Palestine Journal of Mathematics

Vol.15(3), (2026) , 522–531 © Palestine Polytechnic University-PPU 2026

Characteristic Polynomial and Period of a Linear Recurrent Sequence Braiding on an A-Module

T. Zerkaoui and A. Ait Mokhtar

Communicated by Ayman Badawi

MSC 2020 Classifications: Primary 11B39; Secondary 11B37, 13P15.

Keywords and phrases: Linear recurrence sequence, A-module, braiding sequence, periodicity of braiding 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: T. Zerkaoui

Abstract. In this paper, we investigate the algebraic behavior of composite braiding mappings acting on linear recurrence sequences (LRS) over A-modules, where A is a unital commutative ring. Although individual braiding maps $\psi_{d,J,\delta}$ are known to preserve recognizability and recurrence properties, the algebraic structures that arise from their compositions have not been fully described. Prior studies in the Palestine Journal of Mathematics have explored related algebraic and recurrence phenomena, including structural properties of recurrence sequences with braiding [1], analyses of characteristic polynomials and periods under braiding on fields [2], and investigations of specific linear recurrence sequences with matrix and binomial structures [3].

We prove that convolution by polynomials of the form $p(X^{D_n})$ commutes with composite braiding maps

$$\Psi_n = \psi_{d_n,J_n,\delta_n} \circ \cdots \circ \psi_{d_1,J_1,\delta_1}$$

and that such maps preserve both recurrence relations and periodicity of sequences. Several potential applications, particularly in the design of periodic sequences for algebraic coding and cryptographic constructions, are also discussed.

After recalling the necessary definitions and key properties of braiding sequences, we characterize the characteristic polynomials associated with compositions of braiding mappings acting on sequences with values in an A-module.

Furthermore, we generalize a result from [1] by extending known periodicity characterizations for braiding sequences originally stated for fields of characteristic zero to arbitrary shifts and sequences over general A-modules.

1 Introduction

Let A be a unital commutative ring, M an A-module, and let $S(M)$ denote the A-module of sequences over M, i.e., functions from $\mathbb{N}$ to M. A sequence $u = (u(n))_{n\geq 0}$ is called a *linear recurrent sequence* if it satisfies a linear recurrence relation with constant coefficients. Such sequences play a central role in number theory, combinatorics, algebra, and coding theory, where characteristic polynomials describe their structure and solution spaces.

The algebraic behavior of linear recurrent sequences under various operations has been widely studied. Alecci, Barbero, and Murru showed that the set of all linear recurrent sequences, endowed with termwise sum and convolution-type products (binomial/Hurwitz and multinomial/Newton), forms an R-algebra and provided explicit characteristic polynomials for these products [4]. Birmajer, Gil, and Weiner analyzed convolutions via Bell polynomials and derived recurrence relations for the resulting sequences [6]. Classical and modern treatments of convolution formulas and generating function methods further clarify the interaction between recurrence relations and sequence transformations [7].

Within this framework, braiding mappings of the form $\psi_{d,J,\delta}$ have been introduced as structured transformations rearranging subsequences through index permutations and shifts, while preserving recurrence properties under suitable conditions. Foundational contributions include Ait Mokhtar's work on semi-affine applications and braidings of sequences [8], and the study of sequence algebra endomorphisms by Ait Mokhtar, Necer, and Salinier [9].

However, the literature mainly addresses individual braiding operators. In this paper, we study the algebraic effects of *composite braiding mappings*

$$\Psi_n = \psi_{d_n,J_n,\delta_n} \circ \cdots \circ \psi_{d_1,J_1,\delta_1},$$

and analyze their action on linear recurrent sequences over A-modules. We prove that recurrence is preserved under suitable transformations of characteristic polynomials and that convolution by polynomials of the form $p(X^{D_n})$ commutes with such compositions. This provides a systematic extension of braiding theory from single operators to iterated mappings, with applications to recurrence preservation and periodic behavior.

2 Preliminary Results

In this section,

Definition 2.1 ([8]). Let A be a commutative unital ring and M an A-module. The map

$$T : S(M) \to S(M), \quad (Tu)(n) = u(n+1), \quad \forall n \in \mathbb{N},$$

is called the *shift* .

