Algebraic continued fractions in power series fields

Alain LASJAUNIAS

Institut Mathématique de Bordeaux, Université Bordeaux 1

FQ9, DUBLIN
July 16, 2009

Formal power series over a finite field

- There is a well-known analogy:

$$\begin{array}{ccc}
\pm 1 & & \mathbb{F}_q^* \\
\cap & & \cap \\
\mathbb{Z} & \longleftrightarrow & \mathbb{F}_q[T] \\
\cap & & \cap \\
\mathbb{Q} & \longleftrightarrow & \mathbb{F}_q(T) \\
\cap & & \cap \\
\mathbb{R} & & \mathbb{F}_q((1/T))
\end{array}$$

Formal power series over a finite field

- There is a well-known analogy:

$$\begin{array}{ccc} \pm 1 & & \mathbb{F}_q^* \\ \cap & & \cap \\ \mathbb{Z} & \longleftrightarrow & \mathbb{F}_q[T] \\ \cap & & \cap \\ \mathbb{Q} & \longleftrightarrow & \mathbb{F}_q(T) \\ \cap & & \cap \\ \mathbb{R} & & \mathbb{F}_q((1/T)) \end{array}$$

- We replace the number expanded in base b

$$x = \sum_{n \leq k} a_n b^n \in \mathbb{R}$$

by the formal power series

$$\alpha = \sum_{n \leq k} a_n T^n \in \mathbb{F}_q((1/T)) = \mathbb{F}(q).$$

Formal power series over a finite field

- There is a well-known analogy:

$$\begin{array}{ccc} \pm 1 & & \mathbb{F}_q^* \\ \cap & & \cap \\ \mathbb{Z} & \longleftrightarrow & \mathbb{F}_q[T] \\ \cap & & \cap \\ \mathbb{Q} & \longleftrightarrow & \mathbb{F}_q(T) \\ \cap & & \cap \\ \mathbb{R} & & \mathbb{F}_q((1/T)) \end{array}$$

- We replace the number expanded in base b

$$x = \sum_{n \le k} a_n b^n \in \mathbb{R}$$

by the formal power series

$$\alpha = \sum_{n \le k} a_n T^n \in \mathbb{F}_q((1/T)) = \mathbb{F}(q).$$

- For instance: $T/(T-1) = 1 + T^{-1} + \cdots + T^{-n} + \ldots$ in $\mathbb{F}_p(T)$
$\alpha \in \mathbb{F}_q(T) \iff (a_n)_{n \le k}$ is eventually periodic.

Continued fractions in $\mathbb{F}(q)$

- Every $\alpha \in \mathbb{F}(q)$ can be expanded as a continued fraction :

$$\alpha = a_0 + 1/(a_1 + 1/(a_2 + 1/(\cdots = [a_0, a_1, a_2, \ldots]$$

where $a_i \in \mathbb{F}_q[T]$ and $\deg(a_i) > 0$ for $i > 0$.

Continued fractions in $\mathbb{F}(q)$

- Every $\alpha \in \mathbb{F}(q)$ can be expanded as a continued fraction :

$$\alpha = a_0 + 1/(a_1 + 1/(a_2 + 1/(\cdots = [a_0, a_1, a_2, \ldots]$$

where $a_i \in \mathbb{F}_q[T]$ and $\deg(a_i) > 0$ for $i > 0$.

- The expansion is finite $\iff \alpha \in \mathbb{F}_q(T)$.
For instance : $(T^2 - 1)^2/(2T^3 + 4T) = [3T, 2T, 3T, 2T]$ in $\mathbb{F}_5(T)$.

Continued fractions in $\mathbb{F}(q)$

- Every $\alpha \in \mathbb{F}(q)$ can be expanded as a continued fraction :

$$\alpha = a_0 + 1/(a_1 + 1/(a_2 + 1/(\cdots = [a_0, a_1, a_2, \dots]$$

where $a_i \in \mathbb{F}_q[T]$ and $\deg(a_i) > 0$ for $i > 0$.

