نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۱، بهار ۱۳۹۹؛ ص ۱۰۶-۹۵

چند کد جدید روی ماتریس دنباله‌های $t-$ پیل

منصور هاشمی[۱*]، الهه مهربان [۲]

۱- دانشیار، ۲- دانشجوی دکتری، دانشگاه گیلان

(دریافت: ۹۷/۱۱/۱۳، پذیرش: ۹۸/۰۵/۱۹)

چکیده

کدگذاری یکی از شاخه‌های جالب و کاربردی ریاضیات است که به‌طور گسترده در شبکه‌های بی‌سیم ازجمله شبکه‌های تلفن همراه، شبکه‌های بی‌سیم با برد کوتاه، شبکه‌های حسگر بی‌سیم و شبکه‌های ارتباطی ماهواره‌ای مورد استفاده قرار می‌گیرد. هدف ما در این مقاله ارائه کدهای جدیدی با استفاده از دنباله‌های عددی $t-$پیل و حاصل‌ضرب هادامارد است. برای رسیدن به این هدف ابتدا به بررسی خواص ماتریس دنباله‌های عددی $t-$پیل و حاصل‌ضرب هادامارد آن‌ها می‌پردازیم. سپس با استفاده از نتایج به‌دست‌آمده، الگوریتم‌های کدگذاری و کدگشایی متناظر آن‌ها را به دست می‌آوریم. در انتها، الگوریتم بلوک‌بندی را روی ماتریس دنباله‌های عددی $t-$پیل و حاصل‌ضرب هادامارد آن‌ها مطالعه می‌کنیم.

کلیدواژه‌ها: دنباله عددی $t-$ پیل، حاصل‌ضرب هادامارد ماتریس‌ها، دترمینان ماتریس، کدگذاری

Some New Codes Theory on t-Pell Sequences Matrix

M. Hashemi*, E. Mehraban
University of Guilan
(Received: 02/02/2019; Accepted: 10/08/2019)

Abstract

Coding theory is one of the most interesting and applied branches of mathematics that has been widely used in Wireless networking, include mobile networks, wireless local area networks, wireless sensor networks and *satellite communication networks.* In *this paper, our goal is to provide some new codes by using t- Pell number sequences and Hadamard product. In order to achieve this goal, we first study the properties of matrix of t- Pell number sequences and their Hadamard product of these matrices. Then, using the obtained results, we present some coding and decoding algorithms. Finally, we study the blocking algorithm on the matrix of the t- Pell number sequences and their Hadamard product.*

Keywords: T-Pell Number Sequences, Matrix of T-Pell Sequence, Matrix Determinat, Coding

*Corresponding Author E-mail: m_hashemi@guilan.ac.ir

۱. مقدمه

نظریه کدگذاری فیبوناتچی توسط Stokhov و همکارانش [۱] در سال ۱۹۹۹، معرفی گردید. پس‌ازآن مطالعات زیادی به بررسی کدگذاری و رمزگذاری روی دنباله‌های مختلف و ماتریس آن‌ها اختصاص یافته است[۷-۲] . ماتریس مربعی پیام M و ماتریس معکوس‌پذیر A را در نظر می‌گیریم.

در این صورت $M\times A=E$ به‌عنوان الگوریتم کدگذاری و $E\times A^{-1}=M$، الگوریتم کدگشایی نامیده می‌شود. هم‌چنین ماتریس E را ماتریس کد می‌نامیم. n-امین عضو دنباله اعداد فیبوناتچی را با F_n نمایش داده و به‌صورت زیر تعریف می‌کنیم:

$$F_n=F_{n-2}+F_{n-1},\qquad n\geq 3,$$

که $F_1=F_2=1$. همچنین ماتریس Q به‌صورت زیر تعریف می‌شود:

$$Q=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix},$$

با استقرا روی n می‌توان ثابت نمود که درایه‌های توان n- ام ماتریس Q به‌صورت زیر به‌دست می‌آید:

$$Q^n=\begin{bmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{bmatrix},$$

که در آن، $n=0,\pm1,\pm2,\cdots$. Stokhov، به‌ازای عدد طبیعی p ، دنباله

$$\begin{cases}F_p(n)=F_p(n-1)+F_p(n-p-1), & n>p+1\\ F_p(1)=\cdots=F_p(p)=F_p(p+1)=1,\end{cases}$$

را در نظر گرفت و خواص این دنباله و ماتریس نمایش آن را بررسی کرد [۸]. وی همچنین به‌ازای $p=1$ که

$$F_p(n)=F_n$$

روش کدگذاری فیبوناتچی روی ماتریس $F_p(n)$، یعنی $A=Q^n$ را بیان می‌کند. اینک دنباله عددی $t-$ پیل $\left\{P_n^t\right\}_{-\infty}^{\infty}$ ، $t\geq 2$، را به‌صورت زیر در نظر می‌گیریم [۹].

$$\begin{cases}P_n^t=tP_{n-1}^t+P_{n-2}^t & n\geq 2,\\ P_n^t=P_{n+2}^t-tP_{n-1}^t & n<0,\end{cases}$$

که $P_0^t=0$ و $P_1^t=1$.

به‌سادگی می‌توان نشان داد که جواب رابطه بازگشتی دنباله عددی $t-$ پیل به‌صورت

$$P_n^t=\frac{1}{2\sqrt{t^2+4}}\left[\left(t+\sqrt{t^2+4}\right)^n-\left(t-\sqrt{t^2+4}\right)^n\right],$$

است. مقدار $\tau=\lim\frac{P_{n+1}^t}{P_n^t}=\frac{t+\sqrt{t^2+4}}{2}$ را نسبت حدی دنباله عددی $t-$ پیل نامیم [۹ و ۱۰].

لم ۱-۲. فرض کنید m، n و $t\geq 2$ اعداد صحیح باشند. روابط زیر روی دنباله عددی $t-$ پیل برقرار است: (در اینجا فرض می‌کنیم $P_n=P_n^t$)

$$(i)\,P_{-i}=(-1)^{i+1}P_i,$$

$$(ii)\,P_1+P_3+\cdots+P_{2n-1}=\frac{P_{2n}}{t},$$

$$(iii)\,P_0+P_2+\cdots+P_{2n}=\frac{P_{2n-1}-1}{t},$$

$$(iv)\,P_n^2+P_{n+1}^2=P_{2n+1}^2,$$

$$(v)\,P_{2n}=P_n\left(P_{n-1}+P_{n+1}\right),$$

$$(vi)\,P_{n+m}=P_{m-1}P_n+P_mP_{n+1},$$

$$(vii)\,P_{n+1}P_{n-1}-P_n{}^2=(-1)^n.$$

TAS و همکارانش با مطالعه خواص دنباله $\left\{P_n^t\right\}_0^{\infty}$ و ماتریس آن به‌ازای $t=2$، الگوریتم کدگذاری و کدگشایی روی ماتریس دنباله عددی ۲- پیل را ارائه دادند [۷].

در این مقاله با بررسی خواص دنباله $\left\{P_n^t\right\}_0^{\infty}$ و ماتریس آن به‌ازای $t\geq 3$، الگوریتم کدگذاری و کدگشایی بر پایه ماتریس دنباله عددی $t-$پیل، ارائه می‌شود. در بخش‌های دوم و سوم این مقاله، ماتریس دنباله عددی $t-$ پیل و حاصل‌ضرب هادمارد آن را بررسی می‌کنیم. بخش چهارم اختصاص به ارائه یک روش کدگذاری و کدگشایی روی ماتریس‌های $t-$ پیل و حاصل‌ضرب هادمارد آن‌ها دارد. در بخش پنجم روش بلوک‌بندی روی ماتریس دنباله عددی $t-$ پیل و حاصل‌ضرب هادامارد آن را ارائه می‌دهیم.

۲. ماتریس دنباله‌های عددی $t-$ پیل و خواص آن‌ها

در این بخش، به معرفی ماتریس دنباله عددی $t-$ پیل پرداخته و سپس، ماتریس وارون آن را به‌دست می‌آوریم.

