Palestine Journal of Mathematics

Vol 14(1)(2025) , 381–394

SOME PROPERTIES OF LINEAR RECURRENCE SEQUENCES BRAIDING AND APPLICATION IN CRYPTOGRAPHY

S. Kiouche and A. Ait Mokhtar

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 11B37; Secondary 11B99.

Keywords and phrases: Linear recurrence sequence, braiding sequence, periodicity of braiding sequence, Fibonacci braiding sequence, cryptography, encryption, decryption.

Abstract In this paper, we conduct a comprehensive analysis of the intricate relationship between a linear recurrence sequence and its image through braiding mapping. Central to our investigation is the period of the braiding sequence. Our research specifically focuses on determining the order of the braiding sequence of the Fibonacci sequence. This endeavor not only illuminates the theoretical intricacies of braiding sequences but also lays the groundwork for their practical application. A notable achievement of our study is the development of a new cryptographic method, which capitalizes on the distinctive characteristics of the braiding sequence.
We conclude this work by providing an example of cryptography that utilizes the braiding sequence.

1 Introduction

Consider a unitary, commutative ring, denoted by K. We define $S_{\mathbb{N}}(K)$ (or simply $S(K)$) as the set of sequences $u = u(n)$, where $n \in \mathbb{N}$ and the elements are from K, indexed by $\mathbb{N}$.

This set, $S(K)$, when equipped with addition and scalar multiplication, exhibits the structure of a vector space. Furthermore, by equipping $S(K)$ with the usual addition and Hadamard product, we introduce an alternative structure to $S(K)$. This structure is a K-algebra and is referred to as the Hadamard Algebra of Sequences.

Our focus is on $r(K)$, which is the set of linear recurrence sequences with values in K. This set is a subalgebra of $S(K)$ and is known as the rational Hadamard algebra.

In [1], a continuous endomorphism $\psi_{d,J,\sigma}$ of $r(K)$ was constructed, which is termed braiding. The braiding mapping is a composition of the applications: Δ_d, Σ_σ, T_J and E_d.
Properties of the braiding mapping are detailed in [1].

In this article, we concentrate on $r(K)$ where K is a finite field. We analyze the general term of the braiding sequence $\psi_{d,\sigma}u$, examining the relationships between the sequence u and its image under the braiding $\psi_{d,\sigma}$.

This study also includes a rigorous investigation of the periodicity of the braiding sequence. It encompasses the determination of the smallest period of the decimation sequence $u(dn + j)$ and the analysis of factors that influence the period of the braiding sequence.

Our research further explores specific cases where the periodicity of the braiding sequence mirrors that of the original sequence u. We also consider scenarios where the smallest period of the braiding sequence corresponds to the least common multiple of p and d, with p denoting the period of u.

Additionally, we present significant findings regarding the order of the Fibonacci braiding sequence, which enhances understanding of the connections between braiding sequences and classical sequences. For further details on studies related to the Fibonacci sequence, we refer the reader to references [2] and [3]. These works are not the focus of our discussion here.
Finally, we conclude our article with a practical application in cryptography. This demonstrates

the utility of the braiding sequence in bolstering the security of communication systems.

This article offers a novel perspective on methodological advancements and theoretical implications in the study of algebraic structures and sequential dynamics, contributing to the expanding body of knowledge in this dynamic field.

2 Braiding sequence

Definition 2.1.
Let K be a finite field. Let d a positive integer, $J = (j_0, j_1, ..., j_{d-1})$ be a d-tuple from $\mathbb{N}^d$ and σ a permutation in S_d.
Consider the following maps :

(i) The map Δ_d from $r(K)$ to $(r(K))^d$, that associates to every sequence u:
$(\Delta_d u)(n) = (u(dn), u(dn+1), ..., u(dn+d-1))$

(ii) The map Σ_σ from $(r(K))^d$ to $(r(K))^d$ that associates to every d-tuple $(u_0, u_1, ..., u_{d-1})$ the d-tuple $(u_{\sigma(0)}, u_{\sigma(1)}, ..., u_{\sigma(d-1)})$.

(iii) The map T_J from $(r(K))^d$ to $(r(K))^d$ that associates to every d-tuple $(u_0, u_1, ..., u_{d-1})$ the d-tuple $(T^{j_0}u_0, T^{j_1}u_1, ..., T^{j_{d-1}}u_{d-1})$

(iv) The map E_d from $(r(K))^d$ to $r(K)$, that associates to every d-tuple $(u_0, u_1, ..., u_{d-1})$ the sequence u defined by:
$\forall j \in \{0, 1, ..., d-1\}, \forall n \in \mathbb{N}$,
$E_d(u_0, u_1, ..., u_{d-1})(dn + j) = u_j(n)$ which is called nesting.

Definition 2.2.
The map $E_d \circ \Sigma_\sigma \circ T_J \circ \Delta_d$ denoted by $\psi_{d,J,\sigma}$ is called Braiding mapping.

Proposition 2.3. *[1]*
Let d be a non-zero natural number, J be a d-tuple of natural numbers, and σ be a permutation of the set $\{0, ..., d-1\}$. Then
The braiding $\psi_{d,J,\sigma}$ is an automorphism if and only if $J = (0, ..., 0)$.

Remark 2.4.
We agree to write $\psi_{d,\sigma}$ instead of $\psi_{d,J,\sigma}$ when $J = (0, \ldots, 0)$.