Definition 2.2 (see [9]). Let A be a commutative unital ring, and let M be an A-module. We define an external action $(*)$ of the ring $A[X]$ on the set of sequences $S(M)$ as follows:

For any polynomial $P(X) = \sum_{i=0}^{h} a_i X^i \in A[X]$ and any sequence $u \in S(M)$, we define:

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

Equivalently, this can be written as:

$$P(X) * u = P(T)(u).$$

Remark 2.3. This external action turns $S(M)$ into an $A[X]$-module. The annihilator of a sequence $u \in S(M)$, denoted by $\mathrm{Ann}_{A[X]}(u)$, is defined as:

$$\mathrm{Ann}_{A[X]}(u) = \left\{ P(X) \in A[X] \,\middle|\, P(X) * u = 0_{S(M)} \right\}.$$

Definition 2.4. Let M be an A-module and $u \in S(M)$. We say that u is a *linear recurrence sequence with constant coefficients in* A if and only if its annihilator ideal $\mathrm{Ann}_{A[X]}(u)$ contains a monic polynomial. This ideal is called the *characteristic ideal* of the sequence u, and its monic elements are called the *characteristic polynomials* of u.

Notations.

- The set of all linear recurrence sequences with coefficients in A and values in M is denoted by $\mathrm{r}(A; M)$.
- If $M = A$, then we write $\mathrm{r}(A)$ instead of $\mathrm{r}(A; M)$.
- The set of all such sequences with characteristic polynomial $P(X)$ is denoted by $\mathrm{r}_{P(X)}(A; M)$.
- If $M = A$, we write $\mathrm{r}_{P(X)}(A)$ instead of $\mathrm{r}_{P(X)}(A; M)$.
- The set of polynomials over A of degree less than or equal to m is denoted by $A_m[X]$.

- The finite set $\{1, 2, \ldots, m\}$ is denoted by $\mathbb{N}_m$.

Definition 2.5 ([9]). Let $d \in \mathbb{N}^*$, $I = \{0, \ldots, d-1\}$, $J = (j_0, j_1, \ldots, j_{d-1}) \in \mathbb{N}^d$, and let σ be a permutation of the set I. Following the classical case where M is a field (for the more general ring case, see [8, 1]), we define the following maps:

$$\begin{aligned}
\theta_d &: S(M) \longrightarrow S(M),\\
\Delta_d &: S(M) \longrightarrow S(M)^d,\\
E_d &: S(M)^d \longrightarrow S(M),\\
\Sigma_\sigma &: S(M)^d \longrightarrow S(M)^d,\\
T_J &: S(M)^d \longrightarrow S(M)^d,
\end{aligned}$$

defined by:

(a) For all $u \in S(M)$ and $n \in \mathbb{N}$, we set $\theta_d(u)(n) = u(dn)$.

(b) For all $u \in S(M)$, we define $\Delta_d(u) = (\theta_d(u), \theta_d \circ T(u), \ldots, \theta_d \circ T^{d-1}(u))$.

(c) For all $(u_0, \ldots, u_{d-1}) \in S(M)^d$, all $j \in J$, and all $n \in \mathbb{N}$, we define:

$$E_d(u_0, \ldots, u_{d-1})(dn + j) = u_j(n).$$

(d) $\Sigma_\sigma(u_0, u_1, \ldots, u_{d-1}) = (u_{\sigma(0)}, u_{\sigma(1)}, \ldots, u_{\sigma(d-1)})$.

(e) $T_J(u_0, \ldots, u_{d-1}) = (T^{j_0}u_0, T^{j_1}u_1, \ldots, T^{j_{d-1}}u_{d-1})$.

These maps are morphisms of A-modules, with $\Delta_d^{-1} = E_d$. Moreover, if M is an A-algebra, then these maps are morphisms of A-algebras with respect to the Hadamard (pointwise) product. Several properties of these maps over commutative unital rings can be found in [5], and their generalization to modules over commutative rings is straightforward.

Definition 2.6. The application $E_d \circ \Sigma_\sigma \circ T_J \circ \Delta_d$, denoted by $\psi_{d,J,\sigma}$, is called a *braiding mapping*.

Proposition 2.7 ([9]). *Let A be a commutative unital ring, M an A-module, and $d \in \mathbb{N}^*$. Then:*

(i) For every $(u_0, \ldots, u_{d-1}) \in S(M)^d$,

$$X * E_d(u_0, \ldots, u_{d-1}) = E_d(u_1, \ldots, u_{d-1}, X * u_0).$$

(ii) For every $(u_0, \ldots, u_{d-1}) \in S(M)^d$ and any polynomial $p(X) \in A[X]$,

$$p(X^d) * E_d(u_0, \ldots, u_{d-1}) = E_d\big(p(X) * u_0, \ldots, p(X) * u_{d-1}\big).$$

Proposition 2.8. *[8] A braiding $\psi_{d,J,\sigma}$ is an automorphism of $\mathrm{r}(K)$ if and only if $J = (0, \ldots, 0)$.*

