (2)), $(f_{i+l}/f_i) = (f_{i+l}) - (f_i)$ is supported entirely at infinity, which means that $\infty^+ - \infty^-$ is a torsion divisor. Conversely, suppose $\infty^+ - \infty^-$ is torsion of order $R > 0$. Take $h \in K(C)$ with $(h) = R(\infty^+ - \infty^-)$ and let D be any generic finite divisor of degree $\leq p$. Then we can write

$$(h) = -D + D + R(\infty^+ - \infty^-)$$

whence, by Cor.2.3, there exists for the CFE of f_D an index l such that $h = c f_l, c$ constant, and $Z_l = D$. From this it follows that $g_l = c g_1, c$ constant which implies the quasiperiodicity of the sequence $\{g_i\}$, with quasiperiod l . Note that the sequence of divisors Z_i is genuinely periodic, with period l . The inequality $l \leq R$ follows from $R = v_+(h) = v_+(f_l) = \deg q_{l+1}$ and $\deg q_i \geq i$ for $i \geq 1$. \square

3.3 Baby-Step Giant-Step

The Baby-Step Giant Step algorithm in hyperelliptic function fields is a translation of the algorithm of the same name invented by Shanks for real quadratic number fields, for which see [2].

Let D be a standard finite divisor of degree $\leq p$ and let f_i, g_i, p_i, q_i, Z_i be, respectively, the approximants, reducts, and convergents obtained in the CFE of the pole function f_D of D (or any standard function whose finite pole divisor is D). We consider also the CFE of y , with corresponding quantities $y_i, \gamma_i, r_i, s_i, \Phi_i$. For $f \in K(C)$ we write $\delta f = |v_-(f)|$, which avoids confusion over signs, and is consistent with the terminology of [3, 8]. Note that

$$\delta f_{i+1} = \delta f_i + \deg a_i \quad (6)$$

where a_i is the partial quotient, as follows from Prop. 2.1(3) and equation (1). Thus there is virtually no overhead in keeping a table of the δf_i .

A baby step of the Baby-Step Giant Step algorithm is just an iterative step in one of the continued fraction expansions mentioned above. A giant step, which we now describe, is an algorithm which takes as input $(Z_i, \delta f_i, \Phi_j, \delta y_j)$ and outputs a pair (Z, δ) , such that there exists an index $k \approx i + j$ for which $Z = Z_k, \delta = \delta f_k$ (k remains unknown, in general). In practice, the Z_i, Φ_j are described by the functions g_i, γ_j , so for computational purposes the input can be thought of as $g_i, \delta f_i, \gamma_j, \delta y_j$ and the output is $g = g_k, \delta = \delta_k$. Thus the giant step replaces approximately j baby steps in the CFE of f_D , at the cost of losing sight of the convergents and approximants.

For $i \geq 1$ we can write

$$(f_i) = -D + Z_i + v_+(f_i)\infty^+ - \delta f_i\infty^- \quad (7)$$

$$(y_j) = \Phi_j + v_+(y_j)\infty^+ - \delta y_j\infty^- \quad (8)$$

Adding,

$$(f_i y_j) = -D + Z_i + \Phi_j - (v_+(f_i) + v_+(y_j))\infty^+ - (\delta f_i + \delta y_j)\infty^- \quad (9)$$

Now, using total reduction we have (c.f. equation (4))

$$Z_i + \Phi_j = (G/f) + Z + (\deg G + a)\infty^+ + (\deg G + b)\infty^-$$

with Z a standard finite divisor of degree $\leq p$, $f \in K(C), G \in K[x]$. Substituting in (9), and collecting divisors of rational functions

$$\left(f \frac{f_i y_j}{G} \right) = -D + Z + (v_+(f_i) + v_+(y_j) + \deg G + a)\infty^+ - (\delta f_i + \delta y_j - \deg G - b)\infty^- \quad (10)$$

Suppose that

$$\delta f_i + \delta f_j - \deg G - b \geq 0 \quad (11)$$

Then the hypotheses of Cor.2.3 are satisfied, and $\exists k$ such that the rational function on the left in equation (10) is a constant multiple of f_k , and $Z = Z_k$. Moreover, from (10),

$$\delta f_k = \delta f_i + \delta y_j - d \quad (12)$$

where $d = \deg G + b$, so δf_k is known. Thus, finally, output (Z, δ) where δ is given by the right-hand side of (12). We shall say that the pair (Z, δ) is obtained by a giant step, and denote it $(Z_i * \Phi_j, \delta f_i * \delta y_j)$.