Let's recall that in article [1], we find the following result:

Proposition 2.5.
Let $u \in r(K)$, $d \in \mathbb{N}$, and σ be a permutation in S_d.
Then, the inverse bijection of the bijective braiding $\psi_{d,\sigma}$ is the bijective braiding $\psi_{d,\sigma^{-1}}$.

Remark 2.6.
Let $u \in r(K)$, $d \in \mathbb{N}$, and σ be a permutation in S_d.
It is then easy to see that we have: $(\psi_{d,\sigma}u)(dn + j) = u(dn + \sigma(j))$
and $(\psi_{d,\sigma^{-1}}u)(dn + j) = u(dn + \sigma^{-1}(j))$ for all $j \in \{1, 2, ..., d-1\}$

We are going to demonstrate a result given in [1].
Let x be a real number. Let's recall the notations $[x]$ for the integer part of x and $\{x\} = x - [x]$ for its fractional part.

Proposition 2.7.
Let $u \in r(K)$, $d \in \mathbb{N}$ and $\sigma \in S_d$.
Then the braiding $\psi_{d,\sigma}$ is written $\psi_{d,\sigma}(u) = u \circ \varphi$ where φ is a mapping from $\mathbb{N}$ to $\mathbb{N}$ defined by:

$$\begin{aligned} \forall n \in \mathbb{N},\ \varphi(n) &= d\left[\frac{n}{d}\right] + \sigma\left(d\left\{\frac{n}{d}\right\}\right) \\ &= d\left[\frac{n}{d}\right] + \sigma(m) \text{ where } n \equiv m \mod d. \end{aligned}$$

Proof.
Let $n \in \mathbb{N}$, by performing the euclidean division of n by d, we obtain

$$n = d\alpha + j \text{ with } j \in \{0, 1, ..., d-1\}$$

Then

$$\frac{n}{d} = \alpha + \frac{j}{d}$$

Thus

$$\left[\frac{n}{d}\right] = \alpha \text{ and } \left\{\frac{n}{d}\right\} = \frac{j}{d}$$

Hence

$$\begin{aligned}(u \circ \varphi)(n) &= u\Big(d\Big[\frac{n}{d}\Big] + \sigma\Big(d\Big\{\frac{n}{d}\Big\}\Big)\Big)\\ &= u\Big(d\alpha + \sigma\Big(d.\frac{j}{d}\Big)\Big)\\ &= u(d\alpha + \sigma(j)) \quad (2)\end{aligned}$$

And

$$\begin{aligned}(\psi_{d,\sigma}u)(n) &= (\psi_{d,\sigma}u)(d\alpha + j)\\ &= u_{\sigma(j)}(\alpha)\\ &= u(d\alpha + \sigma(j)) \quad (3)\end{aligned}$$

From (2) and (3):

$$(\psi_{d,\sigma}u)(n) = (u \circ \varphi)(n)$$

□

3 Study of periodicity

Let $u \in r(K)$. Then the braiding sequence $\psi_{d,\sigma}u$ is a linear recurrence sequence with constant coefficients over a finite field (by definition).
Let's determine the smallest period of the braiding sequence $\psi_{d,\sigma}u$.
We set p the smallest period of u and $u_j(n) = u(dn + j)$ where $j \in \{0, 1, ..., d-1\}$.

Proposition 3.1.

The smallest period of u_j where $j \in \{0, 1, ..., d-1\}$ is equal to $\dfrac{p}{\gcd(d,p)} = \dfrac{\text{lcm}(d,p)}{d}$.

Proof.
Let $n \in \mathbb{N}$ and $j \in \{0, 1, ..., d-1\}$:

(i) If d divides p then $\exists\, m \in \mathbb{N}$ such that $p = dm$.

$$\begin{aligned}u_j(n+m) &= u(d(n+m) + j)\\ &= u(dn + dm + j)\\ &= u(dn + j) \text{ because } dm = p\\ &= u_j(n)\end{aligned}$$

Thus m is a period of u_j.
Let's show that m is the smallest period of u_j.
We assume that the smallest period of u_j is m_0, then:
$u_j(n + m_0) = u_j(n), \forall\, n \in \mathbb{N}$ and m_0 divides m which means that $\exists\, l \in \mathbb{N}$ such that

$$m = lm_0 \quad (1)$$

We have

$$\begin{aligned} u_j(n+m_0) &= u(dn+dm_0+j) \\ &= u(dn+j) \\ &= u_j(n). \end{aligned}$$

Then dm_0 is a multiple of p thus $\exists\, k \in \mathbb{N}$ such that $dm_0 = kp$.
We multiply the equation (1) by d, we obtain:

$$dm = dlm_0 = lkp$$

But $dm = p$, so

$$p = lkp$$

This implies that $lk = 1$; since $l, k \in \mathbb{N}$ then $l = k = 1$.
Thus

$$m = m_0$$

Since d divides p then $\gcd(p,d) = d$, thus $\dfrac{p}{\gcd(d,p)} = m$.

(ii) If p divides d then $\exists\, k \in \mathbb{N}; d = kp$. We have

$$\begin{aligned} u_j(n+1) &= u(dn+d+j) \\ &= u(dn+kp+j) \\ &= u(dn+j) \\ &= u_j(n). \end{aligned}$$

It is clear that 1 is the smallest period of u_j, $1 = \dfrac{p}{p} = \dfrac{p}{\gcd(d,p)}$.

