BULL. AUSTRAL. MATH. SOC. 11J70, 11A65, 11J68
VOL. 64 (2001) [331–343]

NON-PERIODIC CONTINUED FRACTIONS IN HYPERELLIPTIC FUNCTION FIELDS

ALFRED J. VAN DER POORTEN

Dedicated to George Szekeres on his 90th birthday

We discuss the exponential growth in the height of the coefficients of the partial quotients of the continued fraction expansion of the square root of a generic polynomial.

1. BASICS

Given a Laurent series

$$F(X) = \sum_{h=-m}^{\infty} f_h X^{-h},$$

in a variable X^{-1} and over some field $\mathbb{F}$, define its sequence $(F_i)_{i\geqslant 0}$ of *complete quotients* by setting $F_0 = F$, and $F_{i+1} = 1/(F_i - a_i)$. Here, the sequence $(a_i)_{i\geqslant 0}$ of *partial quotients* of F is given by $a_i = \lfloor F_i \rfloor$ where $\lfloor\ \rfloor$ denotes the polynomial part in X of its argument. Plainly we have

$$F = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

It is only the partial quotients that matter, so such a continued fraction expansion may be conveniently denoted just by $[a_0\,,\, a_1\,,\, a_2\,,\, a_3\,,\, \ldots]$.

The truncations $[a_0\,,\, a_1\,,\, \ldots\,,\, a_h]$ plainly are rational functions x_h/y_h. Here, the pairs of relatively prime polynomials x_h, y_h are given by the matrix identities

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix}$$

and the remark that the empty matrix product is the identity matrix.

Received 11th April, 2001
The author was supported by a grant from the Australian Research Council.

The correspondence here alleged, whereby matrix products provide the sequences of *continuants* $(x_h)_{h\geqslant 0}$ and $(y_h)_{h\geqslant 0}$, and thus the *convergents* x_h/y_h, may be confirmed by induction on the number of matrices on recalling the definition

$$[a_0, a_1, \ldots, a_h] = a_0 + 1/[a_1, \ldots, a_h], \qquad [a_0] = a_0.$$

Because $F = [a_0, a_1 \ldots, a_h, F_{h+1}]$, we see by the correspondence that

$$(1)\quad F \longleftrightarrow \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} F_{h+1} & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix}\begin{pmatrix} F_{h+1} & 1 \\ 1 & 0 \end{pmatrix} \longleftrightarrow \frac{x_hF_{h+1} + x_{h-1}}{y_hF_{h+1} + y_{h-1}}.$$

That is, we have

$$F = \frac{x_hF_{h+1} + x_{h-1}}{y_hF_{h+1} + y_{h-1}}, \quad \text{and so} \quad F_{h+1} = -\frac{y_{h-1}F - x_{h-1}}{y_hF - x_h}.$$

Recalling that $x_{-1} = 1$, $y_{-1} = 0$ because an empty matrix product is the identity matrix, we obtain

$$(2)\qquad (-1)^hF_1F_2\cdots F_{h+1} = (x_h - Fy_h)^{-1}.$$

Taking determinants in the matrix correspondence entails

$$x_h/y_h = x_{h-1}/y_{h-1} + (-1)^{h-1}/y_{h-1}y_h$$

whence, by induction, $F = a_0 + \sum_{i=1}^{\infty}(-1)^{i-1}/y_{i-1}y_i$, and so

$$\deg(y_hF - x_h) = -\deg y_{h+1} = -(\deg a_{h+1} + \deg y_h) < -\deg y_h.$$

This displays the excellent quality of approximation to F provided by its convergents. Incidentally, (1) readily yields the evaluation

$$y_hF - x_h = \frac{y_hx_{h-1} - y_{h-1}x_h}{y_hF_{h+1} + y_{h-1}} = \frac{(-1)^h}{y_h}\cdot\frac{1}{(F_{h+1} + y_{h-1}/y_h)}.$$

PROPOSITION 1. *Let x, y be relatively prime polynomials. Then*

$$\deg(yF - x) < -\deg y$$

if, and only if, the rational function x/y is a convergent to F.

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

PROOF: The 'if' part of the claim is given immediately above, so we may take h so that $\deg y_{h-1} \leqslant \deg y < \deg y_h$, and note that supposing x/y is not a convergent entails that y is not a constant multiple of y_{h-1}. Because $x_h y_{h-1} - x_{h-1} y_h = \pm 1$, there are nonzero polynomials a and b such that

$$y = a y_{h-1} + b y_h$$
$$x = a x_{h-1} + b x_h ,$$

and so $yF - x = a(y_{h-1}F - x_{h-1}) + b(y_h F - x_h)$. Now suppose that the two terms on the right are of different degree, $\deg a - \deg y_h$ and $\deg b - \deg y_{h+1}$, respectively. In that case plainly $\deg(yF - x) > \deg(y_{h-1}F - x_{h-1}) > \deg(y_h F - x_h)$, confirming that the convergents provide the locally best approximations to F.

