

کدگذاری روی ماتریس دنباله های پادوان

منصور هاشمی^۱، الهه مهربان^۲، آزاده رجیبی نژاد^{۳*}

۱- دانشیار، دانشگاه گیلان

۲- دکتری ریاضی محض، دانشگاه گیلان

۳- دانشجوی دکتری ریاضی محض، دانشگاه گیلان

چکیده

در این مقاله دنباله عددی پادوان و کدگذاری روی این دنباله را مورد مطالعه قرار می دهیم. برای رسیدن به این هدف، ابتدا دنباله عددی 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 توانایی تصحیح خطا به کمک این روش ۹۹/۸٪ است.

کلمات کلیدی: دنباله عددی پادوان، الگوریتم کدگذاری و کد گشایی، ماتریس

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 با برد کوتاه، 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 و رمزگذاری روی دنباله های مختلف و ماتریس آنها اختصاص یافته است. در سال ۲۰۰۷، Gogin [2] به معرفی دنباله عددی پادوان به صورت زیر پرداخت:

دنباله عددی پادوان که با $\{P(n)\}_{-\infty}^{\infty}$ نمایش می دهیم به صورت $P(n) = P(n-2) + P(n-3)$ با شرایط

اولیه $P(0) = P(1) = P(2) = 1$ تعریف می شود. تعدادی از عناصر دنباله پادوان در جدول زیر آمده است.

جدول ۱- عناصر دنباله عددی پادوان

n	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10
$P(n)$	2	-1	0	1	-1	1	0	0	1	0	1	1	1	2	2	3	4	5	7	9	12

*Email: a.rajabinejad1373@gmail.com

سپس در سال ۲۰۱۵، Devenci این تعریف را تعمیم داد و دنباله عددی پیل پادوان را تعریف کرد [3]. سرانجام او در سال ۲۰۱۷، ماتریس مولد این دنباله را ساخت. برای مطالعه بیشتر به [4] مراجعه نمایید. دنباله پادوان به کمک ماتریس زیر ساخته می شود:

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

واضح است که $\det(Q) = 1$.

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

$$Q^k = \begin{bmatrix} P_{(k-5)} & P_{(k-3)} & P_{(k-4)} \\ P_{(k-4)} & P_{(k-2)} & P_{(k-3)} \\ P_{(k-3)} & P_{(k-1)} & P_{(k-2)} \end{bmatrix}$$

برهان. برای $k = 1$ و $k = 2$ داریم:

$$Q^1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} P_{(-4)} & P_{(-2)} & P_{(-3)} \\ P_{(-3)} & P_{(-1)} & P_{(-2)} \\ P_{(-2)} & P_{(0)} & P_{(-1)} \end{bmatrix}$$

9

$$Q^2 = Q \times Q = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} P_{(-3)} & P_{(-1)} & P_{(-2)} \\ P_{(-2)} & P_{(0)} & P_{(-1)} \\ P_{(-1)} & P_{(1)} & P_{(0)} \end{bmatrix}.$$

برای $k = 1$ و $k = 2$ رابطه بالا برقرار است. فرض کنیم حکم به ازای $k = m$ برقرار باشد یعنی

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

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

$$\begin{aligned} Q^{m+1} &= Q^m \times Q = \begin{bmatrix} P_{(m-5)} & P_{(m-3)} & P_{(m-4)} \\ P_{(m-4)} & P_{(m-2)} & P_{(m-3)} \\ P_{(m-3)} & P_{(m-1)} & P_{(m-2)} \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} P_{(m-4)} & P_{(m-5)} + P_{(m-4)} & P_{(m-3)} \\ P_{(m-3)} & P_{(m-4)} + P_{(m-3)} & P_{(m-2)} \\ P_{(m-2)} & P_{(m-3)} + P_{(m-2)} & P_{(m-1)} \end{bmatrix} = \begin{bmatrix} P_{(m-4)} & P_{(m-2)} & P_{(m-3)} \\ P_{(m-3)} & P_{(m-1)} & P_{(m-2)} \\ P_{(m-2)} & P_{(m)} & P_{(m-1)} \end{bmatrix}. \end{aligned}$$

بنابراین حکم برقرار است. ■

مقدار $\alpha = \lim_{k \rightarrow \infty} \frac{P(k)}{P(k-1)}$ را نسبت حدی دنباله عددی پادوان می نامیم که تنها ریشه حقیقی معادله مشخصه این

دنباله به صورت $x^3 - x - 1 = 0$ می باشد، بنابراین $\alpha = 1/32511$.