لم ۲-۱. ماتریس دنباله عددی $t-$پیل که با $Q_t\left(n,P_n^t\right)$ نشان می‌دهیم، به استقرا می‌توان ثابت کرد که

$$Q_t\left(n,P_n^t\right)=\begin{bmatrix}P_{n+1}^t & P_n^t\\ P_n^t & P_{n-1}^t\end{bmatrix}.$$

به‌خصوص در حالت $t=3$، با توجه به فرمول

$$P_n^3 = 3P_{n-1}^3 + P_{n-2}^3$$

داریم:

$$Q_3\left(4, P_4^3\right) = \begin{bmatrix} 109 & 33 \\ 33 & 10 \end{bmatrix}.$$

اینک به محاسبه وارون $Q_t\left(n, P_n^t\right)$ می‌پردازیم. ابتدا دترمینان $Q_t\left(n, P_n^t\right)$ را محاسبه می‌کنیم.

لم ۲-۲. دترمینان ماتریس $Q_t\left(n, P_n^t\right)$ برابر با $(-1)^n$ است.

برهان. بنا به لم ۲-۱ داریم:

$$Q_t\left(n, P^t{}_n\right) = \begin{bmatrix} P_{n+1}^t & P^t{}_n \\ P^t{}_n & P^t{}_{n-1} \end{bmatrix},$$

در نتیجه $Det Q_t\left(n, P_n^t\right) = P_{n+1}^t P_{n-1}^t - (P_n^t)^2$. لذا، با توجه به لم ۱-۲ (vii) خواهیم داشت:

$$Det\, Q_t\left(n, P_n^t\right) = (-1)^n.$$

با استفاده از لم قبل داریم:

لم ۲-۳. وارون ماتریس $Q_t\left(n, P_n^t\right)$ که $t \geq 2$ به‌صورت زیر است:

$$Q_t^{-1}\left(n, P_n^t\right) = \frac{1}{(-1)^n}\begin{bmatrix} P_{n-1}^t & -P^t{}_n \\ -P^t{}_n & P^t{}_{n+1} \end{bmatrix}.$$

برای سادگی نمادهای مورد استفاده، وقتی‌که مقدار t مشخص باشد بجای $Q_t\left(n, P_n^t\right)$ می‌نویسیم $Q_t\left(n, P_n\right)$. در جدول زیر، ماتریس دنباله عددی ۳- پیل و وارون آن، به‌ازای $n = 0, 1, 2, 3, 4$، قابل‌مشاهده است.

n	0	1	2	3	4
$Q_3(n,P_n)$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 33 & 10 \\ 10 & 3 \end{bmatrix}$	$\begin{bmatrix} 109 & 33 \\ 33 & 10 \end{bmatrix}$
$Q_3^{-1}(n,P_n)$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix}$	$\begin{bmatrix} 1 & -3 \\ -3 & 10 \end{bmatrix}$	$\begin{bmatrix} -3 & 10 \\ 10 & -33 \end{bmatrix}$	$\begin{bmatrix} 109 & -33 \\ -33 & 10 \end{bmatrix}$

به‌عنوان‌مثال ماتریس وارون $Q_3\left(n, P_n\right)$ به‌ازای $n = 2k$ به‌صورت ذیل است:

$$Q_3^{-1}\left(2k, P_{2k}\right) = \begin{bmatrix} P_{2k-1} & -P_{2k} \\ -P_{2k} & P_{2k+1} \end{bmatrix},$$

و به‌ازای $n = 2k+1$ داریم:

$$Q_3^{-1}\left(2k+1, P_{2k+1}\right) = \begin{bmatrix} -P_{2k} & P_{2k+1} \\ P_{2k+1} & -P_{2k+2} \end{bmatrix}.$$

۳. حاصل‌ضرب هادمارد روی $Q_t\left(n, P_n^t\right)$

در اینجا، ابتدا حاصل‌ضرب هادمارد ماتریس‌های $Q_t\left(n, P_n^t\right)$ و $Q^{-1}{}_t\left(n, P_n^t\right)$ را تعریف نموده و سپس به بررسی دترمینان این حاصل‌ضرب می‌پردازیم که از آن در بخش چهارم استفاده می‌شود.

فرض کنید A و B دو ماتریس $m \times n$ باشند در این صورت حاصل‌ضرب هادمارد A و B که با $A \bullet B$ نشان می‌دهیم به‌صورت زیر تعریف می‌شود:

$$(A \bullet B)_{ij} = (A)_{ij}(B)_{ij}.$$

تعریف ۳-۱. فرض کنید $Q_t = Q_t\left(n, P_n^t\right)$ ماتریس دنباله عددی $t-$ پیل و Q_t^{-1}، ماتریس وارون آن باشد. در این صورت حاصل‌ضرب هادمارد آن‌ها را با $Q_t\left(n, P_n^t\right) o\, Q^{-1}{}_t\left(n, P_n^t\right)$ نمایش داده و به‌صورت زیر تعریف می‌شود [۱۱].

$$Q_t\left(n, P_n^t\right) o\, Q^{-1}{}_t\left(n, P_n^t\right) = \frac{1}{(-1)^n}\left(Q_t \bullet adj\, Q_t\right)$$

در نتایج زیر دترمینان و وارون حاصل‌ضرب هادمارد را به‌دست می‌آوریم

$$Q_t\left(n, P_n^t\right) o Q^{-1}{}_t\left(n, P_n^t\right)$$

قضیه ۳-۲. داریم:

الف)

$$Q_t\left(n, P_n^t\right) o Q^{-1}{}_t\left(n, P_n^t\right) = \frac{1}{(-1)^n}\begin{bmatrix} P_{n+1}^t P_{n-1}^t & -(P_n^t)^2 \\ -(P_n^t)^2 & P_{n+1}^t P_{n-1}^t \end{bmatrix}$$

ب)

$$Det\left(Q_t\left(n, P_n^t\right) o Q^{-1}{}_t\left(n, P_n^t\right)\right) = \begin{cases} 1 + 2(P_n^t)^2 & n = 2k, \\ 1 - 2(P_n^t)^2 & n = 2k+1. \end{cases}$$

برهان. به‌دلیل اینکه

$$Q_t\left(n, P^t{}_n\right) = \begin{bmatrix} P_{n+1}^t & P^t{}_n \\ P^t{}_n & P_{n-1}^t \end{bmatrix}$$

و

$$adjQ_t\left(n,P^t{}_n\right)=\begin{bmatrix} P^t_{n-1} & -P^t{}_n \\ -P^t{}_n & P^t{}_{n+1}\end{bmatrix}$$

حکم الف، از تعریف به‌دست می‌آید. برای اثبات قسمت دوم، ابتدا فرض می‌کنیم $n=2k$. بنا بر قسمت هفتم از لم ۱-۲ داریم:

$$\begin{aligned} Det\left(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right)\right) &= Det\begin{bmatrix} P^t_{2k+1}P^t_{2k-1} & -(P^t_{2k})^2 \\ -(P^t_{2k})^2 & P^t_{2k+1}P^t_{2k-1}\end{bmatrix} \\ &=\left(P^t_{2k+1}P^t_{2k-1}-(P^t_{2k})^2\right)\left(P^t_{2k+1}P^t_{2k-1}+(P^t_{2k})^2\right) \\ &=(-1)^{2k}\,(1+2(P^t_{2k})^2)=1+2(P^t_{2k})^2. \end{aligned}$$

برای عدد فرد $n=2k+1$ داریم:

$$Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right)=\begin{bmatrix} -P^t_{2k+2}P^t_{2k} & (P^t_{2k+1})^2 \\ (P^t_{2k+1})^2 & -P^t_{2k+2}P^t_{2k}\end{bmatrix}.$$

لذا،

$$\begin{aligned} Det(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right)) &= \left(P^t_{2k+2}P^t_{2k}-(P^t_{2k+1})^2\right)\left(P^t_{2k+2}P^t_{2k}+(P^t_{2k+1})^2\right) \\ &=(-1)^{2k+1}(-1+2(P^t_{2k+1})^2)=1-2(P^t_{2k+1})^2. \end{aligned}$$

با استفاده از قضیه ۳-۱، اثر ماتریس حاصل‌ضرب هادمارد $Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right)$ به‌صورت زیر است:

نتیجه ۳-۳.

$$trac(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right))=\begin{cases} 2(1+(P^t_n)^2), & n=2k, \\ 2(1-(P^t_n)^2), & n=2k+1. \end{cases}$$

