

چند کد جدید روی ماتریس دنباله های 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 شاخه های جالب و کاربردی ریاضیات است که به طور گسترده در شبکه های بی سیم از جمله شبکه های تلفن همراه، شبکه های بی سیم با برد کوتاه، شبکه های حسگر بی سیم و شبکه های ارتباطی ماهواره ای مورد استفاده قرار می گیرد. هدف ما در این مقاله ارائه کدهای جدیدی با استفاده از دنباله های عددی t -پیل و حاصل ضرب هادامارد است. برای رسیدن به این هدف ابتدا به بررسی خواص ماتریس دنباله های عددی t -پیل و حاصل ضرب هادامارد آن ها می پردازیم. سپس با استفاده از نتایج به دست آمده، الگوریتم های کدگذاری و کدگشایی متناظر آن ها را به دست می آوریم. در انتها، الگوریتم بلوک بندی را روی ماتریس دنباله های عددی t -پیل و حاصل ضرب هادامارد آن ها مطالعه می کنیم.

کلیدواژه ها: دنباله عددی t -پیل، حاصل ضرب هادامارد ماتریس ها، 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

۱. مقدمه

است. مقدار $\tau = \lim_{n \rightarrow \infty} \frac{P_{n+1}^t}{P_n^t} = \frac{t + \sqrt{t^2 + 4}}{2}$ 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) $P_1 + P_3 + \dots + P_{2n-1} = \frac{P_{2n}}{t}$,
- (iii) $P_0 + P_2 + \dots + P_{2n} = \frac{P_{2n+1} - 1}{t}$,
- (iv) $P_n^2 + P_{n+1}^2 = P_{2n+1}^2$,
- (v) $P_{2n} = P_n(P_{n-1} + P_{n+1})$,
- (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 $\{P_n^t\}_0^\infty$ و ماتریس آن به‌ازای $t=2$ ، الگوریتم کدگذاری و کدگشایی روی ماتریس دنباله عددی -2 پیل را ارائه دادند [۷].

در این مقاله با بررسی خواص دنباله $\{P_n^t\}_0^\infty$ 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 حاصل ضرب هادامارد آن را بررسی می‌کنیم. بخش چهارم اختصاص به ارائه یک روش کدگذاری و کدگشایی روی ماتریس‌های $-t$ پیل و حاصل ضرب هادامارد آن‌ها دارد. در بخش پنجم روش بلوک‌بندی روی ماتریس دنباله عددی $-t$ پیل و حاصل ضرب 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 $Q_t(n, P_n^t)$ نشان می‌دهیم، به استقرا می‌توان ثابت کرد که

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

نظریه کدگذاری فیبوناتچی توسط Stokhov و همکارانش [۱] در سال ۱۹۹۹، معرفی گردید. پس‌از آن مطالعات زیادی به بررسی کدگذاری و رمزگذاری روی دنباله‌های مختلف و ماتریس آن‌ها اختصاص یافته است [۷-۲]. ماتریس مربعی پیام M و ماتریس معکوس پذیر 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:

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

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، $n = 0, \pm 1, \pm 2, \dots$. Stokhov، به‌ازای عدد طبیعی p ، دنباله

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

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 $\{P_n^t\}_{-\infty}^\infty$ 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 $P_1^t = 1$ و $P_0^t = 0$ به‌سادگی می‌توان نشان داد که جواب رابطه بازگشتی دنباله

عددی $-t$ پیل به‌صورت

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

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

۳. حاصل ضرب هادامارد روی $Q_t(n, P_n^t)$

در اینجا، ابتدا حاصل ضرب هادامارد ماتریس‌های $Q_t(n, P_n^t)$ و $Q_t^{-1}(n, P_n^t)$ را تعریف نموده و سپس به بررسی دترمینان این حاصل ضرب می‌پردازیم که از آن در بخش چهارم استفاده می‌شود.

