ACTA ARITHMETICA
LX.4 (1992)

Approximation exponents for algebraic functions in positive characteristic

by

Bernard de Mathan (Talence)

In this paper, we study rational approximations for algebraic functions in characteristic $p > 0$. We obtain results for elements satisfying an equation of the type $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$, where q is a power of p.

1. Introduction and notations. Let K be a field, and let $K((T^{-1}))$ be the field of formal Laurent series in $1/T$. For $f \in K((T^{-1}))$, $\deg(f)$ is the integer defined by $f = \sum_{n=-\infty}^{\deg(f)} a_n T^n$, with $a_{\deg(f)} \neq 0$. We define an absolute value on $K((T^{-1}))$ by $|f| = |T|^{\deg(f)}$, where $|T| > 1$. For each $f \in K((T^{-1}))$, there exists a polynomial $E(f)$ in $K[T]$ (*integral part* of f) such that $|f - E(f)| < 1$. We denote $|f - E(f)|$ by $\|f\|$.

Let $\alpha \in K((T^{-1}))$. For any real number μ, define

$$B(\alpha, \mu) = \liminf_{|Q|\to\infty} |Q|^{\mu} \|Q\alpha\| .$$

We define the *approximation exponent* of α by

$$\nu(\alpha) = \sup\{\mu \mid B(\alpha, \mu) < \infty\} .$$

Clearly $B(\alpha, 1) \leq 1/|T|$, hence $\nu(\alpha) \geq 1$ for every α. Let $(Q_n)_{n\in\mathbb{N}}$ be the sequence of the denominators of the convergents in the continued fraction expansion of α. One has

$$\nu(\alpha) = \limsup \deg(Q_{n+1})/\deg(Q_n) .$$

It is easy to see that $\nu(\alpha)$ may be any real number $\nu \geq 1$ or $\nu = +\infty$.

It is well known that if K has characteristic 0, Roth's Theorem remains valid ([7]), i.e. $\nu(\alpha) = 1$ for every algebraic irrational element α of $K((T^{-1}))$. On the other hand, if K has a positive characteristic, p, Roth's Theorem fails. The Liouville Theorem holds, i.e. $\nu(\alpha) \leq n - 1$ if α is algebraic, of degree $n > 1$, over $K(T)$. But this result is the best possible, as many examples show. For instance, let q be a power of p, and $q > 2$. Let $\alpha = T^{-1} + \ldots + T^{-q^k} + \ldots$; this element satisfies the equation $\alpha^q - \alpha + T^{-1} =$

0, and $\nu(\alpha) = q-1$ (Mahler's example). Osgood's example is α such that $\alpha^{q-1} = 1 + T^{-1}$, for which $\nu(\alpha) = q-2$ ($q > 3$). One can also cite $\alpha = 1/T + 1/T^q + \ldots + 1/T^{q^k} + \ldots$; this element α satisfies $\alpha^{q+1} + T\alpha - 1 = 0$, and $\nu(\alpha) = q$ (for $q \geq 2$).

Nevertheless, there exist in $K((T^{-1}))$ algebraic elements α of degrees > 2 for which $\nu(\alpha) = 1$. The first example was obtained by Baum and Sweet ([1]): in $\mathbb{F}_2((T^{-1})), \alpha$ such that $\alpha^3 + T^{-1}\alpha + 1 = 0$ is a cubic element for which $\nu(\alpha) = 1$ (and $B(\alpha, 1) = |T|^{-2}$). Other examples were given by W. H. Mills and D. P. Robbins ([4]), for other characteristics. Examples of algebraic elements α such that $1 < \nu(\alpha) < d(\alpha) - 1$, where $d(\alpha)$ is the degree of α over $K(T)$, were also found by Y. Taussat ([6]): for $\alpha \in \mathbb{F}_3((T^{-1}))$ such that $\alpha^4 + T^{-1}\alpha - 1 = 0$, one has $\nu(\alpha) = 23/19$ (and $B(\alpha, \nu(\alpha)) = |T|^{-21/19}$, $d(\alpha) = 4$). See also [8].

We always suppose K to be of positive characteristic p, and we prove the following result:

THEOREM. *Let α be an irrational element of $K((T^{-1}))$. Suppose that there exist a power $q = p^s$ of p (s integer, $s > 0$), and polynomials A, B, C, D in $K[T]$, with $AD - BC \neq 0$, such that $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$. Then $\nu(\alpha)$ is a rational number, and $B(\alpha, \nu(\alpha)) \neq 0, \neq \infty$.*

Of course, this result is also true when $q = 1$ and $C \neq 0$, for then α is quadratic. Hence we suppose $q > 1$.

It was already proved by J. F. Voloch ([8]) that for such an algebraic element α, one has $B(\alpha, \nu(\alpha)) \neq 0$, but this result is also a direct consequence of the proof of the above theorem.

Let us remark that every algebraic element α in $K((T^{-1}))$ of degree 3 over $K(T)$ satisfies an equation as in the Theorem. One can take $q = p$, since the elements 1, α, α^p, α^{p+1} are linearly dependent over $K(T)$.