قضیه ۳-۴. برای معکوس ماتریس حاصل‌ضرب هادمارد $Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right)$ داریم:

$$(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right))^{-1}=\begin{cases} \begin{bmatrix} \frac{1+(P^t_n)^2}{1+2(P^t_n)^2} & \frac{(P^t_n)^2}{1+2(P^t_n)^2} \\ \frac{(P^t_n)^2}{1+2(P^t_n)^2} & \frac{1+(P^t_n)^2}{1+2(P^t_n)^2}\end{bmatrix} & n=2k, \\ \begin{bmatrix} \frac{1-(P^t_n)^2}{1-2(P^t_n)^2} & -\frac{(P^t_n)^2}{1-2(P^t_n)^2} \\ -\frac{(P^t_n)^2}{1-2(P^t_n)^2} & \frac{1-(P^t_n)^2}{1-2(P^t_n)^2}\end{bmatrix} & n=2k+1 \end{cases}$$

برهان. اگر $n=2k$ آنگاه،

$$adj(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right))=\begin{bmatrix} P^t_{2k+1}P^t_{2k-1} & (P^t_{2k})^2 \\ (P^t_{2k})^2 & P^t_{2k+1}P^t_{2k-1}\end{bmatrix}.$$

با استفاده از رابطه $P^t_{2k+1}P^t_{2k-1}-(P^t_{2k})^2=(-1)^n$، داریم:

$$adj(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right))=\begin{bmatrix} 1+(P^t_{2k})^2 & (P^t_{2k})^2 \\ (P^t_{2k})^2 & 1+(P^t_{2k})^2\end{bmatrix}.$$

چون n عدد زوجی است،

$$(Q_t\left(n,P^t_n\right)oQ^{-1}{}_t\left(n,P^t_n\right))^{-1}=\begin{bmatrix} \frac{1+(P^t_{2k})^2}{1+2(P^t_{2k})^2} & \frac{(P^t_{2k})^2}{1+2(P^t_{2k})^2} \\ \frac{(P^t_{2k})^2}{1+2(P^t_{2k})^2} & \frac{1+(P^t_{2k})^2}{1+2(P^t_{2k})^2}\end{bmatrix}.$$

برای حالتی که n عددی فرد است، حکم به‌صورت مشابه اثبات می‌شود.

۴. کدگذاری و کدگشایی روی ماتریس دنباله‌های عددی $t-$ پیل و حاصل‌ضرب هادمارد آن‌ها

در این بخش به بررسی روش کدگذاری و کدگشایی روی ماتریس $Q_t\left(n,P^t_n\right)$ و حاصل‌ضرب هادمارد آن‌ها می‌پردازیم. فرض کنید $M\times Q_t\left(n,P^t_n\right)=E$ یک الگوریتم کدگذاری ماتریس دنباله عددی $t-$ پیل و $E\times Q^{-1}_t\left(n,P^t_n\right)=M$ الگوریتم متناظر کدگشایی ماتریس دنباله عددی $t-$ پیل باشند که در آن، M پیام کد شده به‌صورت ماتریس 2×2 با نمایش زیر است:

$$M=\begin{bmatrix} m_1 & m_2 \\ m_3 & m_4\end{bmatrix}$$

به‌طوری‌که $m_i>0$، $1\le i\le 4$. برای ارائه یک مثال، قرار می‌دهیم:

$$Q_3\left(3,P^3_3\right)=\begin{bmatrix} 33 & 10 \\ 10 & 3\end{bmatrix},$$

که ماتریس وارون آن برابراست با:

$$Q^{-1}_3\left(3,P^3_3\right)=\begin{bmatrix} -3 & 10 \\ 10 & -33\end{bmatrix}.$$

در این صورت، بر طبق الگوریتم $M\times Q_t\left(n,P^t_n\right)=E$ خواهیم داشت:

$$\begin{aligned} M\times Q_3\left(3,P^3_3\right) &= \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4\end{bmatrix}\times\begin{bmatrix} 33 & 10 \\ 10 & 3\end{bmatrix} \\ &=\begin{bmatrix} 33m_1+10m_2 & 10m_1+3m_2 \\ 33m_3+10m_4 & 10m_3+3m_4\end{bmatrix} \qquad (1) \\ &=\begin{bmatrix} e_1 & e_2 \\ e_3 & e_4\end{bmatrix}=E, \end{aligned}$$

که در آن،

$$\begin{aligned} e_1&=33m_1+10m_2, \\ e_2&=10m_1+3m_2, \\ e_3&=33m_3+10m_4, \\ e_4&=10m_3+3m_4. \end{aligned}$$

بنابراین، یک پیام کدگذاری شده به‌صورت $E=e_1,e_2,e_3,e_4$ به کانال ارتباطی فرستاده می‌شود. حال الگوریتم کدگشایی از ماتریس E به‌صورت زیر خواهد بود.

$$\begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} \times \begin{bmatrix} -3 & 10 \\ 10 & -33 \end{bmatrix} = \begin{bmatrix} (-3)e_1+10e_2 & 10e_1+(-33)e_2 \\ (-3)e_3+10e_4 & 10e_3+(-33)e_4 \end{bmatrix} = \begin{bmatrix} e_1' & e_2' \\ e_3' & e_4' \end{bmatrix}. \quad (۲)$$

با درنظرگرفتن فرمول (۱) و محاسبه درایه‌های ماتریس (۲) خواهیم داشت:

$$\begin{bmatrix} e_1' & e_2' \\ e_3' & e_4' \end{bmatrix} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} = M.$$

به‌سادگی می‌توان نشان داد روش فوق به‌ازای $t \geq 3$ برقرار است. اینک، دترمینان ماتریس کدگذاری شده E را به‌دست می‌آوریم.

قضیه ۴-۱. فرض کنید E ماتریس کدگذاری و M پیام کد شده باشد. در این صورت:

$$Det\,E = \begin{cases} Det\,M, & n=2k, \\ -Det\,M, & n=2k+1. \end{cases}$$

برهان. با توجه به الگوریتم کدگذاری $E=M\times Q_t\left(n,P_n^t\right)$ نتیجه می‌شود:

$$Det\,E = Det(M\times Q_t\left(n,P_n^t\right)) = Det\,M \times Det\,Q_t\left(n,P_n^t\right).$$

اینک با توجه به لم ۲-۲، داریم:

$$Det\,E = Det\,M \times (-1)^n.$$

و حکم ثابت می‌شود. در این قسمت، خطای الگوریتم کدگذاری را مورد بررسی قرار می‌دهیم. در ابتدا، به بررسی خطای الگوریتم کدگذاری روی ماتریس دنباله عددی -3 پیل پرداخته و سپس با تعمیم آن نشان می‌دهیم که حکمی مشابه برای هر $t \geq 3$ برقرار است. الگوریتم کدگذاری شده را می‌توان به‌صورت زیر نوشت:

$$E = M\times Q_3\left(n,P_n^3\right) = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \times \begin{bmatrix} P_{n+1}^3 & P_n^3 \\ P_n^3 & P_{n-1}^3 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}, \quad (۳)$$

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} = E\times Q_3^{-1}\left(n,P_n^3\right) = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} \times Q_3^{-1}\left(n,P_n^3\right). \quad (۴)$$

در حالتی که n عددی فرد باشد، با استفاده از لم ۲-۲ و قرار دادن آن در فرمول (۴)، رابطه زیر به‌دست می‌آید:

$$\begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} \times \begin{bmatrix} -P_{n-1}^3 & P_n^3 \\ P_n^3 & -P_{n+1}^3 \end{bmatrix}. \quad (۵)$$

با توجه به فرمول (۵)، هریک از درایه‌های ماتریس M را می‌توان به شکل زیر محاسبه کرد:

$$\begin{aligned} m_1 &= -P_{n-1}^3 e_1 + P_n^3 e_2, \\ m_2 &= P_n^3 e_1 - P_{n+1}^3 e_2, \\ m_3 &= -P_{n-1}^3 e_3 + P_n^3 e_4, \\ m_4 &= P_n^3 e_3 - P_{n+1}^3 e_4. \end{aligned}$$

چون $m_i > 0$، برای $1 \leq i \leq 4$ داریم:

$$-P_{n-1}^3 e_1 + P_n^3 e_2 > 0, \quad (۶)$$

$$P_n^3 e_1 - P_{n+1}^3 e_2 > 0, \quad (۷)$$

$$-P_{n-1}^3 e_3 + P_n^3 e_4 > 0, \quad (۸)$$

$$P_n^3 e_3 - P_{n+1}^3 e_4 > 0. \quad (۹)$$

نامساوی‌های زیر با توجه به روابط (۶) و (۷) به‌دست می‌آیند.

