On Skew Periodic Sequences

Ahmed Cherchem and André Leroy

USTHB, Faculté de Mathématiques, LA3C, Algiers — Université d'Artois, Faculté des Sciences, LML, Lens

Abstract

In this work, we introduce the notion of **skew period of skew linear recurring sequence** over a finite field. This notion is related to the notion of exponent of skew polynomial. Some properties and examples are presented.

The ring of skew polynomials

Let q be a power of a prime, $\mathbb{F}_q$ the finite field of q elements and θ be the Frobenius automorphism of $\mathbb{F}_q$: $\theta(a) = a^p$. Let $\mathbb{F}_q[t;\theta] := R$ the noncommutative ring of skew polynomials. The elements of R are polynomials $\sum_{i=0}^{n} a_i t^i, a_i \in \mathbb{F}_q$. They are added as ordinary polynomials and the multiplication is based on the commutation law :

$$ta = \theta(a)\,t = a^p t, \text{ for } a \in \mathbb{F}_q.$$

This ring is called an Ore-Frobenius extension and its elements are skew polynomials. It is a left and right Euclidean domain. In particular, for $f(t) \in \mathbb{F}_q[t;\theta]$ and $a \in \mathbb{F}_q$, there exists a unique polynomial $q(t) \in \mathbb{F}_q[t;\theta]$ and a unique $r \in \mathbb{F}_q$ such that $f(t) = q(t)(t-a) + r$. We define $f(a)$, the evaluation of f at a, by $f(a) := r$.

Exponents of skew polynomials

Let $f(t) \in R$ with nonzero constant term. It is shown in [2] that there exists a positive integer e such that $f(t)$ right divides $t^e - 1$. The least such an integer is the **right exponent** of $f(t)$. The left exponent is defined similarly. This generalizes the classical exponent (a.k.a. order) of a polynomial in $\mathbb{F}_q[t]$, see [3]. A concrete way for computing this exponent and some of its properties are given in the same reference. For $C = (c_{ij})_{0\le i,j\le n} \in M_n(\mathbb{F}_q)$ a matrix with entries in $\mathbb{F}_q$, we set $\theta(C) = (\theta(c_{ij}))_{0\le i,j\le n}$. Let C_f be the companion matrix of $f(t)$. Then the (right or left) exponent e of $f(t)$ is the least integer such that

$$\theta^{e-1}(C_f)\cdots\theta(C_f)\,C_f = Id.$$

The integer e is also called the θ-order of the matrix C_f.

Short example

Let $\mathbb{F}_4 = \{0, 1, a, a^2 = a+1\}$ be the field of 4 elements and θ be the Frobenius automorphism defined by $\theta(a) = a^2$. Consider the polynomial $f(t) = t - a \in \mathbb{F}_4[t;\theta]$. In the classical case, when $f \in \mathbb{F}_4[t]$, the exponent is 3. However, when $f \in \mathbb{F}_4[t;\theta]$, we have $(t-a^2)(t-a) = t^2 - ta - a^2 t + a^3 = t^2 - (\theta(a) + a^2)t + 1 = t^2 - 1$. Thus we conclude that the exponent is 2.

Another example

Consider the polynomial $g(t) = t^3 + at + 1 \in \mathbb{F}_4[t;\theta]$. The companion matrix of g is

$$C_g = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a & 0 \end{pmatrix}$$

Computing the θ-order of the matrix C_g, we get the exponent 8. One can verify that

$$\left(t^5 + a^2 t^3 + t^2 + at + 1\right)\left(t^3 + at + 1\right) = t^8 + 1.$$