فرض کنید A و B دو ماتریس $m \times n$ باشند در این صورت حاصل ضرب هادامارد A و B که با $A \bullet B$ نشان می‌دهیم به صورت زیر تعریف می‌شود:

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

تعریف ۳-۱. فرض کنید $Q_t = Q_t(n, P_n^t)$ ماتریس دنباله عددی t -پیل و Q_t^{-1} ، ماتریس وارون آن باشد. در این صورت حاصل ضرب هادامارد آن‌ها را با $Q_t(n, P_n^t) \circ Q_t^{-1}(n, P_n^t)$ نمایش داده و به صورت زیر تعریف می‌شود [۱۱].

$$Q_t(n, P_n^t) \circ Q_t^{-1}(n, P_n^t) = \frac{1}{(-1)^n} (Q_t \bullet \text{adj} Q_t)$$

در نتایج زیر دترمینان و وارون حاصل ضرب هادامارد را به دست می‌آوریم

$$Q_t(n, P_n^t) \circ Q_t^{-1}(n, P_n^t)$$

قضیه ۳-۲. داریم:

(الف)

$$Q_t(n, P_n^t) \circ Q_t^{-1}(n, P_n^t) = \frac{1}{(-1)^n} \begin{bmatrix} P_{n+1}^t P_{n-1}^t & -(P_n^t)^2 \\ -(P_n^t)^2 & P_{n+1}^t P_{n-1}^t \end{bmatrix}$$

(ب)

$$\text{Det}(Q_t(n, P_n^t) \circ Q_t^{-1}(n, P_n^t)) = \begin{cases} 1 + 2(P_n^t)^2 & n = 2k, \\ 1 - 2(P_n^t)^2 & n = 2k + 1. \end{cases}$$

برهان. به دلیل اینکه

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

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

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

داریم:

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

اینک به محاسبه وارون $Q_t(n, P_n^t)$ می‌پردازیم. ابتدا

دترمینان $Q_t(n, P_n^t)$ را محاسبه می‌کنیم.

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

برهان. بنا به لم ۱-۲ داریم:

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

در نتیجه $\text{Det} Q_t(n, P_n^t) = P_{n+1}^t P_{n-1}^t - (P_n^t)^2$ ، لذا، با

توجه به لم ۲-۱ (vii) خواهیم داشت:

$$\text{Det} Q_t(n, P_n^t) = (-1)^n.$$

با استفاده از لم قبل داریم:

لم ۳-۲. وارون ماتریس $Q_t(n, P_n^t)$ که $t \geq 2$ به صورت زیر

است:

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

برای سادگی نمادهای مورد استفاده، وقتی که مقدار t مشخص

باشد بجای $Q_t(n, P_n^t)$ می‌نویسیم $Q_t(n, P_n)$ در جدول

زیر، ماتریس دنباله عددی ۳-پیل و وارون آن، به ازای $n = 0, 1, 2, 3, 4$ قابل مشاهده است.

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

به عنوان مثال ماتریس وارون $Q_3(n, P_n)$ به ازای $n = 2k$

به صورت ذیل است:

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

و به ازای $n = 2k + 1$ داریم:

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

برای حالتی که n عددی فرد است، حکم به صورت مشابه اثبات می شود.

۴. کدگذاری و کدگشایی روی ماتریس دنباله های عددی t -پیل و حاصل ضرب هادمارد آن ها

در این بخش به بررسی روش کدگذاری و کدگشایی روی ماتریس $Q_t(n, P_n^t)$ و حاصل ضرب هادمارد آن ها می پردازیم. فرض کنید $M \times Q_t(n, P_n^t) = E$ یک الگوریتم کدگذاری ماتریس دنباله عددی t -پیل و $E \times Q_t^{-1}(n, P_n^t) = M$ الگوریتم متناظر کدگشایی ماتریس دنباله عددی t -پیل باشند که در آن، M پیام کد شده به صورت ماتریس 2×2 با نمایش زیر است:

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

به طوری که $m_i > 0, 1 \leq i \leq 4$. برای ارائه یک مثال، قرار می دهیم:

$$Q_3(3, P_3^3) = \begin{bmatrix} 33 & 10 \\ 10 & 3 \end{bmatrix},$$

که ماتریس وارون آن برابر است با:

$$Q_3^{-1}(3, P_3^3) = \begin{bmatrix} -3 & 10 \\ 10 & -33 \end{bmatrix}.$$

در این صورت، بر طبق الگوریتم $M \times Q_t(n, P_n^t) = E$ خواهیم داشت:

$$\begin{aligned} M \times Q_3(3, P_3^3) &= \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \times \begin{bmatrix} 33 & 10 \\ 10 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 33m_1 + 10m_2 & 10m_1 + 3m_2 \\ 33m_3 + 10m_4 & 10m_3 + 3m_4 \end{bmatrix} \quad (1) \\ &= \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = E, \end{aligned}$$