$$\frac{P_{n+1}^3}{P_n^3} e_2 < e_1 < \frac{P_n^3}{P_{n-1}^3} e_2$$

درنتیجه

$$\lim \frac{P_{n+1}^3}{P_n^3} < \lim \frac{e_1}{e_2} < \lim \frac{P_n^3}{P_{n-1}^3}.$$

و داریم $e_1 \approx \tau e_2$ که در آن $\tau = \frac{3+\sqrt{13}}{2}$ نسبت حدی دنباله عددی ۳-پیل است. به‌روش مشابه، با توجه به نامساوی‌های (۸) و (۹) داریم:

$$\frac{P_{n+1}^3}{P_n^3} e_4 < e_3 < \frac{P_n^3}{P_{n-1}^3} e_4$$

بنابراین،

$$\lim \frac{P_{n+1}^3}{P_n^3} < \lim \frac{e_3}{e_4} < \lim \frac{P_n^3}{P_{n-1}^3}.$$

و $e_3 \approx \tau e_4$. نتایج فوق برای هر دنباله $t-$پیل، $t \geq 3$، برقراراست که در آن $\tau = \frac{t+\sqrt{t^2+4}}{2}$، نسبت حدی دنباله فوق است. اینک به بررسی مقدار خطا و تصحیح آن در این الگوریتم کدگذاری و کدگشایی روی دنباله عددی $t-$ پیل می‌پردازیم. فرض اول ما این است که فقط یک خطا در ماتریس E از کانال انتقال دریافت شود. واضح است که برای آن چهار حالت مختلف وجود دارد.

$$(a)\begin{bmatrix} x & e_2 \\ e_3 & e_4 \end{bmatrix},\ (b)\begin{bmatrix} e_1 & y \\ e_3 & e_4 \end{bmatrix},\ (c)\begin{bmatrix} e_1 & e_2 \\ z & e_4 \end{bmatrix},\ (d)\begin{bmatrix} e_1 & e_2 \\ e_3 & t \end{bmatrix}, \quad (۱۰)$$

که در آن، x,y,z,t عناصر همراه با خطا هستند.

می‌خواهیم رابطه (۳) را برای حالت‌های مختلف (a)، (b)، (c) و (d) بررسی کنیم. با توجه به اینکه $xe_4 - e_2e_3 = (-1)^n DetM$ یک خطا برای عضو e_1، $e_1e_4 - ye_3 = (-1)^n DetM$ یک خطا برای عضو e_2، $e_1e_4 - e_2z = (-1)^n DetM$ یک خطا برای عضو e_3 و $e_1t - e_2e_3 = (-1)^n DetM$ یک خطا برای عضو e_4 است، داریم:

$$x = \frac{(-1)^n Det\,M + e_2e_3}{e_4}, \qquad (۱۱)$$

$$y = \frac{-(-1)^n Det\,M + e_1e_4}{e_3}, \qquad (۱۲)$$

$$z = \frac{-(-1)^n Det\,M + e_1e_4}{e_2}, \qquad (۱۳)$$

$$t = \frac{(-1)^n Det\,M + e_2e_3}{e_1}. \qquad (۱۴)$$

روابط (۱۴- ۱۱) مقادیر عناصر همراه با خطا را نشان می‌دهد. با توجه به این‌که $e_1 \approx \tau e_2$ و $e_3 \approx \tau e_4$، در عمل تنها می‌توانیم یک انتخاب از متغیرهای x, y, z, t داشته باشیم. به‌روش مشابه، می‌توان خطای دوگانه را نیز روی ماتریس E به‌دست آورد. به‌عنوان‌مثال حالت دومتغیره زیر را برای ماتریس E در نظر می‌گیریم.

$$\begin{bmatrix} x & y \\ e_3 & e_4 \end{bmatrix}, \qquad (۱۵)$$

با استفاده از قضیه ۴-۱، روابط زیر از ماتریس (۱۵) به‌دست می‌آید:

$$xe_4 - ye_3 = (-1)^n Det\,M.$$

هم‌چنین، رابطه $x \approx \tau y$ بین x و y وجود دارد. به‌روش مشابه، می‌توان همه حالت‌های ممکن را برای خطای سه‌گانه و چهارگانه به‌دست آورد. با توجه به‌روش فوق، پانزده حالت ممکن خطا، در الگوریتم (۳) وجود دارد که می‌توان چهارده حالت از خطاهای فوق را تصحیح کرد و این نشان می‌دهد توانایی تصحیح خطا در این روش برابراست با:

$$\frac{14}{15} = 0.933 = \%93.3$$

به‌ویژه زمانی که یک سطر از ماتریس کدگذاری شده همگی با خطا دریافت شود، برای کدگشایی از روابط $e_1 \approx \tau e_2$ و $e_3 \approx \tau e_4$ استفاده می‌شود. حال سؤالی که پیش می‌آید این است که مقدار n تا چه اندازه باید بزرگ باشد تا بتوان ادعا نمود که فرایند کدگشایی صحیح انجام می‌شود. مثال زیر به‌طور تقریبی به این سؤال پاسخ می‌دهد.

مثال ۴-۲. فرض کنید $t = 3$ و ماتریس پیام M به‌صورت زیر باشد:

$$M = \begin{bmatrix} 451 & 897 \\ 918 & 102 \end{bmatrix}.$$

بنابراین،

$$\tau = \frac{t + \sqrt{t^2 + 4}}{2} = \frac{3 + \sqrt{13}}{2} = 3.3027.$$

با در نظر گرفتن $n = 4$، داریم:

$$E = \begin{bmatrix} 78760 & 23853 \\ 103428 & 31314 \end{bmatrix}, \quad \begin{cases} \frac{e_1}{e_2} = \frac{78760}{23853} = 3.3018 \\ \frac{e_3}{e_4} = \frac{103428}{31314} = 3.329 \end{cases}$$

اگر $n = 8$ آنگاه $E = \begin{bmatrix} 9371989 & 2837610 \\ 12307014 & 3726264 \end{bmatrix}$ و

$$\begin{cases} \frac{e_1}{e_2} = \frac{9371989}{2837610} = 3.3027 \\ \frac{e_3}{e_4} = \frac{12307014}{3726264} = 3.3027 \end{cases}$$

با مشاهده نتایج به‌دست‌آمده برای حالت $n = 4, 8$، واضح است که با توجه به ماتریس پیام M مقدار $n=8$ مناسب‌تر است. سرانجام برای مناسب بودن تصحیح خطای این روش کدگذاری، کد همینگ را در حالت $n=15$ و $k=10$ در نظر بگیرید. توانایی تصحیح خطا در این حالت برابر است با

$$\frac{31744}{32505856} = 0.0009765 = \%0.09765.$$

از طرفی چون توانایی تصحیح خطا در روش t-پیل برابر با $\%93.3$ است. روش t-پیل در مقایسه با کد همینگ در اینجا ۹۵۰ بار بیشتر توانایی تصحیح خطا دارد. اکنون، به بررسی کدگذاری روی حاصل‌ضرب هادمارد ماتریس دنباله عددی t-پیل می‌پردازیم. ابتدا، مانند قبل، پیام کد شده M را به‌صورت ماتریس 2×2 زیر در نظر می‌گیریم:

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}$$

که در آن، $m_i > 0,\ i = 1,2,3,4$.

