Continued Fractions for Certain Algebraic Power Series over a Finite Field

Alain Lasjaunias

Université de Bordeaux I
CNRS-UMR 5465
351, Cours de la Libération
F33405 Talence Cedex - France
E-mail: lasjauni@math.u-bordeaux.fr

Abstract. In this survey we discuss rational approximation properties of certain algebraic power series over a finite field using continued fractions. These algebraic elements are fixed points of the composition of a linear fractional transformation and of the Frobenius homomorphism.

1 The Fields of Power Series over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be the field with q elements and let p be its characteristic. We consider the field $\mathbb{F}_q(T)$ of rational functions in the indeterminate T, with coefficients in $\mathbb{F}_q$. On this field $\mathbb{F}_q(T)$ we consider the ultrametric absolute value defined by

$$|P/Q| = |T|^{\deg P - \deg Q} \quad \text{and} \quad |0| = 0$$

where $|T| > 1$ is a fixed real number. The field obtained by completion from $\mathbb{F}_q(T)$ for this absolute value will be denoted by $\mathbb{F}(q)$. If $\Theta \in \mathbb{F}(q)$ and $\Theta \neq 0$, we can write it as a power series expansion

$$\Theta = \sum_{k \leq k_0} \theta_k T^k \quad \text{with} \quad k_0 \in \mathbb{Z}, \quad \theta_k \in \mathbb{F}_q \quad \theta_{k_0} \neq 0$$

and the absolute value is extended by $|\Theta| = |T|^{k_0}$. This construction is analogous to the classical construction of the field of real numbers from the ring of integers. The resulting field $\mathbb{F}(q)$ has many similar properties with $\mathbb{R}$ and hence could be called the field of formal numbers over $\mathbb{F}_q$. In the two statements below we consider $\Theta \in \mathbb{F}(q)$ written as $\Theta = P(T) + \sum_{n \geq 0} \theta_n T^{-n}$ where $P(T)$ is the integral (polynomial) part of Θ. The first result is an illustration of the similarity with real numbers.

Theorem 1.1. *$\Theta \in \mathbb{F}_q(T)$ if and only if the sequence $(\theta_n)_{n \geq 0}$ is ultimately periodic.*

Since we are concerned with algebraic elements in $\mathbb{F}(q)$ over $\mathbb{F}_q(T)$, it is interesting to mention a deeper result concerning the power series expansion, due to Christol.

Theorem 1.2. *Θ is algebraic over $\mathbb{F}_q(T)$ if and only if the set of subsequences*

$$\{(\theta_{q^i n + r})_{n \geq 0} : i \geq 0 \text{ and } 0 \leq r \leq q^i - 1\}$$

is finite.

Clearly the same construction as above can be made from an arbitrary base field K instead of $\mathbb{F}_q$. Then the resulting field is called the field of power series over K and denoted by $K((T^{-1}))$. Indeed the finiteness of the base field is essential in many results and this makes the field $\mathbb{F}(q)$ particularly interesting. We study here, in the case $K = \mathbb{F}_q$, rational approximation to algebraic power series over $K(T)$. For a study in a larger context and for more references see [L1].

Many classical questions in number theory, which have been studied in the setting of real numbers, can be transposed and studied in fields of power series. The starting point in the study of rational approximation to algebraic real numbers is a famous theorem established by Liouville in 1850. This theorem has been adapted by Mahler [M] in fields of power series with an arbitrary base field.

Theorem 1.3. *Let K be a field. Let $\Theta \in K((T^{-1}))$ be an algebraic element over $K(T)$, of degree $n > 1$. Then there is positive real number C such that*

$$|\Theta - P/Q| \geq C|Q|^{-n}$$

for all $P, Q \in K[T]$, with $Q \neq 0$.

In the case of real numbers, we know that Liouville's theorem was the first step in the study of rational approximation to algebraic numbers. A deeper result was obtained with Roth's theorem established in 1955. This last theorem can be transposed in fields of power series if and only if the base field has characteristic zero. In this case the exponent n in the right hand side of the inequality in the above theorem can be replaced by $2 + \epsilon$ for all $\epsilon > 0$ with the constant C depending upon ϵ. But this is not so in the case of the field $\mathbb{F}(q)$ and consequently the study of rational approximation to algebraic elements becomes more complex.

