Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Finite Fields and Their Applications ••• (••••) •••–•••
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Continued fractions for hyperquadratic power series over a finite field

Alain Lasjaunias

C.N.R.S.-UMR 5465, Université Bordeaux I, Talence 33405, France

Received 5 October 2006; revised 15 December 2006

Communicated by Arne Winterhof

Abstract

An irrational power series over a finite field $\mathbb{F}_q$ of characteristic p is called hyperquadratic if it satisfies an algebraic equation of the form $x = (Ax^r + B)/(Cx^r + D)$, where r is a power of p and the coefficients belong to $\mathbb{F}_q[T]$. These algebraic power series are analogues of quadratic real numbers. This analogy makes their continued fraction expansions specific as in the classical case, but more sophisticated. Here we present a general result on the way some of these expansions are generated. We apply it to describe several families of expansions having a regular pattern.

Keywords: Finite fields; Fields of power series; Continued fractions

1. Introduction

The study of continued fractions for certain algebraic power series over a finite field was initiated about thirty years ago by Baum and Sweet [1] and carried on ten years later by Mills and Robbins [8]. In the area of diophantine approximation and continued fractions, as in many other areas in number theory, the analogies between the case of real numbers and the case of power series over a finite field (i.e. the function field case in positive characteristic or formal case) are striking. In the real case, quadratic elements are badly approximable by rationals and it is conjectured that they are the only algebraic elements having this property. Nevertheless diophantine approximation in the formal case appears to be more complex in some way than

E-mail address: alain.lasjaunias@math.u-bordeaux1.fr.

1071-5797/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2007.01.001

Please cite this article in press as: A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.01.001

it is in the real case. This is due to the existence of the Frobenius isomorphism. We are led to consider a special subset of algebraic elements containing the quadratic ones but also elements of arbitrary large degree. Some of these elements (not only quadratic ones) are badly approximable by rational functions, while others are very well approximable. Because of this analogy, the elements of this subset are called hyperquadratic power series. For a general presentation of continued fractions and diophantine approximation in the function field case, the reader may consult W. Schmidt's work [9], and also for historical comments on this subject, see [4].

We introduce now the definitions and notations concerning power series over a finite field. Let p be a given prime number and $\mathbb{F}_q$ the finite field of characteristic p having q elements. Then we denote by $\mathbb{F}_q[T]$, $\mathbb{F}_q(T)$ and $\mathbb{F}(q)$ respectively the ring of polynomials, the field of rational functions and the field of power series in $1/T$ over $\mathbb{F}_q$. So $\mathbb{F}(q)$ is the completion of $\mathbb{F}_q(T)$ for the ultrametric absolute value $|P/Q| = |T|^{\deg P - \deg Q}$ where $|T|$ is a fixed real number greater than one. For a nonzero element $\alpha \in \mathbb{F}(q)$, we have the power series expansion

$$\alpha = \sum_{k \leqslant k_0} u_k T^k, \quad \text{where } k_0 \in \mathbb{Z},\ u_k \in \mathbb{F}_q,\ u_{k_0} \neq 0 \text{ and } |\alpha| = |T|^{k_0}.$$

An irrational element of $\mathbb{F}(q)$ is called hyperquadratic if it satisfies an algebraic equation of the form

$$x = \left(Ax^r + B\right)/\left(Cx^r + D\right), \quad \text{where } r = p^t \text{ and } t \in \mathbb{N},$$

the coefficients A, B, C and D belonging to $\mathbb{F}_q[T]$. For complements on hyperquadratic elements the reader may consult [2].

We introduce now the definitions and notations concerning continued fractions for elements of $\mathbb{F}(q)$. We recall that every irrational (rational) element of $\mathbb{F}(q)$ can be uniquely expanded as an infinite (finite) continued fraction. Let $(a_i)_{i \geqslant 1}$ be an infinite sequence of polynomials in $\mathbb{F}_q[T]$ with $\deg a_i \geqslant 1$ for $i \geqslant 1$. For $i \geqslant 1$, using the traditional notation, we denote by α_i (with $\alpha_1 = \alpha$ and $|\alpha| = |a_1| \geqslant |T|$) the following infinite continued fraction expansion in $\mathbb{F}(q)$,

$$\alpha_i = [a_i, a_{i+1}, \ldots, a_n, \ldots]. \tag{1}$$

Consequently for $j \geqslant i \geqslant 1$ we can write

$$\alpha_i = [a_i, a_{i+1}, \ldots, a_j, \alpha_{j+1}]. \tag{2}$$

Given the sequence of partial quotients $(a_i)_{i \geqslant 1}$, we introduce the sequence of polynomials $(x_{i,k})_{i \geqslant -1, k \geqslant 1}$ in $\mathbb{F}_q[T]$ defined for $k \geqslant 1$ recursively by

$$x_{-1,k} = 0, \quad x_{0,k} = 1 \quad \text{and} \quad x_{i,k} = a_{k+i-1} x_{i-1,k} + x_{i-2,k} \quad \text{for } i \geqslant 1. \tag{3}$$

For instance we have $x_{1,1} = a_1$, $x_{1,2} = a_2$ and $x_{2,1} = a_1 a_2 + 1$. Actually for $i \geqslant 1$, $x_{i,k}$ is a polynomial in i variables $a_k, \ldots, a_{k+i-1}$. Observe that the first index i corresponds to the number of variables and the second k is the lowest index of these variables. It is clear that if we denote $x_{i,k} = \langle a_k, \ldots, a_{k+i-1} \rangle$ we have $\langle a_k, \ldots, a_{k+i-1} \rangle = \langle a_{k+i-1}, \ldots, a_k \rangle$ for $i \geqslant 1$ and $k \geqslant 1$. We also have $x_{i,k} = a_k x_{i-1,k+1} + x_{i-2,k+2}$ for $i \geqslant 1$ and $k \geqslant 1$. These polynomials, which are at the heart of the continued fractions algorithm, are called continuants. We state below some classical and fundamental identities satisfied by these polynomials which can easily be proved by induction. For $n \geqslant 1$ and for $i \geqslant 1$ we have

$$[a_1, a_2, \dots, a_n] = x_{n,1}/x_{n-1,2} \tag{4}$$

and

$$[a_n, a_{n-1}, \dots, a_1] = x_{n,1}/x_{n-1,1}. \tag{5}$$

For $m \geqslant n \geqslant 0$ and for $k \geqslant 1$ we have

$$x_{m+1,k}x_{n,k+1} - x_{n+1,k}x_{m,k+1} = (-1)^n x_{m-n-1,k+n+2}. \tag{6}$$

Finally for $m \geqslant n+1$ and $n \geqslant 1$ we also have

$$\alpha_n = (x_{m-n,n}\alpha_m + x_{m-n-1,n})/(x_{m-n-1,n+1}\alpha_m + x_{m-n-2,n+1}). \tag{7}$$

Now we consider a particular sequence of polynomials $(F_n)_{n\geqslant -1}$ in $\mathbb{F}_p[T]$. This sequence was introduced by Mills and Robbins [8, p. 400] and is linked to some continued fractions that are studied in this note. It is defined recursively by

$$F_{-1} = 0, \quad F_0 = 1 \quad \text{and} \quad F_{n+1} = TF_n + F_{n-1} \quad \text{for } n \geqslant 0.$$

This sequence is the analogue in the function field case of the Fibonacci sequence of integers. We clearly have $F_n/F_{n-1} = [T, T, \dots, T]$ for $n \geqslant 1$. Thus we introduce

$$\omega = [T, T, T, \dots, T, \dots] = \lim_{n\to\infty} F_n/F_{n-1}.$$

Since we have $\omega = T + 1/\omega$, we see that ω is quadratic over $\mathbb{F}_p(T)$. This element ω belongs to $\mathbb{F}(p)$ for all p and is the analogue of the golden mean in the case of real numbers. Most of the classical formulas concerning the Fibonacci sequence of integers in relation with the golden number can be transposed in our context. We state below some of the corresponding formulas. These assertions are easily obtained by induction and can probably be found in standard textbooks. We will not need them here, so we omit the proof. We only want to pay attention to the last equalities (13)–(15) which are related to the Frobenius isomorphism. We have

$$F_n = \sum_{0\leqslant k\leqslant n/2} \binom{n-k}{k} T^{n-2k} \quad \text{for } n \geqslant 0, \tag{8}$$

$$F_{n-1} = \bigl(\omega^n - (-1/\omega)^n\bigr)/(\omega + 1/\omega) \quad \text{for } n \geqslant 0, \tag{9}$$

$$\omega^k = \lim_{n\to\infty} (F_{n+k}/F_n) \quad \text{for } k \geqslant 0, \tag{10}$$

$$\omega^{n+1} = F_n\omega + F_{n-1} \quad \text{for } n \geqslant 0, \tag{11}$$

$$\omega^{n+1} + (-1/\omega)^{n+1} = F_{n+1} + F_{n-1} \quad \text{for } n \geqslant 0. \tag{12}$$

Moreover, if $p > 2$ and $r = p^t$ with an integer $t \geqslant 1$, we also have

Please cite this article in press as: A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.01.001

$$F_{r-1} = (T^2+4)^{(r-1)/2}, \tag{13}$$

$$F_r + F_{r-2} = T^r, \tag{14}$$

$$F'_{r-2} = -2(T^2+4)^{(r-3)/2} \tag{15}$$

(here as later on in this note we denote by P' the formal differentiation of the polynomial P).

