کد گذاری روی ماتریس مولد دنباله عددی پیل- پادوان

منصور هاشمی [۱]،آزاده رجبی نژاد[۲]، الهه مهربان [۳]

۱- دانشیار، دانشگاه گیلان

m_hashemi@guilan.ac.ir

۲- دانشجوی دکتری ریاضی محض، دانشگاه گیلان

a.rajabinejad1373@gmail.com

۳-دکتری ریاضی محض، دانشگاه TRNC، ترکیه

e.mehraban.math@gmail.com

چکیده

در این مقاله دنباله عددی پیل - پادوان و کدگذاری روی این دنباله را مورد مطالعه قرار می دهیم. برای رسیدن به این هدف، ابتدا دنباله عددی پیل - پادوان را معرفی می کنیم و سپس الگوریتم های کدگذاری و کدگشایی روی این دنباله را به دست می آوریم. در پایان، نتیجه می گیریم که توانایی تصحیح خطا به کمک این روش ۹۹/۸٪ است.

کلمات کلیدی: دنباله عددی پیل - پادوان، الگوریتم کدگذاری و کد گشایی، ماتریس مولد.

۱. مقدمه

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، شبکه های حسگر بی سیم و شبکه های ارتباطی ماهواره ای مورد استفاده قرار می گیرد. نظریه کدگذاری فیبوناتچی توسط Stokhov و همکارانش [1] در سال ۱۹۹۹ معرفی گردید. پس از آن، مطالعات زیادی به بررسی کدگذاری روی دنباله های مختلف و ماتریس آنها اختصاص یافته است.

Deveci در سال ۲۰۱۵ در [2]، دنباله عددی پیل– پادوان $\{PP_{(n)}\}_{-\infty}^{\infty}$ را به صورت زیر تعریف کرد:

$$PP_{(n)} = 2PP_{(n-2)} + PP_{(n-3)}$$

که $PP_{(0)} = PP_{(1)} = PP_{(2)} = 1$.

واضح است که وقتی $n < 0$ می توان از رابطه

$$PP_{(n)} = PP_{(n+3)} - 2PP_{(n+1)}$$

برای محاسبه $PP_{(n)}$ کمک گرفت. تعدادی از جملات دنباله عددی پیل – پادوان در جدول ۱ آمده است.

جدول ۱- جملات دنباله عددی پیل - پادوان

n	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
$PP_{(n)}$	۱	۱	۱	۳	۳	۷	۹	۱۷	۲۵	۴۳	۶۷

دنباله عددی پیل - پادوان به کمک ماتریس زیر ساخته می شود [3]:

$$Q = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

واضح است که $det\,(Q) = 1$.

مقدار $\alpha = \lim_{k\to\infty} \frac{PP_{(k+1)}}{PP_{(k)}}$ را نسبت حدی دنباله عددی پیل - پادوان می نامیم که $\alpha = \frac{1+\sqrt{5}}{2} \sim 1/618$ تنها ریشه حقیقی مثبت معادله مشخصه آن می باشد.

در بخش دوم این مقاله ، برخی از خواص ماتریس Q^k را که در بخش های بعدی مورد استفاده قرار می گیرند، بررسی می کنیم. در بخش سوم ، کدگذاری و کدگشایی روی دنباله عددی پیل - پادوان را به دست آورده و توانایی تصحیح خطای آن را محاسبه می کنیم.

۲. برخی از خواص ماتریس Q^k

ابتدا ماتریس Q^k را محاسبه می کنیم. داریم:

لم۲-۱. برای هر عدد صحیح $k \geq 1$ داریم:

$$Q^k = \begin{bmatrix} \frac{PP_{(k)} - PP_{(k-1)}}{2} & \frac{PP_{(k+2)} - PP_{(k+1)}}{2} & \frac{PP_{(k+1)} - PP_{(k)}}{2} \\ \frac{PP_{(k+1)} - PP_{(k)}}{2} & \frac{PP_{(k+3)} - PP_{(k+2)}}{2} & \frac{PP_{(k+2)} - PP_{(k+1)}}{2} \\ \frac{PP_{(k+2)} - PP_{(k+1)}}{2} & \frac{PP_{(k+4)} - PP_{(k+3)}}{2} & \frac{PP_{(k+3)} - PP_{(k+2)}}{2} \end{bmatrix}$$