2 The Continued Fraction Algorithm

As in the classical context of the real numbers, we have a continued fraction algorithm in $\mathbb{F}(q)$. For a general reference on this subject see [S]. If $\Theta \in \mathbb{F}(q)$

we can write

$$\Theta = a_0 + 1/(a_1 + 1/(a_2 + ... = [a_0, a_1, a_2, ...] \quad \text{where} \quad a_i \in \mathbb{F}_q[T].$$

The a_i's are called the *partial quotients* and we have $\deg a_i > 0$ for $i > 0$. This continued fraction expansion is finite if and only if $\Theta \in \mathbb{F}_q(T)$. As in the classical theory we define recursively the two sequences of polynomials $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ by

$$x_n = a_n x_{n-1} + x_{n-2} \quad \text{and} \quad y_n = a_n y_{n-1} + y_{n-2},$$

with the initial conditions $x_0 = a_0$, $x_1 = a_0 a_1 + 1$, $y_0 = 1$ and $y_1 = a_1$. We have $x_{n+1}y_n - y_{n+1}x_n = (-1)^n$, whence x_n and y_n are coprime polynomials. The rational x_n/y_n is called a *convergent* to Θ and we have $x_n/y_n = [a_0, a_1, a_2, ..., a_n]$. Because of the ultrametric absolute value we have

$$|\Theta - x_n/y_n| = |x_{n+1}/y_{n+1} - x_n/y_n| = |y_n y_{n+1}|^{-1} = |a_{n+1}|^{-1}|y_n|^{-2}. \quad (1)$$

We mention an important result which is an analogue of Lagrange's theorem (see [S]).

Theorem 2.1. *Let $\Theta \in \mathbb{F}(q)$ be irrational. Then the sequence of partial quotients in the continued fraction expansion of Θ is ultimately periodic if and only if Θ is quadratic over $\mathbb{F}_q(T)$.*

3 The Approximation Exponent

Let $\Theta \in \mathbb{F}(q)$ be an irrational element. We define the *approximation exponent* of Θ by

$$\nu(\Theta) = \limsup_{|Q|\to\infty}\left(-\frac{\log|\alpha - P/Q|}{\log|Q|}\right)$$

where P and Q run over polynomials in $\mathbb{F}_q[T]$ with $Q \neq 0$. Let us consider the continued fraction expansion $\Theta = [a_0, a_1, \ldots, a_n, \ldots]$. Since the convergents are the best rational approximations to Θ, it is clear, using (1), that the approximation exponent can also be defined directly by

$$\nu(\Theta) = 2 + \limsup_k(\deg a_{k+1}/\deg y_k).$$

Observe that $\deg y_k = \sum_{1\leq i\leq k} \deg a_i$ and therefore $\nu(\Theta)$ is directly connected to the growth of the sequence $(\deg a_i)_{i\geq 1}$. In particular if the sequence $(\deg a_i)_{i\geq 1}$ is bounded then $\nu(\Theta) = 2$. Clearly we may have $\nu(\Theta) = 2$ without this assumption.

Because of Mahler's theorem, for all $\Theta \in \mathbb{F}(q)$ algebraic over $\mathbb{F}_q(T)$ and of degree $n > 1$, we have

$$\nu(\Theta) \in [2, n].$$

We give now two classical examples, in some sense dual of each other, of algebraic elements for which the approximation exponent is maximal. The second was first introduced in [M]. Here $r = p^t$ where $t \geq 0$ is an integer.

Example 1 : We define $\Theta \in \mathbb{F}(p)$ by

$$\Theta = [0, T, T^r, \ldots, T^{r^k}, \ldots].$$

Because of the Frobenius homomorphism, we have $\Theta = 1/(T + \Theta^r)$. It is easy to see that $\nu(\Theta) = r + 1$.

Example 2 : Here we assume that $t \neq 0$ and we define $\Theta \in \mathbb{F}(p)$ by

$$\Theta = \sum_{k\geq 0} T^{-r^k}.$$

In that case we have $\Theta = 1/T + \Theta^r$ and $\nu(\Theta) = r$ (see [M]). It is interesting to observe that the continued fraction for this algebraic element can be given explicitly.