- The expansion is finite $\iff$ $\alpha \in \mathbb{F}_q(T)$.
For instance : $(T^2 - 1)^2/(2T^3 + 4T) = [3T, 2T, 3T, 2T]$ in $\mathbb{F}_5(T)$.

- $[\mathbb{F}_q(T, \alpha) : \mathbb{F}_q(T)] = 2 \iff (a_n)_{n \geq 0}$ is eventually periodic.

Continued fractions in $\mathbb{F}(q)$

- Every $\alpha \in \mathbb{F}(q)$ can be expanded as a continued fraction :

$$\alpha = a_0 + 1/(a_1 + 1/(a_2 + 1/(\cdots = [a_0, a_1, a_2, \dots]$$

where $a_i \in \mathbb{F}_q[T]$ and $\deg(a_i) > 0$ for $i > 0$.

- The expansion is finite $\iff$ $\alpha \in \mathbb{F}_q(T)$.
For instance : $(T^2 - 1)^2/(2T^3 + 4T) = [3T, 2T, 3T, 2T]$ in $\mathbb{F}_5(T)$.

- $[\mathbb{F}_q(T,\alpha) : \mathbb{F}_q(T)] = 2 \iff (a_n)_{n\geq 0}$ is eventually periodic.

- For $\alpha \in \mathbb{F}(q) \backslash \mathbb{F}_q(T)$ we define (the approximation exponent):

$$\nu(\alpha) = 2 + \limsup_{n>0}(\deg(a_{n+1})/\sum_{0\leq i\leq n}\deg(a_i)).$$

- Let p be the characteristic of $\mathbb{F}_q$ and $r = p^t$ where $t \geq 0$ is an integer.

Hyperquadratic Formal Power Series in $\mathbb{F}(q)$

- Let p be the characteristic of $\mathbb{F}_q$ and $r = p^t$ where $t \geq 0$ is an integer.
- We write $\alpha \in \mathbb{H}_r(q)$, if $\alpha \in \mathbb{F}(q) \backslash \mathbb{F}_q(T)$ and it satisfies

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

where $(A, B, C, D) \in (\mathbb{F}_q[T])^4$.

Hyperquadratic Formal Power Series in $\mathbb{F}(q)$

- Let p be the characteristic of $\mathbb{F}_q$ and $r = p^t$ where $t \geq 0$ is an integer.
- We write $\alpha \in \mathbb{H}_r(q)$, if $\alpha \in \mathbb{F}(q) \backslash \mathbb{F}_q(T)$ and it satisfies

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

  where $(A, B, C, D) \in (\mathbb{F}_q[T])^4$.
- $\alpha \in \mathbb{H}_1(q) \iff \alpha$ is quadratic over $\mathbb{F}_q(T)$.

Hyperquadratic Formal Power Series in $\mathbb{F}(q)$

- Let p be the characteristic of $\mathbb{F}_q$ and $r = p^t$ where $t \geq 0$ is an integer.
- We write $\alpha \in \mathbb{H}_r(q)$, if $\alpha \in \mathbb{F}(q) \backslash \mathbb{F}_q(T)$ and it satisfies

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

  where $(A, B, C, D) \in (\mathbb{F}_q[T])^4$.
- $\alpha \in \mathbb{H}_1(q) \iff \alpha$ is quadratic over $\mathbb{F}_q(T)$.
- $\alpha \in \mathbb{F}(q)$ is hyperquadratic if $\alpha \in \mathbb{H}(q) = \bigcup_{t \geq 0} \mathbb{H}_r(q)$.

Hyperquadratic Formal Power Series in $\mathbb{F}(q)$

- Let p be the characteristic of $\mathbb{F}_q$ and $r = p^t$ where $t \geq 0$ is an integer.
- We write $\alpha \in \mathbb{H}_r(q)$, if $\alpha \in \mathbb{F}(q) \backslash \mathbb{F}_q(T)$ and it satisfies
  $$\alpha = (A\alpha^r + B)/(C\alpha^r + D)$$
  where $(A, B, C, D) \in (\mathbb{F}_q[T])^4$.
- $\alpha \in \mathbb{H}_1(q) \iff \alpha$ is quadratic over $\mathbb{F}_q(T)$.
- $\alpha \in \mathbb{F}(q)$ is hyperquadratic if $\alpha \in \mathbb{H}(q) = \bigcup_{t\geq 0} \mathbb{H}_r(q)$.
- $\alpha \in \mathbb{H}(q) \Rightarrow \alpha' = b_0 + b_1\alpha + b_2\alpha^2$ where $b_i \in \mathbb{F}_q(T)$.
  α is hyperquadratic $\Rightarrow \alpha$ is "differential-quadratic".

