Palestine Journal of Mathematics

Vol 14(3)(2025) , 1083–1091

Characteristic polynomial and period of a linear recurrent sequence braiding on a field

Hocine AIT MOHAMMED and Ahmed AIT MOKHTAR

Communicated by Ayman Badawi

MSC 2020 Classifications: Primary 11B83; Secondary 11B37, 11C08.

Keywords and phrases: Braiding application, Linear recurrent sequences, Braided linear recurrent sequences, Annihilating ideal, Minimal characteristic polynomial of a linear recurrent sequence, Period and numeric of a linear recurrent sequence

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper

Corresponding Author: Ahmed AIT MOKHTAR

Abstract. Let K be a commutative field of characteristic zero, K^{alg} its algebraic closure assumed to be commutative, and $r(K)$ the set of linear recurrent sequences with coefficients and values in K. This paper discusses some properties of braided sequences $\psi_{d,\sigma}u$, where $d \in \mathbb{N}^*$, σ is a permutation of the set $\{0, 1, ..., d-1\}$ and $u \in r(K)$, these are the images of the bijective braided applications $\psi_{d,\sigma}$ from $r(K)$ to $r(K)$. In particular, we provide a result on determining the characteristic polynomial of the braided sequence $\psi_{d,\sigma}u$ and the determination of the minimal characteristic polynomial of a sequence in $r(K)$. We then give a characterization of a periodic sequence in $r(K)$ and the determination of its primitive period and primitive numeric, followed by the determination of the period and numeric of the braiding $\psi_{d,\sigma}u$.

1 Introduction

Let K be a commutative field with zero characteristic, ($Car(K) = 0$), and $r(K)$ be the set of linear recurrent sequences on K with constant coefficients, K^{alg} be the algebriac closure of K assumed to be commutative with $Car(K^{alg}) = 0$ and $S(K^{alg})$ be the K^{alg}-Hadamard algebra sequences with values in K^{alg}.
First of all, we recall the definitions of a shift, a decimation and a nesting and the definition of a bijective braiding application [1, 2, 7, 8, 10, 11]. Then, recalling the definition of the canceling ideal of a sequence of $r(K)$ and the kernel lemma, we determine a polynomial characteristic of a recurrent linear braiding sequence (see proposition(3.1) and proposition (3.4)), we determine the minimal characteristic polynomial of a sequence of $r(K)$ (see proposition(3.7)). Then by recalling the definition of a periodic numerical sequence n_0, of a purely periodic sequence, we characterize the periodic sequences of $r(K)$ (see proposition(3.10)) and we determine the period primitive and the primitive numerical of a periodic sequence of $r(K)$ (see proposition(3.13)) and finally we determine a period and a numerical of a recurring linear braiding sequence (see proposition(3.17)).

2 Preliminary results

Definition 2.1. Let K be a commutative field with zero characteristic and K^{alg} its algebraic closure. The map $T : S(K^{alg}) \longrightarrow S(K^{alg})$ which assigns to any sequence u the sequence Tu, defined by :

$$\forall n \in \mathbb{N},\ Tu(n) = u(n+1), \tag{2.1}$$

is called shift.

Definition 2.2. Let $d \in \mathbb{N}^*$. The map $\varphi_d : r(K) \longrightarrow r(K)$ which assigns to any sequence u the sequence $\varphi_d u$, defined by :

$$\forall n \in \mathbb{N},\ \varphi_d u(n) = u(dn), \tag{2.2}$$

is called decimation.

Definition 2.3. Let $d \in \mathbb{N}^*$. The map $E_d : r(K)^d \longrightarrow r(K)$ which assigns to any d-tuple $(u_0, u_1, ..., u_{d-1})$ the sequence $E_d(u_0, u_1, ..., u_{d-1})$, defined by :

$$\forall j \in \{0, 1, ..., d-1\}, \forall n \in \mathbb{N},\ E_d(u_0, u_1, ..., u_{d-1})(dn + j) = u_j(n), \tag{2.3}$$

is called nesting.

Definition 2.4. Let $d \in \mathbb{N}^*$ and σ is a permutation of the set $\{0, 1, ..., d-1\}$. The map $\psi_{d,\sigma} : r(K) \longrightarrow r(K)$ which assigns to any sequence u the sequence $\psi_{d,\sigma} u$, defined by:

$$\forall j \in \{0, 1, ..., d-1\}, \forall n \in \mathbb{N},\ \psi_{d,\sigma} u(dn + j) = u(dn + \sigma(j)), \tag{2.4}$$

is called braiding map.

Remark 2.5. The braiding map $\psi_{d,\sigma}$ is bijective and $\psi_{d,\sigma} u$ is called braiding sequence. $(see[1])$.