برهان. برای $k = 1$ داریم:

$$Q^1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} \frac{PP_{(1)} - PP_{(0)}}{2} & \frac{PP_{(3)} - PP_{(2)}}{2} & \frac{PP_{(2)} - PP_{(1)}}{2} \\ \frac{PP_{(2)} - PP_{(1)}}{2} & \frac{PP_{(4)} - PP_{(3)}}{2} & \frac{PP_{(3)} - PP_{(2)}}{2} \\ \frac{PP_{(3)} - PP_{(2)}}{2} & \frac{PP_{(5)} - PP_{(4)}}{2} & \frac{PP_{(4)} - PP_{(3)}}{2} \end{bmatrix}.$$

فرض کنیم حکم به ازای $k = m$ برقرار باشد. یعنی

$$Q^m=\begin{bmatrix} \frac{PP_{(m)}-PP_{(m-1)}}{2} & \frac{PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{PP_{(m+1)}-PP_{(m)}}{2} \\ \frac{PP_{(m+1)}-PP_{(m)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} & \frac{PP_{(m+2)}-PP_{(m+1)}}{2} \\ \frac{PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{PP_{(m+4)}-PP_{(m+3)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} \end{bmatrix}.$$

حال ثابت می کنیم، حکم به ازای $k=m+1$ نیز برقرار است.

$$Q^{m+1}=Q^m\times Q=\begin{bmatrix} \frac{PP_{(m)}-PP_{(m-1)}}{2} & \frac{PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{PP_{(m+1)}-PP_{(m)}}{2} \\ \frac{PP_{(m+1)}-PP_{(m)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} & \frac{PP_{(m+2)}-PP_{(m+1)}}{2} \\ \frac{PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{PP_{(m+4)}-PP_{(m+3)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} \end{bmatrix}\times\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

$$=\begin{bmatrix} \frac{PP_{(m+1)}-PP_{(m)}}{2} & \frac{2PP_{(m+1)}-PP_{(m)}-PP_{(m-1)}}{2} & \frac{PP_{(m+2)}-PP_{(m+1)}}{2} \\ \frac{PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{2PP_{(m+2)}-PP_{(m+1)}-PP_{(m)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} \\ \frac{PP_{(m+3)}-PP_{(m+2)}}{2} & \frac{2PP_{(m+3)}-PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{PP_{(m+4)}-PP_{(m+3)}}{2} \end{bmatrix}$$

$$=\begin{bmatrix} \frac{PP_{(m+1)}-PP_{(m)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} & \frac{PP_{(m+2)}-PP_{(m+1)}}{2} \\ \frac{PP_{(m+2)}-PP_{(m+1)}}{2} & \frac{PP_{(m+4)}-PP_{(m+3)}}{2} & \frac{PP_{(m+3)}-PP_{(m+2)}}{2} \\ \frac{PP_{(m+3)}-PP_{(m+2)}}{2} & \frac{PP_{(m+5)}-PP_{(m+4)}}{2} & \frac{PP_{(m+4)}-PP_{(m+3)}}{2} \end{bmatrix}.$$

بنابراین حکم برقرار است. ■

لم۲-۲. برای هر عدد صحیح $k\geq 1$ ، داریم:

۱) $Q^k=2Q^{k-2}+Q^{k-3}$.

۲) $det(Q^k)=1$.

۳) $Q^{-k}=\frac{1}{4}\begin{bmatrix} q_{1k} & q_{2k} & q_{3k} \\ q_{4k} & q_{5k} & q_{6k} \\ q_{7k} & q_{8k} & q_{9k} \end{bmatrix}$ که

$q_{1k}=(PP_{(k+3)}-PP_{(k+2)})^2-(PP_{(k+2)}-PP_{(k+1)})(PP_{(k+4)}-PP_{(k+3)})$;

$q_{2k}=(PP_{(k+1)}-PP_{(k)})(PP_{(k+4)}-PP_{(k+3)})-(PP_{(k+2)}-PP_{(k+1)})(PP_{(k+3)}-PP_{(k+2)})$;

$q_{3k}=(PP_{(k+2)}-PP_{(k+1)})^2-(PP_{(k+1)}-PP_{(k)})(PP_{(k+3)}-PP_{(k+2)})$;

$q_{4k}=(PP_{(k+2)}-PP_{(k+1)})^2-(PP_{(k+1)}-PP_{(k)})(PP_{(k+3)}-PP_{(k+2)})$;