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

۲. برخی از خواص ماتریس Q^k

در اینجا، با در نظر گرفتن ماتریس Q^k ، به بررسی برخی خواص آن می پردازیم.

لم ۱-۲. برای هر عدد صحیح $k \geq 1$ ، داریم:

$$Q^k = Q^{k-2} + Q^{k-3} \quad (۱)$$

برهان.

$$\begin{aligned} Q^k &= \begin{bmatrix} P_{(k-5)} & P_{(k-3)} & P_{(k-4)} \\ P_{(k-4)} & P_{(k-2)} & P_{(k-3)} \\ P_{(k-3)} & P_{(k-1)} & P_{(k-2)} \\ P_{(k-7)} & P_{(k-5)} & P_{(k-6)} \\ P_{(k-6)} & P_{(k-4)} & P_{(k-5)} \\ P_{(k-5)} & P_{(k-3)} & P_{(k-4)} \end{bmatrix} = \begin{bmatrix} P_{(k-7)+P_{(k-8)}} & P_{(k-5)+P_{(k-6)}} & P_{(k-6)+P_{(k-5)}} \\ P_{(k-6)+P_{(k-7)}} & P_{(k-4)+P_{(k-5)}} & P_{(k-5)+P_{(k-4)}} \\ P_{(k-5)+P_{(k-6)}} & P_{(k-3)+P_{(k-4)}} & P_{(k-4)+P_{(k-3)}} \\ P_{(k-8)} & P_{(k-6)} & P_{(k-5)} \\ P_{(k-7)} & P_{(k-5)} & P_{(k-4)} \\ P_{(k-6)} & P_{(k-4)} & P_{(k-3)} \end{bmatrix} \\ &= \begin{bmatrix} P_{(k-7)} & P_{(k-5)} & P_{(k-6)} \\ P_{(k-6)} & P_{(k-4)} & P_{(k-5)} \\ P_{(k-5)} & P_{(k-3)} & P_{(k-4)} \end{bmatrix} + \begin{bmatrix} P_{(k-8)} & P_{(k-6)} & P_{(k-5)} \\ P_{(k-7)} & P_{(k-5)} & P_{(k-4)} \\ P_{(k-6)} & P_{(k-4)} & P_{(k-3)} \end{bmatrix} = Q^{k-2} + Q^{k-3} \quad \blacksquare \end{aligned}$$

$$\det(Q^k) = 1 \quad (۲)$$

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

(۳)

$$Q^{-k} = \begin{bmatrix} P^2_{(k-2)} - P_{(k-3)}P_{(k-1)} & P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)} & P^2_{(k-3)} - P_{(k-4)}P_{(k-2)} \\ P^2_{(k-3)} - P_{(k-4)}P_{(k-2)} & P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)} & P^2_{(k-4)} - P_{(k-5)}P_{(k-3)} \\ P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)} & P^2_{(k-3)} - P_{(k-5)}P_{(k-1)} & P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)} \end{bmatrix}$$

برهان. به استقرا روی k عمل می‌کنیم. داریم:

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

بنابراین،

$$\begin{aligned} Q^{-1} &= \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0^2 - 1 \times 1 & 0 \times 1 - 1 \times 0 & 1^2 - 0 \times 0 \\ 1^2 - 0 \times 0 & 0 \times 0 - 0 \times 1 & 0^2 - 0 \times 1 \\ 0 \times 1 - 1 \times 0 & 1^2 - 0 \times 1 & 0 \times 0 - 0 \times 1 \end{bmatrix} = \\ &= \begin{bmatrix} P^2_{(-1)} - P_{(-2)}P_{(0)} & P_{(-3)}P_{(0)} - P_{(-2)}P_{(-1)} & P^2_{(-2)} - P_{(-3)}P_{(-1)} \\ P^2_{(-2)} - P_{(-3)}P_{(-1)} & P_{(-4)}P_{(-1)} - P_{(-3)}P_{(-2)} & P^2_{(-3)} - P_{(-4)}P_{(-2)} \\ P_{(-3)}P_{(0)} - P_{(-2)}P_{(-1)} & P^2_{(-2)} - P_{(-4)}P_{(0)} & P_{(-4)}P_{(-1)} - P_{(-3)}P_{(-2)} \end{bmatrix} \\ Q^{-2} &= Q^{-1} \times Q^{-1} = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} P^2_{(0)} - P_{(-1)}P_{(1)} & P_{(-2)}P_{(1)} - P_{(-1)}P_{(0)} & P^2_{(-1)} - P_{(-2)}P_{(0)} \\ P^2_{(-1)} - P_{(-2)}P_{(0)} & P_{(-3)}P_{(0)} - P_{(-2)}P_{(-1)} & P^2_{(-2)} - P_{(-3)}P_{(-1)} \\ P_{(-2)}P_{(1)} - P_{(-1)}P_{(0)} & P^2_{(-1)} - P_{(-3)}P_{(1)} & P_{(-3)}P_{(0)} - P_{(-2)}P_{(-1)} \end{bmatrix} \end{aligned}$$

