کاربردهایی از ماتریس دنباله ۳- ناسی درکدگذاری

دکتر منصور هاشمی [۱]،الهه مهربان [۲,*]

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

۲- دانشجوی دکتری ریاضی محض ، دانشگاه گیلان – دانشکده علوم ریاضی- گروه ریاضی محض

چکیده

دنباله k- ناسی $\left\{F_n^k\right\}_0^\infty$، $n\in\square$ و $k\geq 2$ به صورت زیر تعریف می‌شود:

$$F_0^k=0,\ldots,F_{k-2}^k=0,F_{k-1}^k=1,\ F_n^k=F_{n-1}^k+F_{n-2}^k+\cdots+F_{n-k}^k,n\geq k.$$

دراین مقاله، ابتدا به معرفی ماتریس دنباله‌های ۳- ناسی پرداخته و سپس دترمینان این ماتریس را محاسبه می‌کنیم و در انتها با استفاده از این ماتریس دو روش کدگذاری ارائه می‌دهیم

کلمات کلیدی: دنباله k- ناسی، دترمینان ماتریس، کدگذاری.

۱. مقدمه

اخیراً افراد زیادی به بررسی کدگذاری وکدگشایی روی دنباله‌های مختلف و ماتریس آن‌ها پرداخته‌اند بعنوان مثال [1, 2, 3] ملاحظه فرمایید. Stakhov در [4] با استفاده از نمایش ماتریسی دنباله‌های فیبوناتچی $Q_p{}^n$ که $p=1$ ، یک روش کد گذاری ارائه داد Q_1^n یک ماتریس 2×2 ماتریس کدگذاری و Q_1^{-n} یک ماتریس با همان مرتبه ماتریس کد گشایی معرفی گردید. سپس یک انتقال به صورت $M\times Q_1^n=E$ به عنوان الگوریتم کدگذاری فیبوناتچی و انتقال $E\times Q_1^{-n}=M$، الگوریتم کدگشایی فیبوناتچی نامیده شد. هم چنین ماتریس E، ماتریس کدگذاری شده و M، ماتریس پیام می‌باشد. سپس در [5]، به ازای $p=2$ ، روش کدگذاری فوق ارایه گردید.

دراینجا، دربخش دوم ماتریس دنباله ۳- ناسی را تعریف کرده و دترمینان آن را بدست می‌آوریم. در بخش سوم به روش بلوک بندی روی آن می‌پردازیم. بخش چهارم اختصاص به ارائه یک روش کد گذاری و کد گشایی روی ماتریس دنباله ۳- ناسی دارد.

۲- ماتریس دنباله ۳- ناسی و برخی خواص آن

دراین بخش، به معرفی ماتریس دنباله ۳- ناسی پرداخته و سپس، دترمینان آن را به دست می‌آوریم.

ابتدا، دنباله ۳- ناسی را با توجه به دنباله k- ناسی تعریف می‌کنیم. دنباله ۳- ناسی، $\left\{F_n^3\right\}_{-\infty}^{+\infty}$ ، بصورت زیر تعریف می شود:

* **Corresponding author: الهه مهربان**
Email: e.mehraban.math@gmail.com

$$F_0^3=0, F_1^3=0, F_2^3=1, \begin{cases} F_n^3=F_{n-1}^3+F_{n-2}^3+F_{n-3}^3, & n\geq 0, \\ F_{n-1}^3=F_{n+2}^3-(F_n^3+F_{n+1}^3), & n<0. \end{cases}$$

برای مطالعه بیشتر به [6] مراجعه نمایید.

توجه. در سرتاسر این مقاله فرض می‌کنیم $F_n=F_n^3$.

تعریف ۲-۱. ماتریس دنباله ۳- ناسی که آن را Q_n نشان می‌دهیم، به صورت زیر تعریف می‌شود:

$$Q_n=\begin{bmatrix} F_{n+2} & F_{n+1} & F_n \\ F_{n+1} & F_n & F_{n-1} \\ F_n & F_{n-1} & F_{n-2} \end{bmatrix},$$

که در آن، $n=0,\pm 1,\pm 2,\ldots$ و F_n اعضای دنباله ۳- ناسی هستند. بعنوان مثال برای $n=3$، Q_3 به صورت زیر است:

$$Q_3=\begin{bmatrix} F_5 & F_4 & F_3 \\ F_4 & F_3 & F_2 \\ F_3 & F_2 & F_1 \end{bmatrix}=\begin{bmatrix} 4 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

قضیه ۲-۲. دترمینان ماتریس دنباله ۳- ناسی Q_n برابر با ۱- است.

