ACTA ARITHMETICA
124.3 (2006)

Hyperquadratic power series of degree four

by

Antonia W. Bluher (Fort Meade, MD)
and Alain Lasjaunias (Bordeaux)

1. Introduction. Let p be a prime number and $q = p^s$ with a positive integer s. We consider the finite field $\mathbb{F}_q$ with q elements. Then we introduce, with an indeterminate T, the ring of polynomials $\mathbb{F}_q[T]$ and the field of rational functions $\mathbb{F}_q(T)$. We also consider the absolute value defined on $\mathbb{F}_q(T)$ by $|P/Q| = |T|^{\deg P - \deg Q}$ for $P, Q \in \mathbb{F}_q[T]$, where $|T|$ is a fixed real number greater than one. By completing $\mathbb{F}_q(T)$ with this absolute value we obtain a field, denoted by $\mathbb{F}(q)$, which is the field of formal power series in $1/T$ with coefficients in $\mathbb{F}_q$. We recall that this field is often denoted by $\mathbb{F}_q((T^{-1}))$. Thus if α is a nonzero element of $\mathbb{F}(q)$ we have

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

There is a strong analogy between the classical construction of the field of real numbers and the fields of power series which we are considering here. The rôles of $\{\pm 1\}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are played by $\mathbb{F}_q^*$, $\mathbb{F}_q[T]$, $\mathbb{F}_q(T)$, and $\mathbb{F}(q)$ respectively.

The study of rational approximation to algebraic elements in the field $\mathbb{F}(q)$ was initiated by K. Mahler [M] by adapting a classical theorem of Liouville concerning rational approximation to algebraic real numbers. In his article Mahler pointed at the difference with the classical case by introducing an example. Given a prime p and an integer $r = p^t$ with $t \ge 1$, the element $\alpha \in \mathbb{F}(p)$ defined by $\alpha = \sum_{k \ge 0} T^{r^k}$ does satisfy the algebraic equation $\alpha - \alpha^r = T^{-1}$. We know by Roth's theorem that algebraic real numbers are badly approximable by rational numbers, but in the case of power series over a finite field there is no analogue of Roth's theorem and the element introduced above appears to be a counterexample. Following Mahler's work it became progressively necessary to consider a special subset of alge-

2000 *Mathematics Subject Classification*: 11T55, 11J61, 12E10.
Key words and phrases: finite fields, projective polynomials, fields of power series.

braic power series having particular properties of rational approximation. The reader who is interested in a survey on the different contributions to this topic and for full references can consult for example [L] and [T, Chap. 9].

We introduce a special subset of elements in $\mathbb{F}(q)$ which are algebraic over $\mathbb{F}_q(T)$. Let $r = p^t$ where $t \geq 0$ is an integer. We denote by $H_t(q)$ the subset of irrational elements α in $\mathbb{F}(q)$ such that there exist $A, B, C, D \in \mathbb{F}_q[T]$ with

$$\alpha = \frac{A\alpha^r + B}{C\alpha^r + D}. \tag{1}$$

We can observe that if $\alpha \in \mathbb{F}(q)$ is irrational then so is α^r and therefore we have $A\alpha^r + B \neq 0$ and $C\alpha^r + D \neq 0$. Consequently we see that $AD - BC = (A - C\alpha)(C\alpha^r + D) \neq 0$. Now we put $\mathcal{H}(q) = \bigcup_{t\geq 0} H_t(q)$. Because of further analogies with quadratic real numbers, we call the elements of this subset *hyperquadratic elements*. In previous works the term *algebraic element of class I* has been used but we think the present denomination is more descriptive and also convenient for later precision. In view of the shape of equation (1), $\mathcal{H}(q)$ can be viewed as the analogue of the subset of quadratic real numbers, the Frobenius isomorphism being replaced by the identity map.

If $\alpha \in \mathcal{H}(q)$ then it is a root of the polynomial

$$uX^{r+1} + vX^r + wX + z \in \mathbb{F}_q[T][X] \quad \text{with } uz - vw \neq 0. \tag{2}$$

These polynomials, where the coefficients belong to an arbitrary field F of characteristic p, arise in other contexts of number theory and have been studied from an algebraic point of view by Carlitz, Serre, Abhyankar, and others; see [C], [A], and [B].

Note that if $\alpha \in H_t(q)$ then $\alpha = f(\alpha^r)$ where f is the linear fractional transformation with integer coefficients involved in equation (1). By iteration we obtain $\alpha = f((f(\alpha^r))^r) = g(\alpha^{r^2})$ where g is another linear fractional transformation with integer coefficients. Consequently, recursively we see that if α is a root of a polynomial of type (2) then it satisfies for all integers $n \geq 1$ an algebraic equation of the type

$$u_n\alpha^{r^n+1} + v_n\alpha^{r^n} + w_n\alpha + z_n = 0.$$

So $H_t(q) \subset H_{nt}(q)$ for all positive integers n.