To verify the suggestion that the degrees of the two terms *are* different, notice that $\deg a y_{h-1} = \deg b y_h$, otherwise $\deg y < \deg y_h$ is not possible, so

$$\deg a - \deg y_h = \deg b - \deg y_{h-1} > \deg b - \deg y_{h+1}.$$

Moreover, $\deg a - \deg y_h = \deg(yF - x)$. Finally, because $\deg a$ must be at least as large as $\deg y_h - \deg y_{h-1}$, it is plain that $\deg a - \deg y_h \geqslant -\deg y$. □

2. CONTINUED FRACTION EXPANSION OF THE SQUARE ROOT OF A POLYNOMIAL

Let D a polynomial in X over $\mathbb{F}$, not a square, and consider the Laurent series $F = \sqrt{D}$. Plainly F is in $\mathbb{F}\big((X^{-1})\big)$ if and only if D is of even degree, say $\deg D = 2g+2$ for some nonnegative integer g, *and* its leading coefficient is a square in $\mathbb{F}$. We assume those conditions in the sequel.

Then it is easy to see that the complete quotients F_h of F are all of the shape

$$F_h = (P_h + \sqrt{D})/Q_h ,$$

with $Q_h \big| D - P_h^2$ and, this remark is in part just setting the notation, the generic step in the continued fraction algorithm for $F = \sqrt{D}$ is

$$F_h = (P_h + \sqrt{D})/Q_h = a_h - (P_{h+1} - \sqrt{D})/Q_h . \tag{3}$$

Here the sequences of polynomials (P_h) and (Q_h) are given sequentially by

$$P_{h+1} + P_h = a_h Q_h, \quad \text{and} \quad Q_{h+1} Q_h = D - P_{h+1}^2 .$$

PROPOSITION 2. *The polynomials Q and P satisfy $\deg Q_h \leqslant g = (\deg D - 1)/2$ and $\deg P_{h+1} = g + 1 = (\deg D)/2$ for all $h = 0, 1, \ldots$.*

PROOF: Given $\deg Q_h \leqslant g$ it follows from $-(P_{h+1} - \sqrt{D})/Q_h$ being a remainder, so that it is of negative degree, that $\deg P_{h+1} = g + 1$ and $\deg(P_{h+1} - \sqrt{D})$ is less than $\deg Q_h$. Thus $Q_{h+1} Q_h = D - P_{h+1}^2$ entails that $\deg Q_{h+1} \leqslant g$. Finally, $F_0 = \sqrt{D}$ displays that $Q_0 = 1$, so $\deg Q_0$ is no more than g. □

Notice that $P_{h+1} + P_h = a_h Q_h$ entails that $\deg Q_h = 0$ is equivalent to $\deg a_h = g+1$.

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

3. Numbers and Functions

The continued fraction expansion of the square root of an *integer*, which is not a square is always periodic. The main features of the example $\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$ are general. Just so, those features are shared by the continued fraction expansion of a square root of a polynomial, *provided that the expansion is quasi-periodic.*

In particular, the convergent $[7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1] = 29718/3805$ yields the fundamental unit $29718 + 3805\sqrt{61}$ of the domain $\mathbb{Z}[\sqrt{61}]$; it is the cube of the fundamental unit of the ring of all integers of $\mathbb{Q}(\sqrt{61})$. However, periodicity *per se* is of little interest. Periodicity of expansions such as that for $\sqrt{61}$ is important *because* periodicity coincides with the production of a unit. In the function field case, however, all nonzero elements of the base field F are units. One is therefore interested in all convergents $x(X)/y(X)$ of, say, $\sqrt{D(X)}$ so that $x^2 - Dy^2$ is a nonzero constant. If that constant is different from 1 such a convergent x/y corresponds to a *quasi*-period.

It happens, as is nicely explained by Berry [**2**] (see also [**11**], and remarks of Friesen [**7**] that first drew the issue to my attention), that if the continued fraction expansion of the square root of a polynomial has a quasi-period, then 'twice that quasi-period' yields a period proper. Incidentally, the results of [**4**] do not contradict this fact. David Cantor deals with rational functions $D(X)/X^2$, where $D(X)$ is a quadratic polynomial.

For an integer D, not a square, one finds the inequalities $0 < P_{h+1} < \sqrt{D}$ and $0 < Q_h < 2\sqrt{D}$. Thus, in the numerical case, there are only finitely many possibilities for the pairs (P_h, Q_h), and periodicity follows by the box principle. In the function field case, however, the constraints on the degrees of the P_{h+1} and of the Q_h nonetheless allow infinitely many possibilities for the pairs (P_h, Q_h) whenever the base field $\mathbb{F}$ is infinite. In that case, when $\deg D$ is greater than 2, periodicity of the continued fraction expansion of $\sqrt{D(X)}$ is only happenstance; it is an improbable event. [The fact that any quadratic is a square up to a constant (by 'completing the square') means one always gets periodicity when $\deg D = 2$.]