All the examples of algebraic irrational elements in $K((T^{-1}))$ for which the value of $\nu(\alpha)$ is known satisfy an equation as in the Theorem. Nevertheless, there exist algebraic irrational elements which do not satisfy any equation of this type. For instance, let $f(X)$ be the following polynomial over $K(T)$:

$$f(X) = X^{p^2} + T^2X^p - T^2X + T\,.$$

This polynomial is irreducible over $K(T)$, since it is a T-Eisenstein polynomial. It has p roots in $K((T^{-1}))$ since the polynomial $T^{-2}f(X)$ becomes $X^p - X$ in the residue class field K. A root α of $f(X)$ in $K((T^{-1}))$ may not satisfy an equation of the type $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$. Indeed, there exist polynomials A_s, B_s, C_s in $K[T]$, for each $s \geq 0$, with

$$\alpha^{p^s} = A_s\alpha^p + B_s\alpha + C_s$$

and, by induction, it is easily seen that for $s \geq 2$,

$$\deg(A_s) = \deg(B_s) = 2(p^{s-1} - 1)/(p - 1)\,.$$

Hence $A_s \neq 0$ for every $s \geq 1$. But

$$\alpha^{p^s+1} = A_s\alpha^{p+1} + B_s\alpha^2 + C_s\alpha$$

and the elements $1, \alpha, \alpha^2, \ldots, \alpha^{p+1}$ are linearly independent over $K(T)$. So the elements $\alpha^{p^s+1}, \alpha^{p^s}, \alpha, 1$ are linearly independent over $K(T)$ for every $s \geq 1$.

To prove the Theorem, we will construct chains of rational approximations of α in the following way: starting from a rational approximation P_0/Q_0, we take

$$P_1/Q_1 = (AP_0^q + BQ_0^q)/(CP_0^q + DQ_0^q)\,,$$

and then we iterate the process. Let P'_n, Q'_n be relatively prime polynomials in $K[T]$ such that $P'_n/Q'_n = P_n/Q_n$. A critical point is to calculate $\deg(Q'_n)$. The next section is devoted to this.

2. Iterated sequences. Admissible equations

LEMMA 1. *Let E be a complete field of positive characteristic p, with a discrete valuation. Suppose that the residue class field K of E is a finitely generated extension of $\mathbb{F}_p$. Let A, B, C and D be elements of E such that $AD - BC \neq 0$. Let $q = p^s$ with s integer, $s > 0$. Set $E' = E \cup \{\infty\}$, and consider the map $\varphi : E' \to E'$, defined by $\varphi(z) = (Az^q + B)/(Cz^q + D)$. There exists an integer $h > 0$ (depending only upon φ) such that for every sequence $(u_n)_{n\in\mathbb{N}}$ in E' for which $u_n = \varphi(u_{n-1})$ for each $n \geq 1$, either the sequence $(u_{hn})_{n\in\mathbb{N}}$ is convergent in E', or for each $a \in E$, the sequence $(|u_n - a|)_{n\in\mathbb{N}}$ is constant, except for two values of n at most.* (The last eventuality is possible only when K is infinite.)

Proof. Let us begin with the particular case $C = 0$, i.e. φ of the type $\varphi(z) = a_1z^q + b_1$, where a_1, b_1 are elements of E, $a_1 \neq 0$. Since we may replace E by an extension of finite degree, we can suppose that there exists $z_1 \in E$ such that $\varphi(z_1) = z_1$. Define $\phi(z) = a_1z^q$. Then $\varphi(z) - z_1 = \phi(z - z_1)$ for every $z \in E'$, thus the sequence $u'_n = u_n - z_1$ satisfies $u'_n = \phi(u'_{n-1})$ for $n \geq 1$. We can furthermore suppose that there exists $z_2 \in E$ such that $z_2^{1-q} = a_1$. Then the sequence $u''_n = u'_n/z_2$ satisfies $u''_n = (u''_{n-1})^q$. Accordingly, we have $u''_n = (u''_0)^{q^n}$ for each n. Hence if $|u''_0| < 1$, we have $\lim u''_n = 0$; if $|u''_0| > 1$, we have $\lim u''_n = \infty$. Now suppose $|u''_0| = 1$. Since the residue class field K is finitely generated, the set of the elements of K algebraic over $\mathbb{F}_p$ is a finite extension $\mathbb{F}_r$ of $\mathbb{F}_p$. Let h be a positive integer such that $\mathbb{F}_r \subset \mathbb{F}_{q^h}$ (one can take for h the degree of $\mathbb{F}_r$ over $\mathbb{F}_p$). Denote by