در این حالت، $M \times (Q_t(n, P_n^t) o Q_t^{-1}(n, P_n^t)) = E$ الگوریتم کدگذاری حاصل‌ضرب هادمارد ماتریس دنباله عددی

$-t$ پیل و $E\times(Q_t\left(n,P_n^t\right)oQ_t^{-1}\left(n,P_n^t\right))^{-1}=M$ الگوریتم کدگشایی آن است. ابتدا با یک مثال به بیان روش فوق می‌پردازیم. ماتریس $Q_2\left(4,P_4^2\right)oQ_2^{-1}\left(4,P_4^2\right)$ را در نظر می‌گیریم، داریم:

$$Q_2\left(4,P_4^2\right)o\,Q_2^{-1}\left(4,P_4^2\right)=\begin{bmatrix}P_3P_5 & -(P_4)^2\\ -(P_4)^2 & P_3P_5\end{bmatrix}=\begin{bmatrix}145 & -144\\ -144 & 145\end{bmatrix}, \quad (۱۶)$$

از طرف دیگر

$$(Q_2\left(4,P_4^2\right)oQ^{-1}{}_2\left(4,P_4^2\right))^{-1}=\begin{bmatrix}\frac{1+(P_4^2)^2}{1+2(P_4^2)^2} & \frac{(P_4^2)^2}{1+2(P_4^2)^2}\\ \frac{(P_4^2)^2}{1+2(P_4^2)^2} & \frac{1+(P_4^2)^2}{1+2(P_4^2)^2}\end{bmatrix}=\begin{bmatrix}\frac{145}{289} & \frac{144}{289}\\ \frac{144}{289} & \frac{145}{289}\end{bmatrix}, \quad (۱۷)$$

با توجه به ماتریس پیام کد شده M و رابطه (۱۶) داریم:

$$M\times(Q_2\left(4,P_4^2\right)oQ_2^{-1}\left(4,P_4^2\right))=\begin{bmatrix}m_1 & m_2\\ m_3 & m_4\end{bmatrix}\times\begin{bmatrix}145 & -144\\ -144 & 145\end{bmatrix}=\begin{bmatrix}145m_1-144m_2 & -144m_1+145m_2\\ 145m_3-144m_4 & -144m_3+145m_4\end{bmatrix}=\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix}=E,$$

که در آن،

$$\begin{aligned}e_1&=145m_1-144m_2,\\ e_2&=-144m_1+145m_2,\\ e_3&=145m_3-144m_4,\\ e_4&=-144m_3+145m_4.\end{aligned} \quad (۱۸)$$

لذا، پیام کدگذاری شده $E=e_1,e_2,e_3,e_4$ به کانال ارتباطی فرستاده می‌شود. کدگشایی از ماتریس کدگذاری شده E به‌روش زیر است:

$$\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix}\times\begin{bmatrix}\frac{145}{289} & \frac{144}{289}\\ \frac{144}{289} & \frac{145}{289}\end{bmatrix}=\begin{bmatrix}\frac{145}{289}e_1+\frac{144}{289}e_2 & \frac{144}{289}e_1+\frac{145}{289}e_2\\ \frac{145}{289}e_3+\frac{144}{289}e_4 & \frac{144}{289}e_3+\frac{145}{289}e_4\end{bmatrix}=\begin{bmatrix}e_1' & e_2'\\ e_3' & e_4'\end{bmatrix}=E. \quad (۱۹)$$

بنابراین، از روابط (۱۸) و (۱۹) داریم:

$$\begin{bmatrix}e_1' & e_2'\\ e_3' & e_4'\end{bmatrix}=\begin{bmatrix}m_1 & m_2\\ m_3 & m_4\end{bmatrix}=M.$$

۵. ارائه روش بلوک‌بندی روی ماتریس دنباله‌های عددی $-t$ پیل و حاصل‌ضرب هادامارد آن‌ها

در اینجا، به‌روش بلوک‌بندی روی ماتریس دنباله‌های عددی $-t$ پیل و حاصل‌ضرب هادمارد آن‌ها می‌پردازیم. در این روش ماتریس پیام M، ماتریس مربعی به ابعاد $2m$ است. درصورتی‌که تعداد درایه‌های ماتریس کم‌تر باشد درایه‌های باقیمانده را با صفر کامل می‌کنیم. تقسیم ماتریس M، به ماتریس‌های 2×2، $B_i\ \left(1\le i\le m^2\right)$ از چپ به راست را یک بلوک‌بندی ماتریس M نامیم. اینک به معرفی نمادهای موردنیاز در این روش می‌پردازیم: ماتریس‌های B_i را به‌صورت زیر در نظر می‌گیریم:

$$B_i=\begin{bmatrix}b_{i1} & b_{i2}\\ b_{i3} & b_{i4}\end{bmatrix}.$$

قرار می‌دهیم:

$$n=\begin{cases}3 & m\le1,\\ \left[\frac{m^2}{2}\right] & m>1.\end{cases}$$

همچنین با توجه به لم ۲-۱ داریم:

$$Q_t\left(n,P_n^t\right)=\begin{bmatrix}P_{n+1}^t & P_n^t\\ P_n^t & P_{n-1}^t\end{bmatrix},\ t\ge3$$

قرار می‌دهیم

$$Q_t\left(n,P_n^t\right)=\begin{bmatrix}P_1 & P_2\\ P_3 & P_4\end{bmatrix}$$

بنابراین،

$$B_iQ_t(n,P_n^t)=\begin{bmatrix}b_{i1}P_1+b_{i2}P_3 & b_{i1}P_2+b_{i2}P_4\\ b_{i3}P_1+b_{i4}P_4 & b_{i3}P_2+b_{i3}P_4\end{bmatrix}, \quad (۲۰)$$

و

$$trc(B_iQ_t(n,P_n^t))=b_{i1}P_1+b_{i2}P_3+b_{i3}P_2+b_{i4}P_4,$$

$$\det(B_iQ_t(n,P_n^t))=(b_{i1}P_1+b_{i2}P_3)\times(b_{i3}P_2+b_{i3}P_4)-(b_{i1}P_2+b_{i2}P_4)\times(b_{i3}P_1+b_{i4}P_4). \quad (۲۱)$$

سرانجام برای ارائه مثال‌های مناسب، در جدول (۱) به کد کردن حروف الفبای زبان فارسی به پیمانه 34 می‌پردازیم.

جدول ۱. کدگذاری حروف الفبای فارسی

الف	ب	پ	ت	ث	ج	چ	ح	خ
1	2	3	4	5	6	7	8	9
د	ذ	ر	ز	ژ	س	ش	ص	ض
10	11	12	13	14	15	16	17	18
ط	ظ	ع	غ	ف	ق	ک	گ	ل
19	20	21	22	23	24	25	26	27
م	ن	و	ه	ی	0	:		
28	29	30	31	32	33	34		

۵-۱. الگوریتم‌های کد بلوک‌بندی نوع اول

الف) مراحل الگوریتم کدگذاری

۱- بلوک‌بندی ماتریس M، به بلوک‌های $B_i \left(1\le i\le m^2\right)$.

۲- تعیین مقادیر n و t

۳- محاسبه $C_i = B_i Q_t(n, P_n^t)$

۴- تعیین $c_{ij}\ (1\le i\le 4)$

۵- محاسبه $\det(C_i)$

۶- ساختن ماتریس کدگذاری شده

$$E=\left[d_i,\quad C_{ik}\right]_{k\in\{2,3,4\}}$$

که $d_i = \det(C_i)$.

۷- پایان الگوریتم.

ب) الگوریتم کدگشایی

۱- قرار دادن $P = Q_t\left(n, P_n^t\right)$ و تعیین P_j به‌ازای $1\le j\le 4$.

۱- محاسبه $P_1 c_{j3} + P_3 c_{j4}$ و جایگذاری آن در e_{j3} برای $(1\le j\le 4)$.

۲- پیگیری فرایند

$$P_2 c_{j3} + P_4 c_{j4} \to e_{j4},\quad (1\le j\le 4).$$

۳- به‌دست آوردن x_i از

$$\left(P_1 e_{i4} - P_2 e_{i3}\right)x_i + \left(P_3 e_{i4} - P_4 e_{i3}\right)c_{i2} = (-1)^n \times d_i.$$

۵- محاسبه $C_i\ (1\le i\le 4)$ به‌وسیله جایگذاری x_i در درایه c_{i1}

.

۶- محاسبه $B_i\ (1\le i\le 4)$ توسط

$$B_i = C_i\left(Q_t(n, P_n^t)\right)^{-1}.$$

۷- به‌دست آوردن ماتریس پیام M.

۸- پایان الگوریتم.

با مثال زیر روش بلوک‌بندی روی ماتریس دنباله عددی $t-$ پیل را توضیح می‌دهیم. توجه شود که بجای فاصله بین دو کلمه (فضای خالی بین دو کلمه) از نماد 0 استفاده می‌کنیم.