برای $k = 1$ و $k = 2$ رابطه بالا برقرار است. فرض کنیم حکم به ازای $k = m$ برقرار باشد یعنی

$$Q^{-m} = \begin{bmatrix} P^2_{(m-2)} - P_{(m-3)}P_{(m-1)} & P_{(m-4)}P_{(m-1)} - P_{(m-3)}P_{(m-2)} & P^2_{(m-3)} - P_{(m-4)}P_{(m-2)} \\ P^2_{(m-3)} - P_{(m-4)}P_{(m-2)} & P_{(m-5)}P_{(m-2)} - P_{(m-4)}P_{(m-3)} & P^2_{(m-4)} - P_{(m-5)}P_{(m-3)} \\ P_{(m-4)}P_{(m-1)} - P_{(m-3)}P_{(m-2)} & P^2_{(m-3)} - P_{(m-5)}P_{(m-1)} & P_{(m-5)}P_{(m-2)} - P_{(m-4)}P_{(m-3)} \end{bmatrix}$$

حال ثابت می‌کنیم حکم به ازای $k = m + 1$ نیز برقرار است.

$$Q^{-(m+1)} = Q^{-1} \times Q^{-m} = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\times \begin{bmatrix} P^2_{(m-2)} - P_{(m-3)}P_{(m-1)} & P_{(m-4)}P_{(m-1)} - P_{(m-3)}P_{(m-2)} & P^2_{(m-3)} - P_{(m-4)}P_{(m-2)} \\ P^2_{(m-3)} - P_{(m-4)}P_{(m-2)} & P_{(m-5)}P_{(m-2)} - P_{(m-4)}P_{(m-3)} & P^2_{(m-4)} - P_{(m-5)}P_{(m-3)} \\ P_{(m-4)}P_{(m-1)} - P_{(m-3)}P_{(m-2)} & P^2_{(m-3)} - P_{(m-5)}P_{(m-1)} & P_{(m-5)}P_{(m-2)} - P_{(m-4)}P_{(m-3)} \end{bmatrix}$$

$$= \begin{bmatrix} P^2_{(m-1)} - P_{(m-2)}P_{(m)} & P_{(m-3)}P_{(m)} - P_{(m-2)}P_{(m-1)} & P^2_{(m-2)} - P_{(m-3)}P_{(m-1)} \\ P^2_{(m-2)} - P_{(m-3)}P_{(m-1)} & P_{(m-4)}P_{(m-1)} - P_{(m-3)}P_{(m-2)} & P^2_{(m-3)} - P_{(m-4)}P_{(m-2)} \\ P_{(m-3)}P_{(m)} - P_{(m-2)}P_{(m-1)} & P^2_{(m-2)} - P_{(m-4)}P_{(m)} & P_{(m-4)}P_{(m-1)} - P_{(m-3)}P_{(m-2)} \end{bmatrix}$$

۳. کدگذاری و کدگشایی روی ماتریس دنباله‌های عددی پادوان

در این بخش، به بررسی روش کدگذاری و کدگشایی روی ماتریس Q^k می‌پردازیم. ماتریس مربعی 3×3 پیام P و ماتریس معکوس پذیر Q^k را در نظر می‌گیریم. در این صورت، عبارت $P \times Q^k = E$ الگوریتم کدگذاری و عبارت $E \times Q^{-k} = P$ الگوریتم کدگشایی نامیده می‌شود. ماتریس E را ماتریس کد می‌نامیم.

لم ۳-۱. برای هر عدد صحیح $k \geq 1$ ، داریم $\det(E) = \det(P)$.

برهان.