که در آن،

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

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

حکم الف، از تعریف به دست می آید. برای اثبات قسمت دوم، ابتدا فرض می کنیم $n = 2k$. بنا بر قسمت هفتم از لم ۲-۱ داریم:

$$\begin{aligned} Det(Q_t(n, P_n^t) \circ Q^{-1}_t(n, P_n^t)) &= Det \begin{bmatrix} P_{2k+1}^t P_{2k-1}^t & -(P_{2k}^t)^2 \\ -(P_{2k}^t)^2 & P_{2k+1}^t P_{2k-1}^t \end{bmatrix} \\ &= (P_{2k+1}^t P_{2k-1}^t - (P_{2k}^t)^2) (P_{2k+1}^t P_{2k-1}^t + (P_{2k}^t)^2) \\ &= (-1)^{2k} (1+2(P_{2k}^t)^2) = 1+2(P_{2k}^t)^2. \end{aligned}$$

برای عدد فرد $n = 2k + 1$ داریم:

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

لذا،

$$\begin{aligned} Det(Q_t(n, P_n^t) \circ Q^{-1}_t(n, P_n^t)) &= (P_{2k+2}^t P_{2k}^t - (P_{2k+1}^t)^2) (P_{2k+2}^t P_{2k}^t + (P_{2k+1}^t)^2) \\ &= (-1)^{2k+1} (-1+2(P_{2k+1}^t)^2) = 1-2(P_{2k+1}^t)^2. \end{aligned}$$

با استفاده از قضیه ۳-۱، اثر ماتریس حاصل ضرب هادمارد $Q_t(n, P_n^t) \circ Q^{-1}_t(n, P_n^t)$ به صورت زیر است:

نتیجه ۳-۳

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

قضیه ۳-۴. برای معکوس ماتریس حاصل ضرب هادمارد

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

داریم:

$$(Q_t(n, P_n^t) \circ Q^{-1}_t(n, P_n^t))^{-1} = \begin{cases} \begin{bmatrix} \frac{1+(P_n^t)^2}{1+2(P_n^t)^2} & \frac{(P_n^t)^2}{1+2(P_n^t)^2} \\ \frac{(P_n^t)^2}{1+2(P_n^t)^2} & \frac{1+(P_n^t)^2}{1+2(P_n^t)^2} \end{bmatrix} & n=2k, \\ \begin{bmatrix} \frac{1-(P_n^t)^2}{1-2(P_n^t)^2} & -\frac{(P_n^t)^2}{1-2(P_n^t)^2} \\ -\frac{(P_n^t)^2}{1-2(P_n^t)^2} & \frac{1-(P_n^t)^2}{1-2(P_n^t)^2} \end{bmatrix} & n=2k+1 \end{cases}$$

برهان. اگر $n = 2k$ آنگاه،

$$adj(Q_t(n, P_n^t) \circ Q^{-1}_t(n, P_n^t)) = \begin{bmatrix} P_{2k+1}^t P_{2k-1}^t & (P_{2k}^t)^2 \\ (P_{2k}^t)^2 & P_{2k+1}^t P_{2k-1}^t \end{bmatrix}$$

با استفاده از رابطه $P_{2k+1}^t P_{2k-1}^t - (P_{2k}^t)^2 = (-1)^n$ داریم:

$$adj(Q_t(n, P_n^t) \circ Q^{-1}_t(n, P_n^t)) = \begin{bmatrix} 1+(P_{2k}^t)^2 & (P_{2k}^t)^2 \\ (P_{2k}^t)^2 & 1+(P_{2k}^t)^2 \end{bmatrix}$$

چون n عدد زوجی است،

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

$$m_1 = -P_{n-1}^3 e_1 + P_n^3 e_2,$$

$$m_2 = P_n^3 e_1 - P_{n+1}^3 e_2,$$

$$m_3 = -P_{n-1}^3 e_3 + P_n^3 e_4,$$

$$m_4 = P_n^3 e_3 - P_{n+1}^3 e_4.$$

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) به دست می‌آیند.