$\overline{u''_n}$ the image of u''_n in K. If $\overline{u''_0}$ is algebraic over $\mathbb{F}_p$, we have $(\overline{u''_0})^{q^h} = \overline{u''_0}$. That means that

$$|(u''_0)^{q^h} - u''_0| < 1\,.$$

Since

$$|(u''_0)^{q^{h(n+1)}} - (u''_0)^{q^{hn}}| = |(u''_0)^{q^h} - u''_0|^{q^{hn}}\,,$$

the sequence $(u''_{hn})_{n\in\mathbb{N}}$ is convergent in E. Finally, if $\overline{u''_0}$ is transcendental over $\mathbb{F}_p$, we have $(\overline{u''_0})^k \neq (\overline{u''_0})^j$ for each pair (k,j) of distinct integers. Let $b \in E$. If $|b| \neq 1$, we have $|u''_n - b| = \max(|b|, 1)$ for every $n \in \mathbb{N}$; if $|b| = 1$, let $\bar{b}$ be the residue class of b ($\bar{b} \in K$). There exists at most one integer $n \geq 0$ such that $(\overline{u''_0})^{q^n} = \bar{b}$, so $|u''_n - b| = 1$ for every integer $n \geq 0$, except possibly for one value of n. Accordingly the sequence (u_n) satisfies the same condition, i.e. either the sequence $(u_{hn})_{n\in\mathbb{N}}$ is convergent in E' or, for each $a \in E$, $|u_n - a|$ is constant except for one value of n, at most.

In the general case $\varphi(z) = (Az^q + B)/(Cz^q + D)$, we can suppose that there exists $z_0 \in E$ such that $\varphi(z_0) = z_0$. Then there exists a function ψ of the previous form such that $1/(\varphi(z) - z_0) = \psi(1/(z - z_0))$. Hence there exists $h > 0$ (depending only upon φ) such that, if we set $v_n = 1/(u_n - z_0)$, then either $(v_{hn})_{n\in\mathbb{N}}$ is convergent in E', or $|v_n - b|$ is constant except for at most one value of n, for each $b \in E$. Thus either $(u_{hn})_{n\in\mathbb{N}}$ is convergent in E', or $|u_n - a|$ is constant except for two values of n at most, for each $a \in E$. Indeed,

$$|u_n - a| = |1/v_n + z_0 - a| = |(1 + (z_0 - a)v_n)/v_n|\,,$$

and the sequences $(|v_n|)$ and $(|v_n + 1/(z_0 - a)|)$, when $a \neq z_0$, are both constant, except for two values of n at most.

Corollary. *Let E be a field of positive characteristic p, with a discrete valuation. Suppose that the residue class field K of E is a finitely generated extension of $\mathbb{F}_p$. Let A, B, C and D be elements of E such that $AD - BC \neq 0$. Let $q = p^s$ where s is a positive integer. Denote by φ the map from $E' = E \cup \{\infty\}$ into E', defined by $\varphi(z) = (Az^q + B)/(Cz^q + D)$. For any positive integer h, define $\varphi^h = \varphi \circ \ldots \circ \varphi$ (h times). Then there exist coefficients A_h, B_h, C_h, D_h in E, with $A_hD_h - B_hC_h \neq 0$, such that*

$$\varphi^h(z) = (A_h z^{q^h} + B_h)/(C_h z^{q^h} + D_h)\,.$$

There is a positive integer h such that for every sequence $(u_n)_{n\in\mathbb{N}}$ in $E \setminus \{0\}$ such that $u_n = \varphi(u_{n-1})$ for each $n \geq 1$ the sequences $(|C_h u_{hn}^{q^h} + D_h|)_{n\in\mathbb{N}}$ and $(|A_h + B_h/u_{hn}^{q^h}|)_{n\in\mathbb{N}}$ have both a constant finite positive value when n is large.

Proof. The form of φ is clear. We take the matrices

$$M_h = \begin{bmatrix} A_h & B_h \\ C_h & D_h \end{bmatrix}$$

satisfying

$$M_h = M_{h-1} \begin{bmatrix} A^{q^{h-1}} & B^{q^{h-1}} \\ C^{q^{h-1}} & D^{q^{h-1}} \end{bmatrix} .$$

We have

$$A_h D_h - B_h C_h = \det M_h = (AD - BC)^{(q^h-1)/(q-1)} .$$

Since we may replace E by its completion, we can suppose that E is complete. We choose h just as in Lemma 1; then we can suppose that $h = 1$. If the sequence $(u_n)_{n\in\mathbb{N}}$ is convergent in E', then $|Cu_n^q + D|$ is constant for n large. Indeed, let $\beta = \lim u_n$. If $\beta = \infty$, one has $C = 0$, for $\varphi(\infty) = \infty$, and the result is trivial. If $\beta \neq \infty$, the sequence $(Cu_n^q + D)$ is convergent in E to the limit $C\beta^q + D \neq 0$, for $\varphi(\beta) = \beta$. Hence $|Cu_n^q + D| = |C\beta^q + D|$ when n is large. One sees in a similar way that $|A + B/u_n^q|$ is constant for large n. If now the sequence (u_n) is not convergent in E', then $|u_n - a|$ is constant except for two values of n at most. Clearly the same is true for $|Cu_n^q + D|$ and for $|A + B/u_n^q|$.