$q_{5k}=(PP_{(k)}-PP_{(k-1)})(PP_{(k+3)}-PP_{(k+2)})-(PP_{(k+1)}-PP_{(k)})(PP_{(k+2)}-PP_{(k+1)})$;

$q_{6k}=(PP_{(k+1)}-PP_{(k)})^2-(PP_{(k+2)}-PP_{(k+1)})(PP_{(k)}-PP_{(k-1)})$;

$q_{7k}=(PP_{(k+4)}-PP_{(k+3)})(PP_{(k+1)}-PP_{(k)})-(PP_{(k+3)}-PP_{(k+2)})(PP_{(k+2)}-PP_{(k+1)})$;

$q_{8k}=(PP_{(k+2)}-PP_{(k+1)})^2-(PP_{(k+4)}-PP_{(k+3)})(PP_{(k)}-PP_{(k-1)})$;

$q_{9k}=(PP_{(k)}-PP_{(k-1)})(PP_{(k+3)}-PP_{(k+2)})-(PP_{(k+2)}-PP_{(k+1)})(PP_{(k+1)}-PP_{(k)})$;

برهان.

۱. داریم:

$$2Q^{k-2}+Q^{k-3}=2\times\begin{bmatrix}\frac{PP_{(k-2)}-PP_{(k-3)}}{2} & \frac{PP_{(k)}-PP_{(k-1)}}{2} & \frac{PP_{(k-1)}-PP_{(k-2)}}{2}\\ \frac{PP_{(k-1)}-PP_{(k-2)}}{2} & \frac{PP_{(k+1)}-PP_{(k)}}{2} & \frac{PP_{(k)}-PP_{(k-1)}}{2}\\ \frac{PP_{(k)}-PP_{(k-1)}}{2} & \frac{PP_{(k+2)}-PP_{(k+1)}}{2} & \frac{PP_{(k+1)}-PP_{(k)}}{2}\end{bmatrix}$$
$$+\begin{bmatrix}\frac{PP_{(k-3)}-PP_{(k-4)}}{2} & \frac{PP_{(k-1)}-PP_{(k-2)}}{2} & \frac{PP_{(k-2)}-PP_{(k-3)}}{2}\\ \frac{PP_{(k-2)}-PP_{(k-3)}}{2} & \frac{PP_{(k)}-PP_{(k-1)}}{2} & \frac{PP_{(k-1)}-PP_{(k-2)}}{2}\\ \frac{PP_{(k-1)}-PP_{(k-2)}}{2} & \frac{PP_{(k+1)}-PP_{(k)}}{2} & \frac{PP_{(k)}-PP_{(k-1)}}{2}\end{bmatrix}$$
$$=\begin{bmatrix}\frac{PP_{(k)}-PP_{(k-1)}}{2} & \frac{PP_{(k+2)}-PP_{(k+1)}}{2} & \frac{PP_{(k+1)}-PP_{(k)}}{2}\\ \frac{PP_{(k+1)}-PP_{(k)}}{2} & \frac{PP_{(k+3)}-PP_{(k+2)}}{2} & \frac{PP_{(k+2)}-PP_{(k+1)}}{2}\\ \frac{PP_{(k+2)}-PP_{(k+1)}}{2} & \frac{PP_{(k+4)}-PP_{(k+3)}}{2} & \frac{PP_{(k+3)}-PP_{(k+2)}}{2}\end{bmatrix}=Q^k.\ \blacksquare$$

۲. با توجه به اینکه $det\ (Q)=1$ ، واضح است که $det(Q^k)=1$.

۳. برای اثبات قسمت سوم به استقرا روی k عمل می کنیم. داریم $Q^1=\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 2 & 0\end{bmatrix}$. بنابراین

$$Q^{-1}=\begin{bmatrix}-2 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}$$