Lemma 2.9. *[8] Let $D = de$ for some integer $e \geq 1$. Then there exists a permutation τ of $\{0, \ldots, D-1\}$ such that the bijective braidings $\psi_{d,(0,\ldots,0),\sigma}$ and $\psi_{D,(0,\ldots,0),\tau}$ coincide.*

Proposition 2.10. *[8] The set of bijective braidings forms a subgroup of the group of bicontinuous automorphisms of the rational Hadamard algebra.*

3 Main Results

Corollary 3.1. *Let A be a commutative unital ring, M an A-module, $d \in \mathbb{N}^*$, and $u \in S(M)$. Then for all $p(X) \in A[X]$ and all $(m, j) \in \mathbb{N}^2$, we have:*

$$p(X) * \left(\theta_d^j \circ T^m\right)(u) = \left(\theta_d^j \circ T^m\right)\left(p(X^{d^j}) * u\right).$$

Proof. Let $p(X) = \sum_{i=0}^{\ell} a_i X^i \in A[X]$. Then:

$$p(X) * (\theta_d^j \circ T^m)(u) = \sum_{i=0}^{\ell} a_i T^i \left((\theta_d^j \circ T^m)(u) \right) = \sum_{i=0}^{\ell} a_i \left((T^i \circ \theta_d^j \circ T^m)(u) \right).$$

Using the equality [8]: $T^i \circ \theta_d^j = \theta_d^j \circ T^{id^j}$, we obtain:

$$\sum_{i=0}^{\ell} a_i \theta_d^j \circ T^{id^j+m}(u) = \theta_d^j \circ T^m \left(\sum_{i=0}^{\ell} a_i T^{id^j}(u) \right) = \left(\theta_d^j \circ T^m \right) (p(X^{d^j}) * u).$$

□

Lemma 3.2. *Let A be a commutative unital ring, M an A-module, and $d \in \mathbb{N}^*$. Let δ be a permutation of $\{0, 1, \ldots, d-1\}$, let $J = (j_i)_{0 \le i < d} \in \mathbb{N}^d$, and let $u \in S(M)$. Then:*

(i) We have

$$\forall n \in \mathbb{N}, \quad \psi_{d,J,\delta}(u)(n) = E_d\Big(\big(\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)}(u) \big)_{0 \le i < d} \Big).$$

(ii) $\forall n \in \mathbb{N}$, *If $n = dq + r$ with $0 \le r < d$, then*

$$\psi_{d,J,\delta}(u)(n) = u\big(dq + dJ_{\delta(r)} + \delta(r)\big).$$

(iii) Define the function φ by:

$$\forall n \in \mathbb{N}, \quad \varphi(n) = d \left\lfloor \frac{n}{d} \right\rfloor + dJ_{\delta(n \bmod d)} + \delta(n \bmod d).$$

Then $\psi_{d,J,\delta}(u) = u \circ \varphi$.

Proof. Recall that

$$\Delta_d(u) = \big(\theta_d(u),\ \theta_d \circ T(u),\ \ldots,\ \theta_d \circ T^{d-1}(u) \big).$$

Hence

$$(T_J \circ \Delta_d)(u) = \big(T^{J_0} \circ \theta_d(u),\ T^{J_1} \circ \theta_d \circ T(u),\ \ldots,\ T^{J_{d-1}} \circ \theta_d \circ T^{d-1}(u) \big).$$

Applying Σ_δ, we obtain

$$(\Sigma_\delta \circ T_J \circ \Delta_d)(u) = \big(T^{J_{\delta(0)}} \circ \theta_d \circ T^{\delta(0)}(u),\ \ldots,\ T^{J_{\delta(d-1)}} \circ \theta_d \circ T^{\delta(d-1)}(u) \big).$$

By Corollary 3.1,

$$T^{J_{\delta(i)}} \circ \theta_d \circ T^{\delta(i)} = \theta_d \circ T^{dJ_{\delta(i)}+\delta(i)},$$

and therefore

$$\psi_{d,J,\delta}(u)(n) = E_d\Big(\big(\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)}(u) \big)_{0 \le i < d} \Big),$$

which proves (1).

Let $n = dq + r$ with $0 \le r < d$. Then

$$\begin{aligned}
\psi_{d,J,\delta}(u)(n) &= [E_d \circ \Sigma_\delta \circ T_J \circ \Delta_d(u)](n) \\
&= \Big[E_d\big(\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)}(u) \big)_{0 \le i < d} \Big](dq + r) \\
&= \big(\theta_d \circ T^{dJ_{\delta(r)}+\delta(r)}(u) \big)(q) \\
&= \theta_d\big(X^{dJ_{\delta(r)}+\delta(r)} * u \big)(q) \\
&= u\big(dq + dJ_{\delta(r)} + \delta(r) \big),
\end{aligned}$$

which proves (2).