Note that $0 \leq d \leq 2p - 1$, as follows from the inequality (5) of §2, using $\deg Z_i, \deg \Phi_j \leq p$, so that we have a bound for the difference between $\delta f_i + \delta y_j$ and $\delta f_i * \delta y_j$.

Practical details of the algorithm are given in [5],[8]. The main application has been to calculation of the regulator of a hyperelliptic function field (c.f. the following section and the papers just cited); there is a cryptographic application in [3].

Using the estimate for d , and the values of $\delta f_i, \delta y_i$, we find a sufficient condition for the constraint (11) to hold is

$$\deg q_i + \deg s_j \geq \deg D - 3$$

a condition vacuously satisfied when $D = 0$, i.e. $f = y$.

Example. The genus 1 case. This is remarkably simple. The following example uses freely the notation established in the present section and also the notation of the reduction and total reduction algorithms (c.f. Cor.3.1 et. seq). We also use results of continued fraction expansions in the genus 1 case established in §4.1.

We deal with divisors of degree $\leq p = 1$, and a divisor of degree 1 is a point. Thus let f be the pole function of a point. The expansions of f, y may or may not be periodic (since we make no hypotheses on the groundfield K). If they are periodic, take indices i, j which do not coincide with the periods of f, y , respectively, and $j \geq 1$. Then Z_i and Φ_j both have degree 1 (they have degrees ≤ 1 , by Theorem 3.1(3), and it is a consequence of Prop. 4.3 that the degree is exactly 1.) Thus $Z_i = P, \Phi_j = Q$, for some points $P, Q \in C$. We claim:

If $P = Q^-$ then $(Z_i * \Phi_j, \delta_i * \delta_j) = (0, \delta_i + \delta_j - 1)$

If $P \neq Q^-$ then $(Z_i * \Phi_j, \delta_i * \delta_j) = (S, \delta_i + \delta_j)$

for some point S of the curve.

Indeed, if $P = Q^-$ then (c.f. eqn. (3.3)) $Z_i + \Phi_j = P + P^-$; but $P + P^- = (G) + \infty^+ + \infty^-$ for some polynomial $G \in K[X]$ of degree 1. Thus, in the notation of total reduction, $A_{red} = Z_i * \Phi_j = 0$, and, by eqn.(9), $\delta f_i * \delta y_j = \delta f_i + \delta y_j - 1$, which establishes the first assertion. If $P \neq Q^-$ then $P + Q$ is a divisor of degree 2 without hyperelliptic pairs, (thus $G = 0$) and with pole function of the form $h = (L + y)/M$, where $\deg M = 2$ and $\deg L \leq 1$. This function has no poles at infinity. Thus, by Cor. 3.1(1), a reducing function for $P + Q$ is $h_1 = h - a_0$, where a_0 is a constant. Then $b = v_-(h_1) = 0$, and the second affirmation follows again using eqn (9). The point S is defined by $(h_1) = -P - Q + S + \infty^+$.

4 Calculating the Regulator

The regulator is the order of torsion of the divisor $\infty^+ - \infty^-$, i.e. it is the least integer $R > 0$ such that $R(\infty^+ - \infty^-) \equiv 0$. If K is infinite we assume $R < \infty$. A function $h \in K(C)$ such that $(h) = \pm R(\infty^+ - \infty^-)$ is called a *fundamental unit*.

Suppose then that $(h) = R(\infty^+ - \infty^-)$. Then as shown in §3.2, if D is any standard finite divisor and $\{f_i\}$ the CFE of its pole function then $\exists l | f_i = ch$, for some constant $c \in K$. Thus R can be calculated from any CFE. However, it is best to take $D = 0$, i.e. to look at the CFE of y , because one can take advantage of symmetries in the CFE of y which do not exist in the general case.

We use the results of the previous section with $f = y$. All quantities concerned come from the CFE of y , and are denoted: $a_i, p_i, q_i, g_i, y_i, Z_i$, the g_i being the reducts and the y_i the approximants.

We have, for $i \geq 1$,

$$(y_i) = Z_i + (\deg q_{i+1})\infty^+ - (\deg q_i + p + 1)\infty^- \quad (13)$$

whence

$$R = v_-(y_i) = v_+(y_i) = \deg q_{i+1} = p + 1 + \deg q_i \quad (14)$$

where as in §3.2, $l = \min i | Z_i = 0$ is the quasiperiod.