(iii) If neither p divides d nor d divides p, we set $\gcd(p,d) = n_0$ then :

$$\begin{aligned} u_j(n+\frac{p}{n_0}) &= u(dn+\frac{dp}{n_0}+j) \\ &= u(dn+k'p+j) \\ &= u(dn+j) \\ &= u_j(n). \end{aligned}$$

Then $\dfrac{p}{n_0}$ is a period u_j.
Let's show that $\dfrac{p}{n_0}$ is the smallest period of u_j:
We assume that the smallest period of u_j is equal to p', then p' divides $\dfrac{p}{n_0}$, so

$$\exists\, k \in \mathbb{N}; \frac{p}{n_0} = kp'$$

so

$$p' = \frac{p}{n_0 k}$$

this implies that $n_0 k$ divides p.
We have

$$\begin{aligned} u_j(n+p') &= u(dn+dp'+j) \\ &= u(dn+\frac{dp}{n_0 k}+j) \\ &= u_j(n). \end{aligned}$$

Then

$$\frac{d}{n_0 k} \in \mathbb{N}$$

Thus $n_0 k$ divides d.
We deduce that $n_0 k$ divides $\gcd(d,p) = n_0$, so $k = 1$.
Thus

$$p' = \frac{p}{n_0}$$

□

In the following, we denote by $sp(u)$ the smallest period of the sequence u.

Proposition 3.2.
Let $u \in r(K)$ where $sp(u) = p$ and $d \in \mathbb{N}$. Then the smallest period of the braiding sequence $\psi_{d,\sigma} u$ divides $\operatorname{lcm}(p,d)$.

Proof.
We set $p_0 = \operatorname{lcm}(p,d)$ and $\psi_{d,\sigma} u = v$, then:

$$v(n) = u\Big(d\Big[\frac{n}{d}\Big] + \sigma(m)\Big) \text{ where } n \equiv m \mod d$$

We have p_0 is a common multiple of d and of p then

$$\exists\, k, l \in \mathbb{N};\ p_0 = dk = lp$$

Let $n \in \mathbb{N}$. Therefore:

$$\begin{aligned}
v(n+p_0) &= u\Big(d\Big[\frac{n+p_0}{d}\Big] + \sigma(m')\Big) \text{ where } (n+p_0) \equiv m' \mod d \\
&= u\Big(d\Big(\Big[\frac{n}{d}\Big] + k\Big) + \sigma(m)\Big) \text{ because } n + p_0 \equiv m \mod d \\
&= u\Big(d\Big[\frac{n}{d}\Big] + dk + \sigma(m)\Big) \text{ where } n \equiv m \mod d \\
&= u\Big(d\Big[\frac{n}{d}\Big] + lp + \sigma(m)\Big) \\
&= u\Big(d\Big[\frac{n}{d}\Big] + \sigma(m)\Big) \\
&= v(n)
\end{aligned}$$

□

3.1 Two specific cases

(i) We assume that p divides d, we set $k = \dfrac{d}{p}$.
Let $\sigma = (i_1, i_2, ..., i_r) \in S_d$ a permutation of r-cycle.
The smallest period of the sequence $\psi_{d,\sigma} u$ is equal to p in the following two cases

a. $2 \le r \le k$ and $i_1 \equiv i_2 \equiv ... \equiv i_r [p]$.

b. $r = l_0 k$ where $2 \le l_0 \le p$ and

$$\begin{cases}
i_1 \equiv i_{l_0+1} \equiv ... \equiv i_{l_0(k-1)+1}[p] \\
i_2 \equiv i_{l_0+2} \equiv ... \equiv i_{l_0(k-1)+2}[p] \\
\vdots \\
i_{l_0} \equiv i_{2l_0} \equiv ... \equiv i_{l_0 k}[p]
\end{cases}$$

Indeed,

(a) Let $\sigma = (i_1, i_2, ..., i_r) \in S_d$ such that $2 \leq r \leq k$ and $i_1 \equiv i_2 \equiv ... \equiv i_r[p]$.
then

$$\begin{cases} \sigma(i_1) = i_2 \equiv i_1[p] \\ \sigma(i_2) = i_3 \equiv i_2[p] \\ \quad\quad \vdots \\ \sigma(i_r) = i_1 \equiv i_r[p] \end{cases}$$

We have
$(\Sigma_\sigma \circ \Delta_d)(u)(n) = (u(dn + \sigma(0)), u(dn + \sigma(1)), ..., u(dn + \sigma(d-1)))$,
since $\sigma(i_j) \equiv i_j[p]$ then
$(\Sigma_\sigma \circ \Delta_d)(u)(n) = (u(dn), u(dn+1), ..., u(dn+p-1), ..., u(dn), ..., u(dn+p-1))$
Thus
$(E_d \circ \Sigma_\sigma \circ \Delta_d)(u)(n) = (u(0), u(1), ..., u(p-1), u(0), ..., u(p-1), u(0), ..., u(p-1), ...)$