When the base field *is* finite, the box principle does guarantee periodicity. The end of the quasi-period is signalled by a partial quotient a_r of degree $g + 1$, that is, by $\deg Q_r = 0$.

To see that, recall the identity (2) of page 332. Noting that $F_h = (P_h + \sqrt{D})/Q_h$ and $P_{h+1}^2 - D = -Q_h Q_{h+1}$, taking norms yields $x_h^2 - Dy_h^2 = (-1)^{h+1} Q_{h+1}$. That is, $x_{r-1} - y_{r-1}\sqrt{D}$ is a unit if and only if $\deg a_r = g + 1$.

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

4. Two Contrasting Examples

Consider $X^4 - 2X^3 + 3X^2 + 2X + 1$, and set

$$\begin{aligned}\delta(X) &= \sqrt{X^4 - 2X^3 + 3X^2 + 2X + 1} \\ &= X^2 - X + 1 + 2X^{-1} + 2X^{-2} - 4X^{-4} - 8X^{-5} - 6X^{-6} + 10X^{-7} + 40X^{-8} \\ &\qquad +58X^{-9} + 2X^{-10} - 188X^{-11} - 442X^{-12} - 382X^{-13} + \cdots .\end{aligned}$$

The following tableau reveals that δ happens to have a periodic continued fraction expansion.

$$\begin{array}{lll}
\delta & = X^2 - X + 1 & - (\bar{\delta} + X^2 - X + 1) \\
(\delta + X^2 - X + 1)/4X & = \frac{1}{2}X - \frac{1}{2} & - (\bar{\delta} + X^2 - X - 1)/4X \\
(\delta + X^2 - X - 1)/X & = 2X - 2 & - (\bar{\delta} + X^2 - X + 1)/X \\
(\delta + X^2 - X + 1)/4 & = \frac{1}{2}X^2 - \frac{1}{2}X + \frac{1}{2} & - (\bar{\delta} + X^2 - X + 1)/4 \\
(\delta + X^2 - X + 1)/X & = 2X - 2 & - (\bar{\delta} + X^2 - X - 1)/X \\
(\delta + X^2 - X - 1)/4X & = \frac{1}{2}X & - (\bar{\delta} + X^2 - X + 1)/4X \\
\delta + X^2 - X + 1 & = 2X^2 - 2X + 2 & - (\bar{\delta} + X^2 - X + 1)
\end{array}$$

The reader might now enjoy noticing that with $a(u) = u^4 - 3u^3 + 5u^2 - 2u$ and $b(u) = u^2 - 2u + 2$ this data shows we have $a^2 - D(u)b^2 = -4$. It follows that

$$\begin{aligned}\int^u \frac{4t - 1}{\sqrt{t^4 - 2t^3 + 3t^2 + 2t + 1}}\, dt \\ = \log\bigl(u^4 - 3u^3 + 5u^2 - 2u + (u^2 - 2u + 2)\sqrt{u^4 - 2u^3 + 3u^2 + 2u + 1}\,\bigr).\end{aligned}$$

The story of such pseudo-elliptic integrals is detailed in [**11**].

However, we need the example

$$\begin{aligned}&\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 1} \\ &= \left[X^2 - X + 1, \overline{\tfrac{1}{2}X - \tfrac{1}{2}, 2X - 2, \tfrac{1}{2}X^2 - \tfrac{1}{2}X + \tfrac{1}{2}, 2X - 2, \tfrac{1}{2}X - \tfrac{1}{2}, 2X^2 - 2X + 2}\right],\end{aligned}$$

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

only so as to contrast it with

$$\begin{aligned}
&\sqrt{D(X)} \\
&= \sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2} \\
&= \Big[X^2 - X + 1 \,,\, \frac{1}{2}X - \frac{5}{8} \,,\, \frac{32}{21}X - \frac{344}{441} \,,\, -\frac{9261}{7936}X - \frac{2963079}{1968128} \,,\, -\frac{488095744}{2572789149}X \\
&+ \frac{16216931891200}{34035427652121} \,,\, -\frac{21440698686186129}{1136033082245120}X + \frac{16653223342998913298 67}{426466819074818048 00} \,, \\
&-\frac{1600956438806866952192000}{886077703526004877158818 61}X - \frac{33719967669565760021504970850304 00}{25635131593910153951220171179626 3641} \,, \\
&\frac{80083198356049188999341382795525473293961}{97596820708323598909850058716348416 0000}X \\
&-\frac{2553693006740627824207318164745239446373641775460 99}{12679074228671726095323776878469612834847195136000} \,, \\
&\frac{41179344298675784686429042081844265661401813989695317606400 00}{50323072383190395298914203629096924328475639338329595521473 3129}X \\
&-\frac{267842912006437191134169045543528305515206296540594830431118591703121920000}{229534747331700751350483883208134421717219205316994988166282206622606708059 21} \,, \\
&\qquad \ldots \Big].
\end{aligned}$$

One can feel instantly that this expansion is not eventually periodic. Happily, it follows from the considerations central to [**11**] that this expansion is indeed not periodic; we provide a more direct proof below. Similarly, one guesses that the coefficients of the partial quotients continue to grow explosively in complexity and one might wonder whether all (excepting of course the zero-th) *are* linear. For this example (and other non-periodic examples with $\deg D = 4$), the linearity of the partial quotients a_h turns out to be obvious. The mild surprise is that we can also *prove* that the number of different primes dividing one or both of the coefficients of each partial quotient grows with h.