In [8, pp. 400–401], Mills and Robbins considered in the field $\mathbb{F}(p)$ for $p > 3$ an irrational element which is hyperquadratic and whose infinite continued fraction expansion $\alpha = [a_1, a_2, \ldots, a_n, \ldots]$ satisfies $(a_1, a_2) = (aT, -a(1+2a)^{-1}T)$ with $a \neq 0, -1, -1/2$ and the equality

$$\alpha^p = F_{p-1}\alpha_3 - F_{p-2}. \tag{16}$$

According to (13) and (15), we have

$$\alpha^p = (T^2+4)^{(p-1)/2}\alpha_3 + 2\int_0^T (x^2+4)^{(p-3)/2}\,dx. \tag{17}$$

In the same article, pp. 403–404, they also considered the unique root in $\mathbb{F}(13)$ of the equation $x^4 - Tx^3 + x^2 + 1 = 0$. See Buck and Robbins work [3, p. 342] for complements on the conjectured continued fraction for this element and also [2] for more explanations on this quartic equation. This root β is hyperquadratic. It can be shown that the infinite continued fraction expansion for β satisfies $(a_1, a_2, a_3, a_4, a_5, a_6) = (T, 12T, 7T, 11T, 8T, 5T)$ and the equality

$$\beta^{13} = (T^2+8)^4\beta_7 + 4\int_0^T (x^2+8)^3\,dx. \tag{18}$$

Comparing (17) and (18), we observe that both definitions for α and β are rather similar. This observation was the starting point for this work. For the first example α, Mills and Robbins proved that the partial quotients in the continued fraction expansion are all linear. While for the second example β, it has been checked by computer on the beginning of the continued fraction expansion that eight out of nine from these partial quotients are linear. In this paper we give a common explanation to both phenomenons.

In Section 2 we state first a general result on certain hyperquadratic continued fractions, Theorem 1. Then we describe a first family of hyperquadratic expansions having a regular and simple pattern, Theorem 2. With Theorem 3, we describe an example of an expansion belonging to a second family which includes the toy examples introduced by Mills and Robbins. The proofs of Theorems 1 and 2 are in Section 3. In the last section we study this second family and we give the proof of Theorem 3.

2. Results

Theorem 1. *Let p be a prime number, $q = p^s$ with an integer $s \geqslant 1$ and $r = p^t$ with an integer $t \geqslant 0$. Let l be an integer with $l \geqslant 1$. Let $(a_1, \ldots, a_l) \in (\mathbb{F}_q[T])^l$ be given with* $\deg a_i > 0$ *for* $1 \leqslant i \leqslant l$. *Let P, Q and R be polynomials in $\mathbb{F}_q[T]$. We assume that $PR \neq 0$ and* $\deg Q < \deg P < r$.

Then there is a unique infinite continued fraction $\alpha = [a_1, \ldots, a_l, \alpha_{l+1}]$ *in* $\mathbb{F}(q)$ *satisfying the following equality*

$$(*) \quad R\alpha^r = P\alpha_{l+1} + Q.$$

This element α *is the unique root, in* $\mathbb{F}(q)$ *with* $|\alpha| \geqslant |T|$, *of the following algebraic equation*

$$x = (Ax^r + B)/(Cx^r + D),$$

where

$$A = Rx_{l,1}, \quad B = Px_{l-1,1} - Qx_{l,1}, \quad C = Rx_{l-1,2} \quad \textit{and} \quad D = Px_{l-2,2} - Qx_{l-1,2}.$$

It results from the above theorem that the continued fraction satisfying $(*)$ is determined by the first l partial quotients and the triple (P, Q, R). We will say that such an expansion is of type (r, l, P, Q, R). These l partial quotients can be viewed as a basis which is reproduced with a deformation induced by the triple (P, Q, R). In some simple cases the expansion can be completely and explicitly described and it has a very regular pattern. The simplest case has already been studied by W. Schmidt [9, p. 154]. Taking $R = 1$, $P = \epsilon \in \mathbb{F}_q^*$ and $Q = 0$, $l \geqslant 1$ and given $(a_1, a_2, \ldots, a_l)$ an arbitrary l-tuple of non-constant polynomials in $\mathbb{F}_q[T]$, then the sequence of partial quotients satisfying $(*)$ is easily determined. In fact it is clear that the relation $\alpha^r = \epsilon\alpha_{l+1}$ is equivalent to $a_{l+i} = \epsilon^{(-1)^i} a_i^r$ for $i \geqslant 1$. Note that in Schmidt's work a finite number of polynomials has been added to the beginning of the expansion. Indeed if we add a finite number of partial quotients at the head of a hyperquadratic expansion then the resulting expansion is obtained as the image of the first one by a linear fractional transformation and consequently it is still hyperquadratic. This remark leads us to ask the following natural question:

> *Let* $\alpha \in \mathbb{F}(q)$ *be a hyperquadratic element. Does there exist an integer* $i \geqslant 1$ *such that* α_i *is an expansion of type* (r, l, P, Q, R)?

The answer to this question is positive in two cases. First if $r = 1$, because it is known that all quadratic power series over a finite field have an ultimately periodic continued fraction expansion. Secondly if the polynomial $AD - BC$ is of degree zero, after Schmidt's work [9, Theorem 4, p. 154].

We now describe expansions corresponding to $R = 1$, $P = \epsilon_1 T$ and $Q = \epsilon_2$, where ϵ_1 and ϵ_2 are nonzero constants in the base field. If we assume that the first l partial quotients have no constant term, we obtain a very regular expansion. We have the following theorem.

Theorem 2. *Let* p *be a prime number,* $q = p^s$ *with an integer* $s \geqslant 1$ *and* $r = p^t$ *with an integer* $t \geqslant 1$. *Let* l *be an integer with* $l \geqslant 1$. *Let* $(a_1, a_2, \ldots, a_l)$ *be an* l*-tuple of polynomials in* $\mathbb{F}_q[T]$ *with* $\deg a_i > 0$ *and* $a_i(0) = 0$ *for* $1 \leqslant i \leqslant l$. *Let* $(\epsilon_1, \epsilon_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. *If* α *is the infinite continued fraction* $\alpha = [a_1, \ldots, a_l, \alpha_{l+1}]$ *in* $\mathbb{F}(q)$ *satisfying*

$$\alpha^r = \epsilon_1 T\alpha_{l+1} + \epsilon_2,$$

then the sequence of partial quotients $(a_i)_{i \geqslant l+1}$ *in* $(\mathbb{F}_q[T])^{\mathbb{N}}$ *is defined for* $k \geqslant 1$ *recursively by*

$$a_{l+4k-3} = (\epsilon_1 T)^{-1} a_k^r, \qquad a_{l+4k-2} = -\epsilon_1 \epsilon_2^{-1} T,$$
$$a_{l+4k-1} = -\epsilon_2^2 (\epsilon_1 T)^{-1} a_{k+1}^r \quad \text{and} \quad a_{l+4k} = \epsilon_1 \epsilon_2^{-1} T.$$

We remark that W. Schmidt, in the same article mentioned above [9, p. 159] has obtained by other arguments the sequence given in this proposition in the case $l = 1$ and $a_1 = T$. We have seen in this section two types of expansions which have a very regular pattern. With the above notations in both cases (up to a multiplicative constant) we have $R = 1$ and the first family corresponds to the choice $(P, Q) = (1, 0)$ (algebraic elements of Class IA introduced by Schmidt) while the second family corresponds to the choice $(P, Q) = (T, 1)$ (Theorem 2). Note that in the second case we have had to introduce a condition on the basis $(a_1, \ldots, a_l)$ to obtain the regularity of the expansion. In the last theorem we consider an example of expansion where $R = 1$ and $(P, Q) = (T^2 - 1, T)$. Here we take $l = 1$ and again the first partial quotient is chosen to ensure the regularity of the expansion.