Two basic examples in $\mathbb{F}(p)$

- **Example 1.** $\alpha = [T, T^r, T^{r^2}, \ldots, T^{r^k}, \ldots]$.
  Hence $\alpha = T + 1/\alpha^r$ and $\alpha \in \mathbb{H}_r(p)$ for all p.

  We observe that here we have $\nu(\alpha) = r + 1$.

Two basic examples in $\mathbb{F}(p)$

- **Example 1.** $\alpha = [T, T^r, T^{r^2}, \ldots, T^{r^k}, \ldots]$.
  Hence $\alpha = T + 1/\alpha^r$ and $\alpha \in \mathbb{H}_r(p)$ for all p.

  We observe that here we have $\nu(\alpha) = r + 1$.

- **Example 2.** K. Mahler (1949) $\alpha = 1/T + 1/T^r + \cdots + 1/T^{r^k} + \ldots$
  Hence $\alpha = 1/T + \alpha^r$ and $\alpha \in \mathbb{H}_r(p)$ for all p.
  We put $\beta = 1/\alpha = [a_1, a_2, \ldots, a_n, \ldots]$.
  For $r > 2$, we have $\beta = [T, \beta_2]$ and $\beta^r = -T^2\beta_2 - T$.

Two basic examples in $\mathbb{F}(p)$

- **Example 1.** $\alpha = [T, T^r, T^{r^2}, \dots, T^{r^k}, \dots]$.
  Hence $\alpha = T + 1/\alpha^r$ and $\alpha \in \mathbb{H}_r(p)$ for all p.

  We observe that here we have $\nu(\alpha) = r + 1$.

- **Example 2.** K. Mahler (1949) $\alpha = 1/T + 1/T^r + \cdots + 1/T^{r^k} + \dots$
  Hence $\alpha = 1/T + \alpha^r$ and $\alpha \in \mathbb{H}_r(p)$ for all p.
  We put $\beta = 1/\alpha = [a_1, a_2, \dots, a_n, \dots]$.
  For $r > 2$, we have $\beta = [T, \beta_2]$ and $\beta^r = -T^2\beta_2 - T$.

  The sequence $(a_i)_{i \geq 1}$ is defined recursively by $a_1 = T$ and :

  $$a_{4k+1} = T \quad a_{4k+2} = -a_{2k+1}^r/T^2 \quad a_{4k+3} = -T \quad a_{4k+4} = a_{2k+2}^r \qquad \text{for } k \geq 0.$$

  We observe that here we also have $\nu(\alpha) = r$.

General Theorems on diophantine approximation in $\mathbb{F}(q)$

- $\alpha \in \mathbb{F}(q)$ and $[\mathbb{F}_q(T,\alpha) : \mathbb{F}_q(T)] = n \quad \Rightarrow \quad \nu(\alpha) \in [2; n]$.
  Liouville (1849) - Mahler (1949).

General Theorems on diophantine approximation in $\mathbb{F}(q)$

- $\alpha \in \mathbb{F}(q)$ and $[\mathbb{F}_q(T,\alpha) : \mathbb{F}_q(T)] = n \quad \Rightarrow \quad \nu(\alpha) \in [2;n]$.
  Liouville (1849) - Mahler (1949).

- $\alpha \in \mathbb{H}(q)$ and $\nu(\alpha) = 2 \quad \Rightarrow \quad (\deg(a_i))_{i\geq 0}$ is bounded.
  Voloch (1988).