5. Some Hints

The fact is that the expansion of $\sqrt{D(X)}$ is perfectly normal both in having its partial quotients of degree 1, and in having the height of the coefficients of those partial quotients growing at exponential rate. [The word 'normal' in this context in fact has the technical meaning that all partial quotients *are* of degree 1 and that the complexity of their coefficients does grow exponentially.] We need only notice that a remainder $\sum_{h\geqslant 1} f_h X^{-h}$ has a reciprocal with polynomial part of degree greater than one, and thus gives rise to a partial quotient of degree greater than one, if and only if $f_1 = 0$. Moreover, the partial quotient is $f_1^{-1}X - f_2 f_1^{-2}$ if $f_1 \neq 0$, and the next remainder is $(f_2^2 - f_1 f_3) f_1^{-3} X^{-1} +$ terms of lower degree in X. Specifically, the critical coefficients of the remainders are multivariate polynomials in the coefficients of the given formal power series, But such a polynomial is 'nonzero "almost always", or "with probability one"' (see [**9**, p.375]). The matter is considered *in extenso* by Knuth [**9**] in the context of his discussion of the

Euclidean algorithm for polynomials over a field. Moreover, that discussion also makes clear that the 'explosive growth' of the coefficients of the partial quotients is precisely the better known extraordinary growth of the coefficients in performing the Euclidean algorithm on a pair of polynomials over the integers $\mathbb{Z}$.

Although the just given expansion seems wild and uncontrolled, factorising the numerators and denominators of its coefficients calms it somewhat. There is then some 'structure' to explain. The observations above, and the following summary remarks, extracted from [10], on formal manipulation of continued fraction expansions may assist the reader in recognising some of the structure of the expansion.

LEMMA 3. (Multiplication)

$$B[Ca_0\,,\,Ba_1\,,\,Ca_2\,,\,Ba_3\,,\,Ca_4\,,\ldots] = C[Ba_0\,,\,Ca_1\,,\,Ba_2\,,\,Ca_3\,,\,Ba_4\,,\ldots].$$

LEMMA 4. (Negation)

$$-\beta = [0\,,\,\bar{1}\,,\,1\,,\,\bar{1}\,,\,0\,,\,\beta] \quad \textit{and} \quad -\beta = [0\,,\,1\,,\,\bar{1}\,,\,1\,,\,0\,;\,\beta].$$

LEMMA 5. (Removal and Creation of Partial Quotients)

$$[a\,,\,B\,,\,\gamma] = [a + B^{-1}\,,\,-B^2\gamma - B] \quad \textit{and} \quad [a + C\,,\,\gamma] = [a\,,\,C^{-1}\,,\,-C^2\gamma - C].$$

6. The Reduction Principle

All this said, the main lesson seems that, morally, one should not study continued fraction expansions of formal power series over infinite fields. To that end we now ask how to reduce to the case of finite fields $\mathbb{F}_p$. A primary restriction is that the given power series should have reduction at p (that it should be defined over $\mathbb{F}_p$). Indeed, because the example power series

$$\begin{aligned}\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2}\\ = X^2 - X + 1 + 2X^{-1} + \frac{5}{2}X^{-2} + \frac{1}{2}X^{-3} - 4X^{-4} - \frac{19}{2}X^{-5} - \frac{77}{8}X^{-6} + \frac{53}{8}X^{-7}\\ + \frac{361}{8}X^{-8} + \frac{167}{2}X^{-9} + \frac{735}{16}X^{-10} - \frac{2841}{16}X^{-11} - \frac{2361}{4}X^{-12} - \frac{12813}{16}X^{-13} + \cdots\end{aligned}$$

has no reduction at 2 we must certainly avoid $p = 2$. (Indeed, in characteristic 2 it is simply not appropriate to study a square root Y, where $Y^2 = D(X)$. Rather, one considers the Artin-Schreier square root Y, where $Y^2 + t(X)Y = D(X)$.) It is also appropriate to avoid the other primes, 3 and 31, dividing the discriminant 13392 of the polynomial $D(X) = X^4 - 2X^3 + 3X^2 + 2X + 2$, where the curve $Y^2 = D(X)$ has bad reduction.