از طرفی داریم:

$$\frac{1}{4}q_{11}=\frac{1}{4}[(PP_{(4)}-PP_{(3)})^2-(PP_{(3)}-PP_{(2)})(PP_{(5)}-PP_{(4)})]=-2$$
$$\frac{1}{4}q_{21}=\frac{1}{4}[(PP_{(2)}-PP_{(1)})(PP_{(5)}-PP_{(4)})-(PP_{(3)}-PP_{(2)})(PP_{(4)}-PP_{(3)})]=0$$
$$\frac{1}{4}q_{31}=\frac{1}{4}[(PP_{(3)}-PP_{(2)})^2-(PP_{(2)}-PP_{(1)})(PP_{(4)}-PP_{(3)})]=1$$
$$\frac{1}{4}q_{41}=\frac{1}{4}[(PP_{(3)}-PP_{(2)})^2-(PP_{(2)}-PP_{(1)})(PP_{(4)}-PP_{(3)})]=1$$
$$\frac{1}{4}q_{51}=\frac{1}{4}[(PP_{(1)}-PP_{(0)})(PP_{(4)}-PP_{(3)})-(PP_{(2)}-PP_{(1)})(PP_{(3)}-PP_{(2)})]=0$$
$$\frac{1}{4}q_{61}=\frac{1}{4}[(PP_{(2)}-PP_{(1)})^2-(PP_{(3)}-PP_{(2)})(PP_{(1)}-PP_{(0)})]=0$$
$$\frac{1}{4}q_{71}=\frac{1}{4}[(PP_{(5)}-PP_{(4)})(PP_{(2)}-PP_{(1)})-(PP_{(4)}-PP_{(3)})(PP_{(3)}-PP_{(2)})]=0$$
$$\frac{1}{4}q_{81}=\frac{1}{4}[(PP_{(3)}-PP_{(2)})^2-(PP_{(5)}-PP_{(4)})(PP_{(1)}-PP_{(0)})]=1$$
$$\frac{1}{4}q_{91}=\frac{1}{4}[(PP_{(1)}-PP_{(0)})(PP_{(4)}-PP_{(3)})-(PP_{(3)}-PP_{(2)})(PP_{(2)}-PP_{(1)})]=0$$

بنابراین

$$\frac{1}{4}\begin{bmatrix} q_{11} & q_{21} & q_{31} \\ q_{41} & q_{51} & q_{61} \\ q_{71} & q_{81} & q_{91} \end{bmatrix} = \begin{bmatrix} -2 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = Q^{-1}$$

فرض کنیم حکم به ازای $k = m$ برقرار باشد یعنی

$$Q^{-m} = \frac{1}{4}\begin{bmatrix} q_{1m} & q_{2m} & q_{3m} \\ q_{4m} & q_{5m} & q_{6m} \\ q_{7m} & q_{8m} & q_{9m} \end{bmatrix}$$

حال ثابت می کنیم، حکم به ازای $k = m + 1$ نیز برقرار است.

$$Q^{-(m+1)} = Q^{-1} \times Q^{-m} = \begin{bmatrix} -2 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \times \frac{1}{4}\begin{bmatrix} q_{1m} & q_{2m} & q_{3m} \\ q_{4m} & q_{5m} & q_{6m} \\ q_{7m} & q_{8m} & q_{9m} \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} -2q_{1m} + q_{7m} & -2q_{2m} + q_{8m} & -2q_{3m} + q_{9m} \\ q_{1m} & q_{2m} & q_{3m} \\ q_{4m} & q_{5m} & q_{6m} \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} q_{1m+1} & q_{2m+1} & q_{3m+1} \\ q_{4m+1} & q_{5m+1} & q_{6m+1} \\ q_{7m+1} & q_{8m+1} & q_{9m+1} \end{bmatrix}. \blacksquare$$

۳. کدگذاری و کدگشایی روی ماتریس دنباله های عددی پیل - پادوان

در این بخش، به بررسی روش کدگذاری و کدگشایی به کمک ماتریس Q^k می پردازیم. ماتریس مربعی 3×3 پیام P و ماتریس معکوس پذیر Q^k را درنظر می گیریم. در این صورت، عبارت $P \times Q^k = E$ الگوریتم کدگذاری و عبارت $E \times Q^{-k} = P$ را الگوریتم کدگشایی نامیده می شود. ماتریس E را ماتریس کد می نامیم.

لم۳-۱. در الگوریتم کدگذاری $P \times Q^k = E$، داریم $det(E) = det(P)$.