This is the basic baby step algorithm: develop the CFE of y until hitting l with $Z_l = 0$, keeping track of $\deg q_i$, or, equivalently, of δy_i (notation of §3.3).

Next we consider some of the structure of this CFE.

Lemma 4.1. *In the CFE of y , $\deg a_i \leq p + 1$ for all i . If $i > 0$ and $\deg a_i = p + 1$ then y_i is a fundamental unit and $R = \deg q_{i+1} = \delta y_i$.*

Proof. Take degrees in equation 13: $0 = \deg Z_i + \deg q_{i+1} - \deg q_i - (p+1)$. The lemma follows since $\deg Z_i \geq 0$ and $\deg a_i = \deg q_{i+1} - \deg q_i$.

The following proposition implies symmetry in the CFE of y up to the quasiperiod. Recall that the action of the hyperelliptic involution is denoted $U \mapsto U^-$.

Proposition 4.2. *For all $i < l$, $Z_i^- = Z_{l-i}$, and*

$$\deg q_{i+1} + \deg q_{l-i} = \deg q_{l-i+1} + \deg q_i = R - p - 1$$

.

Proof. Applying the hyperelliptic involution to equation 13 we obtain, since the involution interchanges ∞^+ and ∞^-

$$(y_i^-) = Z_i^- + (\deg q_{i+1})\infty^- - (\deg q_i + p + 1)\infty^+ \quad (15)$$

Adding $(y_l) = R(\infty^+ - \infty^-)$ to equation (15) gives

$$(y_l y_i^-) = Z_i^- + (R - \deg q_i - p - 1)\infty^+ - (R - \deg q_{i+1})\infty^- \quad (16)$$

By lemma 4.1 $R > \deg q_i + p + 1$. Thus Cor.2.3 applies to the situation described by equation 16, and we conclude that, for some j , and some constant c , $y_j = c y_l y_i^-$ and $Z_j = Z_i^-$. Comparing coefficients of ∞^+ and ∞^- in equations (13) (with j instead of i) and (16) we find

$$\begin{aligned} \deg q_{i+1} + \deg q_j &= \deg q_{j+1} + \deg q_i \\ &= R - p - 1 \end{aligned} \quad (17)$$

This shows that j , considered as function of i , is strictly decreasing and (using lemma 4.1) $\leq l - 1$. It follows that $j = l - i$. \square

Prop. 4.2 shows that R can be calculated in at most $\lceil l/2 \rceil$ baby steps, by calculating the CFE of y until $Z_i = Z_i^-$ or $Z_i = Z_{i+1}^-$.

Now we consider the Baby-Step Giant-Step algorithm. We write δ_i for δy_i (c.f. §3.3). First calculate t terms of the CFE of y , keeping a table (Z_i, δ_i) . We can assume $t < \lceil l/2 \rceil$, otherwise these baby steps would give R . Then, by the periodicity and conjugacy properties of the Z_i discussed above, one knows also the (Z_i, δ_i) in the interval $l - t \leq i \leq l + t$; the situation is illustrated in (18) (19), (20). The symbols a_i -the partial quotients- and $p + 1$ are placed between the Z_i to help with the bookkeeping. The purpose is to have visible the increase in δ_i between i and $i + 1$).

$$Z_0 - p + 1 - Z_1 - a_1 - Z_2 - a_2 - \dots - Z_{t-1} - a_{t-1} - Z_t - a_t - \dots \quad (18)$$

The interval $[l - t, l]$ to the left of $Z_l, \delta_l = R$ may be visualized as

$$Z_{l-t} - a_t - Z_{l-t+1} - a_{t-1} - \dots - Z_{l-1} - a_1 - Z_l \quad (19)$$

where $Z_{l-i} = Z_i^-$, and the interval $[l, l + t]$ to the right of Z_l as

$$Z_l - p + 1 - Z_{l+1} - a_1 - Z_{l+2} - a_{l+2} \dots - Z_{l+t-1} - a_{t-1} - Z_{l+t} \quad (20)$$

where $Z_{l+i} = Z_i$. We calculate: for $1 \leq i \leq t$,

$$\delta_i = p + 1 + \deg q_i = p + 1 + \sum_{j=1}^{i-1} \deg a_j \quad (21)$$

$$\delta_{l+i} = \delta_l + p + 1 + \sum_{j=1}^{i-1} \deg a_j = R + \delta_i \quad (22)$$

$$\delta_{l-i} = \delta_l - \sum_{j=1}^i \deg a_j = R - \sum_{j=1}^i \deg a_j = R - \delta_{i+1} + (p + 1) \quad (23)$$