The idea behind the reduction principle for continued fractions of formal power series is to return to a first principles genesis of the sequence of continuants (y_h) providing the

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

denominators of the convergents to F. It suffices to recall that the convergents x_h/y_h are characterised by the property

$$\deg(y_hF - x_h) < -\deg y_h\,.$$

Set $\deg y_h = d_h$, and notice that $\deg a_h = d_h - d_{h-1}$. So the series F characterises a strictly increasing sequence (d_h) of integers and we may view the y_h as those polynomials, of degree d_h respectively, so that the Laurent series y_hF has no terms of degree -1, -2, $\ldots$, nor $-d_h$. In this spirit, one defines the polynomials x_h so that $\deg(y_hF - x_h) < d_h = \deg y_h$. Notice that this viewpoint encourages us to renormalise the y_h, and thence the x_h, to our convenience.

There is indeed nothing to stop us from normalising the polynomials y_h so that each has integer coefficients not sharing a common factor. Presuming that F has good reduction at p, that entails a normalisation for the x_h that also gives the x_h good reduction at p. Note that the y_h each are constant multiples of the continuants provided by the matrix form.

All this makes us able to consider the continuants in characteristic p for all primes p at which the series F has good reduction. To keep track we mark all reduced quantities with a $\overline{\ }$. The trick in the following argument is, in effect, that notwithstanding $\deg \overline{y}_h \leqslant \deg y_h$, nonetheless, $\deg(\overline{y_hF - x_h}) < -\deg y_h$.

THEOREM 6. (Reduction Principle) *Suppose F has good reduction at p. Then the distinct reductions $\overline{y}_h$ of the renormalised y_h yield* all *the convergents of $\overline{F}$.*

PROOF: Certainly, each $\overline{y}_h$ yields a convergent to $\overline{F}$, because

$$\deg(y_hF - x_h) < -\deg y_h \quad \text{implies that} \quad \deg(\overline{y_hF - x_h}) < -\deg y_h \leqslant -\deg \overline{y}_h\,.$$

However, some of the $\overline{y}_h$ may coincide. Denote representatives of the *distinct* $\overline{y}_h$ by $\overline{y}_{h(0)}$, $\overline{y}_{h(1)}, \cdots, \overline{y}_{h(j)}, \ldots$, where each $h(j)$ is maximal; that is $\overline{y}_{h(j)} = \overline{y}_{h(j)-1} = \cdots = \overline{y}_{h(j-1)+1}$. Then

$$\deg(y_{h(j)}F - x_{h(j)}) = -\deg y_{h(j)+1} \text{ entails } \deg(\overline{y_{h(j)}F - x_{h(j)}}) \leqslant -\deg y_{h(j)+1}\,.$$

The last inequality informs us that the corresponding next partial quotient of $\overline{F}$, let's call it $\overline{b}_{j+1}$, has degree at least $\deg y_{h(j)+1} - \deg \overline{y}_{h(j)}$. But

$$\sum_{j=0}^{n}\bigl(\deg y_{h(j)+1} - \deg \overline{y}_{h(j-1)+1}\bigr) \geqslant \sum_{j=0}^{n}\bigl(\deg y_{h(j)+1} - \deg y_{h(j-1)+1}\bigr) = \deg y_{h(n)+1}\,,$$

where we recall $\overline{y}_{h(j)} = \overline{y}_{h(j-1)+1}$, and that by the formalism $y_{h(-1)+1} = 1$ so that $y_{h(-1)+1}$ is of degree zero.

However, it is plain — say again from the matrix form, that

$$\sum_{j=0}^{n} \deg \overline{b}_{j+1} = \deg \overline{y}_{h(n)+1} \leqslant \deg y_{h(n)+1}\,.$$

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

It follows that the above inequalities all are equalities, that is, $\deg \overline{y}_{h(j-1)+1} = \deg y_{h(j-1)+1}$ and $\deg y_{h(j)+1} - \deg y_{h(j)} = \deg b_{j+1}$, and the $y_{h(j)}$ must account for all the convergents of $\overline{F}$ as claimed. □

In a nutshell, the first partial quotient that has bad reduction 'collapses' to a partial quotient of higher degree.

7. Some Example Reductions

We give several expansions and invite the reader to compare these with the expansion of $\sqrt{D(X)}$ over $\mathbb{Q}[X]$ at the end of Section 4. We take particular note of the *regulator* $m = m_p$ in each case. Here m is the sum of the degrees of the partial quotients making up the quasi-period; that is, if $x - y\sqrt{D(X)}$ is the fundamental unit, it is $\deg x = \deg y + g + 1$. For the reader's convenience, we repeat the expansion of