We can now define an admissible equation. We return to the Theorem: let α be an element of $K((T^{-1}))$ satisfying $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$ where A, B, C, D are polynomials in $K[T]$ with $AD - BC \neq 0$. Let Π be an irreducible polynomial in $K[T]$. We will use the Π-adic absolute value on $K(T)$, which is defined by $|\Pi|_\Pi = 1/|\Pi|$ and $|f|_\Pi = 1$ if f is a polynomial not divisible by Π. Consider the map φ of the set $K((T^{-1})) \cup \{\infty\}$ into itself defined by $\varphi(z) = (Az^q + B)/(Cz^q + D)$. When Π is an irreducible polynomial dividing $AD - BC$, we say that $\alpha = \varphi(\alpha)$ is a *Π-admissible equation* for α if the Corollary of Lemma 1 holds with $h = 1$ for the field $K(T)$ with the Π-adic absolute value. Clearly, in proving the Theorem, we may suppose that K is finitely generated over $\mathbb{F}_p$; then so is the residue class field of $K(T)$ for the Π-adic absolute value. Then the Corollary of Lemma 1 applies, and it is clear from the proof that there exists a positive integer h_Π such that the Corollary holds for every multiple h of h_Π. Hence the equation $\alpha = \varphi^h(\alpha)$ is Π-admissible for every multiple h of h_Π. We say that the equation $\alpha = \varphi(\alpha)$ is *admissible* if it is Π-admissible for each irreducible polynomial Π dividing $AD - BC$. Now, there does exist an admissible equation for α. Indeed, there is only a finite number of irreducible divisors of $AD-BC$, and so if h is a common multiple of the integers h_Π when Π divides $AD - BC$, the equation $\alpha = \varphi^h(\alpha)$ is admissible (since A_h, B_h, C_h, D_h are polynomials such that $A_h D_h - B_h C_h$ is a power of $AD - BC$, it follows that $A_h D_h - B_h C_h$ and $AD - BC$ have the same irreducible divisors).

Examples. For $\alpha \in K((T^{-1}))$ such that $\alpha^{q-1} = D/A$, where A, D are relatively prime polynomials such that $|A| = |D| > 1$, the equation $\alpha = A\alpha^q/D$ is trivially admissible. Baum and Sweet's equation $\alpha = T/(T\alpha^2+1)$ over $\mathbb{F}_2(T)$ is admissible. So is also Taussat's equation $\alpha = T/(T\alpha^3+1)$ over $\mathbb{F}_3(T)$. But over $\mathbb{F}_2(T)$, the equation $\alpha^3 = D/A$, where A, D are relatively prime polynomials such that $|A| = |D| > 1$, has the form $\alpha = D/(A\alpha^2)$, which is not admissible.

3. Chains of convergents

Lemma 2. *Let α be an irrational element of $K((T^{-1}))$ satisfying an equation $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$, where A, B, C, D are polynomials in $K[T]$ such that $AD - BC \neq 0$, and $q = p^s$ (where s is a positive integer). Let P, Q be polynomials in $K[T]$, $Q \neq 0$. Define*

$$R = AP^q + BQ^q, \quad S = CP^q + DQ^q .$$

Assume that

(i) $$|\alpha - P/Q| < |\alpha^q + D/C|^{1/q} \quad \text{if } C \neq 0$$

(*there is no condition if $C = 0$*). *Then $S \neq 0$ and*

$$|\alpha - R/S| = |AD - BC|\,|C\alpha^q + D|^{-2}|\alpha - P/Q|^q .$$

If furthermore we have

(ii) $$|\alpha - P/Q| < |AD - BC|^{-1/(q-1)}|C\alpha^q + D|^{2/(q-1)}$$

and

(iii) $$|\alpha - P/Q| < |AD - BC|^{-1/(q-1)}/|Q|^2$$

then the polynomials R and S satisfy conditions (i), (ii), (iii). *The rational fractions P/Q, R/S, are convergents of α (in the continued fraction expansion). If P', Q', R', S' are polynomials in $K[T]$ such that $(P', Q') = (R', S') = 1$ and $P/Q = P'/Q'$, $R/S = R'/S'$, then $|S'| > |Q'|$.*

Proof. First notice that $|C(P/Q)^q + D| = |C\alpha^q + D|$ by (i). Hence $|S| = |C\alpha^q + D||Q|^q > 0$. Now we write

$$\alpha - R/S = (A\alpha^q + B)/(C\alpha^q + D) - (AP^q + BQ^q)/(CP^q + DQ^q)$$

hence

$$|\alpha - R/S| = |AD - BC||C\alpha^q + D|^{-2}|\alpha - P/Q|^q .$$

Define ε and η by

$$|\alpha - P/Q| = \varepsilon/|Q|^2 , \quad |\alpha - R/S| = \eta/|S|^2 .$$

We have $\eta = |AD - BC|\varepsilon^q$, hence $\eta < \varepsilon$ by (iii). By (ii) we have $|\alpha - R/S| < |\alpha - P/Q|$. Thus conditions (i), (ii), (iii) are satisfied by the couple (R, S).

Since $\eta < \varepsilon < 1$, P/Q and R/S are convergents of α, and $|S'| > |Q'|$ as $|\alpha - R/S| < |\alpha - P/Q|$.

The conditions of Lemma 2 are hereditary, so we can iterate the process. But even if P and Q are relatively prime, R and S are not necessarily so. In order to calculate the degree of their gcd, we have to use an admissible equation for α.

