ارایه یک کد روی ماتریس دنباله t- پیل و حاصل‌ضرب هادمارد آن‌ها

منصور هاشمی[*،۱]، **الهه مهربان**[۲]

۱- رشت– دانشگاه گیلان – دانشکده علوم ریاضی– گروه ریاضی محض

۲- رشت– دانشگاه گیلان – دانشکده علوم ریاضی– گروه ریاضی محض

چکیده

دنباله عددی t- پیل $\{P_n^t\}_{-\infty}^{\infty}$، $t\geq 2$، به صورت زیر تعریف می‌شود:

$$P_0^t=0,\ P_1^t=1,\ \begin{cases} P_n^t=tP_{n-1}^t+P_{n-2}^t, & n\geq 0,\\ P_n^t=P_{n+2}^t-tP_{n-1}^t, & n<0. \end{cases}$$

دراین مقاله، ابتدا به معرفی ماتریس دنباله‌های عددی t- پیل پرداخته و سپس حاصل‌ضرب هادمارد این ماتریس‌ها را محاسبه می‌کنیم و در انتها با استفاده از این ماتریس‌ها یک روش کدگذاری معرفی خواهیم کرد.

کلمات کلیدی: دنباله عددی t- پیل ، حاصل‌ضرب هادمارد ماتریس‌ها، دترمینان ماتریس، کدگذاری .

۱. مقدمه

در [۴] با استفاده از نمایش ماتریسی دنباله‌های فیبوناتچی Q_p، یک روش کدگذاری ارایه شده است که در آن ماتریس‌های $Q_p^{\,n}$ ، $Q_p^{\,-n}$ بترتیب ماتریس کدگذاری و ماتریس کدگشایی و انتقال‌های $M\times Q_p^n=E$ ، $E\times Q_p^{-n}=M$ ، الگوریتم کدگذاری فیبوناتچی و الگوریتم کدگشایی فیبوناتچی (بترتیب) می‌باشند. هم‌چنین، ماتریس $M_{(p+1)\times(p+1)}$ که $p=0,1,\ldots$ ، ماتریس پیام و ماتریس E پیام کد شده می‌باشد. توجه داشته باشید اگر $p=0$ ، آن‌گاه $Q_0=(1)$ ماتریس بدیهی است و در نتیجه کدگذاری و کدگشایی روی آن بدیهی خواهد بود. در [۲]، به بررسی روش کدگذاری فیبوناتچی در حالت $p=1$ روی ماتریس‌های Q_p^n پرداخته شده و آن را با Q^n نمایش می‌دهد. بنا به تعریف فوق، Q^n یک ماتریس مربعی 2×2 به شکل زیر است:

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

[*] **Corresponding author:** Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran.

Email: **Email: m_hashemi@guilan.ac.ir**.

که در آن $n=0,\pm1,\pm2,\cdots$ و F_{n+1} ، F_n ، F_{n-1} اعضای دنباله فیبوناتچی با رابطه بازگشتی زیر هستند:

$$F_1=F_2=1;\ F_{n+1}=F_n+F_{n-1}.$$

فرض کنید A و B دو ماتریس $m\times n$ باشند در این صورت حاصل ضرب هادمارد A و B که با $A\circ B$ نشان می دهیم بصورت زیر تعریف می شود:

$$(A\circ B)_{i,j}=(A)_{i,j}(B)_{i,j}.$$

تعریف۱-۱. فرض کنید Q^n ماتریس فیبوناتچی و Q^{-n}، ماتریس وارون آن باشد. آن گاه حاصل ضرب هادمارد آن را با $Q^n o\, Q^{-n}$ نمایش داده و به صورت زیر تعریف می‌شود، ([3] را ملاحظه کنید)

$$Q^n oQ^{-n}=\begin{cases} Q^n o\ adjQ^{-n}, & n=2k,\\ -(Q^n o\ adjQ^n), & n=2k+1.\end{cases}$$

در این بخش به بررسی دنباله عددی t- پیل می‌پردازیم که نتایج آن دربخش‌های بعدی مورد استفاده قرار می‌گیرد.