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

در نتیجه

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

و داریم $e_1 \approx \tau e_2$ که در آن $\tau = \frac{3 + \sqrt{13}}{2}$ نسبت حدی دنباله عددی ۳-پیل است. به روش 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، $t \geq 3$ ،

برقرار است 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.

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

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

$$= \begin{bmatrix} e_1' & e_2' \\ e_3' & e_4' \end{bmatrix}.$$

با در نظر گرفتن فرمول (۱) و محاسبه درایه‌های ماتریس (۲) خواهیم داشت:

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

به سادگی می‌توان نشان داد روش فوق به ازای $t \geq 3$ برقرار است. اینک، دترمینان ماتریس کدگذاری شده E را به دست می‌آوریم. قضیه ۴-۱. فرض کنید E ماتریس کدگذاری و M پیام کد شده باشد. در این صورت:

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

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

$$\text{Det } E = \text{Det}(M \times Q_t(n, P_n^t)) = \text{Det } M \times \text{Det } Q_t(n, P_n^t).$$

اینک با توجه به لم ۲-۲، داریم:

$$\text{Det } E = \text{Det } M \times (-1)^n.$$

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 ۳-پیل پرداخته و سپس با تعمیم آن نشان می‌دهیم که حکمی مشابه برای هر $t \geq 3$ برقرار است. الگوریتم کدگذاری شده را می‌توان به صورت زیر نوشت:

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

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

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

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

است که مقدار n نا 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:

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

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 ۹۳.۳٪ است. روش t -پیل در مقایسه با کد همینگ در اینجا ۹۵۰ بار بیشتر توانایی تصحیح خطا دارد. اکنون، به بررسی کدگذاری روی حاصل ضرب 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، $i = 1, 2, 3, 4, m_i > 0$.

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

می‌خواهیم رابطه (۳) را برای حالت‌های مختلف (a) ، (b) ، (c) و (d) بررسی کنیم. با توجه به اینکه

$$xe_4 - ye_3 = (-1)^n DetM$$

$$e_1e_4 - ye_3 = (-1)^n DetM$$

$$e_1e_4 - e_2z = (-1)^n DetM$$

$$e_1t - e_2e_3 = (-1)^n DetM$$

داریم:

$$x = \frac{(-1)^n DetM + e_2e_3}{e_4}, \tag{۱۱}$$

$$y = \frac{-(-1)^n DetM + e_1e_4}{e_3}, \tag{۱۲}$$

$$z = \frac{-(-1)^n DetM + e_1e_4}{e_2}, \tag{۱۳}$$

$$t = \frac{(-1)^n DetM + e_2e_3}{e_1}. \tag{۱۴}$$

روابط (۱۱-۱۴) مقادیر عناصر همراه با خطا را نشان می‌دهد. با توجه به این که $e_3 \approx \tau e_4$ و $e_1 \approx \tau e_2$ 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. به‌عنوان مثال حالت دومتغیره زیر را برای ماتریس E در نظر می‌گیریم.

$$\begin{bmatrix} x & y \\ e_3 & e_4 \end{bmatrix}, \tag{۱۵}$$

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

$$xe_4 - ye_3 = (-1)^n DetM.$$

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 برابر است 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

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 حاصل ضرب هادامارد آن‌ها

در اینجا، به روش بلوک‌بندی روی ماتریس دنباله‌های عددی t - پیل و حاصل ضرب هادامارد آن‌ها می‌پردازیم. در این روش ماتریس پیام M ، ماتریس مربعی به ابعاد $2m$ است. در صورتی که تعداد درایه‌های ماتریس کم‌تر باشد درایه‌های باقیمانده را با صفر کامل می‌کنیم. تقسیم ماتریس M ، به ماتریس‌های 2×2 ، B_i ($1 \leq i \leq m^2$) از چپ به راست را یک بلوک‌بندی ماتریس M نامیم. اینک به معرفی نمادهای موردنیاز در این روش می‌پردازیم: ماتریس‌های B_i را به صورت زیر در نظر می‌گیریم:

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

قرار می‌دهیم:

$$n = \begin{cases} 3 & m \leq 1, \\ \left\lfloor \frac{m^2}{2} \right\rfloor & m > 1. \end{cases}$$