Theorem 3.1. *Assume that $r > 2$. We define recursively on $n \geq 1$ a finite sequence Ω_n of elements in $\mathbb{F}_p[T]$ such that*

$$\Omega_1 = T \quad \text{and} \quad \Omega_n = \Omega_{n-1}, -T^{(r-2)r^{n-2}}, -\widetilde{\Omega}_{n-1}$$

If $\Omega_n = a_1, a_2, \ldots, a_m$ then $\widetilde{\Omega}_n = a_m, \ldots, a_2, a_1$ and $-\Omega_n = -a_1, -a_2, \ldots, -a_m$. Further Ω_∞ denotes the infinite sequence beginning by Ω_n for all $n \geq 1$. Then the continued fraction expansion for Θ is $[0, \Omega_\infty]$.

We recall that no explicit continued fraction expansion is known for a non-quadratic algebraic real number.

4 Algebraic Elements of Class

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

$$\Theta = \frac{A\Theta^r + B}{C\Theta^r + D} \quad (2)$$

We put $\mathcal{H}(q) = \bigcup_{r=p^t, t\geq 0} \mathcal{H}(r, q)$. The elements of $\mathcal{H}(q)$ are called algebraic elements of class I. Observe that the elements which are quadratic and also cubic over $\mathbb{F}_q(T)$ are algebraic of class I (indeed the four elements $1, \Theta, \Theta^p$ and Θ^{p+1} are linked over $\mathbb{F}_q(T)$).

These algebraic elements were introduced by Baum and Sweet [BS1] when the base field was $\mathbb{F}_2$. Later they were considered by Mills and Robbins [MR]

in a general context. We give below a theorem which gives the main known rational approximation properties of these elements.

Theorem 4.1. *We have the following properties :*
(i) *If* $\Theta \in \mathcal{H}(q)$ *then* $\nu(\Theta) \in \mathbb{Q}$ *and* $\liminf_{|Q|\to\infty} |Q|^{\nu(\Theta)}|\Theta - P/Q| \neq 0, \infty$.
(ii) *If* $\Theta \in \mathcal{H}(r,q)$ *and if in equation (2) we have* $\deg(AD-BC) < r-1$ *then* $\nu(\Theta) > 2$.
(iii) *If* $\Theta \in \mathbb{F}(q)$ *is algebraic of degree* $n > 1$ *and* $\Theta \notin \mathcal{H}(q)$ *then* $\nu(\Theta) \leq [n/2] + 1$.

For (i) see [dM] and [V], for (ii) see [L3] and for (iii) see [LdM1] and [LdM2]. Observe that the last property implies that the algebraic elements which are best approximable by rational elements must belong to $\mathcal{H}(q)$ (as both examples above). A consequence of the first property in this theorem is that there exists a natural partition of the set $\mathcal{H}(q)$ into two subsets $\mathcal{H}_1(q)$ and $\mathcal{H}_2(q)$.

Corollary 4.2. *Let* $\Theta = [a_0, a_1, a_2, \dots] \in \mathcal{H}(q)$. *Then we have either*
- $\Theta \in \mathcal{H}_1(q)$ *: there is a real number* $\mu > 0$ *such that*

$$\limsup_k (\deg a_{k+1} / \sum_{1\leq i\leq k} \deg a_i) = \mu \qquad (i.e. \quad \nu(\Theta) > 2)$$

or
- $\Theta \in \mathcal{H}_2(q)$ *: there is an integer* B *such that*

$$\deg a_i \leq B \quad for \quad i \geq 0.$$

The two examples given above belong to $\mathcal{H}_1(q)$ when they are not quadratic. Clearly $\mathcal{H}_2(q)$ contains the quadratic formal numbers. The existence of non-quadratic elements in $\mathcal{H}_2(q)$ was first observed by Baum and Sweet [BS1] and latter by Mills and Robbins [MR]. It is interesting to remark that evident computer calculation shows that $\mathcal{H}_1(q)$ is a much larger set than $\mathcal{H}_2(q)$. It is also important to observe that both subsets $\mathcal{H}_1(q)$ and $\mathcal{H}_2(q)$ are stable under three transformations : 1) the Frobenius homomorphism, 2) a linear fractional transformation with polynomial coefficients, 3) the change of T into a polynomial of T. Moreover these three transformations preserve the degree of an algebraic element over $\mathbb{F}_q(T)$.