برهان. قرارمی دهیم $n=3m+i$ که $n,m,i\in\mathbb{Z}$ و $0\leq i\leq 2$ داریم:

$$Q_{3m+i}=\begin{bmatrix} F_{3m+i+2} & F_{3m+i+1} & F_{3m+i} \\ F_{3m+i+1} & F_{3m+i} & F_{3m+i-1} \\ F_{3m+i} & F_{3m+i-1} & F_{3m+i-2} \end{bmatrix}.$$

در $m-1$ ، مرحله نشان می‌دهیم که دترمینان برابر ۱- است. درهرمرحله ، شامل قسمت های زیراست.

(۱) ابتدا ستون دوم وسوم را باهم جمع می‌کنیم سپس آن را از ستون اول کم کرده ودرآن جایگذاری می‌کنیم. بنابراین داریم:

$$\begin{bmatrix} F_{3m+i-1} & F_{3m+i+1} & F_{3m+i} \\ F_{3m+i-2} & F_{3m+i} & F_{3m+i-1} \\ F_{3m+i-3} & F_{3m+i-1} & F_{3m+i-2} \end{bmatrix}.$$

(۲) ستون اول وسوم راجمع می‌کنیم. واز ستون دوم کم می‌کنیم ودر آن جایگذاری می‌کنیم.

$$\begin{bmatrix} F_{3m+i-1} & F_{3m+i-2} & F_{3m+i} \\ F_{3m+i-2} & F_{3m+i-3} & F_{3m+i-1} \\ F_{3m+i-3} & F_{3m+i-4} & F_{3m+i-2} \end{bmatrix}.$$

(۳) ستون اول ودوم را باهم جمع می‌کنیم و از ستون سوم کم کرده ودر آن جایگذاری می‌کنیم.

$$\begin{bmatrix} F_{3m+i-1} & F_{3m+i-2} & F_{3m+i-3} \\ F_{3m+i-2} & F_{3m+i-3} & F_{3m+i-4} \\ F_{3m+i-3} & F_{3m+i-4} & F_{3m+i-5} \end{bmatrix}.$$

درهر مرحله درایه‌های ماتریس $m-1$ کاهش پیدا می‌کنند. در نتیجه داریم:

$$Q_{3(m-1)+i} = \begin{bmatrix} F_{3(m-1)+i+2} & F_{3(m-1)+i+1} & F_{3(m-1)+i} \\ F_{3(m-1)+i+1} & F_{3(m-1)+i} & F_{3(m-1)+i-1} \\ F_{3(m-1)+i} & F_{3(m-1)+i-1} & F_{3(m-1)+i-2} \end{bmatrix}.$$

با انجام مراحل فوق به تعداد $m-1$ باررروی ماتریس دنباله ۳- ناسی خواهیم داشت:

$$Q_i = \begin{bmatrix} F_{i+2} & F_{i+1} & F_i \\ F_{i+1} & F_i & F_{i-1} \\ F_i & F_{i-1} & F_{i-2} \end{bmatrix}.$$

بنابراین داریم:

$$\det Q_n = \det Q_i$$

کافیست دترمینان Q_i را بدست آوریم. با توجه به اینکه $0 \le i \le 2$، سه حالت زیر بدست می‌آید:

(۱) اگر $i=0$ باشد آنگاه:

$$Q_0 = \begin{bmatrix} F_2 & F_1 & F_0 \\ F_1 & F_0 & F_{-1} \\ F_0 & F_{-1} & F_{-2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{bmatrix}.$$

داریم: $\det Q_i = \det Q_0 = -1$.

(۲) اگر $i=1$ باشد آنگاه:

$$Q_1 = \begin{bmatrix} F_3 & F_2 & F_1 \\ F_2 & F_1 & F_0 \\ F_1 & F_0 & F_{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

داریم: $\det Q_i = \det Q_1 = -1$.