همچنین با توجه به لم ۲-۱ داریم:

$$Q_t(n, P_n^t) = \begin{bmatrix} P_{n+1}^t & P_n^t \\ P_n^t & P_{n-1}^t \end{bmatrix}, t \geq 3$$

قرار می‌دهیم

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

بنابراین،

$$B_i Q_t(n, P_n^t) = \begin{bmatrix} b_{i1} P_1 + b_{i2} P_3 & b_{i1} P_2 + b_{i2} P_4 \\ b_{i3} P_1 + b_{i4} P_3 & b_{i3} P_2 + b_{i4} P_4 \end{bmatrix}, (20)$$

$$\text{trc}(B_i Q_t(n, P_n^t)) = b_{i1} P_1 + b_{i2} P_3 + b_{i3} P_2 + b_{i4} P_4, \quad \text{و}$$

$$\det(B_i Q_t(n, P_n^t)) = (b_{i1} P_1 + b_{i2} P_3) \times (b_{i3} P_2 + b_{i4} P_4) - (b_{i1} P_2 + b_{i2} P_4) \times (b_{i3} P_1 + b_{i4} P_3). \quad (21)$$

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

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

$$Q_2(4, P_4^2) \circ Q_2^{-1}(4, P_4^2) = \begin{bmatrix} P_3 P_5 & -(P_4)^2 \\ -(P_4)^2 & P_3 P_5 \end{bmatrix} \quad (16)$$

$$= \begin{bmatrix} 145 & -144 \\ -144 & 145 \end{bmatrix},$$

از طرف دیگر

$$(Q_2(4, P_4^2) \circ Q_2^{-1}(4, P_4^2))^{-1} = \begin{bmatrix} \frac{1+(P_4^2)^2}{1+2(P_4^2)^2} & \frac{(P_4^2)^2}{1+2(P_4^2)^2} \\ \frac{(P_4^2)^2}{1+2(P_4^2)^2} & \frac{1+(P_4^2)^2}{1+2(P_4^2)^2} \end{bmatrix} \quad (17)$$

$$= \begin{bmatrix} \frac{145}{289} & \frac{144}{289} \\ \frac{144}{289} & \frac{145}{289} \end{bmatrix},$$

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

$$M \times (Q_2(4, P_4^2) \circ Q_2^{-1}(4, P_4^2)) = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \times \begin{bmatrix} 145 & -144 \\ -144 & 145 \end{bmatrix}$$

$$= \begin{bmatrix} 145m_1 - 144m_2 & -144m_1 + 145m_2 \\ 145m_3 - 144m_4 & -144m_3 + 145m_4 \end{bmatrix}$$

$$= \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = E,$$

که در آن،

$$\begin{aligned} e_1 &= 145m_1 - 144m_2, \\ e_2 &= -144m_1 + 145m_2, \\ e_3 &= 145m_3 - 144m_4, \\ e_4 &= -144m_3 + 145m_4. \end{aligned} \quad (18)$$

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

$$\begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} \times \begin{bmatrix} \frac{145}{289} & \frac{144}{289} \\ \frac{144}{289} & \frac{145}{289} \end{bmatrix} = \begin{bmatrix} \frac{145}{289}e_1 + \frac{144}{289}e_2 & \frac{144}{289}e_1 + \frac{145}{289}e_2 \\ \frac{145}{289}e_3 + \frac{144}{289}e_4 & \frac{144}{289}e_3 + \frac{145}{289}e_4 \end{bmatrix} \quad (19)$$

$$= \begin{bmatrix} e_1' & e_2' \\ e_3' & e_4' \end{bmatrix} = E.$$

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	۰	:		
28	29	30	31	32	33	34		

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

"ریاضیات زیبا است"

حل. ماتریس M (ماتریس پیام) به صورت زیر است:

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

۱- ابتدا بلوک‌های ماتریس M را به دست می‌آوریم. داریم:

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

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

با توجه به جدول (۱) داریم:

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

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

$$n = \left\lfloor \frac{m^2}{2} \right\rfloor = 2 \text{ داریم } m = 2 > 1 \text{ که این به این دلیل است}$$

بنابراین، $t = n + 1 = 3$.