Now to be more precise, we introduce the following terminology. If t is the smallest nonnegative integer such that $\alpha \in \mathbb{F}(q)$ satisfies an equation of type (1) we will say that α is a *hyperquadratic element of order t*. With our definition, a hyperquadratic element of order zero is simply a quadratic element. We observe that elements of $\mathbb{F}(q)$ which are quadratic or cubic over $\mathbb{F}_q(T)$ belong to $H_1(q)$ since then $1, \alpha, \alpha^p, \alpha^{p+1}$ are linked over $\mathbb{F}_q(T)$ and consequently α satisfies an algebraic equation of type (2). Moreover $\mathcal{H}(q)$

also contains elements of arbitrarily large degree over $\mathbb{F}_q(T)$. Indeed, for the element $\alpha \in \mathbb{F}(p)$ introduced by Mahler and mentioned above with $r = p^t$ and $t \geq 1$, it was proved by arguments of diophantine approximation that it is algebraic of degree r over $\mathbb{F}_p(T)$ and also hyperquadratic of order t. On the other hand, it will become clear in the next section that not all algebraic numbers in $\mathbb{F}(q)$ are hyperquadratic.

We have to recall a general and simple property of the subset $\mathcal{H}(q)$: it is stable under any linear fractional transformation with integer coefficients and also under the Frobenius isomorphism $x \mapsto x^p$; moreover both transformations preserve the algebraic degree of each element as well as the hyperquadratic order.

Rational approximation to certain hyperquadratic power series is well known, which is also due to the possibility of describing explicitly their continued fraction expansion. The first works in this area were undertaken by Baum and Sweet [BS]. Later this has been done for many examples and also for different subclasses of hyperquadratic elements (see in particular [S]). Here again we must underline the analogy with the classical case of real numbers: the continued fraction expansion for quadratic real numbers is well known and this is due to the fact that these elements are fixed points of a linear fractional transformation with integer coefficients. Nevertheless the possibility of describing the continued fraction expansion for all hyperquadratic power series is still an open problem. In [MR] Mills and Robbins have studied this problem and they described an algorithm to obtain in certain cases the continued fraction expansion for a hyperquadratic power series. At the end of their article ([MR, p. 403]) they considered the following algebraic equation: $x^4 + x^2 - Tx + 1 = 0$. They observed that it has a unique solution in $\mathbb{F}(p)$ for all primes p. They noticed that for this solution the continued fraction expansion has a remarkable pattern in both cases $p = 3$ and $p = 13$. The expansion for $p = 3$ has been explicitly described (see [BR]) and this implies that the solution is not hyperquadratic (see [L, pp. 226–227]). For $p = 13$ the expansion was only conjectured (see [BR, pp. 342–344]), but as we will see the solution is then hyperquadratic. This fact may lead to a proof of this conjecture.

Since all algebraic power series of degree two or three are hyperquadratic, it is natural to ask, for a quartic power series over $\mathbb{F}_q$ given by its defining equation, whether it is a hyperquadratic element or not. Inspired by Mills and Robbins' equation we have investigated this question. In the next section we describe the connection between hyperquadratic power series and differential algebra. We derive from it a necessary condition for quartic power series to be hyperquadratic. In the last section we prove that under a simple and general condition a quartic power series is hyperquadratic of order one or two, depending on different possible characteristics.

2. Differentiation of algebraic power series. We consider the formal differentiation on $\mathbb{F}_q(T)$ which can be extended to $\mathbb{F}(q)$. We have the usual rules for differentiation of sums and products of elements in $\mathbb{F}(q)$ and if $x \in \mathbb{F}(q)$ then the derivative is denoted by x'. Observe that because of the positive characteristic p the subfield of constants in $\mathbb{F}(q)$ is the field of power series over $\mathbb{F}_q$ in T^p.