General Theorems on diophantine approximation in $\mathbb{F}(q)$

- $\alpha \in \mathbb{F}(q)$ and $[\mathbb{F}_q(T,\alpha) : \mathbb{F}_q(T)] = n \quad \Rightarrow \quad \nu(\alpha) \in [2; n]$.
  Liouville (1849) - Mahler (1949).
- $\alpha \in \mathbb{H}(q)$ and $\nu(\alpha) = 2 \quad \Rightarrow \quad (\deg(a_i))_{i \geq 0}$ is bounded.
  Voloch (1988).
- $\alpha \in \mathbb{H}(q) \quad \Rightarrow \quad \nu(\alpha) \in \mathbb{Q}$.
  de Mathan (1992).

General Theorems on diophantine approximation in $\mathbb{F}(q)$

- $\alpha \in \mathbb{F}(q)$ and $[\mathbb{F}_q(T, \alpha) : \mathbb{F}_q(T)] = n \quad \Rightarrow \quad \nu(\alpha) \in [2; n]$.
  Liouville (1849) - Mahler (1949).
- $\alpha \in \mathbb{H}(q)$ and $\nu(\alpha) = 2 \quad \Rightarrow \quad (\deg(a_i))_{i \geq 0}$ is bounded.
  Voloch (1988).
- $\alpha \in \mathbb{H}(q) \quad \Rightarrow \quad \nu(\alpha) \in \mathbb{Q}$.
  de Mathan (1992).
- $\alpha \in \mathbb{F}(q) \backslash \mathbb{H}(q)$ and $[\mathbb{F}_q(T, \alpha) : \mathbb{F}_q(T)] = n \quad \Rightarrow \quad \nu(\alpha) \leq [n/2] + 1$.
  Osgood (1975) - de Mathan-L. (1996).

Proposition (L. 2006)

Let $l \geq 1$ be an integer. Let $(a_1, a_2, \ldots, a_l) \in (\mathbb{F}_q[T])^l$ and $(R, P, Q) \in (\mathbb{F}_q[T])^3$ with $\deg(Q) < \deg(P) < r$. Then there exists a unique $\alpha \in \mathbb{H}_r(q)$ such that

$$\alpha = [a_1, a_2, \ldots, a_l, \alpha_{l+1}] \quad \text{and} \quad R\alpha^r = P\alpha_{l+1} + Q.$$

Generating continued fractions in $\mathbb{H}(q)$

Proposition (L. 2006)

Let $l \geq 1$ be an integer. Let $(a_1, a_2, \ldots, a_l) \in (\mathbb{F}_q[T])^l$ and $(R, P, Q) \in (\mathbb{F}_q[T])^3$ with $\deg(Q) < \deg(P) < r$. Then there exists a unique $\alpha \in \mathbb{H}_r(q)$ such that

$$\alpha = [a_1, a_2, \ldots, a_l, \alpha_{l+1}] \quad \text{and} \quad R\alpha^r = P\alpha_{l+1} + Q.$$

****

If $(a_1, a_2, \ldots, a_l, R, P, Q) \in (\mathbb{F}_q[T])^{l+3}$ are well chosen then the continued fraction expansion can be given explicitely.

Mills and Robbins example in $\mathbb{F}(13)$ (1986)

In $\mathbb{F}(p)$ for all p, we have

$$x^4 - Tx^3 + x^2 + 1 = 0 \quad \Rightarrow \quad x = \alpha = T + \sum_{k<0} u_k T^k.$$

Mills and Robbins example in $\mathbb{F}(13)$ (1986)

In $\mathbb{F}(p)$ for all p, we have

$$x^4 - Tx^3 + x^2 + 1 = 0 \quad \Rightarrow \quad x = \alpha = T + \sum_{k<0} u_k T^k.$$

For $p = 13$, $\alpha \in \mathbb{H}_{13}(13)$, we have $\alpha = [T, 12T, 7T, 11T, 8T, 5T, \alpha_7]$ and

$$\alpha^{13} = (T^2 + 8)^4 \alpha_7 + 4 \int_0^T (x^2 + 8)^3 dx.$$

Mills and Robbins example in $\mathbb{F}(13)$ (1986)

In $\mathbb{F}(p)$ for all p, we have

$$x^4 - Tx^3 + x^2 + 1 = 0 \quad \Rightarrow \quad x = \alpha = T + \sum_{k<0} u_k T^k.$$