$$\begin{aligned}
&\sqrt{D(X)} \\
&= \sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2} \\
&= \Bigg[X^2 - X + 1\,,\ \frac{1}{2}X - \frac{5}{2^3}\,,\ \frac{2^5}{3\cdot 7}X - \frac{2^3\cdot 43}{3^2\cdot 7^2}\,,\ -\frac{3^3\cdot 7^3}{2^8\cdot 31}X - \frac{3^2\cdot 7^2\cdot 6719}{2^{11}\cdot 31^2}\,, \\
&\quad -\frac{2^{14}\cdot 31^3}{3^4\cdot 7^4\cdot 13229}X + \frac{2^{11}\cdot 5^2\cdot 31^2\cdot 329591}{3^4\cdot 7^4\cdot 13229^2}\,,\ -\frac{3^3\cdot 7^3\cdot 13229^3}{2^{17}\cdot 5\cdot 31^4\cdot 1877}X \\
&\quad +\frac{3^2\cdot 7^2\cdot 13229^2\cdot 21577726507}{2^{19}\cdot 5^2\cdot 31^4\cdot 1877^2}\,,\ -\frac{2^{21}\cdot 5^3\cdot 31^4\cdot 1877^3}{3\cdot 7\cdot 11\cdot 13229^4\cdot 12524251}X \\
&\quad -\frac{2^{19}\cdot 5^2\cdot 31^4\cdot 47\cdot 1877^2\cdot 2693\cdot 1180897}{3^2\cdot 7^2\cdot 11^2\cdot 13229^4\cdot 12524251^2}\,, \\
&\quad +\frac{11^3\cdot 13229^4\cdot 12524251^3}{2^{25}\cdot 5^4\cdot 31^5\cdot 1877^4\cdot 130960463}X - \frac{11^2\cdot 13229^4\cdot 2109269\cdot 12524251\cdot 208276252871}{2^{29}\cdot 5^3\cdot 31^6\cdot 1877^4\cdot 130960463^2}\,, \\
&\qquad\qquad \frac{2^{33}\cdot 5^4\cdot 31^7\cdot 1877^4\cdot 130960463^3}{3^2\cdot 7\cdot 11^4\cdot 67\cdot 331\cdot 13229^4\cdot 125242514\cdot 32646599}X \\
&\quad -\frac{2^{29}\cdot 5^4\cdot 31^6\cdot 1877^4\cdot 130960463^2\cdot 672668401\cdot 6280895711017969}{3^4\cdot 7^2\cdot 11^4\cdot 67^2\cdot 331^2\cdot 13229^4\cdot 125242514\cdot 32646599^2}\,,\ldots\Bigg].
\end{aligned}$$

Note that the *first* occurrence of a prime p in a denominator of a partial quotient must, according to the Reduction Principle, signal the end of the quasi-period for the expansion over $\mathbb{F}_p$. This is, because the occurrence of a partial quotient of degree greater than $g = 1$ entails the end of a quasi-period. For reasons hinted at in Section 5 such primes then reappear in a denominator of every second subsequent partial quotient.

Over $\mathbb{F}_3$: $\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2} = \left[X^2 + 2X + 1\,,\ \overline{2X + 2\,,\ 2X^2 + X + 2}\right]$.

Over $\mathbb{F}_5$:
$$\begin{aligned}
&\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2} \\
&\quad = \Big[X^2 + 4X + 1\,,\ \overline{3X\,,\ 2X + 1\,,\ 4X + 2\,,\ 4X\,,\ 4X^2 + X + 4\,,} \\
&\qquad\qquad \overline{4X\,,\ 4X + 2\,,\ 2X + 1\,,\ 3X\,,\ 2X^2 + 3X + 2}\Big].
\end{aligned}$$

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

The second half of the period is its first half multiplied by $3 = 1/2$, see Lemma 5. The regulator is $m_5 = 6$. (Recall the definition of 'regulator' at the start of Section 7.)

Over $\mathbb{F}_7$: $\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2} = \left[X^2 + 6X + 1\,,\, \overline{4X + 2\,,\, 2X^2 + 5X + 2}\,\right]$.

The regulator is $m_7 = 3$.

Over $\mathbb{F}_{11}$: $\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2}$

$$= \left[X^2 + 10X + 1\,,\, \overline{6X + 9\,,\, X + 8\,,\, 9X + 3\,,\, X + 8\,,\, 6X + 9\,,\, 2X^2 + 9X + 2}\,\right].$$

We see that $m_{11} = 7$.

Over $\mathbb{F}_{13}$: $\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2}$

$$= \Big[X^2 + 12X + 1\,,\, \overline{7X + 1\,,\, 4X + 6\,,\, 10X + 4\,,\, 9X + 12\,,}$$
$$\overline{2X + 7\,,\, 6X + 5\,,\, 11X + 10\,,\, 12X + 11\,,\, 12X^2 + X + 12\,,\, 12X + 11\,,\, \ldots}\Big].$$

The second half of the period is its first half multiplied by $11 = 1/6$. Note that the quasi-period is of odd length, 9, so the period has length 18. More to the point, the regulator is $m_{13} = 10$.

Over $\mathbb{F}_{17}$: $\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2}$

$$= \Big[X^2 + 16X + 1\,,\, \overline{9X + 10\,,\, 8X + 4\,,\, 10X + 1\,,\, 15X + 3\,,\, 12X + 5\,,\, 13X + 12\,,}$$
$$\overline{4X + 4\,,\, 15X + 5\,,\, 6X + 13\,,\, 15X + 5\,,\, 4X + 4\,,}$$
$$\overline{13X + 12\,,\, 12X + 5\,,\, 15X + 3\,,\, 10X + 1\,,\, 8X + 4\,,\, 9X + 10\,,\, 2X^2 + 15X + 2}\Big].$$

Here the period length is 18. Note that there cannot be a quasi-period of even length. Notice that $m_{17} = 19$.