For (3), define $\varphi : \mathbb{N} \to \mathbb{N}$ by

$$\forall n \in \mathbb{N}, \quad \varphi(n) = d \left\lfloor \frac{n}{d} \right\rfloor + dJ_{\delta(n \bmod d)} + \delta(n \bmod d).$$

Let $n = dq + r$ with $0 \le r < d$. By part (2),

$$\psi_{d,J,\delta}(u)(n) = u\big(dq + dJ_{\delta(r)} + \delta(r)\big).$$

Since $dq = d\lfloor n/d \rfloor$ and $r = n \bmod d$, we obtain

$$\psi_{d,J,\delta}(u)(n) = u(\varphi(n)).$$

Hence $\psi_{d,J,\delta}(u) = u \circ \varphi$. □

Proposition 3.3. *Let A be a commutative unital ring, M an A-module, and $d \in \mathbb{N}^*$. Let δ be a permutation of $\{0, 1, \dots, d-1\}$ and $J = (j_i)_{0 \le i < d} \in \mathbb{N}^d$. Then for every $u \in S(M)$ and every polynomial $p(X) \in A[X]$,*

$$\psi_{d,J,\delta}\big(p(X^d) * u\big) = p(X^d) * \psi_{d,J,\delta}(u).$$

Consequently, the map $\psi_{d,J,\delta} : S(M) \to S(M)$ is an $A[X^d]$-module homomorphism.

Proof. Using the explicit description of $\psi_{d,J,\delta}$, we have

$$\psi_{d,J,\delta}(u) = E_d\Big(\big(\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)}(u)\big)_{0 \le i < d}\Big).$$

Let $p(X) \in A[X]$ and $u \in S(M)$. By Proposition2.7,

$$p(X^d) * E_d(v_0, \dots, v_{d-1}) = E_d\big(p(X) * v_0, \dots, p(X) * v_{d-1}\big),$$

and by Corollary3.1,

$$p(X) * \big(\theta_d \circ T^m\big) = \big(\theta_d \circ T^m\big) \circ p(X^d) \quad \text{for all } m \in \mathbb{N}.$$

Applying these identities with $v_i = (\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)})(u)$, we obtain

$$\begin{aligned} p(X^d) * \psi_{d,J,\delta}(u) &= p(X^d) * E_d\Big(\big(\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)}(u)\big)_{0 \le i < d}\Big) \\ &= E_d\Big(\big(p(X) * (\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)}(u))\big)_{0 \le i < d}\Big) \\ &= E_d\Big(\big((\theta_d \circ T^{dJ_{\delta(i)}+\delta(i)})(p(X^d) * u)\big)_{0 \le i < d}\Big) \\ &= \psi_{d,J,\delta}\big(p(X^d) * u\big). \end{aligned}$$

This shows that $\psi_{d,J,\delta}$ commutes with the action of $A[X^d]$, and therefore it is an $A[X^d]$-module homomorphism. □

Proposition 3.4. *Let A be a commutative unital ring, M an A-module, and let $n \in \mathbb{N}^*$. For each $1 \le i \le n$, let $d_i \in \mathbb{N}^*$, let δ_i be a permutation of $\{0, 1, \dots, d_i - 1\}$, and let $J_i \in \mathbb{N}^{d_i}$. Define the composite braiding mapping*

$$\Psi_n = \psi_{d_n,J_n,\delta_n} \circ \cdots \circ \psi_{d_1,J_1,\delta_1}.$$

Let

$$D_n = \operatorname{lcm}(d_1, \dots, d_n).$$

Then for every $u \in S(M)$ and every $p(X) \in A[X]$,

$$p(X^{D_n}) * \Psi_n(u) = \Psi_n\big(p(X^{D_n}) * u\big).$$

Proof. We proceed by induction on n.

For $n = 1$. Here $\Psi_1 = \psi_{d_1,J_1,\delta_1}$ and $D_1 = d_1$. The statement follows directly from Proposition3.3.

Inductive step. Assume the statement holds for some $n \geq 1$; that is, for all $u \in S(M)$ and all $p(X) \in A[X]$,

$$p(X^{D_n}) * \Psi_n(u) = \Psi_n\big(p(X^{D_n}) * u\big),$$

where $D_n = \operatorname{lcm}(d_1, \ldots, d_n)$.