Definition 2.6. if $u \in S(K^{alg})$ and $P(X) \in K^{alg}[X]$ with $P(X) = \sum_{i=0}^{k} a_i X^i$ then :

$$\forall n \in \mathbb{N},\ (P(X).u)(n) = \sum_{i=0}^{k} a_i u(n + i).$$

Definition 2.7. Let $u \in r(K)$. The ideal $Ann_{K[X]}(u) = \{p(X) \in K[X] \ / \ p(X).u = 0\}$ of $K[X]$ is called canceler of u.

Definition 2.8. Let $u \in r(K)$, $t \in \mathbb{N}^*$ and $n_0 \in \mathbb{N}$.

1. We say that the sequence u is periodic with period t and numeric n_0 if and only if :

$$X^{n_0}(X^t - 1) \in Ann_{K[X]}(u), \tag{2.5}$$

in other words :

$$X^{n_0}(X^t - 1).u = 0. \tag{2.6}$$

2. We say that the sequence u is purely periodic if and only if $n_0 = 0$. If u is periodic then its smallest period is called primitive period and the smallest numeric of u is called primitive numeric.

Lemma 2.9 (Kernel lemma). *Let K be a commutative field with zero characteristic and K^{alg} its algebraic closure, T the shift map and $P(X) = \prod_{j=1}^{j=m} P_j(X)$, where $P_1(X), P_2(X), ..., P_M(X)$ are polynomials of $K^{alg}[X]$ pairwise prime. So :*

$$KerP(T) = \bigoplus_{j=1}^{j=m} KerP_j(T). \tag{2.7}$$

Lemma 2.10. *Let $u \in S(K^{alg})$. Then u is a sequence of $r(K)$ if and only if there exists $Q(X) \in K(X)$, $Q(X)$ unitary, such that $Q(X) \in Ann_{K[X]}(u)$.*

3 Main results

3.1 Determination of a polynomial characteristic of the image of a sequence of $r(K)$ by a bijective braiding map

Proposition 3.1. *Let $d \in \mathbb{N}^*$, σ be a permutation of the set $\{0, 1, ..., d-1\}$, $u \in r(K)$ and $P_u(X) = \prod_{j=1}^{m} (X - \alpha_j)^{s_j}$ a characteristic polynomial of the sequence u with $\alpha_j \in K^{alg}$. Then the polynomial $\prod_{j=1}^{m} \left(X^d - \alpha_j^d\right)^{s_j}$ is a characteristic polynomial of the braiding sequence $\psi_{d,\sigma} u$, where the α_j^d are distinct.*

Proof. Let $r \in \{0, 1, ..., d-1\}$ and $v = \psi_{d,\sigma} u$ and for all $k \in \mathbb{N}$ we pose :

$$v_r(k) = v(dk + r) = u(dk + \sigma(r)),$$

we have : $\forall p \in \mathbb{N}, T^p \in End(S(K^{alg}))$, consequently :

$$\forall w \in S(K^{alg}),\ \forall n \in \mathbb{N}, T^p(w)(n) = w(n + p).$$

Hence : $P_u(T)(u) = 0$, in other words, $u \in KerP_u(T)$ and according to the kernel lemma (2.9) we have :

$$u \in \bigoplus_{j=1}^{j=m} Ker \left(T - \alpha_j Id_{S(K^{alg})}\right)^{s_j}.$$

Thus : $\forall n \in \mathbb{N},\ u(n) = \sum_{j=1}^m P_j(n)\alpha_j^n$, where $P_j(X) \in K^{alg}[X]$ et $degP_j(X) \leq s_j - 1$. Consequently :

$$\forall k \in \mathbb{N},\ v_r(k) = \sum_{j=1}^m P_j(dk + \sigma(r))\alpha_j^{dk+\sigma(r)} = \sum_{j=1}^m Q_j(k)(\alpha_j^d)^k,$$

where $Q_j(X) \in K^{alg}[X]$ and $degQ_j(X) \leq s_j - 1$ and $\alpha_j^d \in K^{alg}$. Since $\bigcup_{j=1}^m \{(k^q \alpha_j^{dk})_{k\in\mathbb{N}}\ /\ q \in \{0, 1, ..., s_j - 1\}\}$ is a basis of $\bigoplus_{j=1}^m Ker\left(T - \alpha_j^d Id_{S(K^{alg})}\right)^{s_j}$ then $v_r \in \bigoplus_{j=1}^m Ker\left(T - \alpha_j^d Id_{S(K^{alg})}\right)^{s_j}$, that is to say $v_r \in Ker(f)$, where

$$f = \left(T - \alpha_1^d Id_{S(K^{alg})}\right)^{s_1} \circ \cdots \circ \left(T - \alpha_m^d Id_{S(K^{alg})}\right)^{s_m}.$$