Take $s \leq t$ and define $(\hat{Z}_j, \hat{\delta}_j), j \geq 1$ by

$$\begin{aligned} (\hat{Z}_1, \hat{\delta}_1) &= (Z_s * Z_t, \delta_s * \delta_t) \\ (\hat{Z}_{j+1}, \hat{\delta}_{j+1}) &= (Z_s * \hat{Z}_j, \delta_s * \hat{\delta}_j) \end{aligned}$$

in the notation of (§3.3). Recall also that for each j there is an i such that $(\hat{Z}_j, \hat{\delta}_j) = (Z_i, \delta_i)$. Although we do not in general know i , we do know $\delta_i = \hat{\delta}_j$.

If however \hat{Z}_j is recognized as Z_k or Z_k^- , $k \leq t$, then we do know i ; we have $i = l + k$ or $l - k$ respectively, and R can be calculated from (22) or (23), provided one can be certain that the size of the giant steps is not so large that one has stepped entirely over the segment around Z_l and landed rather in some segment centred on a multiple of l . Clearly one is certain to land in the correct segment for some j , provided the size of the giant steps, $\hat{\delta}_{j+1} - \hat{\delta}_j$ is positive and does not exceed $\delta_{l+t} - \delta_{l-t}$. This gives conditions on s and $t - s$. In fact, by (22) and (23),

$$\delta_{l+t} - \delta_{l-t} = p + 1 + 2 \sum_{i=1}^{t-1} \deg a_i + \deg a_t$$

The size of the first giant step is in the interval $[\delta_s + \delta_t - (2p + 1), \delta_s + \delta_t]$ and the size of the subsequent steps is in the interval $[2\delta_s - (2p + 1), 2\delta_s]$. Now, $\delta_s = p + 1 + \sum_{i=1}^{s-1} \deg a_i$, so that, for giant steps no larger than $\delta_{l+t} - \delta_{l-t}$ we need

$$2(p + 1 + \sum_{i=1}^{s-1} \deg a_i) \leq p + 1 + 2 \sum_{i=1}^{t-1} \deg a_i + \deg a_t$$

which is

$$\frac{p + 1}{2} \leq \sum_{i=s}^{t-1} \deg a_i + \frac{\deg a_t}{2}$$

Since $\deg a_i \geq 1, i \geq 1$ this inequality is certainly satisfied if $t - s \geq (p - 1)/2$. The choice of s remains. The received wisdom is to take s in the order of \sqrt{B} , where B is an estimate for R . With these choices R is calculated by $O(\sqrt{B})$ polynomial operations.

4.1 Genus 1

Throughout this section the genus p of C is 1. CFE's are particularly simple in this case. We recover results of [1, 4] in a characteristic-free fashion.

A distinguished role is played by y , its reducts g_i , and functions $cg_i + h$ where $c \in K$ and $h \in K[x]$. We refer to such functions as *functions in the cycle of y* .

Proposition 4.3. *Let f be a standard function with finite pole divisor of degree ≤ 1 . We consider the CFE of f , with partial quotients a_i .*

1. If $\infty^+ - \infty^-$ is not torsion, then $\deg a_i = 1$ for all $i \geq 1$.
2. If $\infty^+ - \infty^-$ is torsion, so that CFE's are quasiperiodic, with quasiperiod l say, then:
 - (a) If $f = y$ then $\deg a_i = 1$ for $1 \leq i \leq l - 1$ and $\deg a_l = 2$.
More generally if f is a function in the cycle of y then in each quasiperiod of the CFE of f there is just one index j , such that $\deg a_j = 2$ and for all $i \neq j$ in the quasiperiod, $\deg a_i = 1$.
 - (b) If f is not a function in the cycle of y then $\deg a_i = 1$ for all $i \geq 1$.

The proof is straightforward, using lemma 4.1.

We find the following, for convergents q_i in the CFE of f , recalling $\deg q_i = \sum_{j=1}^{i-1} \deg a_j, i \geq 1$:

- If $f = y, y_i = q_i f - p_i$ then, for $1 \leq i \leq l$

$$(y_i) = Q_i + i\infty^+ - (i+1)\infty^- \quad (24)$$

- If f_1 is not a reduct of y , then, for $1 \leq i$,

$$(f_i) = -R_i + S_i + i(\infty^+ - \infty^-) \quad (25)$$

Q_i, R_i, S_i being points of C . This gives

Proposition 4.4. *Let C have regulator $R < \infty$. Let f be a standard function with finite pole divisor of degree ≤ 1 . If f is in the cycle of y then the CFE of f has quasiperiod $R - 1$, otherwise it has quasiperiod R .*