5 A Particular Subclass in $\mathcal{H}(q)$

If we look for an analogue of the subset $\mathcal{H}(q)$ in the setting of the real numbers, we should consider the subset of quadratic real numbers. Indeed these numbers are fixed points of a linear fractional transformation with integer

coefficients. This implies the peculiar pattern of their continued fraction expansions. Unluckily the possibility of describing explicitly the continued fraction expansion for all the elements of $\mathcal{H}(q)$ seems yet out of reach (see [MR]). Nevertheless this description is possible for a particular subclass.

We will say that an element in $\mathcal{H}(q)$ is of class IA if $AD - BC \in \mathbb{F}_q^*$ in equation (2). Example 1 given above belongs to this subclass. Observe that, according to the second property of Theorem 4.1, if Θ is of class IA and $r \neq 1$ then $\Theta \in \mathcal{H}_1(q)$. Such algebraic elements have been studied by Schmidt [S] and also by Thakur [T] who proved independently the following theorem.

Theorem 5.1. $\Theta \in \mathbb{F}(q)$ *is algebraic of class IA if and only if there exist* $k \geq -1$, $a_j, c_i \in \mathbb{F}_q[T]$ *with* $0 \leq j \leq k$ *and* $i \geq 1$, $t \in \mathbb{N}^*$ *and* $\epsilon \in \mathbb{F}_q^*$ *such that*

$$\Theta = [a_0, a_1, \dots, a_k, c_1, c_2, \dots, c_n, \dots]$$

where for $l \geq 1$ *we have*

$$c_{l+t} = \begin{cases} \epsilon c_l^r & \text{if } l \text{ is odd,} \\ \epsilon^{-1} c_l^r & \text{if } l \text{ is even.} \end{cases}$$

Observe that for $r = 1$ the corresponding element is quadratic and the expansion becomes ultimately periodic. The fact that the continued fraction expansion can be obtained explicitly for algebraic numbers of class IA implies the following result.

Corollary 5.2. *Let* μ *be a rational real number with* $\mu \geq 2$ *then there is an element* Θ *in* $\mathcal{H}(q)$ *such that* $\nu(\Theta) = \mu$.

6 A Particular Subset of $\mathcal{H}_2(q)$

As we noted above non-quadratic elements in $\mathcal{H}_2(q)$ appear to be exceptional. The first examples were given in [BS1], [BS2] and [MR]. In [L2] and later in a joint work with J.-J. Ruch, [LR1] and [LR2], we have searched for these elements with all partial quotients of degree one. For the theorem below, we need to introduce a new notation. If $(a_n)_{n\geq 1}$ is a sequence of polynomials in $\mathbb{F}_q[T]$ then, for $i \geq 1$ and $k \geq 0$, we define the polynomial $x_{i,k}$ as the numerator of the finite continued fraction $[0, a_{k+1}, a_{k+2}, \dots, a_{k+i}]$.

Theorem 6.1. *Let* $r = p^t$ *with* $t \geq 0$ *and* $l \geq r$ *be two integers. Let* Θ *be an irrational element in* $\mathbb{F}(q)$. *Assume that* $\Theta = [0, a_1, a_2, \dots]$ *with* $\deg a_i = 1$ *for* $i \geq 1$. *Then there exists* $\epsilon \in \mathbb{F}_q^*$ *such that*

$$(E) \quad \Theta = \frac{\epsilon x_l + x_{l-r}\Theta^r}{\epsilon y_l + y_{l-r}\Theta^r}$$

if and only if there is a sequence $(\epsilon_n)_{n\geq 0}$ of elements in $\mathbb{F}_q^*$, with $\epsilon_0 = 1$ and $\epsilon_1 = \epsilon$, such that for $n \geq 1$ we have

$$(S) \quad \begin{cases} \epsilon_{n-1} x_{2r,(n-2)r+l} = \epsilon_n a_n^r x_{r,(n-1)r+l} \\ \epsilon_{n+1} x_{r,(n-1)r+l} = \epsilon_{n-1} x_{r,(n-2)r+l} \end{cases}$$