We pose : $Q(X) = \prod_{j=1}^m \left(X - \alpha_j^d\right)^{s_j}$, $Q(X)$ is unitary and $Q(X) \in K[X]$ because its coefficients are expressed in terms of the coefficients of $P_u(X)$. We have : $Q(X).v_r = 0$ because $Q(T)(v_r) = 0$, therefore $v_r \in r(K)$ and $Q(X)$ is one of its characteristic polynomials of degree h with $h = \sum_{j=1}^m s_j$.
We pose :

$$R(X) = Q(X^d) = \prod_{j=1}^m \left(X^d - \alpha_j^d\right)^{s_j},$$

$R(X)$ is unitary and $R(X) \in K[X]$ with $degR(X) = hd$.
Let $Q(X) = \sum_{t=0}^h b_t X^t$ and $R(X) = \sum_{t=0}^h b_t X^{dt}$ with $b_h = 1_K$ and $n \in \mathbb{N}$ such that $n = dk + r$ where $r \in \{0, 1, ..., d-1\}$. Then :

$$\begin{aligned}
(R(X).v)(n) &= \left(X^{dh}.v\right)(n) + \sum_{t=0}^{h-1}\left(b_t X^{dt}.v\right)(n) \\
&= v(n + dh) + \sum_{t=0}^{h-1} b_t v(n + dt) \\
&= v\big(d(h + k) + r\big) + \sum_{t=0}^{h-1} b_t v\big(d(t + k) + r\big) \\
&= v_r\big(k + h\big) + \sum_{t=0}^{h-1} b_t v_r\big(k + t\big) \\
&= (Q(X).v_r)(k) = 0.
\end{aligned}$$

So : $\forall n \in \mathbb{N},\ (R(X).v)(n) = 0$. Consequently, $R(X).v = 0$ that is to say $R(X) \in Ann_{K[X]}(v)$ and $R(X)$ is a characteristic polynomial of the sequence v, in other words of the sequence $\psi_{d,\sigma} u$. □

Remark 3.2.
1. $P_u(X)$ divides $\prod_{j=1}^m \left(X^d - \alpha_j^d\right)^{s_j}$ of which the set of distinct roots is :

$$\{\alpha_j \theta^\varepsilon / (j, \varepsilon) \in \{1, ..., m\} \times \{1, ..., d\}\},\ \ with\ \ \theta^d = 1_K.$$

2. For all $j \in \{1, ..., m\}$, s_j is the order of multiplicity of the roots $\alpha_j \theta^\varepsilon$ with $\varepsilon \in \{1, ..., d\}$.

Example 3.3. let $d = 3$, $\sigma = (0, 1)$ be a permutation of the set $\{0, 1, 2\}$, $\psi_{3,\sigma}$ the bijective braiding map and $u \in r(\mathbb{R})$ such that : $\forall n \in \mathbb{N},\ u(n+2) = 3u(n+1) - 2u(n)$, $u(0), u(1)$ are given. It is clear that $P_u(X) = X^2 - 3X + 2$ is a characteristic polynomial of the sequence u.
Let $v = \psi_{d,\sigma}u$ and $P_v(X)$ be a characteristic polynomial of the sequence v obtained from the polynomial $P_u(X)$ whose roots are $1, 2$. Therefore $P_v(X) = (X^3-1)(X^3-2^3) = X^6-9X^3+8$ and we have :

$$\forall n \in \mathbb{N},\ v(n+6) = 9v(n+3) - 8v(n), \tag{3.1}$$

where :

$$\begin{aligned} v(0) &= u(1),\ \ v(1) = u(0), \\ v(2) &= 3u(1) - 2u(0),\ \ v(3) = 15u(1) - 14u(0), \\ v(4) &= 7u(1) - 6u(0),\ \ v(5) = 31u(1) - 30u(0). \end{aligned}$$

Let's calculate $v(6)$. On the one hand, by using the equality (3.1), we find :

$$v(6) = 9v(3) - 8v(0) = 127u(1) - 126u(0),$$

And in the other hand, by the definition(2.4) we find :

$$v(6) = u(6 + \sigma(0)) = u(7) = 127u(1) - 126u(0).$$

Proposition 3.4. *Let $d \in \mathbb{N}^*$, σ be a permutation of the set $\{0, 1, ..., d-1\}$, $u \in r(K)$, $P_u(X) = \prod_{j=1}^{m}(X - \alpha_j)^{s_j}$ a characteristic polynomial of the sequence u, where $j \in \{1, 2, ..., m\}$, $\alpha_j \in K^{alg}$ and $M(X) = PPCM\Big((X-\alpha_1^d)^{s_1}, (X-\alpha_2^d)^{s_2}, ..., (X-\alpha_m^d)^{s_m}\Big)$. Then $M(X^d)$ is a characteristic polynomial of the braiding sequence $\psi_{d,\sigma}u$.*