(۳) $i=2$، مشابه حالت‌های قبلی است. بنابراین داریم: $\det Q_n = -1$.

مثال ۲-۳. دترمینان Q_{10} برابر با ۱- است. چون $n = 3\times 3+1$، داریم:

$$Q_{10} = \begin{bmatrix} F_{12} & F_{11} & F_{10} \\ F_{11} & F_{10} & F_9 \\ F_{10} & F_9 & F_8 \end{bmatrix} = \begin{bmatrix} 274 & 149 & 81 \\ 149 & 81 & 44 \\ 81 & 44 & 24 \end{bmatrix}.$$

مرحله اول:

$$\begin{bmatrix} F_9 & F_8 & F_7 \\ F_8 & F_7 & F_6 \\ F_7 & F_6 & F_5 \end{bmatrix} = \begin{bmatrix} 44 & 24 & 13 \\ 24 & 13 & 7 \\ 13 & 7 & 4 \end{bmatrix}.$$

مرحله دوم:

$$\begin{bmatrix} F_6 & F_5 & F_4 \\ F_5 & F_4 & F_3 \\ F_4 & F_3 & F_2 \end{bmatrix} = \begin{bmatrix} 7 & 4 & 2 \\ 4 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix}.$$

مرحله سوم:

$$\begin{bmatrix} F_3 & F_2 & F_1 \\ F_2 & F_1 & F_0 \\ F_1 & F_0 & F_{-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

درنتیجه، داریم: $\det Q_{10} = -1$.

۳- ارائه روش بلوک بندی روی ماتریس دنباله ۳- ناسی

دراین جا، به روش بلوک بندی روی ماتریس دنباله ۳- ناسی می‌پردازیم. ماتریس پیام P ، ماتریس مربعی به سایز $3m$ است. در صورتی که تعداد درایه های ماتریس کم تر باشد تمام درایه های باقیمانده را با صفر کامل می‌کنیم. بلوک بندی ماتریس P ، به صورت ماتریس‌هایی به صورت $B_i \left(1 \le i \le m^2\right)$ ، به سایز 3×3 از چپ به راست است. حال به بیان بعضی نمادها می‌پردازیم که دراین روش به کاربرده می‌شود. ماتریس B_i و E_i را بصورت زیر نمایش می‌دهیم:

$$B_i = \begin{bmatrix} b_1^i & b_2^i & b_3^i \\ b_4^i & b_5^i & b_6^i \\ b_7^i & b_8^i & b_9^i \end{bmatrix} \quad , \quad E_i = \begin{bmatrix} e_1^i & e_2^i & e_3^i \\ e_4^i & e_5^i & e_6^i \\ e_7^i & e_8^i & e_9^i \end{bmatrix}.$$

تعداد بلوک‌های ماتریس B_i را با b نمایش می‌دهیم. n را از رابطه زیر بدست می‌آوریم:

$$n = \begin{cases} 3 & b \le 4, \\ \left[\frac{b}{3}\right] & b > 4. \end{cases}$$

از ماتریس دنباله ۳- ناسی که آن را با Q_n نمایش می‌دهیم که به صورت زیر تعریف می‌شود:

$$Q_n = \begin{bmatrix} F_{n+2} & F_{n+1} & F_n \\ F_{n+1} & F_n & F_{n-1} \\ F_n & F_{n-1} & F_{n-2} \end{bmatrix}$$

در این روش مورد استفاده قرار می‌گیرد. با توجه به n، جدول ۲، را به هم نهشتی ۳۴ مطابق زیر بدست می‌آوریم:

جدول ۲: کدگذاری روش بلوک بندی

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

۳-۱. الگوریتم کدگذاری در روش بلوک بندی ماتریس ۳- ناسی

مراحل الگوریتم کدگذاری به روش زیر است:

۱- تقسیم بندی ماتریس P، به بلوک‌های B_i که $\left(1 \le i \le m^2\right)$ است.

۲- محاسبه کردن n.

۳- تعیین $b_j^i \left(1 \le i \le 9\right)$.

۴- محاسبه $\det(B_i) \to d_i$.

۵- ساختن $K = \left[d_i, \quad b_j^i \right]_{j \in \{1,2,4,5,6,7,8,9\}}$.

۶- پایان الگوریتم.