Let $d_{n+1} \in \mathbb{N}^*$, δ_{n+1} a permutation of $\{0, 1, \ldots, d_{n+1} - 1\}$, and $J_{n+1} \in \mathbb{N}^{d_{n+1}}$. Define

$$\Psi_{n+1} = \psi_{d_{n+1}, J_{n+1}, \delta_{n+1}} \circ \Psi_n, \qquad D_{n+1} = \operatorname{lcm}(D_n, d_{n+1}).$$

Since $D_n \mid D_{n+1}$ and $d_{n+1} \mid D_{n+1}$, there exist polynomials

$$R(X) = p\Big(X^{\frac{D_{n+1}}{D_n}}\Big) \in A[X], \qquad Q(X) = p\Big(X^{\frac{D_{n+1}}{d_{n+1}}}\Big) \in A[X].$$

such that

$$p(X^{D_{n+1}}) = R(X^{D_n}) = Q(X^{d_{n+1}}).$$

Then for any $u \in S(M)$:

$$\begin{aligned} p(X^{D_{n+1}}) * \Psi_{n+1}(u) &= Q(X^{d_{n+1}}) * \psi_{d_{n+1}, J_{n+1}, \delta_{n+1}}(\Psi_n(u)) \\ &= \psi_{d_{n+1}, J_{n+1}, \delta_{n+1}}\big(Q(X^{d_{n+1}}) * \Psi_n(u)\big) \quad \text{(by Proposition3.3)} \\ &= \psi_{d_{n+1}, J_{n+1}, \delta_{n+1}}\big(R(X^{D_n}) * \Psi_n(u)\big) \\ &= \psi_{d_{n+1}, J_{n+1}, \delta_{n+1}}\big(\Psi_n(R(X^{D_n}) * u)\big) \quad \text{(by the induction hypothesis)} \\ &= \Psi_{n+1}\big(p(X^{D_{n+1}}) * u\big). \end{aligned}$$

This completes the induction, proving the proposition. □

Lemma 3.5. *Assume the hypotheses of Proposition 3.4. Let Ψ_n be the composite braiding mapping defined therein, and set $D_n = \operatorname{lcm}(d_1, \ldots, d_n)$.*

If $P(X), Q(X) \in A[X]$ satisfy $P(X) \mid Q(X^{D_n})$ and $u \in r_{P(X)}(A; M)$, then

$$\Psi_n(u) \in r_{Q(X^{D_n})}(A; M).$$

Proof. Since $P(X) \mid Q(X^{D_n})$, there exists a polynomial $L_n(X) \in A[X]$ such that

$$Q(X^{D_n}) = L_n(X)\, P(X).$$

Because $u \in r_{P(X)}(A; M)$, we have

$$P(X) * u = 0_{S(M)}.$$

Hence,

$$Q(X^{D_n}) * u = L_n(X) * (P(X) * u) = 0_{S(M)}.$$

By Proposition3.4, convolution with a polynomial commutes with the braiding mapping Ψ_n. Therefore,

$$Q(X^{D_n}) * \Psi_n(u) = \Psi_n\big(Q(X^{D_n}) * u\big) = \Psi_n(0_{S(M)}) = 0_{S(M)}.$$

Thus, $\Psi_n(u) \in r_{Q(X^{D_n})}(A; M)$, as required. □

Corollary 3.6. *[2] Let A be a commutative unital ring and M an A-module. Let $n \in \mathbb{N}^*$, and let $d_1, d_2, \ldots, d_n \in \mathbb{N}^*$. Define*

$$P(X) = \prod_{i=1}^{s} (X - \alpha_i)^{m_i} \in A[X], \quad \alpha_i \in A,\ m_i \in \mathbb{N}^*,$$

and set

$$D_n = \operatorname{lcm}(d_1, \ldots, d_n), \qquad L(X) = \prod_{i=1}^{s} (X - \alpha_i^{D_n})^{m_i}.$$

Let Ψ_n be the composite braiding mapping defined in Proposition 3.4. If $u \in r_{P(X)}(A; M)$, then

$$\Psi_n(u) \in r_{L(X^{D_n})}(A; M).$$

Proof. For each $i \in \{1, \dots, s\}$, we have the factorization in $A[X]$:

$$X^{D_n} - \alpha_i^{D_n} = (X - \alpha_i) \cdot Q_i(X),$$

where

$$Q_i(X) = X^{D_n - 1} + \alpha_i X^{D_n - 2} + \cdots + \alpha_i^{D_n - 1}.$$

It follows that

$$(X - \alpha_i)^{m_i} \mid (X^{D_n} - \alpha_i^{D_n})^{m_i}, \quad \text{for all } i.$$