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

۳-۱. نمونه‌ای از کدگذاری و کدگشایی روی ماتریس دنباله‌های عددی 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، $k = 5$ قرار می‌دهیم. بنابراین خواهیم داشت:

$$Q^5 = \begin{bmatrix} P_{(0)} & P_{(2)} & P_{(1)} \\ P_{(1)} & P_{(3)} & P_{(2)} \\ P_{(2)} & P_{(4)} & P_{(3)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \end{bmatrix}$$

$$Q^{-5} = \begin{bmatrix} P_{(-10)} & P_{(-8)} & P_{(-9)} \\ P_{(-9)} & P_{(-7)} & P_{(-8)} \\ P_{(-8)} & P_{(-6)} & P_{(-7)} \end{bmatrix} = \begin{bmatrix} 2 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}$$

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

$$P \times Q^5 = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \end{bmatrix} = \begin{bmatrix} p_1 + p_2 + p_3 & p_1 + 2p_2 + 2p_3 & p_1 + p_2 + 2p_3 \\ p_4 + p_5 + p_6 & p_4 + 2p_5 + 2p_6 & p_4 + p_5 + 2p_6 \\ p_7 + p_8 + p_9 & p_7 + 2p_8 + 2p_9 & p_7 + p_8 + 2p_9 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix} = E.$$

که در آن،

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

با حل دستگاه بالا نتیجه می‌شود:

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

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 می‌شود. حال الگوریتم کدگشایی از ماتریس E به صورت زیر خواهد بود.

$$E \times Q^{-5} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix} \times \begin{bmatrix} 2 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 2e_1 - e_2 & e_2 - e_3 & -e_1 + e_3 \\ 2e_4 - e_5 & e_5 - e_6 & -e_4 + e_3 \\ 2e_7 - e_8 & e_8 - e_9 & -e_7 + e_9 \end{bmatrix}$$

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

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

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

$$Q^{-5} = \begin{bmatrix} 2 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} \text{ و } Q^5 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \end{bmatrix} \text{ کدگذاری و کدگشایی را به کمک دو ماتریس}$$

دهیم.

ماتریس کد به صورت زیر به دست می‌آید.

$$E = P \times Q^5 = \begin{bmatrix} 0 & 0 & 3 \\ 5 & 6 & 7 \\ 4 & 8 & 9 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 6 \\ 18 & 31 & 25 \\ 21 & 38 & 30 \end{bmatrix}.$$

کدگشایی به صورت زیر انجام می‌شود.

$$P = E \times Q^{-5} = \begin{bmatrix} 3 & 6 & 6 \\ 18 & 31 & 25 \\ 21 & 38 & 30 \end{bmatrix} \times \begin{bmatrix} 2 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 3 \\ 5 & 6 & 7 \\ 4 & 8 & 9 \end{bmatrix}.$$

۲-۳. روابط بین درایه های ماتریس کد E در این بخش، ارتباط بین درایه های ماتریس کد E بررسی می گردد. ماتریس کد E به صورت زیر نوشته می شود.

$$E = P \times Q^k = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{bmatrix} \times \begin{bmatrix} P_{(k-5)} & P_{(k-3)} & P_{(k-4)} \\ P_{(k-4)} & P_{(k-2)} & P_{(k-3)} \\ P_{(k-3)} & P_{(k-1)} & P_{(k-2)} \end{bmatrix} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix}.$$

k را طوری انتخاب می کنیم که برای هر $i = 1, 2, 3$ داشته باشیم $e_i > 0$.

$$P = E \times Q^{-k} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix} \times \begin{bmatrix} P_{(k-5)} & P_{(k-3)} & P_{(k-4)} \\ P_{(k-4)} & P_{(k-2)} & P_{(k-3)} \\ P_{(k-3)} & P_{(k-1)} & P_{(k-2)} \end{bmatrix}^{-1} = \begin{bmatrix} e_1 & e_2 & e_3 \\ e_4 & e_5 & e_6 \\ e_7 & e_8 & e_9 \end{bmatrix}$$

$$\times \begin{bmatrix} P^2_{(k-2)} - P_{(k-3)}P_{(k-1)} & P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)} & P^2_{(k-3)} - P_{(k-4)}P_{(k-2)} \\ P^2_{(k-3)} - P_{(k-4)}P_{(k-2)} & P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)} & P^2_{(k-4)} - P_{(k-5)}P_{(k-3)} \\ P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)} & P^2_{(k-3)} - P_{(k-5)}P_{(k-1)} & P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)} \end{bmatrix}$$

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

و هم چنین

$$\det(Q^k) = P_{(k-5)}(P^2_{(k-2)} - P_{(k-3)}P_{(k-1)}) + P_{(k-3)}(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + P_{(k-4)}(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) = 1 \quad (1 - 2 - 3)$$