Theorem 3. *Let p be a prime number with $p \geqslant 5$. Let α be the infinite continued fraction $\alpha = [a_1, \ldots, a_n, \ldots]$ in $\mathbb{F}(p)$ satisfying*

$$\alpha^p = (T^2 - 1)\alpha_2 + T \quad \text{and} \quad a_1 = 3T.$$

Then, denoting by $v_3(m)$ the largest power of 3 dividing m, we have

$$a_n = \lambda_n A_{v_3(2n-1)+1} \quad \text{with } \lambda_n \in \mathbb{F}_p^* \text{ for } n \geqslant 1,$$

where $(A_i)_{i \geqslant 1}$ is the sequence of polynomials in $\mathbb{F}_p[T]$ defined recursively by

$$A_1 = T \quad \text{and} \quad A_{i+1} = \left[A_i^p / (T^2 - 1)\right] \quad \text{for } i \geqslant 1$$

(here the square brackets denote the integer part of a rational function). More precisely, setting $k_n = [\ln(2n - 1)/\ln 3] + 1$ for $n \geqslant 1$ and introducing the sequence $(l_n)_{n \geqslant 1}$ in $\mathbb{Z}$ defined recursively for $n \geqslant 1$ by

$$l_1 = 1, \quad l_{3n-1} = l_n - 1, \quad l_{3n} = -l_n \quad \text{and} \quad l_{3n+1} = l_n + 1,$$

we have for the sequence $(\lambda_n)_{n \geqslant 1}$ in $\mathbb{F}_p^*$,

$$\lambda_1 = 3, \quad \lambda_{3n-1} = \lambda_n, \quad \lambda_{3n} = (-1)^{k_n+1} 2^{-l_n} \quad \text{and} \quad \lambda_{3n+1} = (-1)^{k_n} 2^{l_n}.$$

3. Proofs of Theorems 1 and 2

Proof of Theorem 1. Given an l-tuple $(a_1, \ldots, a_l) \in (\mathbb{F}_q[T])^l$ with $\deg a_i > 0$ for $1 \leqslant i \leqslant l$, we introduce the following subset of $\mathbb{F}(q)$,

$$E_1 = \left\{\alpha \in \mathbb{F}(q)\colon \alpha = [a_1, \ldots, a_l, \alpha_{l+1}] \text{ with } |\alpha_{l+1}| \geqslant |T|\right\}.$$

Thus if $\alpha \in E_1$, with the above notations and according to Eq. (7) of Section 1, we can write

$$\alpha = (x_{l,1}\alpha_{l+1} + x_{l-1,1})/(x_{l-1,2}\alpha_{l+1} + x_{l-2,2}). \tag{1}$$

Note that $(*)$ is equivalent to $\alpha_{l+1} = (R\alpha^r - Q)/P$. Combining this equality with (1) we see that if $\alpha \in E_1$ satisfies $(*)$ then α satisfies

$$\alpha = \bigl(Rx_{l,1}\alpha^r + Px_{l-1,1} - Qx_{l,1}\bigr)/\bigl(Rx_{l-1,2}\alpha^r + Px_{l-2,2} - Qx_{l-1,2}\bigr). \tag{2}$$

Conversely, if $\alpha \in E_1$ and α satisfies (2), then, combining (1) and (2), we see easily that α satisfies $(*)$. Thus we only need to prove that there is a unique irrational element α in $\mathbb{F}(q)$ satisfying (2) with $\alpha \in E_1$. We put $B = Px_{l-1,1} - Qx_{l,1}$ and $D = Px_{l-2,2} - Qx_{l-1,2}$. We introduce a complete metric subspace of $\mathbb{F}(q)$ defined by

$$E = \bigl\{x \in \mathbb{F}(q)\colon\ |x| \geqslant |T|\bigr\}.$$

It is clear that we have $E_1 \subset E$. We introduce the map f from E into $\mathbb{F}(q)$ defined by

$$f(x) = \bigl(Rx_{l,1}x^r + B\bigr)/\bigl(Rx_{l-1,2}x^r + D\bigr).$$

We will first prove that Eq. (2) has a unique solution in E. This will be obtained by showing that f is well defined and is a contracting map from E into E. Then the fixed point theorem in a complete metric space implies that the equation $f(x) = x$, i.e. Eq. (2), has a unique solution in E. First we observe that $|x_{l-1,1}| < |x_{l,1}|$, $|x_{l-2,2}| < |x_{l-1,2}|$ and $|Q| < |P|$ imply

$$|B| < |Px_{l,1}| \quad \text{and} \quad |D| < |Px_{l-1,2}|. \tag{3}$$

Moreover, if $x \in E$ and since $|P| < |T|^r$, we have

$$\bigl|Rx_{l-1,2}x^r\bigr| \geqslant \bigl|x_{l-1,2}T^r\bigr| > |Px_{l-1,2}| \tag{4}$$

and

$$\bigl|Rx_{l,1}x^r\bigr| \geqslant \bigl|x_{l,1}T^r\bigr| > |Px_{l,1}|. \tag{5}$$

Thus, combining (3)–(5), we obtain

$$\bigl|Rx_{l,1}x^r + B\bigr| = \bigl|Rx_{l,1}x^r\bigr| \quad \text{and} \quad \bigl|Rx_{l-1,2}x^r + D\bigr| = \bigl|Rx_{l-1,2}x^r\bigr|. \tag{6}$$

Equalities (6) imply that for $x \in E$ we have $Rx_{l-1,2}x^r + D \neq 0$ and furthermore $|f(x)| = |x_{l,1}/x_{l-1,2}| \geqslant |T|$. Thus f is well defined and maps E into E. Now we need to prove that f is a contracting map. Assume that $x_1, x_2 \in E$, then we have

$$f(x_1) - f(x_2) = \frac{R(x_{l,1}D - x_{l-1,2}B)(x_1 - x_2)^r}{(Rx_{l-1,2}x_1^r + D)(Rx_{l-1,2}x_2^r + D)}. \tag{7}$$

We also have

$$x_{l,1}D - x_{l-1,2}B = P(x_{l,1}x_{l-2,2} - x_{l-1,1}x_{l-1,2}) = (-1)^l P. \tag{8}$$

Combining (6)–(8), we obtain

$$\bigl|f(x_1) - f(x_2)\bigr| = |P||R|^{-1}|x_{l-1,2}|^{-2}|1/x_1 - 1/x_2|^{r-1}|x_1x_2|^{-1}|x_1 - x_2|. \tag{9}$$

Since $x_1, x_2 \in E$, we have $|1/x_1 - 1/x_2| \leqslant |T|^{-1}$. By the hypothesis we also have $|P| \leqslant |T|^{r-1}$, therefore we get

$$|P||R|^{-1}|x_{l-1,2}|^{-2}|1/x_1 - 1/x_2|^{r-1}|x_1x_2|^{-1} \leqslant |T|^{-2}|R|^{-1}|x_{l-1,2}|^{-2}. \tag{10}$$

Consequently (9) and (10) imply

$$\left|f(x_1) - f(x_2)\right| \leqslant |T|^{-2}|x_1 - x_2|.$$

So we have proved the existence and the unicity of $\alpha \in E$ satisfying (2). To prove that $\alpha \in E_1$ we need to check that $0 < |x_{l-1,2}||x_{l-1,2}\alpha - x_{l,1}| < 1$. A direct computation, with (8), gives

$$\alpha - x_{l,1}/x_{l-1,2} = f(\alpha) - x_{l,1}/x_{l-1,2} = (-1)^{l+1}P/\big(x_{l-1,2}\big(Rx_{l-1,2}\alpha^r + D\big)\big).$$

Using (6) and since $|P/(R\alpha^r)| < 1$, taking the absolute value on both sides we obtain the desired inequality. Finally we shall prove that the solution of (2) is irrational. We assume that it is rational and we shall obtain a contradiction. So we can write $\alpha = a/b$ with $a, b \in \mathbb{F}_q[T]$, $\gcd(a, b) = 1$ and $|a| > |b|$. From the equality $a/b = f(a/b)$ we obtain

$$a/b = a^*/b^* \tag{11}$$

with $a^* = Rx_{l,1}a^r + Bb^r$ and $b^* = Rx_{l-1,2}a^r + Db^r$. Using (8), we have

$$a^*x_{l-1,2} - b^*x_{l,1} = (-1)^{l+1}Pb^r \quad \text{and} \quad a^*D - b^*B = (-1)^l PRa^r. \tag{12}$$

If we introduce $c = \gcd(a^*, b^*)$, we see that (12) and $\gcd(a, b) = 1$ imply $|c| \leqslant |P|$. Besides (6) gives $|a^*| = |Rx_{l,1}a^r|$. Consequently, recalling that $|P| \leqslant |T|^{r-1}$, $|a| \geqslant |T|$ and $|x_{l,1}| \geqslant |T|$, we obtain

$$|a^*/c| \geqslant \left|Rx_{l,1}a^{r-1}/P\right||a| \geqslant |x_{l,1}||a| > |a|. \tag{13}$$

Finally we observe that (11) and (13) are contradictory. So the proof of the theorem is complete. □

Before giving the proof of the second theorem, we state a basic and technical lemma concerning continued fractions. This lemma will be used here and also in the next section. The idea involved in this lemma seems to appear for the first time in works of Mendès France on finite continued fractions in the context of real numbers [7, p. 209]. We recall the proof which is very short.