Consequently,

$$P(X) = \prod_{i=1}^{s} (X - \alpha_i)^{m_i} \;\Big|\; \prod_{i=1}^{s} (X^{D_n} - \alpha_i^{D_n})^{m_i} = L(X^{D_n}) \quad \text{in } A[X].$$

Since $u \in r_{P(X)}(A; M)$ and $P(X) \mid L(X^{D_n})$, Lemma3.5 implies

$$\mathbf{\Psi}_n(u) \in r_{L(X^{D_n})}(A; M),$$

as required. □

Example 3.7. Let $K = \mathbb{Z}$, and let $M = \mathbb{Z}^2$. Define the sequence $u \in S(\mathbb{Z}^2)$ by:

$$\forall n \in \mathbb{N}, \quad u_n = (2, n).$$

Clearly, u satisfies the second-order linear recurrence:

$$\forall n \in \mathbb{N}, \quad u_{n+2} - 2u_{n+1} + u_n = (0, 0),$$

so that $u \in r_{P(X)}(\mathbb{Z}; \mathbb{Z}^2)$, where $P(X) = (X - 1)^2 \in \mathbb{Z}[X]$.

We now define the composed braiding mapping:

$$\mathbf{\Psi} = \psi_{2,J_2,\delta_2} \circ \psi_{3,J_1,\delta_1},$$

with the following parameters:

$$\begin{aligned} &J_1(0) = 0, \quad J_1(1) = 0, \quad J_1(2) = 1, \\ &\delta_1(0) = 0, \quad \delta_1(1) = 1, \quad \delta_1(2) = 2, \\ &J_2(0) = 0, \quad J_2(1) = 1, \\ &\delta_2(0) = 0, \quad \delta_2(1) = 1. \end{aligned}$$

Step 1. Application of ψ_{3,J_1,δ_1}: For $n = 3m + r$ with $r \in \{0, 1, 2\}$:

$$v_n = \psi_{3,J_1,\delta_1}(u)(n) = u\big(3m + 3J_1(\delta_1(r)) + \delta_1(r)\big),$$

which gives:

$$v_n = \begin{cases} u_n, & n \equiv 0, 1 \pmod 3, \\ u_{n+3}, & n \equiv 2 \pmod 3. \end{cases}$$

Step 2. Application of ψ_{2,J_2,δ_2}: For $n = 2q + r$ with $r \in \{0, 1\}$:

$$w_n = \psi_{2,J_2,\delta_2}(v)(n) = v\big(2q + 2J_2(\delta_2(r)) + \delta_2(r)\big),$$

which simplifies to:

$$w_n = \begin{cases} v_n, & n \text{ even}, \\ v_{n+2}, & n \text{ odd}. \end{cases}$$

The values of w_n for $0 \le n \le 15$ are:

n	v_n	Comments	w_n
0	$v_0 = u_0 = (2,0)$	$n \equiv 0 \pmod 3, n \equiv 0 \pmod 2$	$w_0 = v_0 = (2,0)$
1	$v_1 = u_1 = (2,1)$	$n \equiv 1 \pmod 3, n \equiv 1 \pmod 2$	$w_1 = v_3 = (2,3)$
2	$v_2 = u_5 = (2,5)$	$n \equiv 2 \pmod 3, n \equiv 0 \pmod 2$	$w_2 = v_2 = (2,5)$
3	$v_3 = u_3 = (2,3)$	$n \equiv 0 \pmod 3, n \equiv 1 \pmod 2$	$w_3 = v_5 = (2,8)$
4	$v_4 = u_4 = (2,4)$	$n \equiv 1 \pmod 3, n \equiv 0 \pmod 2$	$w_4 = v_4 = (2,4)$
5	$v_5 = u_8 = (2,8)$	$n \equiv 2 \pmod 3, n \equiv 1 \pmod 2$	$w_5 = v_7 = (2,7)$
6	$v_6 = u_6 = (2,6)$	$n \equiv 0 \pmod 3, n \equiv 0 \pmod 2$	$w_6 = v_6 = (2,6)$
7	$v_7 = u_7 = (2,7)$	$n \equiv 1 \pmod 3, n \equiv 1 \pmod 2$	$w_7 = v_9 = (2,9)$
8	$v_8 = u_{11} = (2,11)$	$n \equiv 2 \pmod 3, n \equiv 0 \pmod 2$	$w_8 = v_8 = (2,11)$
9	$v_9 = u_9 = (2,9)$	$n \equiv 0 \pmod 3, n \equiv 1 \pmod 2$	$w_9 = v_{11} = (2,14)$
10	$v_{10} = u_{10} = (2,10)$	$n \equiv 1 \pmod 3, n \equiv 0 \pmod 2$	$w_{10} = v_{10} = (2,10)$
11	$v_{11} = u_{14} = (2,14)$	$n \equiv 2 \pmod 3, n \equiv 1 \pmod 2$	$w_{11} = v_{13} = (2,13)$
12	$v_{12} = u_{12} = (2,12)$	$n \equiv 0 \pmod 3, n \equiv 0 \pmod 2$	$w_{12} = v_{12} = (2,12)$
13	$v_{13} = u_{13} = (2,13)$	$n \equiv 1 \pmod 3, n \equiv 1 \pmod 2$	$w_{13} = v_{15} = (2,15)$
14	$v_{14} = u_{17} = (2,17)$	$n \equiv 2 \pmod 3, n \equiv 0 \pmod 2$	$w_{14} = v_{14} = (2,17)$
15	$v_{15} = u_{15} = (2,15)$	$n \equiv 0 \pmod 3, n \equiv 1 \pmod 2$	$w_{15} = v_{17} = u_{20} = (2,20)$