Skew period of skew linear recurring sequence

Let $S(\mathbb{F}_q)$ be the set of sequences over the finite field $\mathbb{F}_q$. The set $S(\mathbb{F}_q)$, endowed with the ordinary addition and the multiplication defined, for $f(t) = a_0 + a_1 t + \cdots + a_h t^h \in \mathbb{F}_q[t;\theta] := R$, by :

$$\forall u \in S(\mathbb{F}_q), \forall n \in \mathbb{N}, (f(t).u)(n) = a_0 u(n) + a_1\theta(u(n+1)) + \cdots + a_h\theta^h(u(n+h)),$$

is a left R-module. Let $u \in S(\mathbb{F}_q)$. Denote by I_u the annihilator of u in R. We thus have :

$$I_u = \{f \in R, \quad f.u = 0\}.$$

We say that u is a **skew linear recurring sequence** (skew LRS) over $\mathbb{F}_q$ if I_u contains a monic polynomial. Such a polynomial is called **skew characteristic polynomial** of u. A skew characteristic polynomial with minimal degree is called **skew minimal polynomial** of u.
If there exists an integer $r > 0$ such that $\theta^r(u(n+r)) = u(n)$ for $n \ge 0$, we say that u is skew periodic and r is a **skew period** of u. The smallest number among all the possible skew periods of u is called the **least skew period** of u.
.

Some properties

Let u be a skew LRS over a finite field $\mathbb{F}_q$ with skew characteristic polynomial $f(t) = a_0 + a_1 t + \cdots + t^h \in \mathbb{F}_q[t;\theta]$. Assume that $a_0 \ne 0$, then :

1. the skew minimal polynomial of u right divides any skew characteristic polynomial of u,
2. if $f(t)$ is irreducible, then it is the minimal polynomial of u,
3. the sequence u is skew periodic,
4. every skew period of u is divisible by the least skew period,
5. if $f(t)$ is the minimal polynomial of the sequence u, then the least skew period of u is equal to the exponent of $f(t)$.
6. if the order of the automorphism θ divides a skew period of u, then this skew period is also a "classical period" of u.

Examples of skew LRS

1. Consider the sequence u defined over $\mathbb{F}_4$ by $u(0) = 1$ and $\theta(u(n+1)) = au(n)$ for $n \ge 0$. The polynomial $f(t) = t - a \in \mathbb{F}_4[t]$ is the skew minimal polynomial of u. Since the skew exponent of f is 2, then the least skew period of u is 2 and we have
$$\theta^2(u(n+2)) = u(n+2) = u(n), \text{ for } n \ge 0.$$
2. Let $\mathbb{F}_9 = \{0, 1, a, a^2, \cdots, a^7; a^2 = a+1\}$ be the field of 9 elements and θ be the Frobenius automorphism defined by $\theta(a) = a^3$. Consider the polynomial $f(t) = t^2 - at - 1 \in \mathbb{F}_9[t;\theta]$. The exponent of $f(t)$ is 12. Then the skew LRS defined over $\mathbb{F}_9$ by $u(0) = 0, u(1) = 1$ and
$$u(n+2) = a\theta(u(n+1)) + u(n), \text{ for } n \ge 0,$$
is skew periodic with skew period 12.

Families of LRS

Let $f(t) \in R$ monic with nonzero constant term and denote by $U(f)$ the set of skew LRS with skew characteristic polynomial $f(t)$. The set $U(f)$ is a vector space over $\mathbb{F}_q$ under the usual addition and scalar multiplication of sequences and its dimension is equal to the degree of $f(t)$. If f right divides g, then $U(f)$ is a subspace of $U(g)$. This leads to some interesting properties about the subspaces $U(f) \cap U(g)$ and $U(f) + U(g)$. The case when $f(t)$ is the minimal polynomial is of particular interest. These properties are currently being investigated.

Conclusions and Outlook

The introduction of the notion of skew period of skew LRS seems very promising. The main prospects are

1. explore the relationship between the classical periodic sequences and the skew periodic sequences,
2. explore the skew generating function of a skew LRS,
3. applications to Coding Theory.

References

[1] T. Y. Lam, A first course in noncommutative rings, Springer-Verlag, 1991.

[2] A. Cherchem, A. Leroy, Exponents of Skew Polynomials, Submitted to Finite Fields and their Applications.

[3] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994.

Conference presentation

This poster is presented at the IVth NonCommutative Rings and their Applications Conference, Lens, France, June 08-11, 2015.