LEMMA 3. *With the notations of Lemma* 2, *assume moreover that the equation* $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$ *is admissible. Let* P *and* Q *be relatively prime polynomials in* $K[T]$, $Q \neq 0$. *Assume that the couple* (P, Q) *satisfies the conditions* (i), (ii), (iii) *of Lemma* 2. *We define sequences of polynomials* $(P_n)_{n\in\mathbb{N}}$ *and* $(Q_n)_{n\in\mathbb{N}}$ *by*

$$P_0 = P, \quad Q_0 = Q,$$

and for $n \geq 1$:

$$P_n = AP_{n-1}^q + BQ_{n-1}^q, \quad Q_n = CP_{n-1}^q + DQ_{n-1}^q.$$

Then $Q_n \neq 0$ *for each* n. *Let* P_n' *and* Q_n' *be relatively prime polynomials such that* $P_n/Q_n = P_n'/Q_n'$. *There exist real constants* $C_1 > 0$, C_2, $\delta > 1$, $\lambda > 0$ *such that* $\deg(Q_n') = C_1 q^n + C_2$ *and* $|Q_n'|^\delta \|Q_n'\alpha\| = \lambda$ *for all sufficiently large* n. *One has* $0 < C_1 \leq \deg(Q) + m/(q-1)$ *where* $|C\alpha^q + D| = |T|^m$. *Moreover*, δ *is a rational number.*

Proof. It is clear that the couple (P_n, Q_n) satisfies conditions (i), (ii), (iii) in Lemma 2, for each n. Hence $Q_n \neq 0$. Set $\deg(\alpha - P_n/Q_n) = -r_n$ and $\deg(AD - BC) = c$. By Lemma 2, we have $r_n = qr_{n-1} + 2m - c$ for every $n \geq 1$, thus

$$r_n = (r_0 + (2m - c)/(q-1))q^n - (2m - c)/(q-1) \quad \text{for all } n.$$

We are now going to calculate $\deg(Q_n')$. First we calculate $\deg(Q_n)$. Since

$$|Q_n| = |C\alpha^q + D||Q_{n-1}|^q,$$

we have

$$\deg(Q_n) = q\deg(Q_{n-1}) + m;$$

hence

$$\deg(Q_n) = (\deg(Q) + m/(q-1))q^n - m/(q-1).$$

We are going to prove that we also have $\deg(Q_n') = C_1 q^n + C_2$ for all large n. It suffices to prove an analogous form for the degree of the (monic) gcd $D_n = (P_n, Q_n)$:

$$\deg(D_n) = C_3 q^n + C_4 \quad (C_3, C_4 \text{ real constants}).$$

As $(P_0, Q_0) = 1$, P_n and Q_n have no other common irreducible divisors than the irreducible divisors of $AD - BC$. It suffices to calculate $|D_n|_\Pi$ for each element Π of the finite set of the irreducible divisors of $AD - BC$.

Denote by w_Π the Π-adic valuation on $K(T)$ such that $|f|_\Pi = |\Pi|^{-w_\Pi(f)}$ for all $f \in K(T)$, $f \neq 0$. Now it is clear that it suffices to prove that for each irreducible divisor Π of $AD-BC$, there exist real constants F, F', G, G' (depending upon Π) such that $w_\Pi(P_n) = Fq^n + F'$ and $w_\Pi(Q_n) = Gq^n + G'$ when n is large.

We write $Q_n = (C(P_{n-1}/Q_{n-1})^q + D)Q_{n-1}^q$. As the equation $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$ is admissible, $|C(P_{n-1}/Q_{n-1})^q + D|_\Pi$ is constant when n is large. Thus there exists a real constant b such that $w_\Pi(Q_n) = qw_\Pi(Q_{n-1}) + b$ for all large n. So we have $w_\Pi(Q_n) = Gq^n + G'$ where G, G' are real constants, for all large n. We can proceed in the same way to compute $w_\Pi(P_n)$, as $P_n \neq 0$ for all large n. Indeed, in $K((T^{-1}))$ we have $\lim P_n/Q_n = \alpha$. Then we can write $P_n = (A + B(Q_{n-1}/P_{n-1})^q)P_{n-1}^q$ and apply the Corollary of Lemma 1.

Thus $\deg(Q'_n) = C_1 q^n + C_2$ when n is large. As $\lim \deg(Q'_n) = +\infty$, we have $C_1 > 0$. Moreover, $C_1 \leq \deg(Q) + m/(q-1)$, for $\deg(Q'_n) \leq \deg(Q_n)$. Now, let $\delta = (r_0 + (2m-c)/(q-1))/C_1 - 1$. Then $(\delta+1)\deg(Q'_n) - r_n$ is constant when n is large. Hence $|Q'_n|^\delta \|Q'_n\alpha\|$ is a positive constant when n is large. We have $\delta > 1$, for $C_1 \leq \deg(Q) + m/(q-1) < (r_0 + (2m-c)/(q-1))/2$ by (iii). Clearly C_1 is a rational number, accordingly so is δ.