Lemma 3.1. *For $n \geqslant 2$, let $a_1, \ldots, a_n$ and x be $n+1$ indeterminates. Then we have*

$$\big[[a_1, a_2, \ldots, a_n], x\big] = [a_1, a_2, \ldots, a_n, x'],$$

where

$$x' = (-1)^{n-1}x_{n-1,2}^{-2}x - x_{n-2,2}x_{n-1,2}^{-1}.$$

Proof. By (7) of the introduction, we can write

$$[a_1, a_2, \ldots, a_n, x'] = (x_{n,1}x' + x_{n-1,1})/(x_{n-1,2}x' + x_{n-2,2}).$$

Consequently, with (6) of Section 1, we have

$$[a_1, a_2, \ldots, a_n, x'] = (x_{n,1}/x_{n-1,2}) + (-1)^{n-1}/\bigl(x_{n-1,2}^2 x' + x_{n-2,2}x_{n-1,2}\bigr).$$

It follows that

$$[a_1, a_2, \ldots, a_n, x'] = [a_1, a_2, \ldots, a_n] + 1/x = \bigl[[a_1, a_2, \ldots, a_n], x\bigr]$$

and the proof of the lemma is complete. □

Proof of Theorem 2. We start from the relation

$$\alpha^r = \epsilon_1 T \alpha_{l+1} + \epsilon_2. \tag{14}$$

This can be written as $[a_1^r, \alpha_2^r] = \epsilon_1 T \alpha_{l+1} + \epsilon_2$ or again

$$\bigl[\bigl(a_1^r - \epsilon_2\bigr)/(\epsilon_1 T), \epsilon_1 T \alpha_2^r\bigr] = \alpha_{l+1}. \tag{15}$$

Since T divides a_1 and $r > 1$, we have $(a_1^r - \epsilon_2)/(\epsilon_1 T) = [a_1^r(\epsilon_1 T)^{-1}, -\epsilon_1\epsilon_2^{-1}T]$. Then we apply Lemma 3.1 with $n = 2$ and we have

$$\bigl[a_1^r(\epsilon_1 T)^{-1}, -\epsilon_1\epsilon_2^{-1}T, -\epsilon_2^2(\epsilon_1 T)^{-1}\alpha_2^r + \epsilon_2(\epsilon_1 T)^{-1}\bigr] = \alpha_{l+1}. \tag{16}$$

Since $r > 1$ and $\deg \alpha_2 \geqslant 1$, we have $|\epsilon_2^2(\epsilon_1 T)^{-1}\alpha_2^r - \epsilon_2(\epsilon_1 T)^{-1}| > 1$. It follows that

$$a_{l+1} = a_1^r(\epsilon_1 T)^{-1} \quad \text{and} \quad a_{l+2} = -\epsilon_1\epsilon_2^{-1}T. \tag{17}$$

Moreover, we can write $\alpha_{l+3} = -\epsilon_2^2(\epsilon_1 T)^{-1}\alpha_2^r + \epsilon_2(\epsilon_1 T)^{-1}$ or equivalently

$$\alpha_2^r = -\epsilon_1\epsilon_2^{-2}T\alpha_{l+3} + \epsilon_2^{-1}. \tag{18}$$

Now we introduce the map ϕ from $\mathbb{F}_q^* \times \mathbb{F}_q^*$ into itself defined by $\phi(\epsilon_1, \epsilon_2) = (-\epsilon_1\epsilon_2^{-2}, \epsilon_2^{-1})$. It is clear that ϕ is an involution. The same arguments which were used above to obtain (17) and (18) from (14), replacing the pair (ϵ_1, ϵ_2) by the pair $\phi(\epsilon_1, \epsilon_2)$, show that (18) implies

$$a_{l+3} = -\epsilon_2^2(\epsilon_1 T)^{-1}a_2^r, \qquad a_{l+4} = \epsilon_1\epsilon_2^{-1}T \tag{19}$$

and also

$$\alpha_3^r = \epsilon_1 T \alpha_{l+5} + \epsilon_2. \tag{20}$$

Hence, by (17) and (19), the initial conditions, i.e. $k = 1$, stated in the proposition for the sequence of partial quotients are satisfied. Since (20) has the same shape as (14) and observing that $a_i(0) = 0$ for $l + 1 \leqslant i \leqslant l + 4$, the proof of the theorem follows by induction. □

4. Expansions of type (r, l, k) and proof of Theorem 3

In this section we study expansions of type (r, l, P, Q, R) for $R = 1$, $P = (T^2 + u)^k$ and $Q = \int_0^T (x^2 + u)^{k-1}\,dx$, where k is a positive integer and $u \in \mathbb{F}_q^*$. Here the characteristic p is odd and in order to have Q well defined, we make the restriction $k \leqslant (p-1)/2$. Note that the two examples mentioned in the introduction as well as the example described in Theorem 3 belong to this family. Our study is based upon the following identity in the field of rational functions over $\mathbb{Q}$. We are not aware of the existence of this formula in the literature, even though there are many classical formulas concerning continued fraction expansions for rational functions or power series over $\mathbb{Q}$, so we give a proof.

Proposition 4.1. *Let $k \geqslant 1$ be an integer. We have in $\mathbb{Q}(x)$ the following continued fraction expansion*

$$\left(x^2-1\right)^k \left(\int_0^x \left(t^2-1\right)^{k-1} dt\right)^{-1} = [u_1 x, u_2 x, \ldots, u_{2k} x],$$

where $u_i \in \mathbb{Q}^*$ for $1 \leqslant i \leqslant 2k$. For $1 \leqslant i \leqslant 2k$, we have

$$u_i = (2k - 2i + 1)\left(\prod_{1 \leqslant j < i/2} (2j)(2k-2j) \Big/ \prod_{1 \leqslant j < (i+1)/2} (2j-1)(2k-2j+1)\right)^{(-1)^i}$$

(*where as usual an empty product is equal to* 1). *Moreover, if we set*

$$\omega_k = -16^{k-1}(2k-1)^{-2}\binom{2k-2}{k-1}^{-2},$$

then we also have

$$u_{2k+1-i} = \omega_k^{(-1)^{i+1}} u_i \quad \text{for } 1 \leqslant i \leqslant 2k,$$

and consequently

$$\omega_k \left(x^2-1\right)^k \left(\int_0^x \left(t^2-1\right)^{k-1} dt\right)^{-1} = [u_{2k} x, u_{2k-1} x, \ldots, u_1 x].$$

Proof. As often in this area we will use the classical method of the Riccati differential equation. We put $y_1(x) = (x^2-1)^k (\int_0^x (t^2-1)^{k-1}\,dt)^{-1}$. For $k = 1$ we simply have $y_1(x) = (x^2-1)/x = [x, -x]$ and the proposition is clearly true with $\omega_1 = -1$. So we assume that $k > 1$. In the sequel the degree of a rational function means the difference between the degrees of its numerator and of its denominator. It is easy to check that y_1 satisfies the following differential equation

$$y_1'\left(x^2-1\right) - 2kxy_1 + y_1^2 = 0. \tag{E_1}$$

Observe that $(x^2-1)^k$ and $\int_0^x (t^2-1)^{k-1}\,dt$ are coprime polynomials and y_1 is an odd rational function over $\mathbb{Q}$. Furthermore, the leading terms of the numerator and denominator of y_1 are respectively x^{2k} and $x^{2k-1}/(2k-1)$. Consequently we can write $y_1=(2k-1)x+1/y_2$, where y_2 is another odd rational function of degree greater or equal to one. If we replace $y_1=(2k-1)x+1/y_2$ into Eq. (E_1), we obtain another differential equation satisfied by y_2, which is

$$y_2'\bigl(x^2-1\bigr)-2(k-1)xy_2+(2k-1)y_2^2=1. \tag{E_2}$$

Comparing the degrees of the rational functions on both sides of Eq. (E_2), we see that we must have $\deg(y_2)=1$. Hence, since $k>1$, there exists $u_2\in\mathbb{Q}^*$ such that $y_2=u_2x+1/y_3$, where y_3 is another odd rational function of degree greater or equal to one. Now we will use induction. We assume that, for $2\leqslant i\leqslant 2k$, we have $y_1=[u_1x,u_2x,\ldots,u_{i-1}x,y_i]$, where y_i is an odd rational function satisfying the differential equation

$$y_i'\bigl(x^2-1\bigr)-2(k-i+1)xy_i+v_iy_i^2=w_i, \tag{E_i}$$

where v_i, w_i are rational numbers. So the hypothesis is true for $i=2$ with $v_2=2k-1$ and $w_2=1$. Now comparing the degrees of the rational functions on both sides of Eq. (E_i) we see that we must have $\deg(y_i)=1$. Therefore, since y_i is odd, there exists $u_i\in\mathbb{Q}^*$ such that $y_i=u_ix$ if $i=2k$ or $y_i=u_ix+1/y_{i+1}$ if $i<2k$, where y_{i+1} is another odd rational function of degree greater or equal to one. If $i=2k$, then replacing $y_i=u_ix$ into (E_i) and equating the degrees in both sides of this equation, we obtain $v_iu_i=2k-2i+1$ and the process terminates. Otherwise, replacing $y_i=u_ix+1/y_{i+1}$ into Eq. (E_i), we obtain another differential equation satisfied by y_{i+1},

$$y_{i+1}'\bigl(x^2-1\bigr)-2(v_iu_i-k+i-1)xy_{i+1}+(u_i+w_i)y_{i+1}^2-z_ix^2y_{i+1}^2=v_i,$$

where $z_i=(v_iu_i-2k+2i-1)u_i$. If $\deg(y_{i+1})=n$ and if $z_i\neq 0$, then the degree of the left-hand side of this equality is $2n+2$, while the degree of the right-hand side is zero. Therefore we must have $z_i=0$ or equivalently $v_iu_i=2k-2i+1$. Consequently the above differential equation becomes

$$y_{i+1}'\bigl(x^2-1\bigr)-2(k-i)xy_{i+1}+(u_i+w_i)y_{i+1}^2=v_i, \tag{E_{i+1}}$$

which is of the desired form with $v_{i+1}=u_i+w_i$ and $w_{i+1}=v_i$. Thus we have proved by induction that $y_1(x)=[u_1x,\ldots,u_{2k}x]$. Moreover, we have

$$u_i=(2k-2i+1)/v_i \quad \text{for } 1\leqslant i\leqslant 2k, \tag{1}$$

and also, if $2\leqslant i<2k$, $v_{i+1}=u_i+v_{i-1}$. It follows that the sequence $(v_i)_{1\leqslant i\leqslant 2k}$ is defined recursively by

$$v_{i+1}=(2k-2i+1)/v_i+v_{i-1} \quad \text{with } v_1=1 \text{ and } v_2=2k-1.$$