For $p = 13$, $\alpha \in \mathbb{H}_{13}(13)$, we have $\alpha = [T, 12T, 7T, 11T, 8T, 5T, \alpha_7]$ and

$$\alpha^{13} = (T^2 + 8)^4 \alpha_7 + 4 \int_0^T (x^2 + 8)^3 dx.$$

From this we can deduce : There exists a sequence $(\lambda_n)_{n \geq 1}$ in $\mathbb{F}_{13}^*$ such that

$$a_n = \lambda_n A_{v_9(8n-2)} \quad \text{for} \quad n \geq 1$$

where the sequence $(A_m)_{m \geq 0}$ in $\mathbb{F}_q[T]$ is given by

$$A_0 = T \quad \text{and} \quad A_{m+1} = [A_m^{13}/(T^2 + 8)^4] \quad \text{for} \quad m \geq 0.$$

Mills and Robbins example in $\mathbb{F}(13)$ (1986)

In $\mathbb{F}(p)$ for all p, we have

$$x^4 - Tx^3 + x^2 + 1 = 0 \quad \Rightarrow \quad x = \alpha = T + \sum_{k<0} u_k T^k.$$

For $p = 13$, $\alpha \in \mathbb{H}_{13}(13)$, we have $\alpha = [T, 12T, 7T, 11T, 8T, 5T, \alpha_7]$ and

$$\alpha^{13} = (T^2 + 8)^4 \alpha_7 + 4 \int_0^T (x^2 + 8)^3 dx.$$

From this we can deduce : There exists a sequence $(\lambda_n)_{n \geq 1}$ in $\mathbb{F}_{13}^*$ such that

$$a_n = \lambda_n A_{v_9(8n-2)} \quad \text{for} \quad n \geq 1$$

where the sequence $(A_m)_{m \geq 0}$ in $\mathbb{F}_q[T]$ is given by

$$A_0 = T \quad \text{and} \quad A_{m+1} = [A_m^{13}/(T^2 + 8)^4] \quad \text{for} \quad m \geq 0.$$

Here we have $\nu(\alpha) = 8/3$.

A last and sophisticated example in $\mathbb{H}_3(27)$

We have $\mathbb{F}_{27} = \mathbb{F}_3(u) = \{0, \pm u^k : 0 \leq k \leq 12\}$ where $u^3 + u^2 - u + 1 = 0$.

A last and sophisticated example in $\mathbb{H}_3(27)$

We have $\mathbb{F}_{27} = \mathbb{F}_3(u) = \{0, \pm u^k : 0 \leq k \leq 12\}$ where $u^3 + u^2 - u + 1 = 0$.
In $\mathbb{F}(27)$, we have

$$x = (Tx^3 + u^6 - uT^2)/(x^3 - u^3 T) \quad \Rightarrow \quad x = [\lambda_1 T, \lambda_2 T, \lambda_3 T, \ldots, \lambda_n T, \ldots].$$

A last and sophisticated example in $\mathbb{H}_3(27)$

We have $\mathbb{F}_{27} = \mathbb{F}_3(u) = \{0, \pm u^k : 0 \leq k \leq 12\}$ where $u^3 + u^2 - u + 1 = 0$.
In $\mathbb{F}(27)$, we have

$$x = (Tx^3 + u^6 - uT^2)/(x^3 - u^3 T) \quad \Rightarrow \quad x = [\lambda_1 T, \lambda_2 T, \lambda_3 T, \ldots, \lambda_n T, \ldots].$$

The sequence $(\lambda_n)_{n \geq 1}$ in $\mathbb{F}_{27}^*$ is defined recursively by $\lambda_1 = 1$ and

$$\lambda_{3n-1} = -u^{6(-1)^n} \lambda_n^3, \quad \lambda_{3n} = u^{6(-1)^{n+1}} \delta_n^{-1}, \quad \lambda_{3n+1} = -\lambda_{3n}^{-1} \quad \text{for} \quad n \geq 1$$