مثال ۵ -۲. پیام به‌صورت زیر را در نظر می‌گیریم:

"ریاضیات زیبا است"

حل. ماتریس M (ماتریس پیام) به‌صورت زیر است:

$$M=\begin{bmatrix} \text{ر} & \text{ی} & \text{الف} & \text{ض} \\ \text{ی} & \text{الف} & \text{ت} & 0 \\ \text{ز} & \text{ی} & \text{ب} & \text{الف} \\ 0 & \text{الف} & \text{س} & \text{ت} \end{bmatrix},$$

۱- ابتدا بلوک‌های ماتریس M را به‌دست می‌آوریم. داریم:

$$B_1=\begin{bmatrix} \text{ر} & \text{ی} \\ \text{الف} & \text{ی} \end{bmatrix},\ B_2=\begin{bmatrix} \text{ض} & \text{الف} \\ \text{ت} & 0 \end{bmatrix},$$

$$B_3=\begin{bmatrix} \text{ز} & \text{ی} \\ 0 & \text{الف} \end{bmatrix},\ B_4=\begin{bmatrix} \text{ب} & \text{الف} \\ \text{س} & \text{ت} \end{bmatrix}.$$

با توجه به جدول (۱) داریم:

$$B_1=\begin{bmatrix} 12 & 32 \\ 32 & 1 \end{bmatrix},\ B_2=\begin{bmatrix} 1 & 18 \\ 4 & 33 \end{bmatrix}$$

$$B_3=\begin{bmatrix} 13 & 32 \\ 33 & 1 \end{bmatrix},\ B_4=\begin{bmatrix} 2 & 1 \\ 15 & 4 \end{bmatrix}$$

۲- با توجه به این‌که $m=2>1$ داریم $n=\left[\frac{m^2}{2}\right]=2$.

بنابراین، $t=n+1=3$.

۳- از رابطه $C_i = B_i Q_t(2, P_2^3)$ داریم:

$$C_1=\begin{bmatrix} 12 & 32 \\ 32 & 1 \end{bmatrix}\times\begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix}=\begin{bmatrix} 12 & 0 \\ 17 & 29 \end{bmatrix}(\text{mod}\,34),$$

$$C_2=\begin{bmatrix} 1 & 18 \\ 4 & 33 \end{bmatrix}\times\begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix}=\begin{bmatrix} 30 & 21 \\ 3 & 11 \end{bmatrix}(\text{mod}\,34),$$

$$C_3=\begin{bmatrix} 226 & 71 \\ 333 & 100 \end{bmatrix}=\begin{bmatrix} 22 & 3 \\ 27 & 32 \end{bmatrix}(\text{mod}\,34),$$

$$C_4=\begin{bmatrix} 23 & 7 \\ 26 & 15 \end{bmatrix}(\text{mod}\,34).$$

۴- درایه‌های ماتریس $C_i \left(1\le i\le m^2\right)$، را به‌دست می‌آوریم.

$c_{11}=12$	$c_{12}=0$	$c_{13}=17$	$c_{14}=29$
$c_{21}=30$	$c_{22}=21$	$c_{23}=3$	$c_{24}=11$
$c_{31}=22$	$c_{32}=3$	$c_{33}=27$	$c_{34}=32$
$c_{41}=23$	$c_{42}=7$	$c_{43}=26$	$c_{44}=15$

۵- همچنین داریم:

$$d_1=\det(C_1)=-1012,\quad d_2=\det(C_2)=267,$$
$$d_3=\det(C_3)=623,\ d_4=\det(C_4)=163.$$

۶- اینک ماتریس کدگذاری شده E را با استفاده از قرار دادن d_i بجای b_{i1} $(1\le i\le 4)$، در جدول قبل به‌دست می‌آوریم.

$$E=\begin{bmatrix}-1012 & 0 & 17 & 29\\ 267 & 21 & 3 & 11\\ 623 & 3 & 27 & 32\\ 163 & 7 & 26 & 15\end{bmatrix}=\begin{bmatrix}8 & 0 & 17 & 29\\ 29 & 21 & 3 & 11\\ 11 & 3 & 27 & 32\\ 27 & 7 & 26 & 15\end{bmatrix}$$

یعنی جمله کد شده به‌صورت " ح: صننعپذذپلیلچگس " است.

۷- پایان الگوریتم.

کدگشایی الگوریتم

۱- داریم:

$$Q_3\left(2,P_2^3\right)=\begin{bmatrix}P_3^3 & P_2^3\\ P_2^3 & P_1^3\end{bmatrix}=\begin{bmatrix}10 & 3\\ 3 & 1\end{bmatrix}.$$

قرار می‌دهیم:

$$P_1=10,\quad P_2=3,\quad P_3=3,\quad P_4=1.$$

۲- مقادیر e_{i3} را به‌دست می‌آوریم.

$$e_{13}=257,\quad e_{23}=63,$$
$$e_{33}=366,\quad e_{43}=305.$$

۳- مقادیر e_{i4} را محاسبه می‌کنیم.

$$e_{14}=80,\quad e_{24}=20,$$
$$e_{34}=113,\quad e_{44}=93.$$

۴- x_i به‌ازای $1\le i\le 4$ را به‌دست می‌آوریم.

$$(10\times 80-3\times 257)x_1+(3\times 80-1\times 257)\times 0=(-1)^2\times(8)$$
$$\Rightarrow 29x_1=8\Rightarrow -5x_1=-60\Rightarrow x_1=12,$$
$$(10\times 20-3\times 63)x_2+(3\times 20-1\times 63)\times 21=(-1)^2\times(29)$$
$$\Rightarrow 11x_2=92=-44\ (\mathrm{mod}\,34)\Rightarrow x_2=-4=30(\mathrm{mod}\,34),$$
$$(10\times 113-3\times 366)x_3+3(339-366)=(-1)^2\times 11$$
$$\Rightarrow 32x_3=92\Rightarrow -2x_3=24(\mathrm{mod}\,34)\Rightarrow x_3=22$$
$$(10\times 93-3\times 305)x_4+(3\times 93-305)\times 7=(-1)^2\times 27$$
$$\Rightarrow 15x_4=209=5(\mathrm{mod}\,34)\Rightarrow x_4=23$$

و بنابراین داریم:

$$c_{11}=x_1=12,\quad c_{21}=x_2=30,$$
$$c_{31}=x_3=22,\quad c_{41}=x_4=23.$$

۵- ماتریس‌های C_i را به‌دست می‌آوریم.

$$C_1=\begin{bmatrix}12 & 0\\ 17 & 29\end{bmatrix},\qquad C_2=\begin{bmatrix}30 & 21\\ 3 & 11\end{bmatrix},$$
$$C_3=\begin{bmatrix}22 & 3\\ 27 & 32\end{bmatrix},\quad C_4=\begin{bmatrix}23 & 7\\ 26 & 15\end{bmatrix}.$$

۶ - محاسبه بلوک‌های B_i $(1\le i\le 4)$ با استفاده از فرمول

$$B_i=C_i\left(Q_3(2,P_2^3)\right)^{-1}$$

از لم ۲-۲ داریم:

$$\left(Q_3(2,P_2^3)\right)^{-1}=\begin{bmatrix}1 & -3\\ -3 & 10\end{bmatrix}.$$

درنتیجه

$$B_1=\begin{bmatrix}12 & 0\\ 17 & 29\end{bmatrix}\times\begin{bmatrix}1 & -3\\ -3 & 10\end{bmatrix}=\begin{bmatrix}12 & -36\\ -70 & 239\end{bmatrix}$$
$$=\begin{bmatrix}12 & 32\\ 32 & 1\end{bmatrix}(\mathrm{mod}\,34)$$
$$B_2=\begin{bmatrix}30 & 21\\ 3 & 11\end{bmatrix}\times\begin{bmatrix}1 & -3\\ -3 & 10\end{bmatrix}=\begin{bmatrix}1 & 18\\ 4 & 33\end{bmatrix}(\mathrm{mod}\,34).$$

و

$$B_3=\begin{bmatrix}13 & 32\\ 33 & 1\end{bmatrix},\qquad B_4=\begin{bmatrix}2 & 1\\ 15 & 4\end{bmatrix}.$$

۷- به‌دست آوردن ماتریس پیام M.

$$M=\begin{bmatrix}12 & 32 & 1 & 18\\ 32 & 1 & 4 & 33\\ 13 & 32 & 2 & 1\\ 33 & 1 & 15 & 4\end{bmatrix}=\begin{bmatrix}\text{ر} & \text{ی} & \text{الف} & \text{ض}\\ \text{ی} & \text{الف} & \text{ت} & 0\\ \text{الف} & \text{ب} & \text{ی} & \text{ز}\\ 0 & \text{الف} & \text{س} & \text{ت}\end{bmatrix}$$

توجه شود که با تغییر ماتریس $Q_t(n,P_n^t)$ و بردار d_i می‌توان به الگوریتم کدگذاری و کدگشای متفاوتی دست یافت. در مثال بعدی فرار می‌دهیم:

$$P=Q_t\left(n,P_n^t\right)oQ_t^{-1}\left(n,P_n^t\right),\ C_i=B_iP$$
$$t_i=trc(C_i),\ E=\left[t_i,\quad b_{ik}\right]_{k\in\{2,3,4\}}$$

بنابراین، در الگوریتم کدگذاری و کدگشایی **کد بلوک‌بندی نوع اول**، تغییرات زیر را داریم:

الف) الگوریتم کدگذاری

۱- محاسبه $C_i = B_i Q_t\left(n, P_n^t\right) o Q_t^{-1}\left(n, P_n^t\right)$

۲- محاسبه $t_i = trc(C_i)$.