(b) Let $\sigma \in S_d$ a permutation of r-cycle such that $r = l_0 k$ where $2 \leq l_0 \leq p$.
we set $\sigma = (i_1, i_2, ..., i_{l_0}, i_{l_0+1}, ..., i_{2l_0}, ..., i_{l_0(k-1)+1}, ..., i_{kl_0})$. We assume that

$$\begin{cases} i_1 \equiv i_{l_0+1} \equiv ... \equiv i_{l_0(k-1)+1}[p] \\ i_2 \equiv i_{l_0+2} \equiv ... \equiv i_{l_0(k-1)+2}[p] \\ \quad\quad \vdots \\ i_{l_0} \equiv i_{2l_0} \equiv ... \equiv i_{l_0 k}[p] \end{cases}$$

We set $i_j \equiv i'_j[p]$ where $j \in \{1, ..., l_0\}$ with $0 \leq i'_j \leq p-1$. Then

$$\begin{cases} \sigma(i_1) = i_2 \equiv i'_2[p] \\ \sigma(i_2) = i_3 \equiv i'_3[p] \\ \quad\quad \vdots \\ \sigma(i_{l_0-1}) = i_{l_0} \equiv i'_{l_0}[p] \\ \sigma(i_{l_0}) = i_{l_0+1} \equiv i_1[p] \equiv i'_1[p] \end{cases} \quad \text{and} \quad \begin{cases} \sigma(i_{l_0+1}) = i_{l_0+2} \equiv i'_2[p] \\ \sigma(i_{l_0+2}) = i_{l_0+3} \equiv i'_3[p] \\ \quad\quad \vdots \\ \quad\quad \vdots \\ \sigma(i_{2l_0}) = i_{2l_0+1} \equiv i'_1[p] \end{cases}$$

until

$$\begin{cases} \sigma(i_{l_0(k-1)+1}) = i_{l_0(k+1)+2} \equiv i'_2[p] \\ \sigma(i_{l_0(k+1)+2}) = i_{l_0(k+1)+3} \equiv i'_3[p] \\ \quad\quad \vdots \\ \quad\quad \vdots \\ \sigma(i_{kl_0}) = i_1 \equiv i'_1[p] \end{cases}$$

Then

$$\begin{cases} \sigma(i_1) \equiv \sigma(i_{l_0+1}) \equiv ... \equiv \sigma(i_{l_0(k-1)+1})[p] \\ \sigma(i_2) \equiv \sigma(i_{l_0+2}) \equiv ... \equiv \sigma(i_{l_0(k-1)+2})[p] \\ \quad\quad \vdots \\ \quad\quad \vdots \\ \sigma(i_{l_0}) \equiv \sigma(i_{2l_0}) \equiv ... \equiv \sigma(i_{kl_0})[p] \end{cases} \tag{2}$$

and we have
If $i \notin \{i_1, ..., i_{l_0 k}\}$ then $\sigma(i_j) = i_j$, and since $i_j + p \equiv i_j[p]$ for $0 \leq l \leq k-1$ then

$$\sigma(i_j + lp) \equiv \sigma(i_j)[p] \tag{3}$$

From (2) and (3), we obtain

$$\begin{aligned}(\Sigma_\sigma \circ \Delta_d)(u)(n) &= (u(dn+\sigma(0)), u(dn+\sigma(1)), ..., u(dn+\sigma(p-1)), ..., u(dn+\sigma(0)),\\ &\quad u(dn+\sigma(1)), ..., u(dn+\sigma(p-1)), ..., u(dn+\sigma(0)), ..., u(dn+\sigma(p-1)))\end{aligned}$$

Thus

$(E_d \circ \Sigma_\sigma \circ \Delta_d)(u)(n) = (u(0), u(1), ..., u(p-1), u(0), ..., u(p-1), u(0), ..., u(p-1), ...)$
Hence the smallest period of $(E_d \circ \Sigma_\sigma \circ \Delta_d)(u)$ is equal to p.

(ii) We assume that $\gcd(p,d) = 1$ and that $p < d$.

The smallest period of $\psi_{d,\sigma}u$ is equal to p if $\sigma = (i_1, i_2, ..., i_j)$ where $2 \leq j \leq \left[\frac{d}{p}\right] + 1$
and $i_1 \equiv i_2 \equiv ...i_j[p]$.
Indeed, we have $i_1 \equiv i_2 \equiv ...i_j[p]$ then :

$$\begin{cases} \sigma(i_1) = i_2 \equiv i_1[p] \\ \sigma(i_2) = i_3 \equiv i_2[p] \\ \quad\quad \vdots \\ \sigma(i_j) = i_1 \equiv i_j[p] \end{cases} \quad \text{and } \sigma(i_l) = i_l \text{ if } l \notin \{1, ..., j\}$$

Thus

$$\sigma(k) = k, \ \forall\, k \in \{1, ..., d-1\}$$

Therefore

$$\begin{aligned}(\Sigma_\sigma \circ \Delta_d)(u)(n) &= (u(dn+\sigma(0)), u(dn+\sigma(1)), ..., u(dn+\sigma(d-1)))\\ &= (u(dn+0)), u(dn+1), ..., u(dn+d-1))\end{aligned}$$

By performing the Euclidean division of d by p, we obtain $d = pq + r$ such that $r < p$.
Since the smallest period of the sequence u is equal to p and $p < d$ then

$$\begin{aligned}(\Sigma_\sigma \circ \Delta_d)(u)(n) &= (u(dn+0), u(dn+1), ..., u(dn+p), u(dn+p+1), ..., u(dn+2p-1),\\ &\quad u(dn+2p), ..., u(dn+qp), u(dn+qp+1), ..., u(dn+qp+r-1))\\ &= (u(dn), u(dn+1), ..., , u(dn+p-1), u(dn), u(dn+1), ..., u(dn+p-1),\\ &\quad u(dn), u(dn+1), ..., u(dn+p-1))\end{aligned}$$

Thus
$(E_d \circ \Sigma_\sigma \circ \Delta_d)(u)(n) = (u(0), u(1), ..., u(p-1), u(0), u(1), ..., u(p-1), u(0), u(1), ..., u(p-1), ...)$

Therefore the smallest period of $(E_d \circ \Sigma_\sigma \circ \Delta_d)(u)$ is equal to p.