This implies

$$v_{i+1}v_i=2k-2i+1+v_iv_{i-1} \quad \text{with } v_1v_2=2k-1.$$

Finally we have

$$v_{i+1}v_i = \sum_{1 \leqslant j \leqslant i} (2k - 2j + 1) = i(2k - i) \quad \text{for } 1 \leqslant i \leqslant 2k - 1. \tag{2}$$

From here, for $1 \leqslant i \leqslant 2k$ we easily get

$$v_i = \Bigl(\prod_{1 \leqslant j < i/2} (2j)(2k - 2j) \Big/ \prod_{1 \leqslant j < (i+1)/2} (2j - 1)(2k - 2j + 1) \Bigr)^{(-1)^{i+1}}. \tag{3}$$

Combining (1) and (3), we have the formula for u_i stated in the proposition. Moreover, by (2), we obtain

$$v_{i+1}v_i = v_{2k-i+1}v_{2k-i} \quad \text{for } 1 \leqslant i \leqslant 2k - 1, \tag{4}$$

and also

$$v_i v_{i-1} = v_{2k-i+2}v_{2k-i+1} \quad \text{for } 2 \leqslant i \leqslant 2k. \tag{5}$$

Combining (4) and (5), we obtain

$$v_{i+1}v_{2k-i+2} = v_{i-1}v_{2k-i}.$$

Thus, we have

$$v_{2k} = \frac{v_{2k}}{v_1} = \frac{v_{2k-2}}{v_3} = \cdots = \frac{v_2}{v_{2k-1}}$$

and this can be written as

$$v_{2k-i+1} = v_{2k}^{(-1)^{i+1}} v_i \quad \text{for } 1 \leqslant i \leqslant 2k. \tag{6}$$

Now, by (3), we have

$$v_{2k} = \Bigl(\prod_{1 \leqslant j \leqslant k} (2k - 2j + 1) \Big/ \prod_{1 \leqslant j \leqslant k-1} (2k - 2j) \Bigr)^2$$

or equivalently

$$v_{2k} = 16^{1-k}(2k - 1)^2 \binom{2k - 2}{k - 1}^2 = -\omega_k^{-1}. \tag{7}$$

Therefore combining (1), (6) and (7) we have

$$u_{2k-i+1} = \omega_k^{(-1)^{i+1}} u_i \quad \text{for } 1 \leqslant i \leqslant k. \tag{8}$$

That is the second formula of the proposition. The last formula follows immediately. Indeed, according to (8), we have

$$[u_{2k}x,\dots,u_1x]=\left[\omega_k u_1x,\omega_k^{-1}u_2x,\dots,\omega_k^{-1}u_{2k}x\right]=\omega_k[u_1x,\dots,u_{2k}x].$$

So the proof of the proposition is complete. □

Now we return to the positive characteristic and we have the following corollary.

Corollary 4.2. *Let p be an odd prime number. For an integer k, with $1\leqslant k\leqslant (p-1)/2$, we define two polynomials P_k and Q_k in $\mathbb{F}_p[T]$ by*

$$P_k(T)=\left(T^2-1\right)^k \quad \text{and} \quad Q_k(T)=\sum_{0\leqslant i\leqslant k-1}(-1)^{k-i-1}\binom{k-1}{i}(2i+1)^{-1}T^{2i+1}.$$

Then there exists a $2k$-tuple $(u_i,u_2,\dots,u_{2k})\in(\mathbb{F}_p^*)^{2k}$ such that

$$P_k/Q_k=[u_1T,u_2T,\dots,u_{2k}T].$$

There exists $\omega_k\in\mathbb{F}_p^*$ such that

$$\omega_k[u_1T,u_2T,\dots,u_{2k}T]=[u_{2k}T,u_{2k-1}T,\dots,u_1T].$$

With the notation for the continuants used in the introduction, we have

$$\langle u_1T,u_2T,\dots,u_{2k}T\rangle=(-1)^kP_k$$

and

$$\langle u_1T,u_2T,\dots,u_{2k-1}T\rangle=(-1)^k\omega_k^{-1}Q_k.$$

Moreover, if $k=(p-1)/2$ then we have $u_i=2(-1)^i$ for $1\leqslant i\leqslant 2k$.

Proof. It is clear that $Q_k'(T)=(T^2-1)^{k-1}$ and also $Q_k(0)=0$. Thus, according to Proposition 4.1, we have for $P_k(T)/Q_k(T)$ the above continued fraction expansion in $\mathbb{Q}(T)$. But, since $p>2k$, all the rational numbers involved have no factor p in their denominators or numerators. Consequently by reduction modulo p, we have the continued fraction expansion in $\mathbb{F}_p(T)$ given in the corollary, where we have kept the same notations for $u_i\in\mathbb{Q}^*$ and its reduction in $\mathbb{F}_p^*$. By reducing modulo p the relation between u_i and u_{2k+1-i} in Proposition 4.1, we obtain the same relation replacing ω_k by its reduction in $\mathbb{F}_p^*$. This implies the proportionality between the continued fraction and the continued fraction obtained reversing the order. Thus we can write

$$\langle u_1T,u_2T,\dots,u_{2k}T\rangle\langle u_2T,\dots,u_{2k}T\rangle^{-1}=P_k/Q_k.$$

Since the denominators on both sides have the same degree, the numerators are proportional. Comparing the constant terms of the numerators, we have 1 in the left side because the continuant has an even number of terms and $(-1)^k$ on the right side. Therefore we have the third equality stated in the corollary. Since we have $[u_{2k}T, u_{2k-1}T, \dots, u_1T] = \omega_k P_k/Q_k$, we can write

$$\langle u_{2k}T, u_{2k-1}T, \dots, u_1T\rangle \langle u_{2k-1}T, \dots, u_1T\rangle^{-1} = P_k/\bigl(\omega_k^{-1}Q_k\bigr).$$

Recalling that the continuants are stable by taking the reverse order of the terms and using the previous equality, we deduce

$$\langle u_1T, u_2T, \dots, u_{2k-1}T\rangle = (-1)^k \omega_k^{-1} Q_k.$$

Thus we have obtained the fourth equality. For the last statement, if $k = (p-1)/2$, formulas (1) and (2) in the proof of Proposition 4.1 become in $\mathbb{F}_p$ $u_i = -2i/v_i$ and $(v_{i+1}/(i+1)) \times (v_i/i) = -1$. Since $v_1 = 1$, by induction, we obtain easily the formula given for u_i in the corollary for $1 \leqslant i \leqslant 2k$. So the proof is complete. □

Now we introduce the following definition.

Definition 4.3. With the notations of Theorem 1 and of Corollary 4.2, we say that a continued fraction expansion is of type (r, l, k) if it is of type (r, l, P, Q, R) with $P = \epsilon_1 P_k$, $Q = \epsilon_2 Q_k$ and $R = 1$, where $(\epsilon_1, \epsilon_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$.

Let us come back to the pair of examples mentioned in the introduction. If we denote by u an element of $\mathbb{F}_{p^2}$ such that $u^2 = -4$, according to the last statement of Corollary 4.2, we can write

$$P_{(p-1)/2}/Q_{(p-1)/2} = (u/2)[uT, uT, \dots, uT] = (u/2)F_{p-1}(uT)/F_{p-2}(uT).$$

Thus, comparing the degree and the constant term of the polynomials in the rational fractions on both sides of this equality, we obtain

$$P_{(p-1)/2} = (-1)^{(p-1)/2} F_{p-1}(uT), \qquad Q_{(p-1)/2} = (-1)^{(p-1)/2}(-u/2)F_{p-2}(uT).$$

This gives a proof of the equalities (13) and (15) stated in the introduction in the case $r = p$. Also if α is the element in $\mathbb{F}(p)$ with $p > 3$, introduced by Mills and Robbins and described in the introduction (17), we can establish that letting $\gamma(T) = u\alpha(uT)$, then γ is of type $(p, 2, (p-1)/2)$ with the pair $(\epsilon_1, \epsilon_2) = (1, 2)$. Note that the restriction $2k < p$ was only sufficient to ensure the existence of the pair (P_k, Q_k) in $\mathbb{F}_p[T]$ with $Q_k' = P_{k-1}$, but not necessary. One could for instance consider this pair for $k = (r-1)/2$. Such expansions of type $(r, l, (r-1)/2)$ have actually been studied in a different approach (only for $l \geqslant r$) in [5] and [6]. Moreover, if β is the element in $\mathbb{F}(13)$, also introduced by Mills and Robbins and mentioned in the introduction (18), we can establish again that letting $\delta(T) = v\beta(vT)$ with $v \in \mathbb{F}_{169}$ and $v^2 = 5$, then δ is of type $(13, 6, 4)$ with the pair $(\epsilon_1, \epsilon_2) = (-1, -4)$.

In the following lemma we introduce a sequence $(A_i)_{i \geqslant 1}$ of polynomials in $\mathbb{F}_p[T]$ which is linked to the pair (P_k, Q_k).