چون $1 \leq i \leq 9, p_i \geq 0$. بنابراین

$$p_1 = e_1(P^2_{(k-2)} - P_{(k-3)}P_{(k-1)}) + e_2(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + e_3(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) \geq 0, \quad (2 - 2 - 3)$$

$$p_2 = e_1(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) + e_2(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}) + e_3(P^2_{(k-3)} - P_{(k-5)}P_{(k-1)}) \geq 0, \quad (3 - 2 - 3)$$

$$p_3 = e_1(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + e_2(P^2_{(k-4)} - P_{(k-5)}P_{(k-3)}) + e_3(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}) \geq 0, \quad (4 - 2 - 3)$$

$$p_4 = e_4(P^2_{(k-2)} - P_{(k-3)}P_{(k-1)}) + e_5(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + e_6(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) \geq 0, \quad (5 - 2 - 3)$$

$$p_5 = e_4(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) + e_5(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}) + e_6(P^2_{(k-3)} - P_{(k-5)}P_{(k-1)}) \geq 0, \quad (6 - 2 - 3)$$

$$p_6 = e_4(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + e_5(P^2_{(k-4)} - P_{(k-5)}P_{(k-3)}) + e_3(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}) \geq 0, \quad (7 - 2 - 3)$$

$$p_7 = e_7(P^2_{(k-2)} - P_{(k-3)}P_{(k-1)}) + e_8(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + e_9(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) \geq 0, \quad (8 - 2 - 3)$$

$$p_8 = e_7(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}) + e_8(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}) + e_9(P^2_{(k-3)} - P_{(k-5)}P_{(k-1)}) \geq 0, \quad (9 - 2 - 3)$$

$$p_9 = e_7(P^2_{(k-3)} - P_{(k-4)}P_{(k-2)}) + e_8(P^2_{(k-4)} - P_{(k-5)}P_{(k-3)}) + e_9(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}) \geq 0, \quad (10 - 2 - 3)$$

از رابطه (2 - 2 - 3) داریم:

$$e_1P^2_{(k-2)} + e_2P^2_{(k-3)} + e_3P_{(k-4)}P_{(k-1)} \geq e_1P_{(k-3)}P_{(k-1)} + e_2P_{(k-4)}P_{(k-2)} + e_3P_{(k-3)}P_{(k-2)}, \quad (11 - 2 - 3)$$

از رابطه (3 - 2 - 3) داریم:

$$e_1P_{(k-4)}P_{(k-1)} + e_2P_{(k-5)}P_{(k-2)} + e_3P^2_{(k-3)} \geq e_1P_{(k-3)}P_{(k-2)} + e_2P_{(k-4)}P_{(k-3)} + e_3P_{(k-5)}P_{(k-1)}, \quad (12 - 2 - 3)$$

از رابطه (4 - 2 - 3) داریم:

$$e_1P^2_{(k-3)} + e_2P^2_{(k-4)} + e_3P_{(k-5)}P_{(k-2)} \geq e_1P_{(k-4)}P_{(k-2)} + e_2P_{(k-5)}P_{(k-3)} + e_3P_{(k-4)}P_{(k-3)}, \quad (13 - 2 - 3)$$

با تقسیم طرفین نامساوی (11 - 2 - 3) بر $e_1P_{(k-3)}P_{(k-1)} > 0$ خواهیم داشت:

$$\begin{aligned} & \left(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)} \right) \frac{e_3}{e_1} \\ & \geq \left(P_{(k-4)}P_{(k-2)} - P^2_{(k-3)} \right) \frac{e_2}{e_1} + \left(P_{(k-3)}P_{(k-1)} - P^2_{(k-2)} \right), \end{aligned} \quad (14 - 2 - 3)$$

با تقسیم طرفین نامساوی (12 - 2 - 3) بر $e_1P_{(k-3)}P_{(k-2)} > 0$ خواهیم داشت:

$$\begin{aligned} & \left(P_{(k-5)}P_{(k-1)} - P^2_{(k-3)} \right) \frac{e_3}{e_1} \\ & \leq \left(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)} \right) \frac{e_2}{e_1} + \left(P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)} \right), \end{aligned} \quad (15 - 2 - 3)$$

با تقسیم طرفین نامساوی (13 - 4) بر $e_1P_{(k-4)}P_{(k-2)} > 0$ خواهیم داشت:

$$\begin{aligned} & \left(P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)} \right) \frac{e_3}{e_1} \\ & \geq \left(P_{(k-5)}P_{(k-3)} - P^2_{(k-4)} \right) \frac{e_2}{e_1} + \left(P_{(k-4)}P_{(k-2)} - P^2_{(k-3)} \right), \end{aligned} \quad (16 - 2 - 3)$$

فرض کنیم $b = P_{(k-5)}P_{(k-1)} - P^2_{(k-3)}$ ، $a = P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}$ و $c = P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}$ باشند بنابراین $3^3 = 27$ حالت به صورت $a <=> . b <=> . c <=>$ وجود دارد.