In the trivial case $r = 1$, we meet with a particular case of Theorem 5.1. Indeed Θ is then quadratic and (S) simply becomes $a_{l+k} = a_k \epsilon^{(-1)^{k+1}}$ for $k \geq 1$. In the general case the existence of a sequence $(a_n)_{n\geq 1}$ solution of (S) will depend upon the choice of ϵ and of the first l partial quotients. It is remarkable that for all q, r and $l \geq r$ there is a trivial solution of (S) given by $a_i = T$ for $i \geq 1$ and $\epsilon_i = 1$ for $i \geq 0$. The corresponding algebraic element is the one given as Example 1 above with $r = 1$ and is thus quadratic. We have given (in [L2] for $q = 3$ and in [LR1] for general q) families of examples of sequences $(a_n)_{n\geq 1}$ satisfying (S). As an illustration in odd characteristic, we give the following corollary [LR1]. Here, if S is a finite sequence and $k \geq 0$ an integer, then $S^{[k]}$ denotes the empty sequence if $k = 0$ or else the sequence S repeated k times. Furt! her if S_1 and S_2 are two finite sequences then $S_1 \oplus S_2$ denotes the sequence obtained by concatenation.

Corollary 6.2. *Let $q = p^s$ with $p \neq 2$ and $s \geq 1$. Let $\alpha, \beta \in \mathbb{F}_q^*$ with $\alpha + \beta = 2$. Let $k \geq 0$ be an integer. Let $\Theta \in \mathbb{F}(q)$ be defined by the following continued fraction expansion*

$$\Theta = [0, T^{[k]}, \oplus_{i\geq 1}(T, (\alpha T, \beta T)^{[(q^i-1)/2]})^{[k+1]}\ ].$$

Then Θ satisfies the algebraic equation

$$y_k X^{q+1} - x_k X^q + (\alpha\beta)^{(q-1)/2} y_{q+k} X - (\alpha\beta)^{(q-1)/2} x_{q+k} = 0.$$

Clearly the complexity of the system (S) in theorem 6.1 is growing with r. In the case of even characteristic, we can choose $r = 2$. By studying the simplest case where the partial quotients are all linear in T, we can prove the following corollary [LR2].

Corollary 6.3. *Let $q = 2^s$ with $s \geq 1$ and $l \geq 2$ be integers. Let $\lambda_1, \lambda_2, \ldots, \lambda_l$ and ϵ be given in $\mathbb{F}_q^*$. We consider the sequence $(\lambda_i)_{i\geq 1}$ defined recursively for $n \geq 1$ by*

$$\begin{cases} \lambda_{l+2n-1} = \lambda_n^2 \lambda_l^{-1} \epsilon^{(-1)^{n+1}} \\ \lambda_{l+2n} = \lambda_l. \end{cases}$$

Let Θ be the irrational element in $\mathbb{F}(q)$ defined by the continued fraction expansion

$$\Theta = [0, \lambda_1 T, \lambda_2 T, \ldots, \lambda_n T, \ldots].$$

Then Θ satisfies the algebraic equation

$$y_{l-2}\Theta^3 + x_{l-2}\Theta^2 + \epsilon y_l \Theta + \epsilon x_l = 0.$$

We conclude by making a last observation. Let us denote by $\mathcal{F}(q)$ the subset of $\mathcal{H}(q)$ containing all the elements satisfying an equation of type (E) as defined in Theorem 6.1. From the subset $\mathcal{F}(q)$, using the three transformations mentioned at the end of section 4, we obtain a wider set of badly approximable algebraic elements (that is to say with bounded partial quotients). Does this set cover $\mathcal{H}_2(q)$? The answer is no if $q = 2$. In that case Baum and Sweet have described all the power series with partial quotients of degree one (see [BS2]). There are among them algebraic elements which are not of class I (see [L1] p. 225). On the other hand Baum and Sweet have given the example of a cubic element with bounded partial quotients (see [BS1] and [L3]). The case of characteristic 2 might be specific since then the existence of badly approximable elements comes from arguments of differential algebra (see [LdM2] p. 5). Consequently it is natural to a! sk : if the characteristic is different from 2, are there badly approximable algebraic elements which are not of class I ? This last question forces us to think of an open problem in number theory : are there badly approximable algebraic real numbers which are not quadratic ?

References

[BS1] Baum L. and Sweet M., Continued fractions of algebraic power series in characteristic 2, Annals of Mathematics, 103(1976), 593–610.

[BS2] Baum L. and Sweet M., Badly approximable power series in characteristic 2, Annals of Mathematics, 105(1977), 573–580.