Proof.
- Suppose that α_1^d, α_2^d,..., α_m^d are distinct. Then, on the one hand , according to the proposition(3.1), $\prod_{j=1}^{m}\left(X^d - \alpha_j^d\right)^{s_j}$ is a characteristic polynomial of the braiding sequence $\psi_{d,\sigma}u$ and on the other hand, we have $M(X) = \prod_{j=1}^{m}\left(X - \alpha_j^d\right)^{s_j}$. Consequently :

$$M(X^d) = \prod_{j=1}^{m}\left(X^d - \alpha_j^d\right)^{s_j}.$$

Thus $M(X^d)$ is a characteristic polynomial of the braiding sequence $\psi_{d,\sigma}u$.
- Suppose that α_1^d, α_2^d,..., α_m^d are not distinct. We pose : $v = \psi_{d,\sigma}u$, $M(X) = \prod_{j=1}^{p}\left(X - \alpha_{i_j}^d\right)^{s_{i_j}}$ with $\alpha_{i_1}^d$, $\alpha_{i_2}^d$,..., $\alpha_{i_p}^d$ are distinct, so we have :

$$\forall \alpha \in \{\alpha_1, \alpha_2, ..., \alpha_m\} - \{\alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_p}\}, \exists \mu \in \{1, 2, ..., p\} : \alpha^d = \alpha_{i_\mu}^d.$$

Let $r \in \{0, 1, ..., d-1\}$. For all $k \in \mathbb{N}$, we pose : $v_r(k) = v(dk + r) = u(dk + \sigma(r))$, and according to the proposition(3.1) we have :

$$\forall n \in \mathbb{N} : u(n) = \sum_{j=1}^{m} P_j(n)\alpha_j^n,$$

where $P_j(X) \in K^{alg}[X]$ and $degP_j(X) \leq s_j - 1$, consequently :

$$\forall k \in \mathbb{N},\ v_r(k) = \sum_{j=1}^{m} P_j(dk + \sigma(r))\alpha_j^{dk+\sigma(r)} = \sum_{j=1}^{p} Q_{i_j}(k)\left(\alpha_{i_j}^d\right)^k,$$

where $Q_{i_j}(X) \in K^{alg}[X]$ with $degQ_{i_j}(X) \leq s_{i_j} - 1$ and $\alpha_{i_1}^d$, $\alpha_{i_2}^d$,..., $\alpha_{i_p}^d$ are in the field K^{alg}.
Since $\bigcup_{j=1}^{p}\{(k^q\alpha_{i_j}^{dk})_{k\in\mathbb{N}}/q \in \{0, 1, ..., s_{i_j} - 1\}\}$ is a basis of $\bigoplus_{j=1}^{j=p} Ker\left(T - \alpha_{i_j}^d Id_{S(K^{alg})}\right)^{s_{i_j}}$, then

$$v_r \in \bigoplus_{j=1}^{j=p} Ker\left(T - \alpha_{i_j}^d Id_{S(K^{alg})}\right)^{s_{i_j}},$$

and according to the kernel Lemma (2.9), we have $v_r \in Ker(f)$, where :

$$f = \left(T - \alpha_{i_1}^d Id_{S(K^{alg})}\right)^{s_{i_1}} \circ \cdots \circ \left(T - \alpha_{i_p}^d Id_{S(K^{alg})}\right)^{s_{i_p}}.$$

Therefore $f(v_r) = 0$, thus $M(X).v_r = 0$. Consequently, $M(X)$ is a characteristic polynomial of the sequence v_r.
Finally, by the same steps used in the proposition (3.1)), we show that $M(X^d)$ is a characteristic polynomial of the braiding sequence $\psi_{d,\sigma}u$. □

Remark 3.5. $P_u(X)$ divise $\prod_{j=1}^{p}\left(X^d - \alpha_{i_j}^d\right)^{s_{i_j}}$.

Example 3.6. let $d = 4$, $\sigma = (0, 1, 2)$ be a permutation of the set $\{0, 1, 2, 3\}$, $u \in r(\mathbb{C})$ such that $u(0), u(1), u(2)$ and $u(3)$ are given, and:

$$\forall n \in \mathbb{N},\ u(n+4) - 3u(n+2) - 4u(n) = 0,$$

We pose $v = \psi_{4,\sigma}u$. We have $P_u(X) = (X-2)(X+2)(X-i)(X+i)$. Since $2^4 = (-2)^4 = 16$, $i^4 = (-i)^4 = 1$, then $M(X) = X^2 - 17X + 16$, consequently, $X^8 - 17X^4 + 16$ is a characteristic polynomial of the braiding sequence $\psi_{d,\sigma}u$, we have :

$$\forall n \in \mathbb{N} : v(n+8) = 17v(n+4) - 16v(n), \tag{3.2}$$

where :

$$\begin{aligned} v(0) &= u(1),\ \ v(1) = u(2),\ \ v(2) = u(0),\ \ v(3) = u(3), \\ v(4) &= 3u(3) + 4u(1),\ \ v(5) = 3u(4) + 4u(2), \\ v(6) &= 3u(2) + 4u(0),\ \ v(7) = 13u(3) + 12u(1). \end{aligned}$$

Let's calculate $v(8)$.
By the equality (3.2), we find : $v(8) = 17v(4) - 16v(0)$.
And by the definition (2.4), we find : $v(8) = u(9) = 51u(3) + 52u(1) = 17v(4) - 16v(0)$.