PROPOSITION 2.1. *Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial in $\mathbb{F}_q(T)[X]$, irreducible over $\mathbb{F}_q(T)$ and of degree $n > 1$. Let M be the $n \times n$ square matrix with coefficients in $\mathbb{F}_q(T)$ defined by*

$$M = \begin{vmatrix} 0 & 0 & 0 & & \dots & -a_0 \\ 1 & 0 & 0 & & \dots & -a_1 \\ 0 & 1 & 0 & & \dots & -a_2 \\ \vdots & & & \ddots & & \vdots \\ 0 & & \dots & 1 & 0 & -a_{n-2} \\ 0 & & \dots & 0 & 1 & -a_{n-1} \end{vmatrix}.$$

Let $U_0 = (u_{i,0})_{0 \le i \le n-1}$ be the column vector with $u_{0,0} = 1$ and $u_{i,0} = 0$ for $1 \le i \le n-1$. Let $(U_m)_{m \ge 1}$ be the sequence of column vectors $U_m = (u_{m,i})_{0 \le i \le n-1}$ in $(\mathbb{F}_q(T))^n$ defined by

$$U_m = M^m U_0 \quad \text{for } m \ge 1.$$

Let A be the $(2n-1) \times (2n-1)$ square matrix with coefficients in $\mathbb{F}_q(T)$ defined by

$$A = \begin{vmatrix} 1 & a_{n-1} & \dots & a_0 & & \dots & 0 \\ 0 & 1 & a_{n-1} & a_{n-2} & & \dots & 0 \\ \vdots & & & & \ddots & & \vdots \\ 0 & \dots & 1 & \dots & a_2 & a_1 & a_0 \\ n & (n-1)a_{n-1} & \dots & a_1 & & \dots & 0 \\ 0 & n & (n-1)a_{n-1} & & \ddots & \dots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \dots & n & \dots & 3a_3 & 2a_2 & a_1 \end{vmatrix}.$$

Let $A_{i,j}$ be the matrix obtained from A by deleting the ith row and jth column. For $0 \le k \le 2n-2$, we set

$$c_k = \sum_{\substack{i+j=k \\ 0 \le i,j \le n-1}} (-1)^j a_i' \det(A_{2n-1-j,2n-1}),$$

and also for $0 \leq k \leq n-1$,

$$b_k = c_k + \sum_{i=n}^{2n-2} c_i u_{i,k}.$$

Finally, we denote by $D(f)$ *the discriminant of the polynomial* f. *Then if* $\alpha \in \mathbb{F}(q)$ *is such that* $f(\alpha) = 0$, *we have*

$$\alpha' = ((-1)^{n(n-1)/2+1}/D(f)) \sum_{k=0}^{n-1} b_k \alpha^k.$$

Proof. Let $\alpha \in \mathbb{F}(q)$ be such that $f(\alpha) = 0$. Then α is algebraic over $\mathbb{F}_q(T)$ of degree n and $\alpha^m \in \mathbb{F}_q(T, \alpha)$ for $m \geq 0$. Consequently, we have $\alpha^m = \sum_{i=0}^{n-1} v_{m,i}\alpha^i$ for a vector $V_m = (v_{m,i})_{0 \leq i \leq n-1}$ of $(\mathbb{F}_q(T))^n$. From $\alpha^m = \sum_{i=0}^{n-1} v_{m,i}\alpha^i$, mutiplying by α and using the relation $\alpha^n = -\sum_{i=0}^{n-1} a_i\alpha^i$, we obtain $V_{m+1} = MV_m$ where M is the matrix defined in the proposition. Since $V_0 = U_0$ we see that $U_m = V_m$ and that $U_m = M^m U_0$ holds for $m \geq 1$.

We introduce the polynomials in $\mathbb{F}_q(T)[X]$ defined by $f'_X(X) = nX^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1}$ and $f'_T(X) = a'_1X^{n-1} + a'_2X^{n-2} + \cdots + a'_n$. Consequently, by formal differentiation of the equality $f(\alpha) = 0$, we obtain

$$\alpha' f'_X(\alpha) + f'_T(\alpha) = 0. \tag{1}$$

Since the extension field $\mathbb{F}_q(T, \alpha)$ of $\mathbb{F}_q(T)$ is separable we have $f'_X(\alpha) \neq 0$. Therefore (1) implies

$$\alpha' = -f'_T(\alpha)/f'_X(\alpha). \tag{2}$$

Now we introduce the resultant $R(f, f'_X)$ of f and f'_X in $\mathbb{F}_q(T)[X]$. It is the determinant of the square matrix A defined in the proposition. Since f is unitary this resultant is known to be equal to $(-1)^{n(n-1)/2}D(f)$ where $D(f)$ is the discriminant of f. Moreover since the extension $\mathbb{F}_q(T, \alpha)$ is separable this discriminant is not zero. Now we know that there are two polynomials P_1 and P_2 in $\mathbb{F}_q(T)[X]$ such that

$$R(f, f'_X) = P_1(X)f(X) + P_2(X)f'_X(X). \tag{3}$$

Therefore replacing X by α in (3) we have $(-1)^{n(n-1)/2}D(f) = P_2(\alpha)f'_X(\alpha)$. Combining this last equality and (2) we obtain

$$\alpha' = ((-1)^{n(n-1)/2+1}/D(f))f'_T(\alpha)P_2(\alpha). \tag{4}$$

The explicit expression for $P_2(X)$ is a classical result. Indeed, with the notations introduced in the proposition we have