به سادگی می‌توان نشان داد که جواب رابطه بازگشتی دنباله عددی t- پیل بصورت

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

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

لم۱-۲ [1]. فرض کنید m، n و $t\geq 2$ اعداد صحیح باشند. روابط زیر برای دنباله عددی t- پیل برقرار است (در این‌جا فرض می کنیم $P_n=P_n^t$).

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

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

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

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

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

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

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

دربخش دوم ماتریس دنباله‌های عددی t- پیل را بررسی می‌کنیم و در بخش سوم حاصل ضرب هادمارد را روی این ماتریس‌ها تعریف می‌کنیم و برخی نتایج، که در بخش بعدی در نظریه کد گذاری مورد نیاز هستند، را به دست می‌آوریم. بخش چهارم اختصاص به ارایه یک کد با استفاده از ماتریس دنباله‌های عددی t- پیل و حاصل ضرب هادمارد آنها دارد.

۲- ماتریس دنباله‌های عددی t- پیل و برخی خواص آن ها

دراین بخش، به معرفی توان n- ام ماتریس دنباله عددی t- پیل پرداخته و سپس، ماتریس وارون آن را به دست می-آوریم.

۲-۱. تعریف

توان n-ام ماتریس دنباله عددی t- پیل که با $Q_t\left(n,P_n^t\right)$ نشان می دهیم، به صورت زیر تعریف می‌شود:

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

که در آن $n=0,\pm1,\pm2,\ldots$.

بعنوان مثال برای $n=3$، $Q_3\left(3,P_3^3\right)$ به صورت زیر است:

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

در این جا به‌ازای عدد ثابت t، فرض می‌کنیم $P_n=P_n^t$. بنا به تعریف دنباله عددی t- پیل داریم:

$$Q_t\left(n,P_n\right)=\begin{bmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{bmatrix}=\begin{bmatrix} tP_n+P_{n-1} & tP_{n-1}+P_{n-2} \\ tP_{n-1}+P_{n-2} & tP_{n-2}+P_{n-3} \end{bmatrix}$$
$$=t\begin{bmatrix} P_n & P_{n-1} \\ P_{n-1} & P_{n-2} \end{bmatrix}+\begin{bmatrix} P_{n-1} & P_{n-2} \\ P_{n-2} & P_{n-3} \end{bmatrix},$$

بنابراین داریم:

$$Q_t\left(n,P_n\right)=tQ_t\left(n-1,P_n\right)+Q_t\left(n-2,P_n\right), \qquad (۱)$$

یا

$$Q_t\left(n-2,P_n\right)=Q_t\left(n,P_n\right)-tQ_t\left(n-1,P_n\right). \qquad (۲)$$

لم۲-۲. دترمینان ماتریس $Q_t\left(n,P_n^t\right)$ برابر با $(-1)^n$ است.

برهان. برای توان n-ام ماتریس دنباله عددی t- پیل به شکل زیر،

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

داریم $DetQ_t\left(n,P_n^t\right)=P_{n+1}^tP_{n-1}^t-(P_n^t)^2$. لذا، با توجه به لم ۱-2-(vii) خواهیم داشت:

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

لم۲-۳. وارون ماتریس $Q_t\left(n, P_n^t\right)$، که $t \geq 2$ به صورت زیر است:

$$Q_t^{-1}\left(n, P^t{}_n\right) = \begin{cases} \begin{bmatrix} P^t_{2k-1} & -P^t{}_{2k} \\ -P^t{}_{2k} & P^t{}_{2k+1} \end{bmatrix}, & n = 2k, \\ \begin{bmatrix} -P_{2k}{}^t & P^t{}_{2k+1} \\ P^t{}_{2k+1} & -P^t{}_{2k+2} \end{bmatrix}, & n = 2k+1. \end{cases}$$

برهان. حکم از لم قبل و روابط بین عناصر دنباله $P^t{}_n$ بدست می‌آید

بعنوان مثال ماتریس وارون $Q_3\left(n, P_n\right)$ به‌صورت زیر هستند:

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

۲- اگر $n = 2k+1$ آنگاه

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

درجدول ۱، ماتریس دنباله عددی ۳- پیل و وارون آن، به ازای $n = 0, 1, 2, \ldots, 5$، قابل مشاهده است.