Over $\mathbb{F}_{31}$: $\varepsilon(X) = \sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2} = \Big[X^2 + 30X + 1\,,$

$$\overline{16X + 15\,,\, 2X + 29\,,\, 16X^2 + 15X + 16\,,\, 2X + 29\,,\, 16X + 15\,,\, 2X^2 + 29X + 2}\Big].$$

$$\begin{aligned}
&\varepsilon && = X^2 + 30X + 1 && - (\bar{\varepsilon} + X^2 + 30X + 1)\\
&(\varepsilon + X^2 + 30X + 1)/4X && = 16X + 15 && - (\bar{\varepsilon} + X^2 + 30X + 30)/4X\\
&(\varepsilon + X^2 + 30X + 30)/X && = 2X + 29 && - (\bar{\varepsilon} + X^2 + 30X + 1)/X\\
&(\varepsilon + X^2 + 30X + 1)/4 && = 16X^2 + 15X + 16 && - (\bar{\varepsilon} + X^2 + 30X + 1)/4\\
&(\varepsilon + X^2 + 30X + 1)/X && = 2X + 29 && - (\bar{\varepsilon} + X^2 + 30X + 30)/X\\
&(\varepsilon + X^2 + 30X + 30)/4X && = 16X + 15 && - (\bar{\varepsilon} + X^2 + 30X + 1)/4X\\
&\varepsilon + X^2 + 30X + 1 && = 2X^2 + 29X + 2 && - (\bar{\varepsilon} + X^2 + 30X + 1)
\end{aligned}$$

I added this reduction and its details for the bemusement of the reader. Why, I ask, does it resonate so closely with the original example $\delta(X)$ periodic in characteristic zero? By the way, $D(X) = (X - 4)^2(X^2 + 6X + 4)$ over $\mathbb{F}_{31}$.

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

8. Non-periodicity

Consider a curve $\mathcal{C} : Y^2 = D(X)$ and let p be a prime of good reduction for $\mathcal{C}$ (that is, p does not divide the discriminant of $4D(X)$). Denote the reduction mod p of $\mathcal{C}$ by $\mathcal{C}_p$. Jing Yu [14] recently pointed out to me that, by the reduction theory of Abelian varieties, if the divisor class of $\infty_+ - \infty_-$ is of order m in $\operatorname{Jac}\mathcal{C}$ then, unless $p|m$, the divisor class of $\infty_+ - \infty_-$ is also of order $m_p = m$ in $\operatorname{Jac}\mathcal{C}_p$.

Conversely, suppose p and q are primes of good reduction for $\mathcal{C}$. Suppose further that the regulator of $\mathcal{C}_p$ is m_p, that $q \nmid m_p$, and that the regulator of $\mathcal{C}_q$ is m_q. Unless there is an integer i so that $m_p p^i = m_q$, $\sqrt{D(X)}$ does not have a periodic continued fraction expansion.

Specifically, the data $m_5 = 6$ and $m_7 = 3$ already shows that our example at the end of Section 4 is indeed not periodic. Notice, also, that a careful glance at the 'factorised' expansion at the start of Section 7 already reveals that the first partial quotient to blow up at $p = 5$ is a_5, so over $\mathbb{F}_5$ the quasi-period has length 5 and thus indeed $m_5 = 6$. Similarly the partial quotient a_2 blows up at 7, so over $\mathbb{F}_7$ the quasi-period has length 2, and $m_7 = 3$. Thus the start itself of the expansion makes it manifest that the expansion is not periodic.

When $\deg D = 4$ we have $g = 1$. Hence, in characteristic 0, all the partial quotients of the example $\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 2}$ *must* be of degree one because, as remarked at the conclusion of Section 3, $\deg a_r = g + 1 = 2$ signals a quasi-period.

Because the expansion *is* periodic over every finite field F_p, p not even, every prime eventually appears in a denominator of a partial quotient.

However, it is the convergents x_h/y_h, rather than the partial quotients a_h, that are important. The issue should not be whether the partial quotients indeed increase in height at exponential rate, but whether the convergents increase in height at a doubly exponential rate. And if the convergents are the issue, we may as well study the sequence $(x_h - y_h\sqrt{D})_{h\geqslant 0}$ of approximants.

9. Padé Approximation

In the periodic case we eventually obtain a unit $x_{r-1} - y_{r-1}\sqrt{D}$. Being a unit, its divisor is supported only at infinity and must be $m(\infty_+ - \infty_-)$, where $m = \deg x_{r-1} = \deg y_{r-1} + g + 1$. Thus the 'point' $\infty_+ - \infty_-$ on the Jacobian is a torsion point, of order m. In this case the sequence of approximants $(x_k - y_k\sqrt{D})_{k\geqslant 0}$ increases in height at just an exponential rate.