3.2 Minimum characteristic polynomial of a sequence of $r(K)$

Proposition 3.7. *Let $u \in r(X)$ and $P_M(X)$ be the minimal characteristic polynomial of the sequence u. Then, we have :*
1. $Ann_{K[X]}(u) = \langle P_M(X)\rangle$.
2. If $f(X) \in Ann_{K[X]}(u)$, $u \neq 0$ and $f(X)$ unitary such that $f(X)$ is irreducible, then $f(X) = P_M(X)$.

Proof.
1. If $u = 0$ the equality (3.7) is true.
Suppose that $u \neq 0$. Since $P_M(X) \in Ann_{K[X]}(u)$, then we have :

$$Ann_{K[X]}(u) \supseteq \langle P_M(X)\rangle, \tag{3.3}$$

Let $f(X) \in Ann_{K[X]}(u)$. There exists $(Q(X), R(X)) \in K[X]^2$ such that :

$$f(X) = Q(X)P_M(X) + R(X),$$

with $degR(X) < degP_M(X)$. Since $R(X).u = 0$, $u \neq 0$ and $P_M(X)$ is the minimum characteristic polynomial of the sequence u, then $R(X) = 0$. Consequently, $f(X) \in \langle P_M(X)\rangle$ and therefore :

$$Ann_{K[X]}(u) \subseteq \langle P_M(X)\rangle, \tag{3.4}$$

From (3.3) and (3.4), we conclude that $Ann_{K[X]}(u) = \langle P_M(X)\rangle$.

2. If $f(X) \in Ann_{K[X]}(u)$ then $P_M(X)$ divides $f(X)$ and since $f(X)$ is irreducible in $K[X]$ and $u \neq 0$ then there exists $\lambda \in K^*$ such that $f(X) = \lambda P_M(X)$. As $f(X)$ and $P_M(X)$ are unitary, then we conclude that $f(X) = P_M(X)$. □

Example 3.8. Let $u \in r(\mathbb{R})$ such that :

$$\forall n \in \mathbb{N},\ u(n+2) + u(n+1) + u(n) = 0, u(0) = 1, u(1) = 2.$$

It is clear that $X^2 + X + 1$ is a characteristic polynomial of the sequence u and that it is irreducible in $\mathbb{R}[X]$. Then $X^2 + X + 1$ is the minimum characteristic polynomial of the sequence u.

3.3 Periodicity of a sequence of the rational K-Hadamard algebra $(r(K), +, ., \otimes)$

Reminder: Let $u \in r(K)$, $t \in \mathbb{N}^*$ and $n_0 \in \mathbb{N}$. We say that the sequence u is periodic with period t and numeric n_0 if and only if :

$$\forall n \in \mathbb{N} - \{0, 1, ..., n_0 - 1\},\ u(n+t) = u(n).$$

We say that the sequence u is purely periodic if and only if $n_0 = 0$.

Example 3.9. Let $u \in r(\mathbb{R})$ such that :

$$\forall n \in \mathbb{N},\ u(n+2) + u(n+1) + u(n) = 0.$$

We have : $Ann_{\mathbb{R}[X]}(u) = \langle X^2 + X + 1 \rangle$, where $X^2 + X + 1$ is the characteristic polynomial minimal of the sequence u.
Since $X^3 - 1 \in Ann_{\mathbb{R}[X]}(u)$ because $X^2 + X + 1$ divides $X^3 - 1$ then $(t, n_0) = (3, 0)$. Therefore u is purely periodic with period 3.

Characterization of periodic sequences of $r(K)$

Proposition 3.10. *Let $u \in r(K)$, u non-stationary, $n_0 \in \mathbb{N}$, $t \in \mathbb{N}^*$ and $P_M(X)$ the minimum characteristic polynomial of the sequence u.*
1. If u is periodic with period t and numeric n_0 then each non-zero root of $P_M(X)$ is simple and of finite order in the multiplicative group $K^{alg} - \{0_K\}$.
2. If each non-zero root of $P_M(X)$ is simple and of finite order in the multiplicative group $K^{alg} - \{0_K\}$ then there exists $(s_0, t_0) \in \mathbb{N} \times \mathbb{N}^*$ such that u is periodic with period t_0 and numeric s_0.