۳-۲. کدگشایی الگوریتم

۱- Q_n را محاسبه کرده و سپس در رابطه زیر قرار می‌دهیم:

$$Q_n = \begin{bmatrix} F_{n+2} & F_{n+1} & F_n \\ F_{n+1} & F_n & F_{n-1} \\ F_n & F_{n-1} & F_{n-2} \end{bmatrix} \to \begin{bmatrix} h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 \\ h_7 & h_8 & h_9 \end{bmatrix}.$$

۲- به ازای $1 \le i \le 6$، محاسبه کردن

$(i)\ b_4^i h_1 + b_5^i h_4 + b_6^i h_7 \to e_1^i,$
$(ii)\ b_4^i h_2 + b_5^i h_5 + b_6^i h_8 \to e_2^i,$
$(iii)\ b_4^i h_3 + b_5^i h_6 + b_6^i h_9 \to e_3^i,$
$(iv)\ b_7^i h_1 + b_8^i h_4 + b_9^i h_7 \to e_4^i,$
$(v)\ b_7^i h_2 + b_8^i h_5 + b_9^i h_8 \to e_5^i,$
$(vi)\ b_7^i h_3 + b_8^i h_6 + b_9^i h_9 \to e_6^i.$

۳- به ازای $1 \le i \le 9$، حل کردن معادله

$$-d_i = \left(b_1^i h_1 + b_2^i h_4 + x_i h_7\right)\left(e_2^i e_6^i - e_3^i e_5^i\right) - \left(b_1^i h_2 + b_2^i h_5 + x_i h_8\right)\left(e_1^i e_6^i - e_3^i e_4^i\right) + \left(b_1^i h_3 + b_2^i h_6 + x_i h_9\right)\left(e_1^i e_5^i - e_2^i e_4^i\right).$$

۴- جایگذاری کردن $x_i = b_3^i$.

۵- ساختن B_i.

۶- درست کردن P.

۷- پایان الگوریتم.

با مثال زیر روش بلوک بندی را روی ماتریس دنباله ۳- ناسی توضیح می‌دهیم.
پیام "ریاضیات شیرین است و مادر تمام علوم به شمار می‌آید"درنظر بگیرید:

$$P=\begin{bmatrix} ش & 0 & ت & الف & ی & ض & الف & ی & ر \\ 0 & ت & س & الف & 0 & ن & ی & ر & ی \\ الف & م & ت & 0 & ر & د & الف & م & و \\ ه & ب & 0 & م & و & ل & ع & 0 & م \\ الف & ی & م & 0 & ر & الف & م & ش & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & د & ی \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

داریم:

$$B_1 = \begin{bmatrix} الف & ی & ر \\ ی & ر & ی \\ الف & م & و \end{bmatrix}, \quad B_2 = \begin{bmatrix} الف & ی & ض \\ الف & 0 & ن \\ 0 & ر & د \end{bmatrix}, \quad B_3 = \begin{bmatrix} ش & ه & ت \\ 0 & ت & س \\ الف & م & ت \end{bmatrix},$$

$$B_4 = \begin{bmatrix} ع & 0 & م \\ م & ش & 0 \\ 0 & د & ی \end{bmatrix}, \quad B_5 = \begin{bmatrix} م & و & ل \\ 0 & ر & الف \\ 0 & 0 & 0 \end{bmatrix}, \quad B_6 = \begin{bmatrix} ه & ب & 0 \\ الف & ی & م \\ 0 & 0 & 0 \end{bmatrix},$$

$$B_7=\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix},\qquad B_8=\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix},\qquad B_9=\begin{bmatrix}0&0&0\\0&0&0\\0&0&0\end{bmatrix}.$$