$$P_2(X) = \sum_{j=0}^{n-1} (-X)^j \det(A_{2n-1-j,2n-1}), \tag{5}$$

From (5) and the expression for $f'_T(X)$, we obtain

$$P_2(\alpha)f'_T(\alpha) = \sum_{k=0}^{2n-2} c_k\alpha^k \tag{6}$$

where c_k is defined as in the proposition for $0 \le k \le 2n-2$. Clearly (6) becomes

$$P_2(\alpha)f'_T(\alpha) = \sum_{k=0}^{n-1} c_k\alpha^k + \sum_{k=n}^{2n-2} c_k\Big(\sum_{i=0}^{n-1} u_{k,i}\alpha^i\Big). \tag{7}$$

Finally, (7) implies

$$P_2(\alpha)f'_T(\alpha) = \sum_{k=0}^{n-1} b_k\alpha^k \tag{8}$$

where b_k is defined as in the proposition for $0 \le k \le n-1$. Now combining (4) and (8) we see that α satisfies the desired differential equation. ∎

PROPOSITION 2.2. *Let $\alpha \in \mathbb{F}(q)$ be a hyperquadratic element of algebraic degree $n > 3$. Then in the differential equation satisfied by α with the above notations we have $b_k = 0$ for $3 \le k \le n-1$. In this case the differential equation satisfied by α is called a* Riccati differential equation.

Proof. Since α is algebraic of degree n it is clear that the differential equation obtained in the previous proposition is unique. Now if α is hyperquadratic then $\alpha = f(\alpha^r)$ where f is a linear fractional transformation with coefficients in $\mathbb{F}_q[T]$. Thus $\alpha^r = f^{-1}(\alpha)$. By differentiating this last equality and recalling that $(\alpha^r)' = 0$, we see that α satisfies a Riccati differential equation. ∎

The introduction of Riccati differential equations in the study of diophantine approximation in positive characteristic goes back to Osgood's work [O]. We must add that the statement of the above proposition was first observed by Voloch in [V, p. 218].

PROPOSITION 2.3. *Let p be a prime with $p > 2$ and q be a power of p. Let $\alpha \in \mathbb{F}(q)$ be hyperquadratic and algebraic of degree four. Then there is $u \in \mathbb{F}_q(T)$ such that $\beta = \alpha + u$ satisfies the algebraic equation*

$$\beta^4 + a\beta^2 + b\beta + c = 0$$

with $a, b, c \in \mathbb{F}_q(T)$ and we have

$$(*) \qquad (9b^2 + 2a^3 - 8ac)(a^2 + 12c)' - 4(3b'b + a'a^2 - 4a'c)(a^2 + 12c) = 0.$$

Proof. If $\alpha \in \mathbb{F}(q)$ is algebraic of degree four then we have

$$\alpha^4 + A\alpha^3 + B\alpha^2 + C\alpha + D = 0$$

with $A, B, C, D \in \mathbb{F}_q(T)$. If we put $\beta = \alpha + A/4$ then

$$\beta^4 + a\beta^2 + b\beta + c = 0 \quad \text{with } a, b, c \in \mathbb{F}_q(T).$$

Now α is hyperquadratic if and only if β is so. Thus, according to the second proposition, β satisfies a differential Riccatti equation. Therefore in the differential equation described in Proposition 2.1 we have $b_3 = 0$. Using the same notations as above we have $b_3 = c_3 + c_4 u_{4,3} + c_5 u_{5,3} + c_6 u_{6,3}$ and finally

$$b_3 = -a' \det(A_{6,7}) + b' \det(A_{5,7}) + (aa' - c') \det(A_{4,7}). \tag{9}$$

If we now compute the determinants of $A_{4,7}$, $A_{5,7}$ and $A_{6,7}$ we obtain

$$\det(A_{4,7}) = 4(9b^2 + 2a^3 - 8ac), \quad \det(A_{5,7}) = 4b(a^2 + 12c), \tag{10}$$

$$\det(A_{6,7}) = 2(21b^2 a + 32c^2 - 24ca^2 + 4a^4). \tag{11}$$

Finally, from (9)–(11) we can see that $b_3 = 0$ is equivalent to the condition $(*)$ stated in the proposition. ∎

This last proposition gives a necessary condition $(*)$ on the coefficients of the algebraic equation satisfied by β for this element to be hyperquadratic. It is clear that $(*)$ is satisfied in two simple cases: if (1) $a = b = 0$ or if (2) $a^2 + 12c = 0$. We will see in the next section that both conditions (1) and (2) are sufficient for the element to be hyperquadratic. We recall Mills and Robbins' algebraic equation $x^4 + x^2 - Tx + 1 = 0$, which has a unique solution in $\mathbb{F}(p)$ for all primes p. As pointed out in the introduction, this solution in $\mathbb{F}(3)$ is not hyperquadratic. Nevertheless, in the case $p = 13$, condition (2) above is satisfied, therefore the solution in $\mathbb{F}(13)$, according to Theorem 3.4 below, is hyperquadratic of order one.