A last and sophisticated example in $\mathbb{H}_3(27)$

We have $\mathbb{F}_{27} = \mathbb{F}_3(u) = \{0, \pm u^k : 0 \leq k \leq 12\}$ where $u^3 + u^2 - u + 1 = 0$.
In $\mathbb{F}(27)$, we have

$$x = (Tx^3 + u^6 - uT^2)/(x^3 - u^3 T) \quad \Rightarrow \quad x = [\lambda_1 T, \lambda_2 T, \lambda_3 T, \dots, \lambda_n T, \dots].$$

The sequence $(\lambda_n)_{n\geq 1}$ in $\mathbb{F}_{27}^*$ is defined recursively by $\lambda_1 = 1$ and

$$\lambda_{3n-1} = -u^{6(-1)^n}\lambda_n^3, \quad \lambda_{3n} = u^{6(-1)^{n+1}}\delta_n^{-1}, \quad \lambda_{3n+1} = -\lambda_{3n}^{-1} \quad \text{for} \quad n \geq 1$$

where the sequence $(\delta_n)_{n\geq 1}$ in $\mathbb{F}_{27}^*$ satisfies $\delta_1 = u^4$ and

$$\delta_{3n-1} = u^{5(-1)^n}\delta_n^3(1+\gamma_n^3), \quad \delta_{3n} = \frac{\gamma_n^3 - 1}{\delta_{3n-1}}, \quad \delta_{3n+1} = \frac{\delta_{3n-1}}{1-\gamma_n^6} \quad \text{for} \quad n \geq 1$$

A last and sophisticated example in $\mathbb{H}_3(27)$

We have $\mathbb{F}_{27} = \mathbb{F}_3(u) = \{0, \pm u^k : 0 \leq k \leq 12\}$ where $u^3 + u^2 - u + 1 = 0$.
In $\mathbb{F}(27)$, we have

$$x = (Tx^3 + u^6 - uT^2)/(x^3 - u^3T) \quad \Rightarrow \quad x = [\lambda_1 T, \lambda_2 T, \lambda_3 T, \ldots, \lambda_n T, \ldots].$$

The sequence $(\lambda_n)_{n\geq 1}$ in $\mathbb{F}_{27}^*$ is defined recursively by $\lambda_1 = 1$ and

$$\lambda_{3n-1} = -u^{6(-1)^n}\lambda_n^3, \quad \lambda_{3n} = u^{6(-1)^{n+1}}\delta_n^{-1}, \quad \lambda_{3n+1} = -\lambda_{3n}^{-1} \quad \text{for} \quad n \geq 1$$

where the sequence $(\delta_n)_{n\geq 1}$ in $\mathbb{F}_{27}^*$ satisfies $\delta_1 = u^4$ and

$$\delta_{3n-1} = u^{5(-1)^n}\delta_n^3(1+\gamma_n^3), \quad \delta_{3n} = \frac{\gamma_n^3 - 1}{\delta_{3n-1}}, \quad \delta_{3n+1} = \frac{\delta_{3n-1}}{1-\gamma_n^6} \quad \text{for} \quad n \geq 1$$

and finally the sequence $(\gamma_n)_{n\geq 1}$ in $\mathbb{F}_{27}^*$ satisfies $\gamma_1 = u$ and

$$\gamma_{3n-1} = \frac{\gamma_n^3}{1+\gamma_n^3}, \quad \gamma_{3n} = \frac{\gamma_n^3}{1-\gamma_n^6}, \quad \gamma_{3n+1} = \frac{\gamma_n^3}{1-\gamma_n^3} \quad \text{for} \quad n \geq 1.$$

A comment on Mathematics

"Roughly speaking, unfashionable mathematics consists of those parts of mathematics which were declared by the mandarins of Bourbaki not to be mathematics. A number of very beautiful mathematical discoveries fall into this category. To be mathematics according to Bourbaki, an idea should be general, abstract, coherent, and connected by clear logical relationships with the rest of mathematics. Excluded from mathematics are particular facts, concrete objects which just happen to exist for no identifiable reason, things which a mathematician would call accidental or sporadic.....things of accidental beauty, special functions, particular number fields, ... "

Freeman J. Dyson