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

$$C_1 = \begin{bmatrix} 12 & 32 \\ 32 & 1 \end{bmatrix} \times \begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 12 & 0 \\ 17 & 29 \end{bmatrix} \pmod{34}$$

$$C_2 = \begin{bmatrix} 1 & 18 \\ 4 & 33 \end{bmatrix} \times \begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 30 & 21 \\ 3 & 11 \end{bmatrix} \pmod{34}$$

$$C_3 = \begin{bmatrix} 226 & 71 \\ 333 & 100 \end{bmatrix} = \begin{bmatrix} 22 & 3 \\ 27 & 32 \end{bmatrix} \pmod{34}$$

$$C_4 = \begin{bmatrix} 23 & 7 \\ 26 & 15 \end{bmatrix} \pmod{34}$$

۴- درایه‌های ماتریس C_i ، $(1 \leq i \leq m^2)$ را به دست

می‌آوریم:

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

۱-۵. الگوریتم‌های کد بلوک‌بندی نوع اول

(الف) مراحل الگوریتم کدگذاری

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

۲- تعیین مقادیر n و t

۳- محاسبه $C_i = B_i Q_t(n, P_n^t)$

۴- تعیین C_{ij} ($1 \leq i \leq 4$)

۵- محاسبه $\det(C_i)$

۶- ساختن ماتریس کدگذاری شده

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

که $d_i = \det(C_i)$

۷- پایان الگوریتم.

(ب) الگوریتم کدگذاری

۱- قرار دادن $P = Q_t(n, P_n^t)$ و تعیین P_j به ازای $1 \leq j \leq 4$.

۱- محاسبه $P_1 C_{j3} + P_3 C_{j4}$ و جایگذاری آن در e_{j3} برای

$$(1 \leq j \leq 4)$$

۲- پیگیری فرایند

$$P_2 C_{j3} + P_4 C_{j4} \rightarrow e_{j4}, (1 \leq j \leq 4)$$

۳- به دست آوردن x_i از

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

۴- محاسبه C_i ($1 \leq i \leq 4$) به وسیله جایگذاری x_i در درایه C_{i1}

۶- محاسبه B_i ($1 \leq i \leq 4$) توسط

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

۷- به دست 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.

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

$$t_3 = \text{trc}(C_3) = 31, \quad t_4 = \text{trc}(C_4) = 18.$$

در جدول زیر درایه‌های ماتریس B_i ($1 \leq i \leq m^2$)، را به دست 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} ($1 \leq i \leq 4$)، در جدول قبل به دست 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 به صورت "ویباجضت هی اضاست" است.

۵- پایان الگوریتم.

کدگذاری الگوریتم:

۱- داریم:

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

قرار می‌دهیم:

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

۲- مقادیر e_j را به دست می‌آوریم.

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

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

۳- x_i به ازای $1 \leq i \leq 4$ را به دست 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:

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

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

بنابراین، در الگوریتم کدگذاری و کدگشایی کد بلوک بندی نوع اول، تغییرات زیر را داریم:

الف) الگوریتم کدگذاری

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

$$t_i = \text{trc}(C_i) \quad ۲- محاسبه$$

۳- ساختن ماتریس کدگذاری شده

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

که $t_i = \text{trc}(C_i)$

ب) الگوریتم کدگشایی

$$۱- \text{قرار دادن } P = Q_t(n, P_n^t) o Q_t^{-1}(n, P_n^t) \text{ و}$$

تعیین P_j به ازای $1 \leq j \leq 4$

$$۲- \text{محاسبه } P_2 b_{j3} + P_3 b_{j2} + P_4 b_{j4} \text{ و جایگذاری آن در}$$

e_j برای $(1 \leq j \leq 4)$.

$$۳- \text{محاسبه } x_i \text{ از معادله } P_1 x_i + e_i = t_i$$

۴- محاسبه بلوک‌های B_i ($1 \leq i \leq 4$)، به وسیله جایگذاری

$$x_i \text{ در درایه } b_{i1}.$$

۵- به دست آوردن ماتریس پیام M .