Proposition 3.3.
Let $u \in r(K)$ where $sp(u) = p \neq 1$.
Let d a prime number such that $d > p$ and $\sigma = (0,1) \in S_d$.
Then the smallest period of the braiding sequence $\psi_{d,\sigma}u$ is equal to $\mathrm{lcm}(p,d) = pd$.

Proof.
We set $\psi_{d,\sigma}u = v$.
We have $\sigma = (0,1)$ then $\forall n \in \mathbb{N}$

$$\begin{aligned} v(dn) &= u(dn+1) \\ v(dn+1) &= u(dn) \\ v(dn+k) &= u(dn+k), \forall k \in \{2,3,...,d-1\} \end{aligned}$$

Let's assume, by contradiction that the smallest period of the braiding sequence $\psi_{d,\sigma}u$ is equal to p'.
Then p' divides $\text{lcm}(d,p) = dp$.
Since d is a prime number thus :

$$(p' \text{ divides } p) \text{ or } (p' = dm \text{ where } m \text{ is a divisor of } p \text{ distinct from } p)$$

If $p' = dm$ where m is a divisor of p with $m \neq p$. Then:

$$v(n+p') = v(n), \forall n \in \mathbb{N}$$

Thus

$$v(n+dm) = v(n), \forall n \in \mathbb{N} \quad (*)$$
$$v(k+dm) = v(k), \forall k \in \{2,3,...,d-1\} \quad (**)$$

We replace n with 1 in equation $(*)$, we obtain

$$u(dm) = v(dm+1) = v(1) = u(0)$$

we have $u(k) = v(k) = v(dm+k) = u(dm+k); \forall k \in \{2,3,...,d-1\}$ And

$$\begin{cases} v(dm) = v(0) = u(1) \\ u(1) = v(0) = v(dm) = u(dm+1) \\ u(dm) = v(dm+1) = v(1) = u(0) \end{cases}$$

Then

$$\begin{cases} u(dm) = u(0) \\ u(dm+1) = u(1) \\ u(dm+k) = u(k), \forall k \in \{2,3,...,d-1\} \end{cases}$$

Let's now show that

$$u(dm+d) = u(d)$$

We have

$$\begin{aligned} u(dm+d) &= u(d(m+1)) \\ &= v(d(m+1)+1) \\ &= v(dm+d+1) \\ &= v(d+1) \\ &= u(d) \end{aligned}$$

Let $n \in \mathbb{N}$ be greater than d.
We perform the Euclidean division of n by d, we obtain

$$n = dq + r \text{ with } 0 \leq r \leq d-1$$

If $r = 0$ then $n = dq$

$$\begin{aligned} u(dm+n) &= u(dm+dq) \\ &= u(d(m+q)) \\ &= v(d(m+q)+1) \\ &= v(dq+1) \\ &= u(dq) \\ &= u(n) \end{aligned}$$

If $r = 1$ then $n = dq + 1$

$$\begin{aligned} u(dm+n) &= u(dm+dq+1) \\ &= u(d(m+q)+1) \\ &= v(d(m+q)) \\ &= v(dm+dq) \\ &= v(dq) \\ &= u(dq+1) \\ &= u(n) \end{aligned}$$

If $r \in \{2, ..., d-1\}$ then

$$\begin{aligned} u(dm+n) &= u(dm+dq+r) \\ &= u(d(m+q)+r) \\ &= v(d(m+q)+r) \\ &= v(dq+r) \\ &= u(dq+r) \\ &= u(n) \end{aligned}$$

Hence

$$u(dm+n) = u(n), \forall n \in \mathbb{N}$$

Thus dm is a period of u.
Since $sp(u) = p$ then p divides dm contradiction (d is a prime number and m is a divisor of p distinct from p).
If p' divides p then $\exists\, l \in \mathbb{N}$ such that $p = lp'$.
We have:
On one hand,

$$\begin{aligned} u(dn+p) &= u(dn) \text{ (because } p \text{ is a period of } u) \\ &= v(dn+1) \end{aligned}$$

On the other hand:

$$\begin{aligned} u(dn+p) &= u(dn+lp') \\ &= v(dn+lp') \text{ (because } p < d \text{ and } p \notin \{0,1\}) \\ &= v(dn) \\ &= u(dn+1) \end{aligned}$$