حالت اول: فرض کنیم $a > 0, b > 0, c > 0$ بنابراین در رابطه (14 - 2 - 3) داریم:

$$\frac{e_3}{e_1} \geq u, \quad u = \frac{e_2}{e_1} \left(\frac{P_{(k-4)}P_{(k-2)} - P^2_{(k-3)}}{P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}} \right) + \frac{P_{(k-3)}P_{(k-1)} - P^2_{(k-2)}}{P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}} \quad (17 - 2 - 3)$$

و از رابطه (15 - 2 - 3) داریم:

$$\frac{e_3}{e_1} \leq v, \quad v = \frac{e_2}{e_1} \left(\frac{P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}}{P_{(k-5)}P_{(k-1)} - P_{(k-3)}^2} \right) + \frac{P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}}{P_{(k-5)}P_{(k-1)} - P_{(k-3)}^2} \quad (18 - 2 - 3)$$

هم چنین از رابطه (16 - 2 - 3) داریم:

$$\frac{e_3}{e_1} \geq w, \quad w = \frac{e_2}{e_1} \left(\frac{P_{(k-5)}P_{(k-3)} - P_{(k-4)}^2}{P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}} \right) + \frac{P_{(k-4)}P_{(k-2)} - P_{(k-3)}^2}{P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}} \quad (19 - 2 - 3)$$

از روابط (17 - 2 - 3) و (18 - 2 - 3) و به کمک (1 - 2 - 3) نتیجه می شود:

$$\frac{e_1}{e_2} \geq \min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (20 - 2 - 3)$$

از روابط (18 - 2 - 3) و (19 - 2 - 3) و به کمک (1 - 2 - 3) نتیجه می شود:

$$\frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (21 - 2 - 3)$$

بنابراین از (20 - 2 - 3) و (21 - 2 - 3) داریم:

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \leq \frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (22 - 2 - 3)$$

به طور مشابه ، داریم:

$$\min \left\{ \frac{P_{(k-3)}}{P_{(k-4)}}, \frac{P_{(k-2)}}{P_{(k-3)}}, \frac{P_{(k-1)}}{P_{(k-2)}} \right\} \leq \frac{e_2}{e_3} \leq \max \left\{ \frac{P_{(k-3)}}{P_{(k-4)}}, \frac{P_{(k-2)}}{P_{(k-3)}}, \frac{P_{(k-1)}}{P_{(k-2)}} \right\} \quad (23 - 2 - 3)$$

و هم چنین ،

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-4)}}, \frac{P_{(k-4)}}{P_{(k-3)}}, \frac{P_{(k-3)}}{P_{(k-2)}} \right\} \leq \frac{e_1}{e_3} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-4)}}, \frac{P_{(k-4)}}{P_{(k-3)}}, \frac{P_{(k-3)}}{P_{(k-2)}} \right\} \quad (24 - 2 - 3)$$

حالت دوم: فرض کنیم $a = 0, b > 0, c > 0$ بنابراین در رابطه (14 - 2 - 3) داریم:

$$\frac{e_1}{e_2} \geq \min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (25 - 2 - 3)$$

از روابط (15 - 2 - 3) و (16 - 2 - 3) و به کمک (1 - 2 - 3) نتیجه می شود:

$$\frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (26 - 2 - 3)$$

و $a = 0$.

بنابراین از (25 - 2 - 3) و (26 - 2 - 3) داریم:

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \leq \frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (27 - 2 - 3)$$

حالت سوم: فرض کنیم $a < 0, b < 0, c < 0$ بنابراین در رابطه (14 - 2 - 3) داریم:

$$\frac{e_3}{e_1} \leq u, \quad u = \frac{e_2}{e_1} \left(\frac{P_{(k-4)}P_{(k-2)} - P_{(k-3)}^2}{P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}} \right) + \frac{P_{(k-3)}P_{(k-1)} - P_{(k-2)}^2}{P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}} \quad (28 - 2 - 3)$$

و از رابطه (15 - 2 - 3) داریم:

$$\frac{e_3}{e_1} \geq v, \quad v = \frac{e_2}{e_1} \left(\frac{P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}}{P_{(k-5)}P_{(k-1)} - P_{(k-3)}^2} \right) + \frac{P_{(k-4)}P_{(k-1)} - P_{(k-3)}P_{(k-2)}}{P_{(k-5)}P_{(k-1)} - P_{(k-3)}^2} \quad (29 - 2 - 3)$$