[L1] Lasjaunias A., A survey of diophantine approximation in fields of power series, Monatshefte für Mathematik, 130(2000), 211–229.

[L2] Lasjaunias A., Quartic power series in $\mathbb{F}_3((T^{-1}))$ with bounded partial quotients, Acta Arithmetica, XCV.1(2000), 49–59.

[L3] Lasjaunias A., Continued fractions for algebraic power series over a finite field, Finite Fields and their Applications, 5(1999), 46–56.

[LdM1] Lasjaunias A. and de Mathan B., Thue's Theorem in positive characteristic, Journal für die reine und angewandte Mathematik, 473(1996), 195–206.

[LdM2] Lasjaunias A. and de Mathan B., Differential equations and diophantine approximation in positive characteristic, Monatshefte für Mathematik, 128(1999), 1–6.

[LR1] Lasjaunias A. and Ruch J-J., Algebraic and badly approximable power series over a finite field, Finite Fields and their Applications, 8(2002), 91–107.

[LR2] Lasjaunias A. and Ruch J-J., Flat power series over a finite field, Journal of Number Theory, to appear.

[M] Mahler K., On a theorem of Liouville in fields of positive characteristic, Canadian Journal of Mathematics, 1(1949), 397–400.

[dM] de Mathan B. Approximation exponents for algebraic functions, Acta Arithmetica, LX.4(1992), 359–370.

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

[S] Schmidt W., On Continued fractions and diophantine approximation in power series fields, Acta Arithmetica, XCV.2(2000), 139–165.

[T] Thakur D., Diophantine approximation exponents and continued fractions for algebraic power series, Journal of Number Theory, 79(1999), 284–291.

[V] Voloch J-F., Diophantine approximation in positive characteristic, Periodica Mathematica Hungarica, 19.3(1988), 217-225.

Linear Complexity and Polynomial Degree of a Function Over a Finite Field

Wilfried Meidl and Arne Winterhof

Institute of Discrete Mathematics, Austrian Academy of Sciences,
Sonnenfelsgasse 19/2, 1010 Vienna, Austria,
E-Mail: {wilfried.meidl, arne.winterhof}@oeaw.ac.at

Abstract. We compare the complexities of the polynomial representation and the periodic sequence representation of a function over a finite field in the complexity measures degree and linear complexity. We prove a sharp inequality describing the relation between degree and linear complexity. These investigations are motivated by results on some cryptographic functions. In particular, as an application of the above mentioned inequality we prove new lower bounds on the linear complexity of sequences related to the Diffie-Hellman mapping.

1 Introduction

One way functions are important topics in cryptography. For example the discrete logarithm is an attractive candidate for the inverse of a one way function. Various cryptographic protocols as the Diffie-Hellman key exchange depend on the intractability of the discrete logarithm (see e. g. [10, Chapter 3]). Unfortunately, there exists no exact definition for intractability of a function and we have to compensate this lack with several complexity measures. In the present paper we consider functions over finite fields and their representations as polynomials and as periodic sequences and compare the complexity measures degree and linear complexity.

Let q be a prime power and fix an ordering $F_q = \{\xi_0, \ldots, \xi_{q-1}\}$ of the elements of the finite field F_q. A q-periodic sequence (σ_n) of elements of F_q can be represented by a uniquely determined polynomial $f(X) \in F_q[X]$ of degree at most $q-1$. Conversely, every polynomial $f(X) \in F_q[X]$ defines a unique q-periodic sequence over F_q. In other words, we have

$$\sigma_n = f(\xi_n) \in F_q \quad \text{for } 0 \le n < q \quad \text{and} \quad \sigma_{n+q} = \sigma_n \quad \text{for } n \ge 0. \qquad (1)$$

Since $\xi^q = \xi$ for all ξ in F_q we may restrict ourselves to the case that the degree of $f(X)$ is at most $q-1$ in the sequel.

The *linear complexity* $L(\sigma_n)$ of the sequence (σ_n) is the shortest positive integer L such that there are constants $\gamma_1, \ldots, \gamma_L \in F_q$ satisfying

$$-\sigma_n = \gamma_1\sigma_{n-1} + \gamma_2\sigma_{n-2} + \ldots + \gamma_L\sigma_{n-L} \qquad \text{for all } n \ge L.$$