Final Observation. The resulting sequence w satisfies the 12-th order linear recurrence:

$$w_{n+12} - 2w_{n+6} + w_n = 0, \quad n \geq 0,$$

i.e., $w \in r_{Q(X)}(\mathbb{Z}; \mathbb{Z}^2)$, where:

$$Q(X) = P(X^{\mathrm{lcm}(2,3)}) = (X^6 - 1)^2 \in \mathbb{Z}[X].$$

Proposition 3.8. *[1] Let A be a commutative unital ring and M an A-module. Let $u \in S(M)$ be a periodic sequence of period N, i.e.,*

$$T^N(u) = u.$$

Let $d_1, \ldots, d_n \in \mathbb{N}^*$, and define the composite braiding mapping

$$\Psi_n = \psi_{d_n, J_n, \delta_n} \circ \cdots \circ \psi_{d_1, J_1, \delta_1}$$

as in Proposition 3.4. Set

$$D_n = \mathrm{lcm}(N, d_1, \ldots, d_n).$$

Then the image $\Psi_n(u)$ satisfies

$$\Psi_n(u) \in r_{X^{D_n}-1}(A; M),$$

i.e., $\Psi_n(u)$ is annihilated by $X^{D_n} - 1$ and thus has period dividing D_n.

Proof. Since u is periodic of period N, we have

$$T^N(u) = u \quad \Longrightarrow \quad (X^N - 1) * u = 0_{S(M)}.$$

By definition, $D_n = \mathrm{lcm}(N, d_1, \ldots, d_n)$, so $N \mid D_n$, and we can write $D_n = N \cdot Q_n$ for some $Q_n \in \mathbb{N}^*$.

Let $p(X) = X^N - 1 \in A[X]$. Then

$$X^{D_n} - 1 = X^{NQ_n} - 1 = (X^N)^{Q_n} - 1 = (X^N - 1) \cdot R_n(X),$$

where

$$R_n(X) = \sum_{i=0}^{Q_n - 1} X^{Ni} \in A[X].$$

Hence, $p(X) \mid X^{D_n} - 1$ in $A[X]$. Using $p(X) * u = 0_{S(M)}$ and Lemma3.5, we conclude

$$\Psi_n(u) \in r_{X^{D_n}-1}(A; M).$$

Therefore, $\Psi_n(u)$ is periodic with period dividing $D_n = \text{lcm}(N, d_1, \ldots, d_n)$. □

Proposition 3.9. *[1] Let A be a commutative unital ring, M an A-module, and let $u \in S(M)$ be a periodic sequence of minimal period $p \in \mathbb{N}^*$. Let $a \in \mathbb{N}^*$, $b \in \mathbb{N}$, and define the sequence $v \in S(M)$ by*

$$\forall n \in \mathbb{N}, \quad v(n) = u(an + b).$$

Then v is periodic with minimal period

$$\text{sp}(v) = \frac{p}{\gcd(a, p)}.$$

Proof. Since u has minimal period p, we have

$$u(n + p) = u(n), \quad \text{for all } n \in \mathbb{N}.$$

Let

$$T = \frac{p}{\gcd(a, p)}.$$

For all $n \in \mathbb{N}$, we compute

$$v(n + T) = u\big(a(n + T) + b\big) = u(an + aT + b).$$

Since $aT = a \cdot \frac{p}{\gcd(a,p)}$ and $\gcd(a, p) \mid a$, we have $aT \equiv 0 \pmod{p}$, which implies

$$u(an + aT + b) = u(an + b) = v(n),$$

so v is periodic with period T.