3. Hyperquadratic power series of degree four. The definition of hyperquadratic can be extended to any field K of characteristic p. Namely, a separable algebraic element $\alpha \in \overline{K}$ will be called *hyperquadratic* if it satisfies an equation $\alpha = \gamma(\alpha^r)$ for some $\gamma \in \mathrm{PGL}_2(K)$, where r is a power of p. In this wider context, we can prove that a large family of algebraic elements of degree four are hyperquadratic.

THEOREM 3.1. *Let p be a prime number with $p \geq 5$. Let $r = p$ if $p \equiv 1 \pmod 3$ and $r = p^2$ if $p \equiv 2 \pmod 3$. Let K be a field of characteristic p. Let $a, b \in K$ and $f \in K[X]$ with $f(x) = x^4 + ax^2 + bx - a^2/12$. Then there is a nontrivial polynomial $g \in K[x]$ of the form $g(x) = Ax^{r+1} + Bx^r + Cx + D$ such that $f(x)$ divides $g(x)$.*

Note that if $AD - BC \neq 0$, then a root of f will be hyperquadratic, because $g(\alpha) = 0$ implies $\alpha = -(B\alpha^r + D)/(A\alpha^r + C)$. In particular, $AD - BC$ is nonzero whenever f has an irrational root α, since $AD - BC = (A - C\alpha)(C\alpha^r + D) \neq 0$.

The proof of our theorem, as a consequence of the lemma below, is obtained by reducing the statement to the case of a finite field K.

LEMMA 3.2. *Suppose that Theorem* 3.1 *holds when* $K = \mathbb{F}_r$. *Then it holds for all fields* K *of characteristic* p.

Proof. Let $R = K[x]/(f)$ be the 4-dimensional K-vector space spanned by $1, x, x^2, x^3$. In particular, there are unique $m_i^{(n)} \in K$ such that

$$x^n = m_1^{(n)}x^3 + m_2^{(n)}x^2 + m_3^{(n)}x + m_4^{(n)}$$

where the equality holds in the ring R. Obviously the $m_i^{(n)}$ depend on a and b. The theorem is equivalent to the assertion that x^{r+1}, x^r, x, and 1 are linearly dependent in R. Since x and 1 are linearly independent, a linear relation would have to involve x^{r+1} and/or x^r. Then it is clear that the theorem holds if and only if $m_1^{(r+1)}m_2^{(r)} - m_2^{(r+1)}m_1^{(r)} = 0$.

Let w, z be transcendentals over $\mathbb{F}_p$, and $F = x^4 + wx^2 + zx - w^2/12 \in \mathbb{F}_p[w, z, x]$. This is a special case of the polynomial f, with a, b being transcendental quantities. Assign to w a weight of 2, to z a weight of 3, and to x a weight of 1. Then F is homogeneous of weight 4. In the ring $\mathbb{F}_p[w, z, x]/(F)$, for $k \geq 4$, we may write x^k as $-x^{k-4}(wx^2 + zx - w^2/12)$, and the resulting polynomial still has weight k and is a polynomial in w, z, and x. Continuing in this manner, we see that $x^k \pmod F$ has the form $\sum_{i=0}^{3} h_i(w, z)x^i$, where each h_i is either zero or a homogeneous polynomial in w and z of weight $k - i$. In particular, each $m_i^{(k)}(w, z)$ belongs to $\mathbb{F}_p[w, z]$, and $m_1^{(k+1)}$, $m_2^{(k+1)}$, $m_1^{(k)}$, $m_2^{(k)}$ have weights $(k+1)-3$, $(k+1)-2$, $k-3$, and $k-2$, respectively (or they are zero). It follows that $m_1^{(k+1)}m_2^{(k)} - m_2^{(k+1)}m_1^{(k)}$ is either zero or a polynomial $H_k(z, w)$ of weight $2k - 4$. If a, b are arbitrary elements of a field K in characteristic p, then f is the specialization of F to $w = a$, $z = b$. Thus, $m_i^{(k)}$ may be obtained by specializing the above polynomials at $w = a$, $z = b$. It follows that there is a polynomial $H_r(w, z) \in \mathbb{F}_p[w, z]$, depending on p but not on K, a, or b, such that $m_1^{(r+1)}m_2^{(r)} - m_2^{(r+1)}m_1^{(r)} = H_r(a, b)$ and $H_r(w, z)$ has the form $\sum h_{ij}w^i z^j$, where the sum is over all $i, j \geq 0$ such that $2i + 3j = 2r - 4$.