برهان. داریم:

$$det(E) = det(P \times Q^k) = det(P) \times det(Q^k) = det(P) \times 1 = det(P) \blacksquare \qquad (1-3)$$

۳-۱. نمونه ای از کدگذاری و کدگشایی روی ماتریس دنباله عددی پیل - پادوان

ماتریس مربعی 3×3 پیام P را به صورت زیر در نظر بگیرید.

$$P = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{bmatrix}$$

به طوری که $p_i \geq 0$، $1 \leq i \leq 9$. به عنوان مثال، برای $k = 4$ داریم:

$$Q^4 = \begin{bmatrix} \frac{PP_{(4)} - PP_{(3)}}{2} & \frac{PP_{(6)} - PP_{(5)}}{2} & \frac{PP_{(5)} - PP_{(4)}}{2} \\ \frac{PP_{(5)} - PP_{(4)}}{2} & \frac{PP_{(7)} - PP_{(6)}}{2} & \frac{PP_{(6)} - PP_{(5)}}{2} \\ \frac{PP_{(6)} - PP_{(5)}}{2} & \frac{PP_{(8)} - PP_{(7)}}{2} & \frac{PP_{(7)} - PP_{(6)}}{2} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 4 & 1 \\ 1 & 4 & 4 \end{bmatrix}$$

و

$$Q^{-4} = \begin{bmatrix} 12 & 4 & -7 \\ -7 & -2 & 4 \\ 4 & 1 & -2 \end{bmatrix}$$

در این صورت طبق الگوریتم کدگذاری $P \times Q^k = E$ خواهیم داشت:

$$P \times Q^4 = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 2 \\ 2 & 4 & 1 \\ 1 & 4 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} 2p_2 + p_3 & p_1 + 4p_2 + 4p_3 & 2p_1 + p_2 + 4p_3 \\ 2p_5 + p_6 & p_4 + 4p_5 + 4p_6 & 2p_4 + p_5 + 4p_6 \\ 2p_8 + p_9 & p_7 + 4p_8 + 4p_9 & 2p_7 + p_8 + 4p_9 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix} = E.$$

که در آن،

$$\begin{aligned} &e_1 = 2p_2 + p_3, \quad e_2 = p_1 + 4p_2 + 4p_3, \quad e_3 = 2p_1 + p_2 + 4p_3, \\ &e_4 = 2p_5 + p_6, \quad e_5 = p_4 + 4p_5 + 4p_6, \quad e_6 = 2p_4 + p_5 + 4p_6, \\ &e_7 = 2p_8 + p_9, \quad e_8 = p_7 + 4p_8 + 4p_9, \quad e_9 = 2p_7 + p_8 + 4p_9. \end{aligned}$$

با حل دستگاه بالا نتیجه می شود :

$$\begin{aligned} &p_1 = 12e_1 - 7e_2 + 4e_3, \quad p_2 = 4e_1 - 2e_2 + e_3, \quad p_3 = -7e_1 + 4e_2 - 2e_3, \\ &p_4 = 12e_4 - 7e_5 + 4e_6, \quad p_5 = 4e_4 - 2e_5 + e_6, \quad p_6 = -7e_4 + 4e_5 - 2e_6, \\ &p_7 = 12e_7 - 7e_8 + 4e_9, \quad p_8 = 4e_7 - 2e_8 + e_9, \quad p_9 = -7e_7 + 4e_8 - 2e_9. \end{aligned}$$

بنابراین، یک پیام کدگذاری شده به صورت

$$E = e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9$$

به کانال ارتباطی فرستاده می شود. حال الگوریتم کدگشایی از ماتریس E به صورت زیر است.

$$E \times Q^{-4} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix} \times \begin{bmatrix} 12 & 4 & -7 \\ -7 & -2 & 4 \\ 4 & 1 & -2 \end{bmatrix}$$

$$= \begin{bmatrix} 12e_1 - 7e_2 + 4e_3 & 4e_1 - 2e_2 + e_3 & -7e_1 + 4e_2 - 2e_3 \\ 12e_4 - 7e_5 + 4e_6 & 4e_4 - 2e_5 + e_6 & -7e_4 + 4e_5 - 2e_6 \\ 12e_7 - 7e_8 + 4e_9 & 4e_7 - 2e_8 + e_9 & -7e_7 + 4e_8 - 2e_9 \end{bmatrix} = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{bmatrix}$$

$$= P.$$

مثال ۳-۱-۱. پیامی به صورت ۳۵۶۷۴۸۹ به شبکه ارتباطی ارسال می شود، ماتریس پیام P به صورت زیر نوشته می شود:

$$P = \begin{bmatrix} 0 & 0 & 3 \\ 5 & 6 & 7 \\ 4 & 8 & 9 \end{bmatrix}$$

کدگذاری و کدگشایی را به کمک دو ماتریس $Q^4=\begin{bmatrix}0&1&2\\2&4&1\\1&4&4\end{bmatrix}$ و $Q^{-4}=\begin{bmatrix}12&4&-7\\-7&-2&4\\4&1&-2\end{bmatrix}$ انجام می دهیم.