Now we fix an admissible equation $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$ for α, and we call a sequence $(P'_n/Q'_n)_{n\in\mathbb{N}}$ of rational approximations of α as in Lemma 3 a *chain* of convergents of α. That means that the couple (P'_0, Q'_0) satisfies the conditions (i), (ii), (iii) of Lemma 2, and that

$$P'_n/Q'_n = (AP'^q_{n-1} + BQ'^q_{n-1})/(CP'^q_{n-1} + DQ'^q_{n-1}) \quad \text{for each } n \geq 1\,.$$

For such a chain $\mathcal{C} = (P'_n/Q'_n)_{n\in\mathbb{N}}$, with relatively prime polynomials P'_n and Q'_n for each n, it follows from Lemma 3 that there exists a rational constant $\delta > 1$ such that $|Q'_n|^\delta \|Q'_n\alpha\|$ is constant when n is large. Then we say that $\mathcal{C}$ is a *δ-chain*. As the sequence $(\deg(Q'_n))$ is strictly increasing, every chain is included in a *maximal* chain, that is to say, a chain $(P''_n/Q''_n)_{n\in\mathbb{N}}$ for which there exists no rational fraction P''_{-1}/Q''_{-1} such that $(P''_n/Q''_n)_{n\geq -1}$ is a chain. Since the map $z \mapsto (Az^q + B)/(Cz^q + D)$ is injective, any two chains are either disjoint, or one is included in the other. Every chain including a δ-chain is also a δ-chain. For any chain $\mathcal{C}$ we denote by $\delta(\mathcal{C})$ the constant δ such that $\mathcal{C}$ is a δ-chain.

LEMMA 4. *Let δ_0 be a real number, $\delta_0 > 1$. There exist only a finite number of maximal chains $\mathcal{C}$ of convergents of α with $\delta(\mathcal{C}) \geq \delta_0$.*

Proof. Distinct maximal chains are disjoint. We will prove that if we have N disjoint chains $\mathcal{C}_k$ $(1 \leq k \leq N)$, with $\delta(\mathcal{C}_k) \geq \delta_0$, then $\delta_0^{N-1} < q$. Define $\mathcal{C}_k = (P_{n,k}/Q_{n,k})_{n\in\mathbb{N}}$ where $P_{n,k}$ and $Q_{n,k}$ are relatively prime polynomials. For each k there exist real constants $C_k > 0$ and C'_k such that $\deg(Q_{n,k}) = C_k q^n + C'_k$ for all sufficiently large n. We can modify the indexation by replacing n by $n + n_k$ for each k, where n_k is an integer in $\mathbb{Z}$, so that we get $1 \le C_k < q$. Notice that for $k \ne j$, the couples (C_k, C'_k) and (C_j, C'_j) are distinct. Indeed, $\deg(Q_{n,k}) \ne \deg(Q_{n,j})$ for each n, since $\mathcal{C}_k$ and $\mathcal{C}_j$ are disjoint. Thus, we can suppose that for each integer k such that $1 \le k < N$, we have $C_k < C_{k+1}$ or $C_k = C_{k+1}$ and $C'_k < C'_{k+1}$. If Q is the denominator of a convergent of α, let Q^* be the denominator of the next convergent. One has $\|Q\alpha\| = 1/|Q^*|$ ([3]). Accordingly, as $\mathcal{C}_k$ is a chain with $\delta(\mathcal{C}_k) \ge \delta_0$, there exists a constant σ such that

$$\deg(Q^*_{n,k}) \ge \delta_0 \deg(Q_{n,k}) - \sigma\,.$$

Since, for any integer k such that $1 \le k < N$, we have $\deg(Q_{n,k+1}) > \deg(Q_{n,k})$ when n is large, thus we have

$$\deg(Q_{n,k+1}) \ge \delta_0 \deg(Q_{n,k}) - \sigma \quad \text{for all large } n\,.$$

Therefore

$$\lim_{n\to\infty} \deg(Q_{n,k+1})/\deg(Q_{n,k}) = C_{k+1}/C_k \ge \delta_0\,.$$

Hence we conclude that $\delta_0^{N-1} < q$. One can notice, with a similar proof, that we even have $\delta_0^N \le q$.

4. Proof of the Theorem. The result is obvious if $B(\alpha, 1) \ne 0$ (thus $\nu(\alpha) = 1$). If $B(\alpha, 1) = 0$, it follows from Lemma 3 that there exist chains of convergents of α (we have fixed an admissible equation for α). By Lemma 4, the numbers $\delta(\mathcal{C})$, where $\mathcal{C}$ runs over the set of chains of α, achieve a *maximum* δ. For every δ-chain $\mathcal{C}$, denote by $\lambda(\mathcal{C})$ the (constant) value of $|Q|^\delta \|Q\alpha\|$ when $P/Q \in \mathcal{C}$, with polynomials P, Q relatively prime, and $\deg(Q)$ large. Since there exist only a finite number of maximal δ-chains (when δ is *maximal*) we can define Λ as being the *minimum* of $\lambda(\mathcal{C})$ for all the δ-chains $\mathcal{C}$. Clearly Λ is finite, but not zero. We are going to prove that $B(\alpha, \delta) = \Lambda$. That will show that $\nu(\alpha) = \delta$, and the Theorem will be proved.