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

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

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

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

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

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

قرار می‌دهیم:

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

بنابراین،

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

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

و همچنین داریم:

۶- به دست 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

$$C_i = B_i Q_t(2, P_2^3)$$

داریم:

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

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

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

$$C_4 = \begin{bmatrix} 23 & 7 \\ 26 & 15 \end{bmatrix} \pmod{34},$$

۵- محاسبه $\det(C_i)$ و $\text{trc}(C_i)$

$$d_1 = \det(C_1) = 8, \quad d_2 = \det(C_2) = 29,$$

$$d_3 = \det(C_3) = 11, \quad d_4 = \det(C_4) = 27.$$

$$t_1 = \text{trc}(C_1) = 7, \quad t_2 = \text{trc}(C_2) = 7,$$

$$t_3 = \text{trc}(C_3) = 20, \quad t_4 = \text{trc}(C_4) = 4$$

۶- ساختن ماتریس کدگذاری شده

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

که $d_i = \det(C_i)$ و $t_i = \text{trc}(C_i)$

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

بنابراین، جمله کد شده به صورت "حچیانچت ذض التست" است.

۷- پایان الگوریتم.

و ماتریس‌های B_i را به دست می‌آوریم

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

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

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

۴-۵. الگوریتم‌های کد بلوک‌بندی نوع دوم

(الف) مراحل الگوریتم کدگذاری

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

۲- تعیین مقادیر n و t

۳- محاسبه $C_i = B_i Q_t(n, P_n^t)$

۴- تعیین C_{ij} ($1 \leq i \leq 4$)

۵- محاسبه $\det(C_i)$ و $\text{trc}(C_i)$

۶- ساختن ماتریس کدگذاری شده

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

که $d_i = \det(C_i)$ و $t_i = \text{trc}(C_i)$

۷- پایان الگوریتم.

(ب) مراحل الگوریتم کدگشایی

۱- قرار دادن $P = Q_t(n, P_n^t)$ و تعیین P_j به ازای

$$1 \leq j \leq 4$$

۲- محاسبه $P_1 b_{j3} + P_3 b_{j4}$ و جایگذاری آن در e_{j3} برای

$$(1 \leq j \leq 4).$$

۳- پیگیری فرایند

$$P_2 b_{j3} + P_4 b_{j4} \rightarrow e_{j4}, \quad (1 \leq j \leq 4).$$

۴- به دست آوردن x_i و y_i از معادلات زیر

$$P_1 x_i + P_3 y_i = t_i - e_{i4}$$

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

۵- محاسبه B_i ($1 \leq i \leq 4$)، به وسیله جایگذاری x_i در درایه

$$b_{i2} \text{ و } y_i \text{ در } b_{i1}$$

کدگذاری الگوریتم

-۱ داریم:

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

قرار می‌دهیم:

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

-۲ مقادیر e_{i3} را به دست می‌آوریم.

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

-۳ مقادیر e_{i4} را محاسبه می‌کنیم.

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

-۴ x_i و y_i به ازای $1 \leq i \leq 4$ را به دست می‌آوریم.ابتدا x_1 و y_1 داریم:

$$\begin{cases} 10x_1 + 3y_1 = 7 - 29 \\ 239x_1 + 70y_1 = 8 \end{cases} \Rightarrow \begin{cases} 10x_1 + 3y_1 = 12 \pmod{34} \\ x_1 + 2y_1 = 8 \pmod{34} \end{cases} \\ \Rightarrow x_1 = 12, \quad y_1 = 32$$

$$\begin{cases} 10x_2 + 3y_2 = -4 \\ 101x_2 + 30y_2 = 29 \end{cases} \Rightarrow \begin{cases} 10x_2 + 3y_2 = 30 \pmod{34} \\ 33x_2 + 30y_2 = 29 \pmod{34} \end{cases} \\ \Rightarrow x_2 = 1, \quad y_2 = 18$$

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

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

در نتیجه 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 به دست آورد. باجایگذاری B_i ماتریس پیام به دست 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 حاصل ضرب هادامارد آن‌ها را تعریف نموده و بعضی از خواص این ماتریس‌ها از جمله 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 به روش بلوک‌بندی روی ماتریس دنباله عددی t -پیل و حاصل ضرب هادامارد آن پرداختیم.

۷. مراجع‌ها

- [1] Stakhov, A.; Massingue, V.; Sluchenkova, A.; "Introduction into Fibonacci Coding and Cryptography"; Kharkov: Osnova, 1999.
- [2] Alaeiyan, M.; Rahimpour, A. R.; Dehnavi, S. M. "Algebraic 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, Solitons 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, Solitons 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 " Matrix and Fibonacci q " Matrix"; Math. Sci. 2006, 1, 753-761.