جدول ۱: $Q_3\left(n, P_n\right)$ و $Q_3^{-1}\left(n, P_n\right)$

n	0	1	2	3	4	5
$Q_3\left(n, P_n\right)$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 33 & 10 \\ 10 & 3 \end{bmatrix}$	$\begin{bmatrix} 109 & 33 \\ 33 & 10 \end{bmatrix}$	$\begin{bmatrix} 360 & 109 \\ 109 & 33 \end{bmatrix}$
$Q_3^{-1}\left(n, P_n\right)$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix}$	$\begin{bmatrix} 1 & -3 \\ -3 & 10 \end{bmatrix}$	$\begin{bmatrix} -3 & 10 \\ 10 & -33 \end{bmatrix}$	$\begin{bmatrix} 109 & -33 \\ -33 & 10 \end{bmatrix}$	$\begin{bmatrix} -33 & 109 \\ 109 & -360 \end{bmatrix}$

۳- حاصل ضرب هادمارد روی $Q_t\left(n, P_n^t\right)$

در این جا، به بررسی دترمینان حاصل ضرب هادمارد و وارون آن می‌پردازیم که از آن در بخش چهارم استفاده می شود. برای این منظور، قضیه‌های زیر را بیان و اثبات می‌کنیم.

قضیه۳-۱. حاصل ضرب هادمارد $Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right)$ را در نظر می‌گیریم. در این صورت

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

برهان. ابتدا، فرض می کنیم n عددی زوج باشد. خواهیم داشت:

$$Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right)=\begin{bmatrix}P_{2k+1}^tP_{2k-1}^t & -(P_{2k}^t)^2\\ -(P_{2k}^t)^2 & P_{2k+1}^tP_{2k-1}^t\end{bmatrix}.$$

بنابراین،

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

برای عدد فرد n داریم:

$$Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right)=\begin{bmatrix}-P_{2k+2}^tP_{2k}^t & (P_{2k+1}^t)^2\\ (P_{2k+1}^t)^2 & -P_{2k+2}^tP_{2k}^t\end{bmatrix}.$$

لذا،

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

نتیجه۳-۲. با استفاده از قضیه ۳-۱، اثر ماتریس حاصل ضرب هادمارد $Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right)$ به صورت زیر است:

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

که در آن $trac(A_{n\times n})=\sum_{i=1}^{n}a_{ii}$.

قضیه۳-۳. وارون ماتریس حاصل ضرب هادمارد $Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right)$ برای مقادیرمختلف n برابراست با:

$$\left(Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right)\right)^{-1}=\begin{cases}\begin{bmatrix}\dfrac{1+(P_{2k}^t)^2}{1+2(P_{2k}^t)^2} & \dfrac{(P_{2k}^t)^2}{1+2(P_{2k}^t)^2}\\ \dfrac{(P_{2k}^t)^2}{1+2(P_{2k}^t)^2} & \dfrac{1+(P_{2k}^t)^2}{1+2(P_{2k}^t)^2}\end{bmatrix}, & n=2k,\\ \begin{bmatrix}\dfrac{1-(P_{2k+1}^t)^2}{1-2(P_{2k+1}^t)^2} & -\dfrac{(P_{2k+1}^t)^2}{1-2(P_{2k+1}^t)^2}\\ -\dfrac{(P_{2k+1}^t)^2}{1-2(P_{2k+1}^t)^2} & \dfrac{1-(P_{2k+2}^t)^2}{1-2(P_{2k+1}^t)^2}\end{bmatrix}, & n=2k+1.\end{cases}$$

برهان. اگر n عددی زوج باشد آنگاه،

$$adj(Q_t\left(n,P_n^t\right)oQ^{-1}{}_t\left(n,P_n^t\right))=\begin{bmatrix}P_{2k+1}^tP_{2k-1}^t & (P_{2k}^t)^2\\ (P_{2k}^t)^2 & P_{2k+1}^tP_{2k-1}^t\end{bmatrix}.$$

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

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

بنابراین اگر $n=2k$ داریم:

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

برای عددی فرد n، حکم به صورت مشابه اثبات می‌شود.