Let (P_n/Q_n) be a sequence of convergents of α, with relatively prime polynomials P_n, Q_n. We suppose that $\lim |Q_n| = +\infty$, and that the sequence $(|Q_n|^\delta \|Q_n\alpha\|)$ is bounded. We must prove that for all large n, P_n/Q_n belongs to the union of the δ-chains. But by Lemma 3, P_n/Q_n is the first term of a chain for all large n. This chain is a ν_n-chain, with $\nu_n = (\varrho_n + (2m - c)/(q-1))/C_n - 1$, where $\varrho_n = -\deg(\alpha - P_n/Q_n)$ and $0 < C_n \le \deg(Q_n) + m/(q-1)$ (see Lemma 3). Since the sequence $(|Q_n|^\delta \|Q_n\alpha\|)$ is bounded, there exists a real constant τ such that $(\delta+1)\deg(Q_n) - \varrho_n \le -\tau$, and thus

$$\nu_n \ge (\delta \deg(Q_n) + \tau + (m - c)/(q-1))/(\deg(Q_n) + m/(q-1))\,.$$

Hence $\lim \nu_n = \delta$. Then we conclude by Lemma 4 that $\nu_n = \delta$ for all large n, so P_n/Q_n belongs to the union of the δ-chains. Hence it is clear that $B(\alpha, \delta) = \Lambda$.

5. Examples. We can now treat examples. We consider the case of an equation $X^e = R$, where e is a positive integer, not divisible by p, and $R \in K(T)$. Such an equation has a root in $K((T^{-1}))$ if (and only if) $\deg(R)$ is a multiple of e and the first coefficient of R belongs to K^e. There exists a positive integer s such that e divides $p^s - 1$ (we can take for s the order of p in the multiplicative group $(\mathbb{Z}/e\mathbb{Z})^*$). Therefore if an element $\alpha \in K((T^{-1}))$ is a root of an equation $\alpha^e = R$, with $R \in K(T)$, it also satisfies an equation $\alpha^{q-1} = R'$, with $q = p^s$ and $R' \in K(T)$. We can write this equation as $\alpha = A\alpha^q/D$ where A, D are polynomials such that $R' = D/A$. Accordingly, if $\alpha \notin K(T)$, our result applies. Notice that the equation $\alpha = A\alpha^q/D$ is trivially admissible.

We give explicit calculations in the case $p = 2$, $e = 3$. We prove:

Corollary. *Let $\alpha, \alpha', \alpha''$ be elements of $\mathbb{F}_2((T^{-1}))$ such that $\alpha^3 = (T^3+T+1)/T^3$, $\alpha'^3 = (T^4+T^2+T+1)/T^4$, $\alpha''^3 = (T^4+T+1)/T^4$. One has*: $\nu(\alpha) = 3/2$, $B(\alpha, 3/2) = 1$; $\nu(\alpha') = 4/3$, $B(\alpha', 4/3) = 1$; $\nu(\alpha'') = 5/4$, $B(\alpha'', 5/4) = |T|^{-3}$.

P r o o f. The first terms of the expansion of α in continued fraction are:

$$\alpha = 1 + 1 \big/ T^2 + T + 1 \big/ T + 1 + 1 \big/ \ldots$$

The first convergents are $P_0/Q_0 = 1$, $P_1/Q_1 = (T^2+T+1)/(T^2+T)$, and $|\alpha - P_1/Q_1| = |T|^{-5}$.

We start from the convergentP_1/Q_1, and we construct by Lemma 2 the sequence of convergents $(P_{n,1}/Q_{n,1})_{n\in\mathbb{N}}$:

$$P_{n,1}/Q_{n,1} = (T^2+T+1)^{4^n}/((T+1)^{4^n}T(T^3+T+1)^{(4^n-1)/3}),$$

which is the sequence of rational (irreducible) fractions obtained from the relations $P_{0,1}/Q_{0,1} = P_1/Q_1$ and, for $n \ge 1$,

$$P_{n,1}/Q_{n,1} = (T^3/(T^3+T+1))(P_{n-1,1}/Q_{n-1,1})^4 .$$

Since $|\alpha - P_1/Q_1| = |T|^{-5}$, we have for each n, $|\alpha - P_{n,1}/Q_{n,1}| = |T|^{-5\cdot 4^n}$. We have $\deg(Q_{n,1}) = 2 \cdot 4^n$, hence $\deg(Q^*_{n,1}) = 3 \cdot 4^n$. The sequence $(P_{n,1}/Q_{n,1})$ is a 3/2-chain (for $n \ge 1$).

Now we notice that if we write the equation for α in the (non-admissible) form $\alpha = D/A\alpha^2$ (with $D = T^3+T+1$ and $A = T^3$), we see by Lemma 2(i) that we can deduce from an approximation P/Q of α, with $|\alpha - P/Q| < 1$, the approximation DQ^2/AP^2. We have $|\alpha - DQ^2/AP^2| = |\alpha - P/Q|^2$. Hence for $n \ge 1$, we obtain from $P_{n,1}/Q_{n,1}$ the convergent

$$P_{n,2}/Q_{n,2} = (T+1)^{2\cdot 4^n}(T^3+T+1)^{(2\cdot 4^n+1)/3}/T(T^2+T+1)^{2\cdot 4^n} .$$