ماتریس کد به صورت زیر به دست می آید.

$$E=P\times Q^4=\begin{bmatrix}0&0&3\\5&6&7\\4&8&9\end{bmatrix}\times\begin{bmatrix}0&1&2\\2&4&1\\1&4&4\end{bmatrix}=\begin{bmatrix}3&12&12\\19&57&44\\25&72&52\end{bmatrix}.$$

کدگشایی به صورت زیر انجام می شود.

$$P=E\times Q^{-4}=\begin{bmatrix}3&12&12\\19&81&44\\25&72&52\end{bmatrix}\times\begin{bmatrix}12&4&-7\\-7&-2&4\\4&1&-2\end{bmatrix}=\begin{bmatrix}0&0&3\\5&6&7\\4&8&9\end{bmatrix}.$$

۳-۲. توانایی تصحیح خطا

اینک به بررسی مقدار خطا و تصحیح آن در این الگوریتم کدگذاری و کدگشایی روی دنباله عددی پیل - پادوان می پردازیم.

فرض اول این است که فقط یک خطا در ماتریس کد E از کانال دریافت شود. بنابراین ۹ حالت زیر ممکن است رخ دهد.

$$\begin{bmatrix}x_1&e_2&e_3\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},\begin{bmatrix}e_1&x_2&e_3\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},\begin{bmatrix}e_1&e_2&x_3\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},$$
$$\begin{bmatrix}e_1&e_2&e_3\\x_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},\begin{bmatrix}e_1&e_2&e_3\\e_4&x_5&e_6\\e_7&e_8&e_9\end{bmatrix},\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&x_6\\e_7&e_8&e_9\end{bmatrix},$$
$$\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\x_7&e_8&e_9\end{bmatrix},\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\e_7&x_8&e_9\end{bmatrix},\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\e_7&e_8&x_9\end{bmatrix},$$

که $x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9$ عناصر همراه با خطا هستند.

حال رابطه $(3-1)$ را برای هریک از حالت های بالا بررسی می کنیم.

$$\begin{aligned}
x_1(e_5e_9-e_6e_8)+e_2(e_6e_7-e_4e_9)+e_3(e_4e_8-e_5e_7)&=\det(P), && (1-2-3)\\
e_1(e_5e_9-e_6e_8)+x_2(e_6e_7-e_4e_9)+e_3(e_4e_8-e_5e_7)&=\det(P), && (2-2-3)\\
e_1(e_5e_9-e_6e_8)+e_2(e_6e_7-e_4e_9)+x_3(e_4e_8-e_5e_7)&=\det(P), && (3-2-3)\\
x_4(e_3e_8-e_2e_9)+e_5(e_1e_9-e_3e_7)+e_6(e_2e_7-e_1e_8)&=\det(P), && (4-2-3)\\
e_4(e_3e_8-e_2e_9)+x_5(e_1e_9-e_3e_7)+e_6(e_2e_7-e_1e_8)&=\det(P), && (5-2-3)\\
e_4(e_3e_8-e_2e_9)+e_5(e_1e_9-e_3e_7)+x_6(e_2e_7-e_1e_8)&=\det(P), && (6-2-3)\\
x_7(e_2e_6-e_3e_5)+e_8(e_3e_4-e_1e_6)+e_9(e_1e_5-e_2e_4)&=\det(P), && (7-2-3)\\
e_7(e_2e_6-e_3e_5)+x_8(e_3e_4-e_1e_6)+e_9(e_1e_5-e_2e_4)&=\det(P), && (8-2-3)\\
e_7(e_2e_6-e_3e_5)+e_8(e_3e_4-e_1e_6)+x_9(e_1e_5-e_2e_4)&=\det(P), && (9-2-3)
\end{aligned}$$