۴- کد ماتریس دنباله عددی t- پیل و حاصل ضرب هادمارد آن ها

در این بخش به بررسی روش کد گذاری و کد گشایی روی ماتریس $Q_t\left(n,P_n^t\right)$ و حاصل ضرب هادمارد آن ها می‌پرازیم.

فرض کنید، $M \times Q_t\left(n, P_n^t\right) = E$ الگوریتم کد گذاری ماتریس دنباله عددی t- پیل و $E \times Q_t^{-1}\left(n, P_n^t\right) = M$ الگوریتم متناظر کد گشایی آن باشد که در آن ماتریس پیام $M_{2\times 2}$ به صورت زیر است:

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

به طوری که $m_i > 0$، $1 \le i \le 4$.

برای ارایه 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:

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

دراین صورت ، برطبق الگوریتم $M \times Q_t\left(n, P_n^t\right) = E$، خواهیم داشت:

$$M \times Q_3\left(3, P_3^3\right) = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \times \begin{bmatrix} 33 & 10 \\ 10 & 3 \end{bmatrix} = \begin{bmatrix} 33m_1 + 10m_2 & 10m_1 + 3m_2 \\ 33m_3 + 10m_4 & 10m_3 + 3m_4 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = E, \qquad (۳)$$

که در آن،

$$e_1 = 33m_1 + 10m_2,$$
$$e_2 = 10m_1 + 3m_2,$$
$$e_3 = 33m_3 + 10m_4,$$
$$e_4 = 10m_3 + 3m_4.$$

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

$$\begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} \times \begin{bmatrix} -3 & 10 \\ 10 & -33 \end{bmatrix} = \begin{bmatrix} (-3)e_1 + 10e_2 & 10e_1 + (-33)e_2 \\ (-3)e_3 + 10e_4 & 10e_3 + (-33)e_4 \end{bmatrix} = \begin{bmatrix} e_1' & e_2' \\ e_3' & e_4' \end{bmatrix} \qquad (۴)$$

با درنظرگرفتن فرمول (۳) و محاسبه درایه‌های ماتریس (۴) خواهیم داشت:

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

واضح است که روش فوق به ازای $t \ge 3$ نیز قابل تعمیم است.

اینک، دترمینان ماتریس پیام کد شده E را به دست می‌آوریم.

قضیه۴-۱. فرض کنید M ماتریس پیام و E ماتریس پیام کد شده باشد. در این صورت:

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

برهان. با توجه به الگوریتم کد گذاری $E=M\times Q_t\left(n,P_n^t\right)$ و لم ۲-۲ داریم:

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

و نتیجه مورد نظر به دست می‌آید.

در این قسمت، خطای این الگوریتم کدگذاری را مورد بررسی قرا ر می‌دهیم. درابتدا، به بررسی مثالی روی ماتریس دنباله عددی ۳- پیل پرداخته و سپس با تعمیم آن نشان می‌دهیم که فرآیند فوق برای هر $t\geq 3$ برقراراست.

الگوریتم‌های کد گذاری و کدگشایی را (بترتیب) می‌توان به صورت زیر نوشت:

$$E=M\times Q_3\left(n,P_n^3\right)=\begin{bmatrix}m_1 & m_2\\ m_3 & m_4\end{bmatrix}\times\begin{bmatrix}P_{n+1}^3 & P_n^3\\ P_n^3 & P_{n-1}^3\end{bmatrix}=\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix},\qquad (۵)$$

$$M=\begin{bmatrix}m_1 & m_2\\ m_3 & m_4\end{bmatrix}=E\times Q_3^{-1}\left(n,P_n^3\right)=\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix}\times Q_3^{-1}\left(n,P_n^3\right).\qquad (۶)$$