Then

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

Thus

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

And this implies that $sp(u) = 1$ contradiction. Then:
the sequence $E_d(v_0, ..., v_{(d-1)}) = \psi_{\sigma,d} u$ is periodic with a period of:

$$d \times \frac{p}{\gcd(p,d)} = \text{lcm}(p,d)$$

□

4 Search for the order of the braiding sequence

Proposition 4.1.
Let u the Fibonacci sequence of $r(K)$ where $sp(u) = p$.
Let d be a natural number strictly greater than p and σ a permutation in S_d.
If $d \equiv 1 \mod p$ then the braiding sequence $\psi_{\sigma,d}u = v$ is of order less than or equal to $2d$, and satisfies the following recurrence relation:

$$v(n+2d) = v(n+d) + v(n), \forall n \in \mathbb{N}$$

Proof.
Let u the Fibonacci sequence of $r(k)$ where $sp(u) = p$.
Then

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

Let d be a natural number strictly greater than p and σ a permutation in S_d.
If $d \equiv 1 \mod p$ then $2d \equiv 2 \mod p$.
Let $n \in \mathbb{N}$ then

$$\begin{aligned}
v(n+2d) &= u\Big(d\Big[\frac{n+2d}{d}\Big] + \sigma(m)\Big) \text{ where } (n+2d) \equiv m \mod d \\
&= u\Big(d\Big[\frac{n}{d}\Big] + 2d + \sigma(m)\Big) \text{ because } n \equiv m \mod d \\
&= u\Big(d\Big[\frac{n}{d}\Big] + 2 + \sigma(m)\Big) \\
&= u\Big(d\Big[\frac{n}{d}\Big] + 1 + \sigma(m)\Big) + u\Big(d\Big[\frac{n}{d}\Big] + \sigma(m)\Big) \\
&= u\Big(d\Big[\frac{n}{d}\Big] + d + \sigma(m)\Big) + u\Big(d\Big[\frac{n}{d}\Big] + \sigma(m)\Big) \\
&= v(n+d) + v(n)
\end{aligned}$$

then the braiding sequence $\psi_{\sigma,d}u = v$ is of order less than or equal to $2d$, and satisfies the following recurrence relation:

$$v(n+2d) = v(n+d) + v(n), \forall n \in \mathbb{N}$$

□

Corollary 4.2.
Let u the Fibonacci sequence of $r(\mathbb{F}_3)$ where $sp(u) = p$.
Let d be a natural number strictly greater than p and σ a permutation in S_d.
If $d \equiv 5 \mod p$ then the braiding sequence $\psi_{\sigma,d}u = v$ is of order less than or equal to $2d$, and satisfies the following recurrene relation:

$$v(n+2d) = 2v(n+d) + v(n), \forall n \in \mathbb{N}$$

Proof.
Let u the Fibonacci sequence $r(\mathbb{F}_3)$, then its smallest period is equal to 8.
Let d be a natural number strictly greater than 8 and σ a permutation in S_d.
If $d \equiv 5 \mod 8$, then $2d \equiv 2 \mod 8$.
We can easily verify in $\mathbb{F}_3$ that :

$$u(n+5) = 2u(n+2) + u(n), \forall n \in \mathbb{N}$$

Thus

$$u(n+2) = 2u(n+5) + u(n), \forall n \in \mathbb{N}$$

Let $n \in \mathbb{N}$, thus

$$\begin{aligned} v(n+2d) &= u\Big(d\Big[\frac{n+2d}{d}\Big] + \sigma(m)\Big) \text{ where } (n+2d) \equiv m \mod d \\ &= u\Big(d\Big[\frac{n}{d}\Big] + 2d + \sigma(m)\Big) \text{ because } n \equiv m \mod d \\ &= u\Big(d\Big[\frac{n}{d}\Big] + 2 + \sigma(m))\Big) \\ &= 2u\Big(d\Big[\frac{n}{d}\Big] + 5 + \sigma(m)\Big) + u\Big(d\Big[\frac{n}{d}\Big] + \sigma(m)\Big) \\ &= 2u\Big(d\Big[\frac{n}{d}\Big] + d + \sigma(m)\Big) + u\Big(d\Big[\frac{n}{d}\Big] + \sigma(m)\Big) \\ &= 2v(n+d) + v(n) \end{aligned}$$

□

5 Application in cryptography

5.1 Recalls

We recall that the readable and understandable text that we send is called the plain text and the method allowing it to be concealed by masking its content is called encryption. The latter consists of transforming the plain text into an unintelligible text called the ciphertext. The reverse process is called decryption.
Public key cryptography is a process associated with a public key which corresponds to encryption and a secret key which corresponds to decryption.
Permutation polynomials play a crucial role in the field of cryptography, particularly in the design and analysis of cryptographic algorithms that operate in finite fields. Finite fields, also known as Galois fields, are mathematical structures used in various cryptographic applications, including encryption, digital signatures, and error-correcting codes. Permutation polynomials are a special class of polynomials that have desirable properties when used in finite field arithmetic.

Definition 5.1.
Cryptography is defined as the art or the process of writing or reading secret messages or codes. So, it is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message.

Definition 5.2.
In the language of cryptography, the codes are called ciphers. The information to be disguised is called plaintext. After transformation to a secret form, the message is called ciphertext.

Definition 5.3.
The process of converting from plaintext to ciphertext is defined as encrypting or enciphering. The inverse process from ciphertext back to plaintext is called decrypting or deciphering.

Definition 5.4.
A cryptosystem is a system for encrypting and decrypting secret messages.

Recall that cryptography with a public key is a process associated with a public key which corresponds to the encrypting and the secret key corresponds to the decrypting.