If the theorem holds when $K = \mathbb{F}_r$, then $H_r(\alpha, \beta) = 0$ for all $\alpha, \beta \in \mathbb{F}_r$. Let $\beta \in \mathbb{F}_r$. Then $H_r(w, \beta) = \sum h_{ij}\beta^j w^i \in \mathbb{F}_r[w]$ is a polynomial of degree at most $(2r - 4)/2 = r - 2$, yet it has at least r roots. Thus, $H(w, \beta)$ is identically zero. This shows that $\sum_j h_{ij}\beta^j$ is zero for each i and for each $\beta \in \mathbb{F}_r$. Thus, $\sum_j h_{ij}z^j$ has at least r roots, for each i. But its degree is at most $(2r - 4)/3$, and so it must also be identically 0. It follows that all h_{ij} are zero, and so $H_r(w, z)$ is identically zero. But then $H_r(a, b)$ is zero for a, b belonging to any field of characteristic p, and so the theorem holds for all such fields. ∎

To finish the proof of Theorem 3.1, it remains to prove it when $K = \mathbb{F}_r$. We do a case-by-case analysis, depending on how f factors and using the following lemma.

LEMMA 3.3. *Let* $f(x) = x^4 + ax^2 + bx - a^2/12 \in \mathbb{F}_r[x]$. *Then* $f(x)$ *factors over* $\mathbb{F}_r$ *in one of the following ways*:

(i) $f(x) = (x-u)^3(x+3u)$ *with* $u \in \mathbb{F}_r$. (*This happens if and only if* $8a^3 = -27b^2$, *in which case* $u = -3b/(4a)$.)
(ii) $f(x)$ *is the product of four distinct linear factors.*
(iii) $f(x)$ *is the product of two distinct irreducible quadratics.*
(iv) $f(x)$ *is the product of a linear factor and an irreducible cubic.*

Proof. The discriminant of f is $-3(8a^3/9 + 3b^2)^2$. Note that -3 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$. Thus, -3 is always a square in $\mathbb{F}_r$. It follows that the discriminant of f is a square in $\mathbb{F}_r$.

Now f has a repeated root if and only if the discriminant is zero, which happens if and only if $8a^3 = -27b^2$. In that case, the reader can verify that (i) holds.

If the discriminant of f is a nonzero square, then by Stickelberger's theorem (see, for example, [Be, p. 164]), the degree of f minus the number of factors of f must be even. That is, f has an even number of factors, and so one of the factorizations (ii), (iii), or (iv) holds. ∎

Now we prove Theorem 3.1 with $K = \mathbb{F}_r$ in each case of Lemma 3.3.

Proof of Theorem 3.1. CASE (i): We have $f(x+u) = x^3(x+4u) = x^4 + 4ux^3$. Then $x^{r+1} + 4ux^r \equiv 0 \pmod{f(x+u)}$. It follows that $(x-u)^{r+1} + 4u(x-u)^r \equiv 0 \pmod{f(x)}$. Since $(x-u)^{r+1} = (x^r - u)(x-u) = x^{r+1} - ux^r - ux + u^2$, this gives the relation

$$x^{r+1} + 3ux^r - ux - 3u^2 \equiv 0 \pmod{f(x)}.$$

CASE (ii): $f(x) = \prod(x - u_i)$ with $u_i \in \mathbb{F}_r$. Since $x^r - x$ vanishes at each u_i, and the u_i are distinct, we see that $f(x)$ divides $x^r - x$.

CASE (iii): $f(x) = (x-\zeta)(x-\zeta^r)(x-\lambda)(x-\lambda^r)$, where ζ, λ belong to $\mathbb{F}_r^2 \setminus \mathbb{F}_r$. Let

$$M = \begin{pmatrix} \zeta \cdot \zeta^r & \lambda \cdot \lambda^r \\ \zeta + \zeta^r & \lambda + \lambda^r \end{pmatrix} \in M_2(\mathbb{F}_r).$$

If M is singular, then there is a row vector $(A\ B) \in \mathbb{F}_r^2$ such that $(A\ B)M = (0\ 0)$. In that case, ζ and λ both satisfy $Ax^{r+1} + Bx^r + Bx = 0$. The conjugates ζ^r, λ^r would also satisfy this equality. Thus, each linear factor of f divides $Ax^{r+1} + Bx^r + Bx$, and so f itself divides that polynomial.