Lemma 4.4. *Let k, p, P_k, Q_k be as in Corollary* 4.2. *Let $q = p^s$ and $r = p^t$ with $s, t \geqslant 1$. Let $(A_i)_{i \geqslant 1}$ be the sequence of polynomials in $\mathbb{F}_p[T]$ defined by*

$$A_1 = T \quad \textit{and} \quad A_{i+1} = \bigl[A_i^r/P_k\bigr] \quad \textit{for } i \geqslant 1$$

(*the square brackets denote the integer part of the rational function*). *We set*

$$\theta_k = (-1)^k 2^{1-2k} \binom{2k-1}{k} \in \mathbb{F}_p^*.$$

Then we have

$$A_{i+1}P_k - A_i^r = 2k\theta_k^i Q_k \quad \text{for } i \geqslant 1.$$

Let $\lambda, \mu \in \mathbb{F}_q$, $X \in \mathbb{F}(q)$ *and set* $\delta = 2k\theta_k^i\lambda + \mu$. *Then we have*:

(∗) *if* $\delta \neq 0$,

$$\left[\left(\lambda A_i^r - \mu Q_k\right)/P_k, X\right] = \left[\lambda A_{i+1}, -\delta^{-1}u_1 T, -\delta u_2 T, \ldots, -\delta u_{2k} T, X'\right],$$

where $X' = XP_k^{-2} + Q_k(\delta\omega_k P_k)^{-1}$;

(∗∗) *if* $\delta = 0$,

$$\left[\left(\lambda A_i^r - \mu Q_k\right)/P_k, X\right] = [\lambda A_{i+1}, X].$$

Proof. By induction we can easily check that A_i is an odd polynomial with degree $d_i = (r^{i-1}(r-1-2k)+2k)/(r-1)$. Observe that, if $r = p$ and $k = (p-1)/2$, then we have $A_i = T$ for $i \geqslant 1$. For $i \geqslant 1$, considering the euclidean division of A_i^r by P_k, we can write

$$A_i^r = A_{i+1}P_k + R_i, \tag{9}$$

where R_i is an odd polynomial with $\deg(R_i) \leqslant 2k-1$. Taking derivatives on both sides of (9), we obtain

$$\left(2kTA_{i+1}(T) + A'_{i+1}(T)\left(T^2-1\right)\right)\left(T^2-1\right)^{k-1} + R'_i(T) = 0. \tag{10}$$

Since $\deg(R'_i) \leqslant 2k-2$, we see that $2kTA_{i+1}(T) + A'_{i+1}(T)(T^2-1)$ must be constant. Therefore, we have

$$2kTA_{i+1}(T) + A'_{i+1}(T)\left(T^2-1\right) = 2kA_{i+1}(1). \tag{11}$$

Combining (10) and (11), we obtain

$$R'_i(T) = -2kA_{i+1}(1)\left(T^2-1\right)^{k-1} = -2kA_{i+1}(1)Q'_k(T).$$

Since $(R_i + 2kA_{i+1}(1)Q_k)' = 0$, $\deg(R_i + 2kA_{i+1}(1)Q_k) < p$ and also R_i and Q_k being odd polynomials, the last equality implies

$$R_i(T) = -2kA_{i+1}(1)Q_k(T). \tag{12}$$

Besides, since $A_i(1) \in \mathbb{F}_p$ and consequently $A_i^r(1) = A_i(1)$, (9) and (12) imply

$$A_i(1) = -2kQ_k(1)A_{i+1}(1). \tag{13}$$

Now an elementary computation gives

$$Q_k(1) = (-1)^{k-1}4^{k-1}(2k-1)^{-1}\binom{2k-2}{k-1}^{-1} = (-2k\theta_k)^{-1}. \tag{14}$$

Hence (13) becomes $A_{i+1}(1) = \theta_k A_i(1)$. Since $A_1(1) = 1$, by iteration, we get

$$A_{i+1}(1) = \theta_k^i. \tag{15}$$

Combining (9), (12) and (15), we have proved the first part of the lemma. For the second part, from $A_i^r = A_{i+1}P_k - 2k\theta_k^i Q_k$ and with the notations of the lemma, we clearly have

$$\left(\lambda A_i^r - \mu Q_k\right)/P_k = \lambda A_{i+1} - \delta Q_k/P_k. \tag{16}$$

In the first case $(*)$, if $\delta \neq 0$, we can write

$$\left(\lambda A_i^r - \mu Q_k\right)/P_k = \lambda A_{i+1} - \delta[u_1T, \dots, u_{2k}T]^{-1},$$

or again

$$\left(\lambda A_i^r - \mu Q_k\right)/P_k = \left[\lambda A_{i+1}, -\delta^{-1}u_1T, -\delta u_2T, \dots, -\delta u_{2k}T\right]. \tag{17}$$

Now, in order to obtain the desired statement, we need to transform

$$\left[\left[\lambda A_{i+1}, -\delta^{-1}u_1T, -\delta u_2T, \dots, -\delta u_{2k}T\right], X\right]. \tag{18}$$

We will use Lemma 3.1. With the same notations and $n = 2k+1$, (18) can be written as

$$\left[\lambda A_{i+1}, -\delta^{-1}u_1T, -\delta u_2T, \dots, -\delta u_{2k}T, X'\right], \tag{19}$$

where

$$X' = x_{n-1,2}^{-2}X - x_{n-2,2}x_{n-1,2}^{-1}, \tag{20}$$

and $x_{n-1,2}$ and $x_{n-2,2}$ are the following continuants:

$$x_{n-1,2} = \left\langle -\delta^{-1}u_1T, -\delta u_2T, \dots, -\delta u_{2k}T\right\rangle, \tag{21}$$

$$x_{n-2,2} = \left\langle -\delta^{-1}u_1T, -\delta u_2T, \dots, -\delta^{-1}u_{2k-1}T\right\rangle. \tag{22}$$

The continuant $x_{n-1,2}$ has an even number of terms, therefore (21) becomes

$$x_{n-1,2} = \langle u_1T, u_2T, \dots, u_{2k}T\rangle.$$

Thus, according to Corollary 4.2, we have

$$x_{n-1,2} = (-1)^k P_k. \tag{23}$$

Since the continuant $x_{n-2,2}$ has an odd number of terms, (22) becomes

$$x_{n-2,2} = -\delta^{-1}\langle u_1T, u_2T, \ldots, u_{2k-1}T\rangle.$$

Finally, using Corollary 4.2, we obtain

$$x_{n-2,2} = -\delta^{-1}\omega_k^{-1}(-1)^k Q_k. \tag{24}$$

Thus combining (20), (23) and (24) we have $X' = XP_k^{-2} + (\delta\omega_k P_k)^{-1}Q_k$. Together with (17) and (19) we have the statement (∗). Besides, if $\delta = 0$, (16) implies directly the statement (∗∗). So the proof of this lemma is complete. □

We have noticed that, in the extremal case $k = (p-1)/2$ and if $r = p$, the sequence $(A_i)_{i\geqslant 1}$ introduced above is constant and we have $A_i = T$ for $i \geqslant 1$. We will see further that, if α is a continued fraction expansion of type (r, l, k) and if the first l partial quotients are linear and well chosen, then this sequence $(A_i)_{i\geqslant 1}$ is the core of the expansion and all other partial quotients are linear up to a certain point. Hence in the extremal case they are all linear up to a certain point. In the sequel the notations will be as in Corollary 4.2, Definition 4.3 and Lemma 4.4. We need one more lemma.

Lemma 4.5. *For $n \geqslant 1$ we set $f(n) = (2k+1)n + l - 2k$. Let $\alpha \in \mathbb{F}(q)$ be irrational with $\alpha = [a_1, \ldots, a_n, \ldots]$. Assume that for an index $n \geqslant 1$ we have*

$$a_n = \lambda_n A_i, \quad \text{where } \lambda_n \in \mathbb{F}_q^* \text{ and } i \geqslant 1,$$

and also

$$\alpha_n^r = \epsilon_{1,n} P_k \alpha_{f(n)} + \epsilon_{2,n} Q_k, \quad \text{where } (\epsilon_{1,n}, \epsilon_{2,n}) \in \mathbb{F}_q^* \times \mathbb{F}_q^*.$$

We set $\delta_n = 2k\theta_k^i\lambda_n^r + \epsilon_{2,n}$. Then we have:

(∗) *if $\delta_n \neq 0$,*

$$a_{f(n)} = \lambda_n^r\epsilon_{1,n}^{-1}A_{i+1}, \quad a_{f(n)+i} = -\left(\delta_n\epsilon_{1,n}^{-1}\right)^{(-1)^i} u_iT \quad \text{for } 1 \leqslant i \leqslant 2k,$$

and

$$\alpha_{n+1}^r = \epsilon_{1,n+1}P_k\alpha_{f(n+1)} + \epsilon_{2,n+1}Q_k,$$

where

$$\epsilon_{1,n+1} = \epsilon_{1,n}^{-1} \quad \text{and} \quad \epsilon_{2,n+1} = -(\delta_n\omega_k)^{-1};$$

(∗∗) *if $\delta_n = 0$,*

$$a_{f(n)} = \lambda_n^r\epsilon_{1,n}^{-1}A_{i+1}, \quad a_{f(n)+1} = \epsilon_{1,n}P_k a_{n+1}^r \quad \text{and} \quad \alpha_{n+2}^r = \epsilon_{1,n}P_k\alpha_{f(n)+2}.$$

Please cite this article in press as: A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.01.001