از نه رابطه بالا تساوی های زیر نتیجه می شود:

$$x_1=\frac{det(P)-e_2(e_6e_7-e_4e_9)-e_3(e_4e_8-e_5e_7)}{e_5e_9-e_6e_8}, \qquad (10-2-3)$$
$$x_2=\frac{det(P)-e_1(e_5e_9-e_6e_8)-e_3(e_4e_8-e_5e_7)}{e_6e_7-e_4e_9}, \qquad (11-2-3)$$
$$x_3=\frac{det(P)-e_1(e_5e_9-e_6e_8)-e_2(e_6e_7-e_4e_9)}{e_4e_8-e_5e_7}, \qquad (12-2-3)$$
$$x_4=\frac{det(P)-e_5(e_1e_9-e_3e_7)-e_6(e_2e_7-e_1e_8)}{e_3e_8-e_2e_9}, \qquad (13-2-3)$$

$$x_5 = \frac{det(P) - e_4(e_3e_8 - e_2e_9) - e_6(e_2e_7 - e_1e_8)}{e_1e_9 - e_3e_7}, \qquad (14-2-3)$$

$$x_6 = \frac{det(P) - e_4(e_3e_8 - e_2e_9) - e_5(e_1e_9 - e_3e_7)}{e_2e_7 - e_1e_8}, \qquad (15-2-3)$$

$$x_7 = \frac{det(P) - e_8(e_3e_4 - e_1e_6) - e_9(e_1e_5 - e_2e_4)}{e_2e_6 - e_3e_5}, \qquad (16-2-3)$$

$$x_8 = \frac{det(P) - e_7(e_2e_6 - e_3e_5) - e_9(e_1e_5 - e_2e_4)}{e_3e_4 - e_1e_6}, \qquad (17-2-3)$$

$$x_9 = \frac{det(P) - e_7(e_2e_6 - e_3e_5) - e_8(e_3e_4 - e_1e_6)}{e_1e_5 - e_2e_4}, \qquad (18-2-3)$$

روابط $(3-2-10)$ تا $(3-2-18)$ قابلیت تصحیح خطاهای یگانه را دارد. در صورتی که خطای ماتریس کد E خطای دوگانه به صورت زیر باشد:

$$\begin{bmatrix} x & y & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix}$$

طبق رابطه $(3-1)$ خواهیم داشت:

$$x(e_5e_9 - e_6e_8) + y(e_6e_7 - e_4e_9) = e_3(e_5e_7 - e_4e_8) + det(P) \qquad (19-2-3)$$

به وضوح، به $\binom{9}{2} = 36$ حالت ممکن است تنها دو خطا در ماتریس کد رخ دهد و به کمک رابطه (۳-۱) و هم چنین روابط $(3-2-10)$ تا $(3-2-18)$ تمامی خطاهای دوگانه قابل تصحیح می باشند. به روش مشابه می توان تمام خطاهای یگانه، دوگانه و .... و هشت گانه را تصحیح کرد. بنابراین

$$\binom{9}{1} + \binom{9}{2} + \binom{9}{3} + \binom{9}{4} + \binom{9}{5} + \binom{9}{6} + \binom{9}{7} + \binom{9}{8} + \binom{9}{9} = 511$$

حالت خطا برای ماتریس کد E ممکن است پیش بیاید که 510 مورد خطاهای یگانه، دوگانه، ... و هشت گانه قابل تصحیح است، لذا توانایی تصحیح خطا به کمک این روش $\frac{510}{511} = 0/9980$ یعنی ۹۹/۸٪ می باشد.

۴. نتیجه گیری

این مقاله به استفاده از ماتریس مولد دنباله عددی پیل - پادوان در نظریه کدگذاری اختصاص دارد. ابتدا این دنباله عددی را تعریف نموده و ماتریس مولد آن را ارائه دادیم. سپس به بررسی الگوریتم کدگذاری روی این ماتریس‌ها پرداخته و نشان دادیم که توانایی تصحیح خطا در این الگوریتم برابر ۹۹/۸٪ است.

۵. مراجع

[1] A. Stokhov, V. Massingue and A. Sluchenkova, "Introduction into Fibonacci Coding and Cryptography," *Kharkov:Osnova* , 1999.

[2] O. Deveci, Y., Akuzum, E., Karadomani., "The Pell-Padovan p-Sequences and Its Applications,"*Util. Math* , 2015, pp. 327-347.

[3] O. Deveci, E., Karadomani ,"On the Padovan p-numbers," *Hacettepe Journal of Mathematics and Statistics*, 2017 , pp. 579-592.