5.2 Preliminaries

Let $E = \{A, B, C, \cdots, Y, Z\}$ and $F = \{00, 01, 02, 03, \cdots, 24, 25\}$. Consider the bijection from E into F given by :

A	B	C	D	E	F	G	H	I	J	K	L	M
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
13	14	15	16	17	18	19	20	21	22	23	24	25

Let $M = M_1M_2\cdots M_k$ be the plaintext, that is to say, the message to be encrypted, where $M_i \in E,\ (1 \leq i \leq k)$.
We take d and σ, where $d \in F$ and $\sigma \in S_d$. We consider d as public key and σ as secret key. For any sequence u, we consider the braiding sequence $\psi_{d,\sigma}u$. Knowing that the braiding application $\psi_{d,\sigma}$ is bijective and that $\psi_{d,\sigma}^{-1} = \psi_{d,\sigma^{-1}}$, then we have, for all $n \in \mathbb{N}$ and all $j \in \{0,\ldots,d-1\}$:

$$(\psi_{d,\sigma}u)(dn+j) = u(dn+\sigma(j)) \ \wedge \ (\psi_{d,\sigma^{-1}}u)(dn+j) = u(dn+\sigma^{-1}(j))$$

The choice of the permutation σ must be made taking into account the fact that $0 \leq dn+\alpha \leq 25$ and $0 \leq dn+\sigma(\alpha) \leq 25$, for $0 \leq \alpha \leq d-1$. Let us set $25 = dn_0+\alpha$.
1. If $\alpha = 1$ then $25 = dn_0+1$ and to have $0 \leq dn+\alpha \leq 25$ we must take $\sigma(1) \in \{0,1\}$.
Indeed:
- for $\sigma(1) = 1$, we have :

$$(\psi_{d,\sigma}u)(25) = (\psi_{d,\sigma}u)(dn_0+1) = u(dn_0+\sigma(1)) = u(dn_0+1) \quad \text{with} \quad dn_0+1 = 25$$

- for $\sigma(1) = 0$, we have :

$$(\psi_{d,\sigma}u)(25) = (\psi_{d,\sigma}u)(dn_0+1) = u(dn_0+\sigma(1)) = u(dn_0) \ \text{ with } \ dn_0 \leq 25$$

- for $\sigma(1) \notin \{0,1\}$, we have $\sigma(1) \geq 2$, this case should be eliminated because $dn_0+\sigma(1) > 25$.

Remark 5.5.
In this case, where $\alpha = 1$, we have necessarily $d \geq 13$ because $25-1 = 24 \neq dn_0$.

2. If $\alpha \neq 1$ then we have to take $\sigma(\alpha) \in \{0,1,\ldots,\alpha\}$ because, in this case, we have $\sigma(\alpha) \leq 25$.

Remark 5.6.
- In this case, where, $\alpha \neq 1$, we have $d \leq 25$.
- If $n_0 = 0$ then $\sigma(\alpha) \in \{0,1,\ldots,d-1\}$.
- If $\alpha = 0$, *i.e.*, $25 = dn_0 = 55$ then we have to take $\sigma(0) = 0$ and for $dn_0+\alpha, \alpha \neq 0$, $d \leq 24$, we have to take $\sigma(\alpha) \in \{0,1,\ldots,\alpha\}$.

5.3 Procedure for encryption and decryption

Encryption
To encrypt the plaintext message $M = M_1M_2.\ldots.M_k$ into the ciphertext message $C = C_1C_2.\ldots.C_k$, we proceed in the following way:

1. We translate each letter $M_i \in E$ into its digital equivalent, using the bijection mentioned above to a positive integer $m_i \in F,\ 1 \leq i \leq k$.
2. the Euclidean division of m_i by the public key d gives :

$$m_i = dn_i+\alpha_i, \ \text{where} \ \ 0 \leq \alpha_i \leq d-1 \ \ \text{and} \ \ 00 \leq m_i \leq 25$$

then, choose the secret key σ as described above.
3. So, we calculate :

$$(\psi_{d,\sigma}u)(m_i) = (\psi_{d,\sigma}u)(dn_i+\alpha_i) = u(dn_i+\sigma(\alpha_i)),\ 00 \leq dn_i+\alpha_i \leq 25$$

4. Taking $c_i = dn_i + \alpha_i$, $0 \leq i \leq k$, the number $c_1c_2 \dots c_k$ is translated into letters by the bijection mentioned above into $C = C_1C_2 \dots C_k$. So, the plaintext M is encrypted by the ciphertext C.

Decryption.

To decrypt the ciphertext message $C = C_1C_2 \dots C_k$, the recipient must proceed as follows :

1. We translate C into numbers which gives the number $c_1c_2 \dots c_k$.

2. The Euclidean division of c_i by d gives :

$$c_i = dt_i + \beta_i, \text{ where } 0 \leq \beta_i \leq d-1 \text{ and } 00 \leq c_i \leq 25$$

3. So, knowing the keys d and σ, we calculate :

$$(\psi_{d,\sigma^{-1}}u)(c_i) = (\psi_{d,\sigma^{-1}}u)(dt_i + \beta_i) = u(dt_i + \sigma^{-1}(\beta_i)),\ \alpha_i = \sigma^{-1}(\beta_i),\ 00 \leq dn_i + \alpha_i \leq 25$$

4. Taking $m_i = dt_i + \alpha_i$, $0 \leq i \leq k$, the number $m_1m_2 \dots m_k$ is translated into letters which give the plaintext message $M = M_1M_2 \dots .M_k$.