Proof. We have $\alpha_n^r = [a_n^r, \alpha_{n+1}^r]$. Hence the hypothesis implies

$$\left[\lambda_n^r A_i^r, \alpha_{n+1}^r\right] = \epsilon_{1,n} P_k \alpha_{f(n)} + \epsilon_{2,n} Q_k$$

or equivalently

$$\left[(\epsilon_{1,n} P_k)^{-1}\left(\lambda_n^r A_i^r - \epsilon_{2,n} Q_k\right), \epsilon_{1,n} P_k \alpha_{n+1}^r\right] = \alpha_{f(n)}. \tag{25}$$

Now we apply Lemma 4.4 with $\lambda = \lambda_n^r \epsilon_{1,n}^{-1}$, $\mu = \epsilon_{2,n}\epsilon_{1,n}^{-1}$ and $\delta = \delta_n \epsilon_{1,n}^{-1}$. Thus, if $\delta_n \neq 0$, we can write

$$\alpha_{f(n)} = \left[\lambda A_{i+1}, -\delta^{-1} u_1 T, -\delta u_2 T, \ldots, -\delta u_{2k} T, X'\right], \tag{26}$$

where

$$X' = \left(\epsilon_{1,n} P_k \alpha_{n+1}^r\right) P_k^{-2} + Q_k (\delta \omega_k P_k)^{-1},$$

or simply

$$X' = \epsilon_{1,n} P_k^{-1} \alpha_{n+1}^r + Q_k (\delta \omega_k P_k)^{-1}.$$

But, we also have

$$\alpha_{f(n)} = \left[a_{f(n)}, a_{f(n)+1}, \ldots, a_{f(n)+2k}, \alpha_{f(n+1)}\right]. \tag{27}$$

We observe that $|Q_k| < |P_k| < |T|^p \leqslant |\alpha_{n+1}^r|$ and consequently $|X'| \geqslant |T|$. Thus, by comparing (26) and (27), we obtain the values given in the lemma for the partial quotients from $a_{f(n)}$ to $a_{f(n)+2k}$ and also the equality

$$\alpha_{f(n+1)} = \epsilon_{1,n} P_k^{-1} \alpha_{n+1}^r + Q_k (\delta \omega_k P_k)^{-1}.$$

Finally we see that this last equality can be written as

$$\alpha_{n+1}^r = \epsilon_{1,n}^{-1} P_k \alpha_{f(n+1)} - (\delta_n \omega_k)^{-1} Q_k.$$

So the case $(*)$ is established. For the case $(**)$ we apply Lemma 4.4 with $\delta = 0$. Since $\epsilon_{2,n} = -2k\theta_k^i \lambda_n^r$ and $A_i^r + 2k\theta_k^i Q_k = P_k A_{i+1}$, (25) becomes

$$\left[\lambda_n^r \epsilon_{1,n}^{-1} A_{i+1}, \epsilon_{1,n} P_k \alpha_{n+1}^r\right] = \alpha_{f(n)}. \tag{28}$$

This implies $a_{f(n)} = \lambda_n^r \epsilon_{1,n}^{-1} A_{i+1}$ and $\alpha_{f(n)+1} = \epsilon_{1,n} P_k \alpha_{n+1}^r$. But we have

$$\epsilon_{1,n} P_k \alpha_{n+1}^r = \left[\epsilon_{1,n} P_k a_{n+1}^r, (\epsilon_{1,n} P_k)^{-1} \alpha_{n+2}^r\right].$$

Since $|(\epsilon_{1,n} P_k)^{-1} \alpha_{n+2}^r| > 1$, we obtain $a_{f(n)+1} = \epsilon_{1,n} P_k a_{n+1}^r$ and $\alpha_{f(n)+2} = (\epsilon_{1,n} P_k)^{-1} \alpha_{n+2}^r$. So the proof of the lemma is complete. □

Please cite this article in press as: A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.01.001

This last lemma shows that for an expansion of type (r,l,k) if $a_1=\lambda_1 A_1$ and $(*)$ is satisfied then the $2k+1$ partial quotients from a_{l+1} on are known and are of the same type that is multiple of A_j for $j=1$ or $j=2$. Moreover, α_2 is also an expansion of type $(r, f(2)-1, k)$ and so we can eventually iterate the process. So, if the l first partial quotients are multiples of T and as long as condition $(*)$ is satisfied, each partial quotient generates a group of $2k+1$ new partial quotients. This allows us to describe the expansion up to a certain point. In the following proposition we give this description of the continued fraction assuming that the l first partial quotients are linear polynomials.

Proposition 4.6. *Let $\Lambda=(\lambda_1,\ldots,\lambda_l)$ be given in $(\mathbb{F}_q^*)^l$. For $1\leqslant i\leqslant l$ we set $a_i=\lambda_i T$. Let $\alpha\in\mathbb{F}(q)$ be an irrational element with $\alpha=[a_1,\ldots,a_l,\alpha_{l+1}]$. Assume that α is an expansion of type (r,l,k) with the pair $(\epsilon_1,\epsilon_2)\in\mathbb{F}_q^*\times\mathbb{F}_q^*$. For $n\geqslant 1$ we set $f(n)=(2k+1)n+l-2k$ and $f(\infty)=\infty$. Then there exist a sequence of positive integers $(i(n))_{n\geqslant 1}$ and $N\in\mathbb{N}^*\cup\{\infty\}$ such that*

$$a_n=\lambda_n A_{i(n)} \quad \textit{with } \lambda_n\in\mathbb{F}_q^* \textit{ for } 1\leqslant n\leqslant f(N).$$

The sequence $(\lambda_n)_{l+1\leqslant n\leqslant f(N)}$ is defined in the following way:

$$\lambda_{f(n)}=\epsilon_1^{(-1)^n}\lambda_n^r \quad \textit{for } 1\leqslant n\leqslant N,$$

and

$$\lambda_{f(n)+i}=-\epsilon_1^{(-1)^{n+i}}\delta_n^{(-1)^i}u_i \quad \textit{for } 1\leqslant i\leqslant 2k \textit{ and } 1\leqslant n\leqslant N-1,$$

where the sequence $(\delta_n)_{1\leqslant n\leqslant N}$ is defined recursively by

$$\delta_n=2k\theta_k^{i(n)}\lambda_n^r-(\delta_{n-1}\omega_k)^{-1} \quad \textit{for } 1\leqslant n\leqslant N,$$

and $\delta_0=-(\omega_k\epsilon_2)^{-1}$. If $N\in\mathbb{N}^*$, then we have $\delta_N=0$ and

$$a_{f(N)+1}=\epsilon_1^{(-1)^{N+1}}P_k a_{N+1}^r.$$

Moreover, the sequence $(i(n))_{1\leqslant n\leqslant f(N)}$ is defined recursively by

$$\text{(I)} \quad i\bigl(f(n)\bigr)=i(n)+1 \quad \textit{for } 1\leqslant n\leqslant N,$$

and the initial conditions

$$\text{(II)} \quad i(n)=1 \quad \textit{if } 1\leqslant n\leqslant l \quad \textit{or} \quad n-l+2k\not\equiv 0 \pmod{2k+1}.$$

Finally, given two integers $m>1$ and $n\geqslant 1$, we denote by $v_m(n)$ the largest power of m dividing n. If $1\leqslant l\leqslant 2k$, then we have

$$i(n)=v_{2k+1}(2kn+l-2k)+1 \quad \textit{for } 1\leqslant n\leqslant f(N).$$

Proof. We have $\alpha^r = \epsilon_1 P_k \alpha_{l+1} + \epsilon_2 Q_k$ and $a_i = \lambda_i T$ for $1 \leqslant i \leqslant l$. Thus we have $i(n) = 1$ for $1 \leqslant n \leqslant l$. We set $\delta_1 = 2k\theta_k\lambda_1^r + \epsilon_2$. If $\delta_1 = 0$ we put $N = 1$. We apply Lemma 4.5 case $(**)$ and obtain $a_{f(1)} = \epsilon_1^{-1}\lambda_1^r A_2$ and $a_{f(1)+1} = \epsilon_1 P_k a_2^r$. Thus we have $i(f(1)) = 2 = i(1) + 1$ and the proposition is clearly true. If $\delta_1 \neq 0$ then we apply the case $(*)$ of this lemma. Thus we have $i(f(1)) = 2$ and $i(n) = 1$ for $l + 1 \leqslant n \leqslant l + 2k + 1$ and $a_n = \lambda_n A_{i(n)}$ where the λ_n are as stated in the proposition. By repeated application of the same case $(*)$ of Lemma 4.5 we build a sequence δ_n satisfying the recursive formula stated in the proposition, until we eventually find an integer N such that $\delta_N = 0$. If there is no such an integer we put $N = \infty$. So all the partial quotients a_n have the desired form $\lambda_n A_{i(n)}$ for a certain integer $i(n)$ with the values of λ_n as stated in the proposition up to $f(N)$. In the case $N \in \mathbb{N}^*$ we obtain the values for $a_{f(N)}$ and $a_{f(N)+1}$ applying the case $(**)$ of this lemma. The integer $i(n)$, according to this lemma, satisfies clearly the property $i(f(n)) = i(n) + 1$ and also the initial conditions stated in this proposition. So all what is left to show is the last formula given for the integer $i(n)$ if $1 \leqslant l \leqslant 2k$. We observe that if $1 \leqslant n \leqslant f(N)$ and n is not as indicated in (II) then there exists an integer m with $n = f(m)$ and $1 \leqslant m \leqslant N$ so that (I) can be applied. We put $j(n) = v_{2k+1}(2kn + l - 2k) + 1$. To prove the equality $i(n) = j(n)$ we will show that $j(n)$ satisfies the same recurrence formula (I) and also the same initial conditions (II) as $i(n)$. Indeed we have $2kf(n) + l - 2k = (2k + 1)(2kn + l - 2k)$ and this implies $j(f(n)) = j(n) + 1$. Moreover, if $2kn + l - 2k \equiv 0 \pmod{2k + 1}$ then by simple computation we have $2k(n - l + 2k) \equiv 0 \pmod{2k + 1}$ and consequently $n - l + 2k \equiv 0 \pmod{2k + 1}$. Thus $j(n) = 1$ if $n - l + 2k \not\equiv 0 \pmod{2k + 1}$. Finally if $1 \leqslant n \leqslant l \leqslant 2k$ then $2kn + l - 2k = (2k + 1)n + u$ with $-2k \leqslant u \leqslant -1$. Consequently we have $2kn + l - 2k \not\equiv 0 \pmod{2k + 1}$ and therefore $j(n) = 1$. So the proof of the proposition is complete. □