If M is nonsingular, then there exists a vector $(A\ B) \in \mathbb{F}_r^2$ such that $(A\ B)M = (1\ 1)$. In that case, f divides $Ax^{r+1} + Bx^r + Bx - 1$ by the same reasoning as above.

Case (iv): Let ζ be a root of the cubic factor, and denote the other two roots by $\zeta' = \zeta^r$ and $\zeta'' = \zeta^{r^2}$. Let τ_1, τ_2, τ_3 denote the elementary symmetric functions of ζ, ζ', ζ''. Let u denote the rational root of f. Then

$$x^4 + ax^2 + bx - a^2/12 = (x-u)(x^3 - \tau_1 x^2 + \tau_2 x - \tau_3),$$

which gives the identities $u = -\tau_1$, $a = \tau_2 - \tau_1^2$, $b = \tau_1\tau_2 - \tau_3$, $\tau_1\tau_3 = a^2/12$. Consequently,

$$12\tau_1\tau_3 = (\tau_2 - \tau_1^2)^2.$$

Let $\mu = \zeta - u$, $\mu' = \mu^r = \zeta' - u$, and $\mu'' = \mu^{r^2} = \zeta'' - u$. Let $\sigma_1, \sigma_2, \sigma_3$ denote the elementary symmetric functions in μ, μ', μ''. Then

$$f(x+u) = x(x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3).$$

We compute:

$$\begin{aligned}
\sigma_1 &= \mu + \mu' + \mu'' = \tau_1 - 3u = 4\tau_1, \\
\sigma_2 &= (\zeta - u)(\zeta' + \zeta'' - 2u) + (\zeta' - u)(\zeta'' - u) \\
&= \tau_2 - 2u\tau_1 + 3u^2 = \tau_2 + 5\tau_1^2, \\
\sigma_3 &= (\zeta - u)(\zeta' - u)(\zeta'' - u) = \tau_3 - u\tau_2 + u^2\tau_1 - u^3 = \tau_3 + \tau_1\tau_2 + 2\tau_1^3.
\end{aligned}$$

We claim that

$$3\sigma_1\sigma_3 = \sigma_2^2.$$

Indeed, $3\sigma_1\sigma_3 = 12\tau_1\tau_3 + 12\tau_1^2\tau_2 + 24\tau_1^4 = (\tau_2 - \tau_1^2)^2 + 12\tau_1^2\tau_2 + 24\tau_1^4 = (\tau_2 + 5\tau_1^2)^2 = \sigma_2^2$. Since $\mathbb{F}_{r^3}$ is a 3-dimensional $\mathbb{F}_r$-vector space with basis $1, \mu, \mu'$, we know there are A, B, C in $\mathbb{F}_r$ such that

$$\mu\mu' = A\mu' + B\mu + C. \tag{1}$$

Taking the trace to $\mathbb{F}_r$, we find

$$\sigma_2 = (A+B)\sigma_1 + 3C. \tag{2}$$

On multiplying equation (1) through by μ'' and then taking the trace, we find

$$3\sigma_3 = (A+B)\sigma_2 + C\sigma_1. \tag{3}$$

Now subtract σ_1 times equation (3) from σ_2 times equation (2). Since $\sigma_2^2 = 3\sigma_1\sigma_3$, the left sides cancel, and we obtain

$$C(3\sigma_2 - \sigma_1^2) = 0.$$

Thus, either $C = 0$ or $3\sigma_2 = \sigma_1^2$.

First assume $C = 0$. Then we have a relation $\mu\mu' = A\mu' + B\mu$, so that $\mu^{r+1} - A\mu^r - B\mu = 0$. Then $(\zeta - u)^{r+1} - A(\zeta - u)^r - B(\zeta - u) = 0$. It follows that ζ satisfies the equation $x^{r+1} - (u+A)x^r - (u+B)x + u^2 + Au + Bu = 0$. Then ζ', ζ'' also satisfy this equation. Furthermore, u satisfies this equation. Since all roots of f satisfy this equation, we conclude that f divides the relevant polynomial, and so the theorem holds for f.

Next assume $C \neq 0$, so $3\sigma_2 = \sigma_1^2$. We also know $3\sigma_1\sigma_3 = \sigma_2^2$. If $\sigma_1 = 0$ then $\sigma_2 = 0$ also, so $a = 0$, and $f(x) = x^4 + bx$. In that case, $x^5 \equiv bx^2 \pmod f$, $x^6 \equiv bx^3 \pmod f$, $x^7 \equiv b^2x \pmod f$, and so on. Note that $r \equiv 1 \pmod 3$, and thus $x^r \equiv cx \pmod f$ for some constant c. Thus, f divides $x^r - cx$, showing the theorem holds in this case. If $\sigma_1 \neq 0$, then $\sigma_2 = \sigma_1^2/3$, $\sigma_3 = \sigma_2^2/(3\sigma_1) = \sigma_1^3/27$. It follows that $\sigma_1/3$ is a root of $x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3$, contradicting that this polynomial is an irreducible cubic.