۳- ساختن ماتریس کدگذاری شده

$$E = \left[t_i, \quad b_{ik}\right]_{k\in\{2,3,4\}}$$

که $t_i = trc(C_i)$.

ب) الگوریتم کدگشایی

۱- قرار دادن $P = Q_t\left(n, P_n^t\right) o Q_t^{-1}\left(n, P_n^t\right)$ و تعیین P_j به‌ازای $1 \le j \le 4$

۲- محاسبه $P_2 b_{j3} + P_3 b_{j2} + P_4 b_{j4}$ و جایگذاری آن در e_j برای $(1 \le j \le 4)$.

۳- محاسبه x_i از معادله $P_1 x_i + e_i = t_i$

۴ - محاسبه بلوک‌های B_i $(1 \le i \le 4)$، به‌وسیله جایگذاری x_i در درایه b_{i1}.

۵ – به‌دست آوردن ماتریس پیام M.

مثال ۵ -۳. با شرایط بالا، **مثال ۵-۲ را حل کنید.**

حل. پس از بلوک‌بندی ماتریس پیام و استفاده از جدول (۱) داریم:

$$B_1 = \begin{bmatrix} 12 & 32 \\ 32 & 1 \end{bmatrix}, \; B_2 = \begin{bmatrix} 1 & 18 \\ 4 & 33 \end{bmatrix}$$

$$B_3 = \begin{bmatrix} 13 & 32 \\ 33 & 1 \end{bmatrix}, \; B_4 = \begin{bmatrix} 2 & 1 \\ 15 & 4 \end{bmatrix}$$

همچنین $n = 2$ و $t = n + 1 = 3$. بنا بر قسمت اول قضیه ۳-۲

$$P = Q_3\left(2, P_2^3\right) o Q_3^{-1}\left(2, P_2^3\right) = \begin{bmatrix} 10 & -9 \\ -9 & 10 \end{bmatrix}.$$

قرار می‌دهیم:

$$P_1 = 10, \quad P_2 = -9, \quad P_3 = -9, \quad P_4 = 10.$$

بنابراین،

$$C_1 = B_1 \times P = \begin{bmatrix} 12 & 32 \\ 32 & 1 \end{bmatrix} \times \begin{bmatrix} 10 & -9 \\ -9 & 10 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 5 & 28 \end{bmatrix},$$

$$C_2 = \begin{bmatrix} 18 & 1 \\ 15 & 22 \end{bmatrix}, \; C_3 = \begin{bmatrix} 12 & 33 \\ 15 & 19 \end{bmatrix}, \; C_4 = \begin{bmatrix} 11 & 26 \\ 12 & 7 \end{bmatrix}.$$

و همچنین داریم:

$$t_1 = trc(C_1) = 30, \quad t_2 = trc(C_2) = 6,$$

$$t_3 = trc(C_3) = 31, \; t_4 = trc(C_4) = 18.$$

در جدول زیر درایه‌های ماتریس $B_i \; \left(1 \le i \le m^2\right)$، را به‌دست می‌آوریم.

$b_{11} = 12$	$b_{12} = 32$	$b_{13} = 32$	$b_{14} = 1$
$b_{21} = 1$	$b_{22} = 18$	$b_{23} = 4$	$b_{24} = 33$
$b_{31} = 13$	$b_{32} = 32$	$b_{33} = 33$	$b_{34} = 1$
$b_{41} = 2$	$b_{42} = 1$	$b_{43} = 15$	$b_{44} = 4$

۴- ماتریس کدگذاری شده E که با استفاده از قرار دادن d_i بجای $b_{i1} \; (1 \le i \le 4)$، در جدول قبل به‌دست می‌آید.

$$E = \begin{bmatrix} 30 & 32 & 32 & 1 \\ 6 & 18 & 4 & 33 \\ 31 & 32 & 33 & 1 \\ 18 & 1 & 15 & 4 \end{bmatrix}$$

یعنی جمله کد شده به‌صورت " ویياجضت هی اضاست " است.

۵- پایان الگوریتم.

کدگشایی الگوریتم:

۱- داریم:

$$P = Q_3\left(2, P_2^3\right) o Q_3^{-1}\left(2, P_2^3\right) = \begin{bmatrix} 10 & -9 \\ -9 & 10 \end{bmatrix}.$$

قرار می‌دهیم:

$$P_1 = 10, \quad P_2 = -9, \quad P_3 = -9, \quad P_4 = 10.$$

۲- مقادیر e_j را به‌دست می‌آوریم.

$$e_1 = -566 = 12 \pmod{34}, \quad e_2 = 30,$$

$$e_3 = 3, \qquad e_4 = 32.$$

۳- x_i به‌ازای $1 \le i \le 4$ را به‌دست می‌آوریم.

$$10x_1 + 12 = 30 \Rightarrow 10x_1 = 18 \Rightarrow x_1 = 12,$$

$$10x_2 + 30 = 6 \Rightarrow 10x_2 = 10 \Rightarrow x_2 = 1,$$

$$10x_3 + 3 = 31 \Rightarrow 10x_3 = 28 \Rightarrow x_3 = 13$$

$$10x_4 + 32 = 18 \Rightarrow 10x_4 = -14 \Rightarrow x_4 = 2$$

۴- بنابراین داریم:

$$b_{11} = x_1 = 12, \quad b_{21} = x_2 = 1,$$

$$b_{31} = x_3 = 13, \quad b_{41} = x_4 = 2.$$

و ماتریس‌های B_i را به‌دست می‌آوریم

۵- با قرار دادن ماتریس‌های B_i، به ترتیب از سمت چپ به راست ماتریس پیام M را به‌دست می‌آوریم. داریم:

$$M=\begin{bmatrix}12&32&1&18\\32&1&4&33\\13&32&2&1\\33&1&15&4\end{bmatrix}=\begin{bmatrix}\text{ض}&\text{الف}&\text{ی}&\text{ر}\\0&\text{ت}&\text{الف}&\text{ی}\\\text{الف}&\text{ب}&\text{ی}&\text{ز}\\0&\text{ت}&\text{س}&\text{الف}\end{bmatrix}.$$

با استفاده از ترکیب این دو الگوریتم می‌توان الگوریتم پیچیده‌تری به شرح زیر به‌دست آورد.

۵-۴. الگوریتم‌های کد بلوک‌بندی نوع دوم

الف) مراحل الگوریتم کدگذاری

۱- بلوک‌بندی ماتریس M، به بلوک‌های B_i $\left(1\le i\le m^2\right)$

.

۲- تعیین مقادیر n و t

۳- محاسبه $C_i=B_iQ_t(n,P_n^t)$

۴- تعیین c_{ij} $(1\le i\le 4)$

۵- محاسبه $\det(C_i)$ و $trc(C_i)$

۶- ساختن ماتریس کدگذاری شده

$$E=\left[d_i,t_i,b_{ik}\right]_{k\in\{3,4\}}$$

که $d_i=\det(C_i)$ و $t_i=trc(C_i)$

۷- پایان الگوریتم.

ب) مراحل الگوریتم کدگشایی

۱- قرار دادن $P=Q_t\left(n,P_n^t\right)$ و تعیین P_j به‌ازای $1\le j\le 4$.

۲- محاسبه $P_1b_{j3}+P_3b_{j4}$ و جایگذاری آن در e_{j3} برای $(1\le j\le 4)$.