In the previous proposition the value of N will depend upon the choice of the l-tuple $(\lambda_1, \ldots, \lambda_l)$ and of the pair (ϵ_1, ϵ_2). Of course we are mainly interested in the case $N = \infty$ and then we will say that the expansion for α is perfect. The existence of perfect expansions is a consequence of Mills and Robbins work [8], with the first example in $\mathbb{F}(p)$ for $p > 3$ mentioned in the introduction. This example corresponds to the case $r = p$, $l = 2$ and $k = (p - 1)/2$. As we observed above, this case is particularly remarkable because then all the partial quotients are linear and that is why it was first introduced. In previous works, Ruch and the author [6] have studied in a different approach continued fraction expansions of this type with all partial quotients linear. It results from this study that the problem of the existence of infinite sequences in $\mathbb{F}_q^*$ satisfying the description given in Proposition 4.6 (at least in the case $k = (p - 1)/2$, $r = p$ and $l = p$) is complex in general, as there can be singular solutions for certain finite fields $\mathbb{F}_q$ which are not prime (see [6, p. 564]). Concerning the second example in $\mathbb{F}(13)$, introduced by Mills and Robbins and mentioned in the introduction, we have seen that it is (up to a simple transformation) of type $(13, 6, 4)$. The continued fraction expansion for this element was checked by computer. The conjecture made about this expansion (see [8, p. 404] and [3, p. 343]) is in agreement with the description given in Proposition 4.6 for the first 547 partial quotients, so that $N \geqslant 61$. Yet it is an open question whether this expansion is perfect or not.

Now we turn to the proof of Theorem 3 which brings out an example of a perfect expansion of type $(p, 1, 1)$.

Proof of Theorem 3. Let $\alpha = [a_1, \ldots, a_n, \ldots]$ be the infinite continued fraction expansion in $\mathbb{F}(p)$ defined by $a_1 = 3T$ and the equality $\alpha^p = (T^2 - 1)\alpha_2 + T$. Using the previous notations with $k = 1$, we have $P_1 = T^2 - 1$, $Q_1 = T$, $(u_1, u_2) = (1, -1)$, $\omega_1 = -1$ and $\theta_1 = -1/2$. Also $(\epsilon_1, \epsilon_2) = (1, 1)$. With the notations of Proposition 4.6 and $l = 1$, we have

$f(n) = 3n - 1$ and $i(n) = v_3(2n-1) + 1$. So according to this proposition the partial quotients are $a_n = \lambda_n A_{v_3(2n-1)+1}$ for $1 \leqslant n \leqslant 3N - 1$. The first element $\lambda_1 \in \mathbb{F}_p^*$ is given and the sequence $(\lambda_n)_{2 \leqslant n \leqslant 3N-1}$ in $\mathbb{F}_p^*$ satisfies

$$\text{(A)} \quad \lambda_{3n-1} = \lambda_n \quad \text{for } 1 \leqslant n \leqslant N,$$

and

$$\text{(B)} \quad \lambda_{3n} = -\delta_n^{-1}, \quad \lambda_{3n+1} = \delta_n \quad \text{for } 1 \leqslant n \leqslant N - 1,$$

where the sequence $(\delta_n)_{1 \leqslant n \leqslant N}$ is defined recursively by

$$\text{(C)} \quad \delta_n = -\lambda_n(-2)^{-v_3(2n-1)} + \delta_{n-1}^{-1} \quad \text{and} \quad \delta_0 = 1.$$

To show that α has the required continued fraction expansion, we give the explicit expression for δ_n and this proves that $N = \infty$. Indeed, setting $\delta_n = (-1)^{k_n} 2^{l_n}$ for $n \geqslant 1$, we shall prove that the sequences $(\lambda_n)_{n \geqslant 1}$ and $(\delta_n)_{n \geqslant 1}$ in $\mathbb{F}_p^*$ satisfy the equalities (A), (B) and (C) stated above for $n \geqslant 1$ with the initial conditions $\lambda_1 = 3$ and $\delta_0 = 1$. For $n \geqslant 1$ we put $x_n = (-2)^{v_3(2n-1)}(\delta_{n-1}^{-1} - \delta_n)$. Thus, (C) will be satisfied if we prove that $x_n = \lambda_n$ for $n \geqslant 1$. We observe that $x_1 = \delta_0^{-1} - \delta_1 = 1 + 2 = \lambda_1$ and also $x_2 = (-2)(\delta_1^{-1} - \delta_2) = (-2)(-1/2 - 1) = x_1$. To prove the equality of these sequences, we have to show that $(x_n)_{n \geqslant 1}$ satisfies (A) and (B). A simple verification shows that, if $n \geqslant 1$ and $k \geqslant 0$ are integers with $2n - 1 \in [3^k; 3^{k+1}[$, then the three integers $6n - 3, 6n - 1$ and $6n + 1$ belong to the interval $[3^{k+1}; 3^{k+2}[$. Consequently we have

$$k_{3n-1} = k_{3n} = k_{3n+1} = k_n + 1 \quad \text{for } n \geqslant 1.$$

Combining these equalities with the recurrence formulas for the sequence $(l_n)_{n \geqslant 1}$, we obtain

$$\delta_{3n-1} = (-2)^{-1}\delta_n, \quad \delta_{3n} = -\delta_n^{-1} \quad \text{and} \quad \delta_{3n+1} = -2\delta_n \quad \text{for } n \geqslant 1.$$

Using these recurrence formulas for $(\delta_n)_{n \geqslant 1}$, for $n \geqslant 2$ we can write

$$\begin{aligned} x_{3n-1} &= (-2)^{v_3(6n-3)}\big(\delta_{3n-2}^{-1} - \delta_{3n-1}\big) \\ &= (-2)^{v_3(2n-1)+1}\big((-2)^{-1}\delta_{n-1}^{-1} - (-2)^{-1}\delta_n\big) = x_n. \end{aligned}$$

So the sequence $(x_n)_{n \geqslant 1}$ satisfies (A) for $n \geqslant 1$. Moreover, for $n \geqslant 1$ we have

$$x_{3n} = (-2)^{v_3(6n-1)}\big(\delta_{3n-1}^{-1} - \delta_{3n}\big) = -2\delta_n^{-1} + \delta_n^{-1} = -\delta_n^{-1}$$

and

$$x_{3n+1} = (-2)^{v_3(6n+1)}\big(\delta_{3n}^{-1} - \delta_{3n+1}\big) = -\delta_n + 2\delta_n = \delta_n.$$

So the sequence $(x_n)_{n \geqslant 1}$ satisfies (B) for $n \geqslant 1$. This completes the proof of the theorem. □

Please cite this article in press as: A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.01.001

References

[1] L. Baum, M. Sweet, Continued fractions of algebraic power series in characteristic 2, Ann. of Math. 103 (1976) 593–610.

[2] A. Bluher, A. Lasjaunias, Hyperquadratic power series of degree four, Acta Arith. 124 (2006) 257–268.

[3] W. Buck, D. Robbins, The continued fraction of an algebraic power series satisfying a quartic equation, J. Number Theory 50 (1995) 335–344.

[4] A. Lasjaunias, A survey of diophantine approximation in fields of power series, Monatsh. Math. 130 (2000) 211–229.

[5] A. Lasjaunias, J.-J. Ruch, Flat power series over a finite field, J. Number Theory 95 (2002) 268–288.

[6] A. Lasjaunias, J.-J. Ruch, On a family of sequences defined recursively in $\mathbb{F}_q^*$ (II), Finite Fields Appl. 10 (2004) 551–565.

[7] M. Mendès France, Sur les fractions continues limitées, Acta Arith. 23 (1973) 207–215.

[8] W. Mills, D. Robbins, Continued fractions for certain algebraic power series, J. Number Theory 23 (1986) 388–404.

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

Please cite this article in press as: A. Lasjaunias, Continued fractions for hyperquadratic power series over a finite field, Finite Fields Appl. (2007), doi:10.1016/j.ffa.2007.01.001