هم چنین از رابطه (16 - 2 - 3) داریم:

$$\frac{e_3}{e_1} \leq w, \quad w = \frac{e_2}{e_1} \left(\frac{P_{(k-5)}P_{(k-3)} - P_{(k-4)}^2}{P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}} \right) + \frac{P_{(k-4)}P_{(k-2)} - P_{(k-3)}^2}{P_{(k-5)}P_{(k-2)} - P_{(k-4)}P_{(k-3)}} \quad (30 - 2 - 3)$$

از روابط (28 - 2 - 3) و (29 - 2 - 3) و به کمک (1 - 2 - 3) نتیجه می شود:

$$\frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (31 - 2 - 3)$$

از روابط (29 - 2 - 3) و (30 - 2 - 3) و به کمک (1 - 2 - 3) نتیجه می شود:

$$\frac{e_1}{e_2} \geq \min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (32 - 2 - 3)$$

بنابراین از (31 - 2 - 3) و (32 - 2 - 3) داریم:

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \leq \frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \quad (33 - 2 - 3)$$

به طور مشابه ، داریم:

$$\min \left\{ \frac{P_{(k-3)}}{P_{(k-4)}}, \frac{P_{(k-2)}}{P_{(k-3)}}, \frac{P_{(k-1)}}{P_{(k-2)}} \right\} \leq \frac{e_2}{e_3} \leq \max \left\{ \frac{P_{(k-3)}}{P_{(k-4)}}, \frac{P_{(k-2)}}{P_{(k-3)}}, \frac{P_{(k-1)}}{P_{(k-2)}} \right\} \quad (34 - 2 - 3)$$

و هم چنین ،

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-4)}}, \frac{P_{(k-4)}}{P_{(k-3)}}, \frac{P_{(k-3)}}{P_{(k-2)}} \right\} \leq \frac{e_1}{e_3} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-4)}}, \frac{P_{(k-4)}}{P_{(k-3)}}, \frac{P_{(k-3)}}{P_{(k-2)}} \right\} \quad (35 - 2 - 3)$$

سایر حالت ها نیز به روش مشابه ثابت می گردد. بنابراین خواهیم داشت:

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\} \leq \frac{e_1}{e_2} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-3)}}, \frac{P_{(k-4)}}{P_{(k-2)}}, \frac{P_{(k-3)}}{P_{(k-1)}} \right\}$$

$$\min \left\{ \frac{P_{(k-3)}}{P_{(k-4)}}, \frac{P_{(k-2)}}{P_{(k-3)}}, \frac{P_{(k-1)}}{P_{(k-2)}} \right\} \leq \frac{e_2}{e_3} \leq \max \left\{ \frac{P_{(k-3)}}{P_{(k-4)}}, \frac{P_{(k-2)}}{P_{(k-3)}}, \frac{P_{(k-1)}}{P_{(k-2)}} \right\}$$

و هم چنین،

$$\min \left\{ \frac{P_{(k-5)}}{P_{(k-4)}}, \frac{P_{(k-4)}}{P_{(k-3)}}, \frac{P_{(k-3)}}{P_{(k-2)}} \right\} \leq \frac{e_1}{e_3} \leq \max \left\{ \frac{P_{(k-5)}}{P_{(k-4)}}, \frac{P_{(k-4)}}{P_{(k-3)}}, \frac{P_{(k-3)}}{P_{(k-2)}} \right\}$$

بنابراین برای مقادیر بزرگ k ، خواهیم داشت:

$$\frac{e_1}{e_2} \approx \frac{1}{\alpha^2}, \quad \frac{e_2}{e_3} \approx \alpha, \quad \frac{e_1}{e_3} \approx \frac{1}{\alpha} \quad (36 - 2 - 3)$$

به طوری که $\alpha = 1/32511$.

به همین ترتیب خواهیم داشت:

$$\frac{e_4}{e_5} \approx \frac{1}{\alpha^2}, \quad \frac{e_5}{e_6} \approx \alpha, \quad \frac{e_4}{e_6} \approx \frac{1}{\alpha} \quad (37 - 2 - 3)$$

و

$$\frac{e_7}{e_8} \approx \frac{1}{\alpha^2}, \quad \frac{e_8}{e_9} \approx \alpha, \quad \frac{e_7}{e_9} \approx \frac{1}{\alpha} \quad (38 - 2 - 3)$$

۳-۳. توانایی تصحیح خطا

اینک به بررسی مقدار خطا و تصحیح آن در این الگوریتم کدگذاری و کدگشایی روی دنباله عددی پادوان می پردازیم. فرض اول این است که فقط یک خطا در ماتریس 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 هر یک از حالت های بالا بررسی می کنیم.