In general however, the 'divisor at infinity' is not torsion. (I owe this remark to a question that Everett Howe asked me at the Oberwolfach meeting on 'Finite Fields' of January, 2001.) In that case the continued fraction process leads to a sequence of approximants $(x_k - y_k\sqrt{D})_{k\geqslant 0}$ which corresponds to the sequence $\big(k(\infty_+ - \infty_-)\big)_{k\geqslant 0}$ of

https://doi.org/10.1017/S000497270003999X Published online by Cambridge University Press

divisors which according to the theory of Néron-Tate height increases in height at doubly exponential rate. (Recall that these heights are normally given as logarithmic heights. It is then well known that that $h(kP) = k^2h(P)$, given that P is not torsion, illustrating the doubly exponential growth alluded to.) A study of [**1**] provides justification for the somewhat vague suggestion that therefore indeed the coefficients of the continuants x_k and y_k grow in height at a doubly exponential rate.

More to the point, exactly this has been proved by Paula Cohen and Enrico Bombieri [**3**] in a wider context. They prove that simultaneous Padé approximation of the powers Y^i, $i = 0, 1, \ldots, r-1$ of an algebraic function Y of degree r leads to Padé approximants whose coefficients increase in height at a doubly exponential rate — unless there is a point Q, with conjugate points $Q_1, \ldots, Q_r$, on the defining curve $\mathcal{C}$ so that $rQ - (Q_1 + \cdots + Q_r)$ is a torsion point on the Jacobian of $\mathcal{C}$.

10. Periodicity

Readers may be interested to have some examples of polynomials D so that $\sqrt{D(x)}$ *does* have a periodic continued fraction expansion. All cases with $\deg D = 4$ have been detailed as elliptic surfaces by my student Xuan Chuong Tran [**13**]; see [**11**] for some examples. The extreme case known to me is $y^2 = x^6 + 4x^4 + 10x^3 + 4x^2 - 4x + 1$ provided by [**6**]. Here the torsion point at infinity is of order 39.

References

[1] W.W. Adams and M.J. Razar, 'Multiples of points on elliptic curves and continued fractions', *Proc. London Math. Soc.* **41** (1980), 481–498.

[2] T.G. Berry, 'On periodicity of continued fractions in hyperelliptic function fields', *Arch. Math. (Basel)* **55** (1990), 259–266.

[3] E. Bombieri and P.B. Cohen, 'Siegel's lemma, Padé approximations and Jacobians', with an appendix by Umberto Zannier and dedicated to Enzio De Giorgi, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **25** (1997), no 1-2, (1998), 155–178.

[4] D.G. Cantor, 'On the continued fractions of quadratic surds', *Acta Arith.* **68** (1994), 295–305.

[5] J.H. Davenport, *On the integration of algebraic functions*, Lecture Notes in Computer Science **102** (Springer-Verlag, Berlin, Heidelberg, New York, 1981).

[6] N. Elkies, 'Simple genus-2 Jacobians with high-order torsion points', (e-mail, January, 2001).

[7] C. Friesen, 'Continued fraction characterization and generic ideals', in *The arithemtic of function fields*, Ohio State University Mathematical Research Institute Publications **2**, (Proceedings of the workshop held at The Ohio State University, Ohio, June 17-26, 1991) (Walter de Gruyter & Co., Berlin, 1992), **pp.** 465–474.

[8] D. Goss, D.R. Hayes and M.I. Rosen, Editors, *The arithmetic of function fields*, Ohio State University Mathematical Research Institute Publications **2**, (Proceedings of the workshop held at The Ohio State University, Columbus, Ohio, June 17–26, 1991) (Walter de Gruyter & Co., Berlin, 1992).

[9] D.E. Knuth, *The art of computer programming* **2**, Seminumerical Algorithms, (2nd printing), 1969.

[10] A. van der Poorten, 'Formal power series and their continued fraction expansion', in *Algorithmic Number Theory*, (Joe Buhler, Editor), Lecture Notes in Computer Science **1423**, (Proc. Third International Symposium, ANTS-III, Portland, Oregon, June 1998) (Springer-Verlag, Berlin, Heidelberg, New York, 1998), **pp.** 358–371.

[11] A.J. van der Poorten and X.C. Tran, 'Quasi-elliptic integrals and periodic continued fractions', *Monatsh. Math.* **131** (2000), 155–169.

[12] W.M. Schmidt, 'On continued fractions and diophantine approximation in power series fields', *Acta Arith.* **95** (2000), 139–166.

[13] X.C. Tran, *Periodic continued fractions in function fields*, Ph.D. Thesis (Macquarie University, Sydney, 2000).

[14] J. Yu, 'Arithmetic of hyperelliptic curves', in *Aspects of Mathematics* (Hong Kong University, 1999).

ceNTRe for Number Theory Research
Macquarie University
Sydney, NSW 2109
Australia
e-mail: alf@math.mq.edu.au