We have $|\alpha - P_{n,2}/Q_{n,2}| = |T|^{-10\cdot 4^n}$ and $\deg(Q_{n,2}) = 4^{n+1}+1$ (of course $P_{n,2}$ and $Q_{n,2}$ are relatively prime). Accordingly $\deg(Q^*_{n,2}) = 6\cdot 4^n - 1$. The sequence $(P_{n,2}/Q_{n,2})_{n\ge 1}$ is another 3/2-chain. There is no other maximal δ-chain, with $\delta \ge 3/2$, than $(P_{n,1}/Q_{n,1})$ and $(P_{n,2}/Q_{n,2})$, with $n \ge 1$. Indeed, for each denominator of a convergent Q of α such that $2\cdot 4^n \le \deg(Q) < 2\cdot 4^{n+1}$, with $n \ge 1$, if $Q \ne Q_{n,1}$ and $Q \ne Q_{n,2}$, then $\deg(Q)$ and $\deg(Q^*)$ both belong to one of the intervals $[3\cdot 4^n, 4^{n+1}+1]$ or $[6\cdot 4^n - 1, 2\cdot 4^{n+1}]$, hence it is clear that any other maximal chain is a δ-chain with $\delta \le 4/3$. Therefore we have $\nu(\alpha) = 3/2$. Since $|Q_{n,1}|^{3/2}\|Q_{n,1}\alpha\| = 1$ and $|Q_{n,2}|^{3/2}\|Q_{n,2}\alpha\| = |T|^{5/2}$ for each $n \ge 1$, we have $B(\alpha, 3/2) = 1$. It is easy to see that the inequality $|Q|^{3/2}\|Q\alpha\| \ge 1$ holds for any polynomial Q of degree > 3.

For α' and α'', we only indicate sufficient chains of convergents; we give the degrees of the denominators of these convergents and of the next convergent.

For α':

$$\begin{gathered}(3\cdot 4^n,\, 4^{n+1}),\quad (6\cdot 4^n, 8\cdot 4^n) \quad (n \ge 0)\,,\\ ((4/3)(4^{n+2}-1),\, (4/3)(17\cdot 4^n + 1)) \quad (n \ge 0)\,,\\ ((4/3)(2\cdot 4^{n+2}+1),\, (4/3)(34\cdot 4^n - 1)) \quad (n \ge 1)\,.\end{gathered}$$

For α'':

$$\begin{gathered}((4/3)(4^n-1),\, (5\cdot 4^n+4)/3) \quad (n \ge 0)\,,\\ ((4/3)(8\cdot 4^n+1),\, (4/3)(10\cdot 4^n - 1)) \quad (n \ge 1)\,,\\ (2\cdot 4^{n+1},\, 9\cdot 4^n),\quad (4^{n+2}, 18\cdot 4^n) \quad (n \ge 0)\,.\end{gathered}$$

6. Open problems. We know nothing (except the Liouville theorem) about the approximation exponent of algebraic elements α which do not satisfy any non-trivial equation of the form $\alpha = (A\alpha^q + B)/(C\alpha^q + D)$, where q is a power of the characteristic $p \ne 0$ of K. One can ask if Roth's theorem $\nu(\alpha) = 1$ holds for these elements. For instance, it is possible to calculate, by computer — I thank Y. Taussat — many terms of the expansion in continued fraction of both the roots in $\mathbb{F}_2((T^{-1}))$ of the equation $X^4 + T^2X^2 + T^2X + T = 0$ (see §1). It seems that for a root α of this equation, one has $\nu(\alpha) = 1$ (but $B(\alpha, 1) = 0$).

For the algebraic elements satisfying a non-trivial equation

$$\alpha = (A\alpha^q + B)/(C\alpha^q + D)\,,$$

there are examples with $\nu(\alpha) = 1$ (see [1], [4]). But no criterion is known. For instance, we do not know whether for an irrational element α of $K((T^{-1}))$ such that there exists a positive integer e with $\alpha^e \in K(T)$, one may have $\nu(\alpha) = 1$ (when α is not quadratic).

References

[1] L. E. Baum and M. M. Sweet, *Continued fractions of algebraic power series in characteristic* 2, Ann. of Math. 103 (1976), 593–610.
[2] A. Blanchard et M. Mendès-France, *Symétrie et transcendance*, Bull. Sci. Math. 106 (3) (1982), 325–335.
[3] B. de Mathan, *Approximations diophantiennes dans un corps local*, Bull. Soc. Math. France. Mém. 21 (1970).
[4] W. H. Mills and D. P. Robbins, *Continued fractions for certain algebraic power series*, J. Number Theory 23 (1986), 388–404.
[5] C. F. 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.
[6] Y. Taussat, *Approximations diophantiennes dans un corps de séries formelles*, Thèse de 3ème cycle, Bordeaux, 1986.
[7] S. Uchiyama, *On the Thue–Siegel–Roth theorem III*, Proc. Japan Acad. 36 (1960), 1–2.
[8] J. F. Voloch, *Diophantine approximation in positive characteristic*, Period. Math. Hungar. 19 (3) (1988), 217–225.

UNIVERSITÉ DE BORDEAUX 1, MATHÉMATIQUES
(AND U.A. C.N.R.S. 226)
351 COURS DE LA LIBÉRATION
F-33405 TALENCE CEDEX, FRANCE

Received on 12.10.1990 (2091)