Proof.
1. Suppose that u is periodic of period t and numeric n_0. Then we have :

$$X^{n_0}(X^t - 1) \in Ann_{K[X]}(u),$$

consequently, $P_M(X)$ divides $X^{n_0}(X^t - 1)$. Since, on the one hand, $X^t - 1$ admits t simple roots in $K^{alg} - \{0_K\}$ then the non-zero roots of $P_M(X)$ are simple and on the other hand, the set of roots of the polynomial $X^t - 1$ provided with multiplication is a cyclic subgroup of order t of the group $K^{alg} - \{0_K\}$. So, the order of each non-zero root of $P_M(X)$ divides t, in other words each non-zero root of $P_M(X)$ is of finite order.
2. Let D^* be the set of non-zero roots of $P_M(X)$ and suppose that each of them is simple and of finite order in the group $K^{alg} - \{0_K\}$. We pose $t_0 = ppcm(o(x))_{x \in D^*}$.
- If $P_M(0_K) \neq 0_K$ then :

$$\forall \alpha \in D^*,\ \alpha^{t_0} - 1 = 0_K.$$

Hence $P_M(X)$ divides $X^{t_0} - 1$ which means that $X^{t_0} - 1 \in Ann_{K[X]}(u)$. Consequently, u is periodic with period t_0 and numeric 0. $(s_0 = 0)$
- If $P_M(0_K) = 0_K$ then $P_M(X)$ divides $X^{s_0}(X^{t_0} - 1)$, where s_0 is the order of multiplicity of the root 0_K. Consequently u is periodic with period t_0 and numeric s_0. □

Remark 3.11. Part 1 of the proposition (3.10) shows a necessary condition for a sequence of $r(K)$ to be periodic and part 2 shows a sufficient condition.

Example 3.12. Let $u \in r(\mathbb{R})$ such that :

$$\forall n \in \mathbb{N},\ u(n+4) + u(n+3) + 2u(n+2) + u(n+1) + u(n) = 0,$$

with $u(3) = -2$, $u(2) = 2$, $u(1) = -1$, $u(0) = 1$. It is clear that

$$P_M(X) = (X^2 + 1)(X^2 + X + 1).$$

The roots of $P_M(X)$ in $\mathbb{C}$ are : $i, -i, j, j^2$ which are simple and not zero then, according to the proposition (3.10) part 2, the sequence u is purely periodic with period t_0 such that :

$$t_0 = ppcm(o(i), o(-i), o(j), o(j^2)) = 12, \quad \text{where } j \in \mathbb{C}, \text{and } j^3 = 1.$$

Indeed : $(X-1)(X^3+1)(X^4-X^2+1)P_M(X) = X^{12} - 1$ by sequence $X^{12} - 1 \in Ann_{\mathbb{R}[X]}(u)$, this means that the sequence u is purely periodic with period 12.

Determination of the primitive period and the primitive numeric of a periodic sequence of $r(K)$

Proposition 3.13. *Let $u \in r(K)$, u be non-stationary, such that u is periodic with period t and numeric n_0, t_0 its primitive period, s_0 its primitive digital, D the set of roots of the minimal characteristic polynomial $P_M(X)$ in the commutative field K^{alg}.*
1. If $0_K \notin D$, then $t_0 = ppcm_{x\in D}(o(x))$ and $s_0 = 0$, where $o(x)$ is the order of x.
2. If $0_K \in D$, then $t_0 = ppcm_{x\in D-\{0_K\}}(o(x))$ and s_0 is the order of multiplicity of the root 0_K.

Proof.
1. Suppose $0_K \notin D$. The roots of $P_u(X)$ are non-zero, simple and of finite order in the group $K^{alg} - \{0_K\}$, therefore, for all $x \in D$, $o(x)$ divides the number t. By posing $t_1 = ppcm_{x\in D}(o(x))$,
we have : t_1 divide the number t and for all $x \in D$, $x^{t_1} - 1 = 0_K$ this means that $P_M(X)$ divided $x^{t_1} - 1$ and therefore $X^{t_1} - 1 \in Ann_{K[X]}(u)$. So, t_1 is the smallest period of u and 0 is the primitive numeric of u, in other words $t_0 = t_1 = ppcm_{x\in D}(o(x))$ and $s_0 = 0$.
2. Suppose $0_K \in D$. Since u is non-stationary, then $D - \{0_K\} \neq \phi$ and for all $x \in D - \{0_K\}$, $o(x)$ divides the number t because $P_M(X)$ divides $X^{n_0}(X^t - 1)$.
By posing $t_2 = ppcm_{x\in D-\{0_K\}}(o(x))$, we have t_2 divide the number t on the other hand :

$$P_M(X) = X^{m_0} \prod_{x\in D-\{0_K\}} (X - x),$$

where m_0 is the order of multiplicity of the root 0_K. So, $P_M(X)$ divides $X^{m_0}(X^{t_2}-1)$, therefore, $X^{m_0}(X^{t_2} - 1) \in Ann_{K[X]}(u)$, that is to say t_2 is the smallest period of u, thus :

$$t_0 = t_2 = ppcm_{x\in D-\{0_K\}}(o(x)).$$

Since $P_M(X)$ divides $X^{n_0}(X^t - 1)$ and X^{m_0} is prime with $X^t - 1$, then X^{m_0} divides X^{n_0}.
So, $m_0 \leq n_0$ which means that m_0 is the numeric primitive of u, therefore : $s_0 = m_0$, and in other words, s_0 is the order of multiplicity of the root 0_K. □

Remark 3.14.
- If $P_M(0_K) \neq 0_K$, then $s_0 = 0$ and t_0 is the smallest divisor of t such that $P_M(X)$ divides $X^{t_0} - 1$.
- If $P_M(0_K) = 0_K$, then s_0 is the order of multiplicity of 0_K and t_0 is the smallest divisor of t such that $Q(X)$ divides $X^{t_0} - 1$, where $Q(X)$ is the quotient of $P_M(X)$ by X^{s_0}.