درحالتی که n عددی فرد باشد با استفاده از لم ۲-۲ و قرار دادن آن در فرمول (۶)، رابطه زیر به دست می‌آید:

$$\begin{bmatrix}m_1 & m_2\\ m_3 & m_4\end{bmatrix}=\begin{bmatrix}e_1 & e_2\\ e_3 & e_4\end{bmatrix}\times\begin{bmatrix}-P_{n-1}^3 & P_n^3\\ P_n^3 & -P_{n+1}^3\end{bmatrix}.\qquad (۷)$$

با توجه به فرمول (۷)، هریک از درایه های ماتریس M را بصورت زیر محاسبه میشود:

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

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

$$-P_{n-1}^3 e_1 + P_n^3 e_2 > 0, \qquad (۸)$$
$$P_n^3 e_1 - P_{n-1}^3 e_2 > 0, \qquad (۹)$$
$$-P_{n-1}^3 e_3 + P_n^3 e_4 > 0, \qquad (۱۰)$$
$$P_n^3 e_3 - P_{n+1}^3 e_4 > 0. \qquad (۱۱)$$

نامساوی‌های زیر با توجه به روابط (۸) و (۹) 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 طلایی دنباله عددی ۳- پیل می‌باشد.. به روش مشابه، با توجه به نامساوی‌های (۱۰) و (۱۱) 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 طلایی دنباله فوق می‌باشد.

اینک به بررسی مقدار خطا و تصحیح آن در این الگوریتم کد گذاری و کد گشایی روی دنباله عددی t- پیل می‌پردازیم. ابتدا فرض می‌کنیم که فقط یک خطا (خطای مفرد) در ماتریس E از کانال انتقال دریافت شود. واضح است که چهارحالت زیر را داریم:

$$(a)\begin{bmatrix} x & e_2 \\ e_3 & e_4 \end{bmatrix}, \quad (b)\begin{bmatrix} e_1 & y \\ e_3 & e_4 \end{bmatrix}, \quad (c)\begin{bmatrix} e_1 & e_2 \\ z & e_4 \end{bmatrix}, \quad (d)\begin{bmatrix} e_1 & e_2 \\ e_3 & t \end{bmatrix}, \qquad (۱۲)$$

که در آن، x, y, z, t عناصرمعیوب هستند. با استفاده از رابطه (۵) درحالت‌های (a)، (b)، (c) و (d) بترتیب داریم:

$$xe_4 - e_2e_3 = (-1)^n\, DetM$$
$$e_1e_4 - ye_3 = (-1)^n\, DetM$$
$$e_4e_1 - e_2z = (-1)^n\, DetM$$
$$e_1t - e_2e_3 = (-1)^n\, DetM$$

:

بنابراین مقدار خطای مفرد e_1، e_2، e_3 و e_4 بترتیب عبارتند از

$$x = \frac{(-1)^n\, Det\, M + e_2e_3}{e_4}, \qquad (۱۳)$$
$$y = \frac{-(-1)^n\, Det\, M + e_1e_4}{e_3}, \qquad (۱۴)$$
$$z = \frac{-(-1)^n\, Det\, M + e_1e_4}{e_2}, \qquad (۱۵)$$
$$t = \frac{(-1)^n\, Det\, M + e_2e_3}{e_1}. \qquad (۱۶)$$

روابط (۱۳) تا (۱۶) چهار مقدار مختلف را برای عناصر معیوب نشان می دهد. با توجه به اینکه این که $e_1 \approx \tau e_2$ و $e_3 \approx \tau e_4$، درعمل تنها می‌توانیم یک انتخاب از متغیرهای x, y, z, t داشته باشیم. به روش مشابه، می‌توان خطای دوگانه را نیز روی ماتریس E به دست آورد. بعنوان مثال حالت دو متغیره زیر را برای ماتریس E درنظر می گیریم. یعنی فرض کنید

$$E = \begin{bmatrix} x & y \\ e_3 & e_4 \end{bmatrix} \qquad (۱۷)$$

بااستفاده از قضیه ۴-۱ در این حالت داریم:

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

هم چنین، رابطه $x \approx \tau y$ بین x و y وجود دارد. به روش مشابه، می توان همه حالت های ممکن را برای خطای سه گانه و چهارگانه به دست آورد. باتوجه به روش فوق پانزده حالت ممکن خطا در الگوریتم (۵) وجود دارد که می-توان چهارده حالت ازخطاهای فوق را تصحیح کرد و این نشان می دهد توانایی تصحیح خطا در این روش برابراست با:

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

اکنون به بررسی کدگذاری روی حاصل ضرب هادمارد ماتریس دنباله عددی t- پیل می پردازیم. ابتدا، مانند قبل، پیام M را به صورت ماتریس 2×2 زیر درنظر می‌گیریم:

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

که در آن، $m_i>0$ $i=1,2,3,4.$ $M\times(Q_t\left(n,P_n^t\right)oQ_t^{-1}\left(n,P_n^t\right))=E$ الگوریتم کدگذاری حاصل ضرب 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 می-باشد.

اینک 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:

$$Q_2\left(4,P_4^2\right)o\,Q_2^{-1}\left(4,P_4^2\right)=\begin{bmatrix} P_3P_5 & -(P_4)^2 \\ -(P_4)^2 & P_3P_5 \end{bmatrix}=\begin{bmatrix} 145 & -144 \\ -144 & 145 \end{bmatrix}, \qquad (18)$$

$$(Q_2\left(4,P_4^2\right)oQ^{-1}{}_2\left(4,P_4^2\right))^{-1}=\begin{bmatrix} \frac{1+(P_4^2)^2}{1+2(P_4^2)^2} & \frac{(P_4^2)^2}{1+2(P_4^2)^2} \\ \frac{(P_4^2)^2}{1+2(P_4^2)^2} & \frac{1+(P_4^2)^2}{1+2(P_4^2)^2} \end{bmatrix}=\begin{bmatrix} \frac{145}{289} & \frac{144}{289} \\ \frac{144}{289} & \frac{145}{289} \end{bmatrix}, \qquad (19)$$

باتوجه به ماتریس پیام M و رابطه (18) داریم:

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

که درآن،

$$\begin{aligned} e_1&=145m_1-144m_2, \\ e_2&=-144m_1+145m_2, \\ e_3&=145m_3-144m_4, \\ e_4&=-144m_3+145m_4. \end{aligned} \qquad (20)$$

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

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

$$= \begin{bmatrix} e_1' & e_2' \\ e_3' & e_4' \end{bmatrix} = E'. \qquad (۲۱)$$

بنابراین از روابط (۲۰) و (۲۱) داریم:

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

در کدگذاری روی حاصل ضرب هادمارد، مشابه قضیه ۴-۱، میتوان قضیه زیر، را برای محاسبه دترمینان ماتریس E ثابت نمود.

قضیه۴-۲. فرض کنید M ماتریس پیام و E ماتریس پیام کد گذاری شده، و $Q_t\left(n, P_n^t\right) o Q_t^{-1}\left(n, P_n^t\right)$، حاصل ضرب هادمارد ماتریس دنباله عددی t- پیل باشد. در این صورت

$$Det\, E = \begin{cases} Det\, M \times \left(2(P_{2k}^t)^2 + 1\right), & n = 2k, \\ Det\, M \times \left(1 - 2(P_{2k}^t)^2\right), & n = 2k+1. \end{cases}$$

.

منابع

1. Falcon, S. and Plaza, A. (2009),” k-Fibonacci sequences modulo m”, Chaos, Solitons and Fractals 41, 497-504.

2. Hoggat, V. E. (1969), “Fibonacci and Lucas number”, Palo Alto, CA: Houghton-Mifflin.

3. Nalli, A. (2006), “ On the Hadamard product of Fibonacci Q^n matrix and Fibonacci Q^{-n} matrix”, Math. Sciences, Vol .1 no. 16, 753-761.

4. Stakhov, A. Massingue, V and Sluchenkova, A. (1999), “ Introduction into Fibonacci coding and cryptography”, Kharkov: Osnova.