۳- پیگیری فرایند

$$P_2bj_3+P_4b_{j4}\to e_{j4},\quad (1\le j\le 4).$$

۴- به‌دست آوردن x_i و y_i از معادلات زیر

$$P_1x_i+P_3y_i=t_i-e_{i4}$$
$$\left(P_1e_{i4}-P_2e_{i3}\right)x_i+\left(P_3e_{i4}-P_4e_{i3}\right)y_i=(-1)^n\times d_i.$$

۵ - محاسبه B_i $(1\le i\le 4)$، به‌وسیله جایگذاری x_i در درایه b_{i1} و y_i در b_{i2}

۶- به‌دست آوردن ماتریس پیام M

۷- پایان الگوریتم

مثال ۵ -۵. با الگوریتم بالا، **مثال ۵-۲ را حل کنید.**

حل. پس از بلوک‌بندی ماتریس پیام و استفاده از جدول (۱) داریم:

$$B_1=\begin{bmatrix}12&32\\32&1\end{bmatrix},\ B_2=\begin{bmatrix}1&18\\4&33\end{bmatrix}$$
$$B_3=\begin{bmatrix}13&32\\33&1\end{bmatrix},\ B_4=\begin{bmatrix}2&1\\15&4\end{bmatrix}$$

همچنین $n=2$ و $t=n+1=3$. از رابطه

$$C_i=B_iQ_t(2,P_2^3)$$

داریم:

$$C_1=\begin{bmatrix}12&32\\32&1\end{bmatrix}\times\begin{bmatrix}10&3\\3&1\end{bmatrix}=\begin{bmatrix}12&0\\17&29\end{bmatrix}(\text{mod}\,34),$$
$$C_2=\begin{bmatrix}1&18\\4&33\end{bmatrix}\times\begin{bmatrix}10&3\\3&1\end{bmatrix}=\begin{bmatrix}30&21\\3&11\end{bmatrix}(\text{mod}\,34),$$
$$C_3=\begin{bmatrix}226&71\\333&100\end{bmatrix}=\begin{bmatrix}22&3\\27&32\end{bmatrix}(\text{mod}\,34),$$
$$C_4=\begin{bmatrix}23&7\\26&15\end{bmatrix}(\text{mod}\,34),$$

۵- محاسبه $\det(C_i)$ و $trc(C_i)$

$$d_1=\det(C_1)=8,\quad d_2=\det(C_2)=29,$$
$$d_3=\det(C_3)=11,\ d_4=\det(C_4)=27.$$
$$t_1=trc(C_1)=7,\quad t_2=trc(C_2)=7,$$
$$t_3=trc(C_3)=20,\ t_4=trc(C_4)=4$$

۶- ساختن ماتریس کدگذاری شده

$$E=\left[d_i,t_i,b_{ik}\right]_{k\in\{3,4\}}$$

که $d_i=\det(C_i)$ و $t_i=trc(C_i)$

$$E=\begin{bmatrix}8&7&32&1\\29&7&4&33\\11&20&33&1\\27&4&15&4\end{bmatrix}$$

بنابراین، جمله کد شده به‌صورت "حچیانچت ذض التست" است.

۷- پایان الگوریتم.

کدگشایی الگوریتم

۱- داریم:

$$Q_3\left(2,P_2^3\right)=\begin{bmatrix}P_3^3 & P_2^3\\ P_2^3 & P_1^3\end{bmatrix}=\begin{bmatrix}10 & 3\\ 3 & 1\end{bmatrix}.$$

قرار می‌دهیم:

$$P_1=10,\quad P_2=3,\quad P_3=3,\quad P_4=1.$$

۲- مقادیر e_{i3} را به‌دست می‌آوریم.

$$e_{13}=17,\ e_{23}=3,\ e_{33}=27,\quad e_{43}=26.$$

۳- مقادیر e_{i4} را محاسبه می‌کنیم.

$$e_{14}=29,\ e_{24}=11,\ e_{34}=32,\ e_{44}=15.$$

۴- x_i و y_i به‌ازای $1\le i\le 4$ را به‌دست می‌آوریم.

ابتدا x_1 و y_1. داریم:

$$\begin{cases}10x_1+3y_1=7-29\\ 239x_1+70y_1=8\end{cases}\Rightarrow\begin{cases}10x_1+3y_1=12\,(\mathrm{mod}\,34)\\ x_1+2y_1=8\ (\mathrm{mod}\,34)\end{cases}$$

$$\Rightarrow x_1=12,\ y_1=32$$

$$\begin{cases}10x_2+3y_2=-4\\ 101x_2+30y_2=29\end{cases}\Rightarrow\begin{cases}10x_2+3y_2=30(\mathrm{mod}\,34)\\ 33x_2+30y_2=29\ (\mathrm{mod}\,34)\end{cases}$$

$$\Rightarrow x_2=1,\ y_2=18$$

$$\begin{cases}10x_3+3y_3=22\\ x_3+y_3=11\end{cases}\Rightarrow x_3=13,\ y_3=32$$

$$\begin{cases}10x_4+3y_4=23\\ 4x_4+19y_4=27\end{cases}\Rightarrow x_4=2,\ y_4=1$$

درنتیجه داریم:

$$b_{11}=x_1=12,\quad b_{12}=y_2=32,$$
$$b_{21}=x_2=1,\quad b_{22}=y_2=18,$$
$$b_{31}=x_3=13,\quad b_{32}=y_3=32,$$
$$b_{41}=x_4=2,\quad b_{42}=y_4=1.$$

۵- بنابراین، ماتریس‌های B_i را می‌توان به‌دست آورد. با جایگذاری B_i ماتریس پیام به‌دست می‌آید.

۶. نتیجه‌گیری

این مقاله به استفاده از ماتریس دنباله عددی $t-$پیل در نظریه کدگذاری اختصاص دارد. ابتدا ماتریس دنباله‌های عددی $t-$پیل و حاصل‌ضرب هادمارد آن‌ها را تعریف نموده و بعضی از خواص این ماتریس‌ها ازجمله دترمینان آن‌ها را مورد بررسی قرار دادیم. سپس با استفاده از دو تعریف فوق به بررسی الگوریتم کدگذاری روی آن‌ها پرداخته و نشان دادیم توانایی تصحیح خطا در این الگوریتم برابر با ۹۳.۳٪ است. سرانجام به بررسی الگوریتم کدگذاری به‌روش بلوک‌بندی روی ماتریس دنباله عددی $t-$ پیل و حاصل‌ضرب هادامارد آن پرداختیم.

۷. مرجع‌ها

[1] Stakhov, A.; Massingue, V.; Sluchenkova, A.; "Introduction into Fibonacci Coding and Cryptograhy"; Kharkov: Osnova, 1999.

[2] Alaeiyan, M.; Rahimpour, A. R.; Dehnavi, S. M. "Algebrical Properties of Modular Addition Modulo 2t with r Operant"; J. Passive Defence Sci. Technol. 2012, 3, 25-32.

[3] Basu, M.; Prased, B. "The Generalized Relations among the Elements for Fibonacci Coding Theory Code"; Chaos, Solitions Fractals 2009, 41, 2517-2525.

[4] Noroozi, Z.; Mohamady, E. "Detection and Correction of Cheat in the Secret Schemes with Ternary Codes"; J. Passive Defence Sci. Techno. 2011, 1, 5-12.

[5] Prased, B. "Coding Theory on Lucas P Numbers"; Discret Mathematics, Algorithms and Applications 2016, 4, 17.

[6] Stakhov, A. P. "Fibonacci Matrices, a Generalization of the Cassini Formula and New Coding Theory"; Chaos, Solitions Fractals 2006, 30, 56-66.

[7] Tas, N.; Ucar, S.; Ozgur. N. Y. "Pell Coding and Pell Decoding Methods with Some Applications"; Math. NT, 2017.

[8] Stakhov, A. P. "Fibonacci matrices, a generalization of the ''Cassiniformula'', and a new coding theory"; Chaos, Solitons and Fractals 2006, 30, 56–66.

[9] Falcon, S.; Plaza, A. "K-Fibonacci Sequences Modulo M"; Chaos, Solitons and Fractals 2009, 41, 497-504.

[10] Hashemi, M.; Mehraban, E. "On the Generalized Order 2-Pell Sequence of some Classes of Groups"; Communications in Algebra 2018, 46, 4104-4119.

[11] Nalli, A. "On the Hadamard Product of Fibonacci Q^n Matrix and Fibonacci Q^{-n} Matrix"; Math. Sci. 2006, 1, 753-761.