Example 3.15. Let $u \in r(\mathbb{C})$ such that :

$$\forall n \in \mathbb{N},\ u(n+3) = (\sqrt{2} + i)u(n+2) - (1 + i\sqrt{2})u(n+1) + iu(n),$$

where $u(0) = 1$, $u(1) = 1 + i$, $u(2) = -1$.
We have $P_M(X) = X^3 - (\sqrt{2} + i)X^2 + (1 + i\sqrt{2})X - i$. $P_M(X)$ admits in $\mathbb{C}$ three non-zero, simple roots which are : i, $\frac{\sqrt{2}}{2}(1 + i)$, $\frac{\sqrt{2}}{2}(1 - i)$, such that:

$$o(i) = 4,\ o\left(\frac{\sqrt{2}}{2}(1+i)\right) = o\left(\frac{\sqrt{2}}{2}(1-i)\right) = 8.$$

So, u is purely periodic with primitive period 8.

Example 3.16. Let $u \in r(\mathbb{R})$, such that : $\forall n \in \mathbb{N},\ u(n+4) + u(n+3) + u(n+2) = 0$, with $u(0) = 1$, $u(1) = 2$, $u(2) = -3$, $u(3) = -1$.
We verify that the sequence u is periodic with primitive period 3 and primitive numeric 2.

3.4 Periodicity and muneric of a braiding sequence

Proposition 3.17. *Let $d \in \mathbb{N}^*$, σ be a permutation of the set $\{0, 1, ..., d-1\}$, $\psi_{d,\sigma}$ the bijective braiding map and $u \in r(K)$. If u is periodic with period t and numeric n_0, then the braiding sequence $\psi_{d,\sigma}u$ is periodic with period $ppcm(t, d)$ and numeric dn_0.*

Proof. We pose $v = \psi_{d,\sigma}$. By hypothesis, we have :

$$\forall n \in \mathbb{N},\ u(n + n_0 + t) = u(n + n_0).$$

We pose $M = ppcm(t, d)$. So, there exists $(\alpha, \beta) \in \mathbb{N}^2$ such that, $M = t\beta = d\alpha$.
Let $n \in \mathbb{N}$. The Euclidean division of n by d gives the existence of $(q, r) \in \mathbb{N}^2$, such that $n + dn_0 = dq + r$.
Consequently : $n + dn_0 + M = d(q + \alpha) + r\ \ with\ \ r \in \{0, 1, ..., d - 1\}$. So :

$$\begin{aligned} v(n + dn_0 + M) &= u(d(q + \alpha) + \sigma(r)) \\ &= u(dq + \beta t + \sigma(r)) \\ &= u(dq + \sigma(r)) \\ &= v(n + dn_0), \end{aligned}$$

therefore : $\forall n \in \mathbb{N},\ v(n + dn_0 + M) = v(n + dn_0)$.
In other words, we have : $\forall n \geq dn_0,\ v(n + M) = v(n)$, this means that the sequence v is periodic with period M and numeric dn_0. In other words, the sequence $\psi_{d,\sigma}u$ is periodic with period $ppcm(t, d)$ and numeric dn_0. □

Example 3.18. Let $u \in r(\mathbb{R})$, such that : $\forall n \in \mathbb{N},\ u(n + 4) + u(n + 2) + u(n) = 0$ with $u(0) = 1$, $u(1) = -1$, $u(2) = 2$, $u(3) = -2$.
The minimal characteristic polynomial $P_M(X)$ of the sequence u is given by :
$P_M(X) = X^4 + X^2 + 1$, which admits in $\mathbb{C}$ four distinct non-zero roots, These roots are j, j^2, $-j$, $-j^2$, where $j = \frac{-1+i\sqrt{3}}{2}$ and $o(j) = o(j^2) = 3$ and $o(-j) = o(-j^2) = 6$ in the multiplicative group $\mathbb{C}^*$. So, the sequence u is periodic with period 6 and numeric 0.
Let $d = 3$ and $\sigma = (0, 1, 2)$, σ is a permutation of the set $\{0, 1, 2\}$, $\psi_{3,\sigma}$ the bijective braiding map. According to the previous proposition (3.13), the sequence $\psi_{3,\sigma}u$ is periodic with period 6 and numeric 0.
Indeed : one of the characteristic polynomials of the sequence $\psi_{3,\sigma}u$ is the polynomial $X^6 - 1$. Therefore : $\forall n \in \mathbb{N},\ \psi_{3,\sigma}u(n + 6) = \psi_{3,\sigma}u(n)$, this shows that 6 is a period of $\psi_{3,\sigma}u$ and the primitive numeric of $\psi_{3,\sigma}u$ is 0.
Let t_0 be the primitive period of the sequence $\psi_{3,\sigma}u$. The minimum characteristic polynomial of $\psi_{3,\sigma}u$ is $(X+1)P_M(X)$, since t_0 is the smallest divisor of 6 such that $X^{t_0} - 1 \in Ann_{\mathbb{R}[X]}(\psi_{3,\sigma}u)$, then $t_0 = 6$ and the primitive numeric of $\psi_{3,\sigma}u$ is 0.