We have completed the proof that the theorem holds when $K = \mathbb{F}_r$, and by Lemma 3.2 this implies the general form of the theorem. ∎

THEOREM 3.4. *Let p be a prime with $p > 2$ and let q be a power of p. Let $\alpha \in \mathbb{F}(q)$ be an algebraic element of degree four. Then there exists $u \in \mathbb{F}_q(T)$ such that $\beta = \alpha + u$ satisfies the algebraic equation*

$$(**) \qquad \beta^4 + a\beta^2 + b\beta + c = 0$$

with $a, b, c \in \mathbb{F}_q(T)$. We have:

(1) *If $a = b = 0$ then α is hyperquadratic of order one.*
(2) *If $a^2 + 12c = 0$ then α is hyperquadratic of order one for $p = 3$ or $p \equiv 1 \pmod 3$ and of order at most two for $p \equiv 2 \pmod 3$.*

Proof. As in Proposition 2.3, it is clear that there is $\beta \in \mathbb{F}(q)$ as stated in the theorem satisfying $(**)$. Since $\beta = \alpha + u$ we know that α is hyperquadratic if and only if β is so and with the same order. In case (1) the result is clear for $p = 3$. Now if $p = 4k + 1$ we have $\beta^p - (-c)^k\beta = 0$ and if $p = 4k + 3$ we have $\beta^{p+1} - (-c)^{k+1} = 0$ so the result follows. In case (2) the result is also clear for $p = 3$ since the condition reduces to $a = 0$ and $(**)$ becomes $\beta^4 + b\beta + c = 0$. If $p > 3$ then the result follows immediately from Theorem 3.1 with $K = \mathbb{F}_q(T)$. ∎

In the above theorem, case (1) is trivial: β is then a fourth root of a rational function. Such power series nth roots of rational functions were first considered in diophantine approximation by Osgood (see [O, p. 109]). In case (2) a natural question arises: if $p \equiv 2 \pmod 3$, what is the exact order of β? With the notations of Lemma 3.2, we have seen that $H_{p^2}(a, b)$ is identically zero. This implies that β is hyperquadratic of order less than two, but this order is one if and only if $H_p(a, b) = 0$. For instance, if $p = 5$, a simple computation gives $H_5(a, b) = a^3 - b^2$. But then $D(f)$, the discriminant of f given in Lemma 3.3, is $3(a^3 - b^2)^2$. Since β is algebraic of degree four we have $D(f) \neq 0$ and therefore $H_5(a, b) \neq 0$, which implies that β has order two. In the same way we have computed the polynomials $H_p(a, b)$ for $p = 5, 11, 17, 23$ and in each case we have checked that $H_p^2 = -3(D(f))^{(p-2)/3}$. So we know with the same argument as above that in these cases β has order two. It is then natural to conjecture that if β satisfies $(**)$ with $a^2 + 12c = 0$ and $p > 3$

then β is hyperquadratic and its order is the residue of p modulo 3. A last and important question remains open: may β be hyperquadratic without conditions (1) or (2)?

References

[A] S. Abhyankar, *Projective polynomials*, Proc. Amer. Math. Soc. 125 (1997), 1643–1650.

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

[Be] E. Berlekamp, *Algebraic Coding Theory*, Mc Graw-Hill, 1968.

[B] A. Bluher, *On* $x^{q+1} + ax + b$, Finite Fields Appl. 10 (2004), 285–305.

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

[C] L. Carlitz, *Resolvents of certain linear groups in a finite field*, Canad. J. Math. 8 (1956), 568–579.

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

[M] K. Mahler, *On a theorem of Liouville in fields of positive characteristic*, Canad. J. Math. 1 (1949), 397–400.

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

[O] C. Osgood, *Effective bounds on the diophantine approximation of algebraic functions over fields of arbitrary characteristic and applications to differential equations*, Indag. Math. 37 (1975), 105–119.

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

[T] D. Thakur, *Function Field Arithmetic*, World Scientific, 2004.

[V] J.-F. Voloch, *Diophantine approximation in positive characteristic*, Period. Math. Hungar. 19 (1988), 217–225.

National Security Agency
Fort George G. Meade
MD 20755-6515, U.S.A.
E-mail: bluher@afterlife.ncsc.mil

Laboratoire A2X – Université Bordeaux I
351 Cours de la Libération
33405 Talence, France
E-mail: lasjauni@math.u-bordeaux1.fr

Received on 7.4.2005
and in revised form on 28.6.2006 (4975)