To show that T is minimal, suppose there exists $T_0 < T$ such that $v(n + T_0) = v(n)$ for all n. Then

$$u(an + aT_0 + b) = u(an + b) \quad \Rightarrow \quad aT_0 \equiv 0 \pmod{p}.$$

Let $d = \gcd(a, p)$. Then there exist integers a_1, p_1 such that $a = da_1$, $p = dp_1$, and $\gcd(a_1, p_1) = 1$. Then

$$dp_1 \mid da_1T_0 \quad \Rightarrow \quad p_1 \mid a_1T_0.$$

Since $\gcd(a_1, p_1) = 1$, it follows that $p_1 \mid T_0$, hence

$$T_0 \geq p_1 = \frac{p}{\gcd(a, p)} = T,$$

which contradicts $T_0 < T$. Therefore, T is the minimal period of v, and

$$\text{sp}(v) = \frac{p}{\gcd(a, p)}.$$

□

4 Conclusion remarks

In this paper, we studied the algebraic behavior of linear recurrence sequences under compositions of braiding mappings. Starting from sequences annihilated by a characteristic polynomial $P(X) \in A[X]$, we established how successive braiding transformations modify the annihilating structure through monomial substitutions of the form $X \mapsto X^{d_i}$. A key contribution was the identification of the resulting recurrence relations for the transformed sequences $\Psi_n(u)$, where Ψ_n denotes a composition of multiple braiding maps. We provided explicit bounds and constructions of new annihilating polynomials $Q(X)$ such that $\Psi_n(u) \in r_{Q(X)}(A; M)$, depending on the degrees d_i involved in the composition.

Moreover, we demonstrated through concrete examples how periodicity and characteristic polynomials evolve under such transformations. In particular, we established that the image of a periodic sequence under a braiding composition remains periodic, with a period dividing the least common multiple of the initial period and the degrees involved in the composition.

These results open several directions for future research. One possible extension is to study the inverse problem: given a recurrence satisfied by $\Psi_n(u)$, can we recover information about the original sequence u. Another potential avenue is the application of these constructions in coding theory and cryptography, especially in designing sequences with controlled algebraic and combinatorial properties.

References

[1] S. Kiouche and A. Ait Mokhtar, *Some Properties of Linear Recurrence Sequences Braiding and Application in Cryptography*, Palestine Journal of Mathematics, **14**(1–2), 381–394 (2025).

[2] H. Ait Mohammed and A. Ait Mokhtar, *Characteristic Polynomial and Period of a Linear Recurrent Sequence Braiding on a Field*, Palestine Journal of Mathematics, **14**(1), 1083–1091 (2025).

[3] M. S. Mahadeva Naika et al., *Matrix Sequence of the Binomial Form of the Complex Combined Jacobsthal-Akin Sequence*, Palestine Journal of Mathematics, **11**(1), 12–20 (2022).

[4] G. Alecci, S. Barbero, and N. Murru, *Some notes on the algebraic structure of linear recurrent sequences*, Ricerche di Matematica, **74**, 431–447 (2025).

[5] D. Ferrand, *Suites récurrentes*, IRMAR, Université de Rennes, 1988.

[6] D. Birmajer, J. B. Gil, and M. D. Weiner, *Linear recurrence sequences and their convolutions via Bell polynomials*, Journal of Integer Sequences, **18**(1), 2014.

[7] Z. Chen and L. Qi, *Some Convolution Formulae Related to the Second-Order Linear Recurrence Sequence*, Symmetry, **11**(6), 788, (2019).

[8] A. Ait Mokhtar, *Applications purement semi-affines et tressages*, C. R. Math. Acad. Sci. Paris, **348**(1–2), 1–4, (2010).

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

[10] J.-P. Allouche and J. Shallit, *Automatic sequences: Theory, applications, generalizations*, Cambridge University Press, (2003).

Author information

T. Zerkaoui, Laboratory of Fixed Point Theory and Applications, Higher Normal School Of Kouba , Algiers, Algeria.
E-mail: tayeb.zerkaoui31@g.ens-kouba.dz

A. Ait Mokhtar, Mathematics department, laboratory of Fixed Point Theory and Applications, Higher Normal School Of Kouba , Algiers, Algeria.
E-mail: ahmed.aitmokhtar@g.ens-kouba.dz

Received: 2025-10-01
Accepted: 2026-02-20