Proof. The results follow from equations (24) and (25), since l is the least index for which $Q_l = \infty^+$ or $R_l = S_l$. \square

Now we relate continued fraction expansions with the group law defined by taking ∞^+ as zero for a group law on C . To put this in perspective, let us start from an elliptic curve E with O as zero of its group. Let $P \neq O$ be any other K -rational point of E . Then there is a unique involution on E in which P and O are paired; we shall denote E with the new hyperelliptic structure defined by this involution as C , and rename P, O as ∞^-, ∞^+ respectively. In concrete terms, one may suppose E given by a Weierstrass equation, and

C described by some other plane model. For Char. $\neq 2$ formulas can be found in [1]; we leave to the reader the pleasure of calculating the analogues in Char. 2.

Recall that $iP = Q$ in the group law on E iff $i(P - O) \equiv Q - O$. The desired connexion between the group law and CFE's is then given by:

Theorem 4.5. 1. P is an R -torsion point on E iff $\infty^+ - \infty^-$ is an R -torsion divisor on C .

2. $iP = Q$ in the group law on E iff Q is a zero of the approximant y_{i-1} , or, equivalently, a pole of the reduct g_{i-1} , of y .

Proof. (1) is immediate from definitions.

(2). Suppose $iP = Q$, so $\exists f \in K(E) = K(C)|(f) = (Q - O) - i(P - O)$. Rewritten in notation appropriate to C , this is

$$(f) = (Q - \infty^+) - i(\infty^- - \infty^+) = Q + (i - 1)\infty^+ - i\infty^-$$

This implies, by Cor. 2.3 (applied with $D = 0$) and equation (24) that f is a constant multiple of y_{i-1} and $Q = Q_{i-1}$. Moreover $g_{i-1} = y_{i-1}/y_{i-2}$ (c.f. Prop. 2.1(4)) so, using equation (24) for i and $i - 1$

$$(g_{i-1}) = -Q + Q_{i-2} - \infty^+ + \infty^-$$

The converse is obtained by chasing backwards through this argument. \square

We note that $g_i \in \mathcal{L}(Q - \infty^+ + \infty^-)$. By Riemann-Roch this space is 1-dimensional, so consists of constant multiples of g_{i-1} . Now it is easy to produce functions in $\mathcal{L}(Q - \infty^+ + \infty^-)$. For example, $f_Q^* = f_Q - \langle f_Q \rangle$ is such a function, where f_Q is the pole function of Q and $\langle f_Q \rangle$ denotes the polynomial part of the Laurent expansion of f_Q at ∞^- . (Warning: in [1], a similar function is denoted f_Q). Thus f_Q^* is a constant multiple of g_i .

The discrete log problem on E is: given P and $Q = iP$, determine i . Theorem 4.5 shows that this is equivalent to the problems:

1. Given Q , determine i so that Q is a zero of y_{i-1} .
2. Given Q , determine i so that Q is a pole of g_{i-1} .
3. Given Q , determine i so that f_Q^* is a constant multiple of g_{i-1} .

This is essentially the result of [4].

References

- [1] W. W. Adams and M.J. Razar. Multiples of points on elliptic curves and continued fractions. *Proc. Lond. Math. Soc.*, 41:481–498, 1980.
- [2] Henri Cohen. *A course in computational algebraic number theory*. Springer-Verlag, Berlin, 1993.
- [3] R. Scheidler, A. Stein, and H. C. Williams. Key-exchange in Real Quadratic Congruence Function Fields. *Des. Codes Crypt.*, 7, 1996.
- [4] A. Stein. Equivalences between elliptic curves and real quadratic congruence function fields. *J. Theor. Nombres Bdx*, 9:75–95, 1997.
- [5] A. Stein and H.C. Williams. Baby Step Giant Step in real quadratic function fields. *Preprint. Available from <http://cacr.math.uwaterloo.ca/astein/publikationen.html>*, 1995.
- [6] T.G.Berry. On periodicity of continued fractions in hyperelliptic function fields. *Archiv der Mathematik*, 55:259–266, 1990.
- [7] T.G.Berry. Construction of linear systems on hyperelliptic curves. *Jour. Sym. Comp.*, 26:315–327, 1998.
- [8] R. Zuccherato. The continued fraction algorithm and regulator for quadratic function fields of characteristic 2. *J. Algebra*, 190:563–587, 1997.