Example 3.19. Let $j = \frac{-1+i\sqrt{3}}{2}$ and $u \in r(\mathbb{C})$, such that : $\forall n \in \mathbb{N}, u(n + 4) + j^2u(n + 2) = 0$ with $u(0) = 1$, $u(1) = -1$, $u(2) = 2$, $u(3) = -2$.
The sequence u is periodic with primitive period 12 and primitive numeric 3. Let $d = 3$ and $\sigma = (2, 1, 0)$, σ is a permutation of the set $\{0, 1, 2\}$, the sequence $\psi_{3,\sigma}u$ is periodic with period 12 and numeric 6, its primitive period 12, its primitive numeric is 3.

4 Conclusion remarks

In this work, we have investigated certain properties of braided linear recurrent sequences, focusing in particular on the determination of their characteristic polynomial and the analysis of their periodicity. This study was based on the orders of the roots of their minimal characteristic polynomials, which divide the associated characteristic polynomials.

References

[1] A. Ait Mokhtar, A. Necer, A. Salinier, Endomorphismes d'algèbres de suites, Journal de Théorie des Nombres de Bordeaux 20 (2008), 1-21.

[2] A. Ait Mokhtar, Quelques propriétés sur les suites récurrentes linéaires à coecients polynomiaux, thèse de Magister, Université des Sciences et de la Technologie Houari Boumédiene (1989).

[3] A. Ait Mokhtar, Endomorphismes d'algèbres de suites, thèse de doctorat, Université de Limoges (2008).

[4] A. Necer, Suites récurrentes linéaires et séries formelles en plusieurs variables, thèse de doctorat, Université de Limoges (1998).

[5] M. F. Atiyah and I. G. MacDonald, Introduction to commutative algebra. Addison-Wesley Publishing Campagny, 1969.

[6] B. Benzaghou, Algèbre de Hadamard, Bull. Soc. Math. France, t. 98, 1970, p .209-252.

[7] S. Badidja, A. Ait Mokhtar, O. Özer, Representation of integers by k-generalized Fibonacci sequences and applications in cryptography, Asian-Eur. J. Math. 14(9), Article ID 2150157, (2021), 11 p.

[8] S. Kiouche and A. Ait Mokhtar, SOME PROPERTIES OF LINEAR RECURRENCE SEQUENCES BRAIDING AND APPLICATION IN CRYPTOGRAPHY, Palestine Journal of Mathematics. Vol 14(1)(2025) , 381–394, https://pjm.ppu.edu/paper/1992-some-properties-linear-recurrence-sequences-braiding-and-application-cryptography.

[9] A. Ait Mokhtar, Théorie des nombres Suites récurrentes linéaires: terme général et idempotents Linear recurrence sequences: General term and idempotents, Comptes Rendus. Mathématique, Volume 350 (2012) no. 7-8, pp. 339-342. doi:10.1016/j.crma.2012.03.004.

[10] A. Necer, Systèmes récursifs et algèbre de Hadamard de suites récurrentes linéaires sur des anneaux commutatifs, Communications in Algebra 27 (12) (1999) 6175–6189.

[11] U. Cerruti, F. Vaccarino, R-Algebras of Linear Recurrent Sequences, Journal of Algebra, Volume 175, Issue 1, 1995, Pages 332-338, ISSN 0021-8693, https://doi.org/10.1006/jabr.1995.1189.

[12] Yashwant K. Panwar, Bijendra Singh and V. K. Gupta, Generalized Fibonacci Sequences and Its Properties, Palestine Journal of Mathematics, Vol. 3(1) (2014) , 141–147.

Author information

Hocine AIT MOHAMMED, Laboratory of Fixed Point and Applications, Height Normal School Kouba, Algiers, BP 92., Algeria.
E-mail: houcine.aitmohamed43@g.ens-kouba.dz

Ahmed AIT MOKHTAR, Laboratory of Fixed Point and Applications, Height Normal School Kouba, Algiers, BP 92., Algeria.
E-mail: ahmed.aitmokhtar@g.ens-kouba.dz

Received: 2024-12-23
Accepted: 2025-06-24