5.4 Examples

1. Taking the public key $d = 4$ then we have $25 = 4.6 + 1$, where $\alpha = 1$, the secret key is $\sigma = (0, 2, 1)$ in S_4. let us encrypt the plaintext message **WORK**.

First, we replace the letters of this message with the corresponding digits. This produces the number :

$$m_1m_2m_3m_4 = 22141710$$

So, we have :

$$(\psi_{4,\sigma}u)(\mathbf{22}) = (\psi_{4,\sigma}u(4.5+2) = u(4.5+\sigma(2)) = u(4.5+1) = u(\mathbf{21})$$

$$(\psi_{4,\sigma}u)(\mathbf{14}) = (\psi_{4,\sigma}u)(4.3+2) = u(4.3+\sigma(2)) = u(4.3+1) = u(\mathbf{13})$$

$$(\psi_{4,\sigma}u)(\mathbf{17}) = (\psi_{4,\sigma}u)(4.4+1) = u(4.4+\sigma(1)) = u(4.4+0) = u(\mathbf{16})$$

$$(\psi_{4,\sigma}u)(\mathbf{10}) = (\psi_{4,\sigma}u)(4.2+2) = u(4.2+\sigma(2)) = u(4.2+1) = u(\mathbf{09})$$

Then, we obtain the following number :

$$c_1c_2c_3c_4 = 21131609$$

which is translated into letters by : **VNQJ** which is the ciphertext.

To decrypt the ciphertext message VNQJ, we replace the letters with the corresponding digits, we find the number: 21131609. knowing the public key $d = 4$ and the secret key $\sigma = (0, 2, 1)$ such that $\sigma^{-1} = (0, 1, 2)$, we have :

$$(\psi_{4,\sigma^{-1}}u)(21) = (\psi_{4,\sigma^{-1}}u)(4.5+1) = u(4.5+\sigma^{-1}(1)) = u(4.5+2) = u(\mathbf{22})$$

$$(\psi_{4,\sigma^{-1}}u)(13) = (\psi_{4,\sigma^{-1}}u)(4.3+1) = u(4.3+\sigma^{-1}(1)) = u(4.3+2) = u(\mathbf{14})$$

$$(\psi_{4,\sigma^{-1}}u)(16) = (\psi_{4,\sigma^{-1}}u)(4.4+0) = u(4.4+\sigma^{-1}(0)) = u(4.4+1) = u(\mathbf{17})$$

$$(\psi_{4,\sigma^{-1}}u)(09) = (\psi_{4,\sigma^{-1}}u)(4.2+1) = u(4.2+\sigma^{-1}(1)) = u(4.2+2) = u(\mathbf{10})$$

Then, we obtain the following number :

$$c_1c_2c_3c_4 = 22141710$$

which is translated into letters by WORK which is the plaintext message.

2. Taking the public key $d = 7$ then we have $25 = 7.3 + 4$, where $\alpha = 4 \neq 1$, the secret key is $\sigma = (1, 4, 2, 6)$ in S_7. let us encrypt the plaintext message **STUDIES**.

We replace the letters of this message with the corresponding digits. This produces the number: 18192003070418. using the same method as above, we obtain the number 161915031100 which is translated into letters by **QTPDLA**.

6 Conclusion remarks

In this paper, we investigated the properties of linear recurrence sequences through braiding mapping. We exploited its latest to develop a new cryptographic method. This method demonstrates the practical applicability of braiding sequences in enhancing cryptographic security. Future research could extend these insights to other sequence types and explore further cryptographic applications, broadening the scope of sequence-based security solutions.

References

[1] A. Ait Mokhtar, A. Necer and A. Salinier, *Endomorphismes d'algèbre de suites* , Journal de Théorie des Nombres de Bordeaux, tome 20, numéro 1 (2008),p. 1-21.

[2] 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.

[3] S. H. Jafari Petroudi, M. Pirouz, S. Jabee and M. Shadab, *A new symmetric approach to Fibonacci numbers and their properties*, Palestine Journal of Mathematics, Vol. 12(3)(2023) , 34–43.

[4] A. Ait Mokhtar, *Applications semi-affines et applications tressages*, C.R. Acad. Sci. Paris, Ser. I 348, 2010, 1-4.

[5] S. Badidja, A. Ait Mokhtar and O. OZEN, *Representation of Integers by k-Generalized Fibonacci Sequences and Applications In Cryptography*, Asian-European Journal of Mathematics (AEJM), November 28, 2020.

[6] D.J. Cantor, *On arithmetic properties of the Taylor series of rational functions*, Canad. J. Math., 21:378-382, 1969.

[7] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev and A. A. Nechaev, *Linear recurring sequences over rings and modules*, J. of Math. Sci., 76(6):2793-2915, 1995.

[8] A. C. Yeates , *Application of linear sequences to cryptography* , BSC thesis in department of mathematics at the University of Southern Mississippi (2013), 52 pp.

Author information

S. Kiouche, National School of Built and Ground Works Engineering, Kouba, Algiers.
Laboratory of Fixed Point Theory and Applications, École Normale Supérieure Kouba, Algiers,, Algeria.
E-mail: s.kiouche@yahoo.com

A. Ait Mokhtar, Laboratory of Fixed Point Theory and Applications, École Normale Supérieure Kouba, Algiers., Algeria.
E-mail: ahmed.aitmokhtar@yahoo.fr

Received: 2024-02-09
Accepted: 2024-07-23