$$x_1(e_5e_9 - e_6e_8) + e_2(e_6e_7 - e_4e_9) + e_3(e_4e_8 - e_5e_7) = \det(P), \quad (1 - 3 - 3)$$

$$e_1(e_5e_9 - e_6e_8) + x_2(e_6e_7 - e_4e_9) + e_3(e_4e_8 - e_5e_7) = \det(P), \quad (2 - 3 - 3)$$

$$e_1(e_5e_9 - e_6e_8) + e_2(e_6e_7 - e_4e_9) + x_3(e_4e_8 - e_5e_7) = \det(P), \quad (3 - 3 - 3)$$

$$x_4(e_3e_8 - e_2e_9) + e_5(e_1e_9 - e_3e_7) + e_6(e_2e_7 - e_1e_8) = \det(P), \quad (4 - 3 - 3)$$

$$e_4(e_3e_8 - e_2e_9) + x_5(e_1e_9 - e_3e_7) + e_6(e_2e_7 - e_1e_8) = \det(P), \quad (5 - 3 - 3)$$

$$e_4(e_3e_8 - e_2e_9) + e_5(e_1e_9 - e_3e_7) + x_6(e_2e_7 - e_1e_8) = \det(P), \quad (6 - 3 - 3)$$

$$x_7(e_2e_6 - e_3e_5) + e_8(e_3e_4 - e_1e_6) + e_9(e_1e_5 - e_2e_4) = \det(P), \quad (7 - 3 - 3)$$

$$e_7(e_2e_6 - e_3e_5) + x_8(e_3e_4 - e_1e_6) + e_9(e_1e_5 - e_2e_4) = \det(P), \quad (8 - 3 - 3)$$

$$e_7(e_2e_6 - e_3e_5) + e_8(e_3e_4 - e_1e_6) + x_9(e_1e_5 - e_2e_4) = \det(P), \quad (9 - 3 - 3)$$

از نه رابطه بالا تساوی های زیر نتیجه می شود:

$$x_1 = \frac{\det(P) - e_2(e_6e_7 - e_4e_9) - e_3(e_4e_8 - e_5e_7)}{e_5e_9 - e_6e_8}, \quad (10 - 3 - 3)$$

$$x_2 = \frac{\det(P) - e_1(e_5e_9 - e_6e_8) - e_3(e_4e_8 - e_5e_7)}{e_6e_7 - e_4e_9}, \quad (11 - 3 - 3)$$

$$x_3 = \frac{\det(P) - e_1(e_5e_9 - e_6e_8) - e_2(e_6e_7 - e_4e_9)}{e_4e_8 - e_5e_7}, \quad (12 - 3 - 3)$$

$$x_4 = \frac{\det(P) - e_5(e_1e_9 - e_3e_7) - e_6(e_2e_7 - e_1e_8)}{e_3e_8 - e_2e_9}, \quad (13 - 3 - 3)$$

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

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

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

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

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

روابط (10 - 3 - 3) تا (18 - 3 - 3) قابلیت تصحیح خطاهای یگانه ای را دارد که روابط (36 - 2 - 3) تا (38 - 2 - 3) را محقق نمی‌کنند. 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 (1 - 3) خواهیم داشت:

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

طبق رابطه (36 - 2 - 3) رابطه بین x و y به صورت زیر خواهد بود.

$$x \approx \frac{y}{\alpha^2} \quad (20 - 3 - 3)$$

رابطه (19 - 3 - 3) جواب‌های زیادی دارد اما پاسخی قابل قبول خواهد بود که در رابطه (20 - 3 - 3) صدق کند.

به وضوح، به $\binom{9}{2} = 36$ حالت ممکن است تنها دو خطا در ماتریس کد رخ دهد و به روش مشابه می‌توان تمام

خطاهای دوگانه 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 $0/9980 = \frac{510}{511}$ یعنی $99/8\%$ می‌باشد.

۴. نتیجه گیری

این مقاله به استفاده از ماتریس مولد دنباله عددی 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 توانایی تصحیح خطا در این الگوریتم برابر $99/8\%$ است.

۵. مراجع

- [1] A. Stokhov , V. Massingue and A. Sluchenkova, "Introduction into Fibonacci Coding and Cryptography," Kharkov:Osnova. 1999.
- [2] N. Gogin,.;A.A. Millari ,;"The Fibonacci- Padovan Sequences and MacWilliams transform matrices ";Programming and Computer Software, published in Programmirovanie. 2007.
- [3] O. Deveci, Y., Akuzum, E., Karadomani., "The Pell-Padovan p-Sequences and Its Applications,"Util. Math. 2015
- [4] O. Deveci , E., Karadomani , "On the Padovan p-numbers," Hacettepe Journal of Mathematics and Statistics. 2017.