باتوجه به اینکه $n=\left[\frac{9}{3}\right]=3$ ، داریم:

$$b_1^1=15,\ b_2^1=1,\ b_3^1=4,\ b_4^1=1,\ b_5^1=15,\ b_6^1=1,\ b_7^1=33,\ b_8^1=31,\ b_9^1=4,$$
$$b_1^2=21,\ b_2^2=1,\ b_3^2=4,\ b_4^2=32,\ b_5^2=2,\ b_6^2=4,\ b_7^2=13,\ b_8^2=15,\ b_9^2=2,$$
$$b_1^3=7,\ b_2^3=2,\ b_3^3=19,\ b_4^3=18,\ b_5^3=7,\ b_6^3=2,\ b_7^3=7,\ b_8^3=31,\ b_9^3=4,$$
$$b_1^4=31,\ b_2^4=2,\ b_3^4=24,\ b_4^4=2,\ b_5^4=19,\ b_6^4=31,\ b_7^4=1,\ b_8^4=13,\ b_9^4=2,$$
$$b_1^5=30,\ b_2^5=33,\ b_3^5=31,\ b_4^5=4,\ b_5^5=15,\ b_6^5=2,\ b_7^5=2,\ b_8^5=2,\ b_9^5=2,$$
$$b_1^6=2,\ b_2^6=5,\ b_3^6=0,\ b_4^6=31,\ b_5^6=1,\ b_6^6=4,\ b_7^6=2,\ b_8^6=2,\ b_9^6=2,$$
$$b_1^7=2,\ b_2^7=2,\ b_3^7=2,\ b_4^7=2,\ b_5^7=2,\ b_6^7=2,\ b_7^7=2,\ b_8^7=2,\ b_9^7=2,$$
$$b_1^8=2,\ b_2^8=2,\ b_3^8=2,\ b_4^8=2,\ b_5^8=2,\ b_6^8=2,\ b_7^8=2,\ b_8^8=2,\ b_9^8=2,$$
$$b_1^9=2,\ b_2^9=2,\ b_3^9=2,\ b_4^9=2,\ b_5^9=2,\ b_6^9=2,b_7^9=2,\ b_8^9=2,\ b_9^9=2.$$

باتوجه به $\det(B_i)\to d_i$ ، $1\le i\le 9$ ، داریم:

$$d_1=-1450\cong 12 \pmod{34},d_2=628\cong 16 \pmod{34},d_3=8883\cong 9 \pmod{34},$$
$$d_4=11537\cong 11 \pmod{34},d_5=-166\cong 4 \pmod{34},d_6=-282\cong 24 \pmod{34},$$
$$d_7=0 \pmod{34},\qquad d_8=0 \pmod{34},\qquad d_9=0 \pmod{34}.$$

بنابراین:

$$K=\begin{bmatrix}12&15&1&1&15&1&33&31&4\\16&21&1&32&2&4&13&15&2\\9&7&2&18&7&2&7&31&4\\11&31&2&2&19&31&1&13&2\\4&30&33&4&15&2&2&2&2\\24&2&5&31&1&4&2&2&2\\0&2&2&2&2&2&2&2&2\\0&2&2&2&2&2&2&2&2\\0&2&2&2&2&2&2&2&2\end{bmatrix}.$$

وپیام کدشده به صورت زیر است:

"خییرین مازفین آدرجتست تماحم عشمید آلوار"

اینک به الگوریتم کدگشایی می‌پردازیم:

ابتدا با توجه به اینکه $n=3$ ، داریم:

$$Q_3=\begin{bmatrix}F_5 & F_4 & F_3\\ F_4 & F_3 & F_2\\ F_3 & F_2 & F_1\end{bmatrix}=\begin{bmatrix}4 & 2 & 1\\ 2 & 1 & 1\\ 1 & 1 & 0\end{bmatrix}.$$

درنتیجه:

$$Q_n=\begin{bmatrix}F_{n+2} & F_{n+1} & F_n\\ F_{n+1} & F_n & F_{n-1}\\ F_n & F_{n-1} & F_{n-2}\end{bmatrix}=\begin{bmatrix}4 & 2 & 1\\ 2 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}\to\begin{bmatrix}h_1 & h_2 & h_3\\ h_4 & h_5 & h_6\\ h_7 & h_8 & h_9\end{bmatrix}.$$

همچنین

$$\begin{aligned}&e_1^1=35,e_2^1=18,e_3^1=16,e_4^1=138,e_5^1=71,e_6^1=34,\\ &e_1^2=136,e_2^2=70,e_3^2=34,e_4^2=84,e_5^2=43,e_6^2=28,\\ &e_1^3=88,e_2^3=45,e_3^3=25,e_4^3=94,e_5^3=49,e_6^3=38,\\ &e_1^4=75,e_2^4=54,e_3^4=21,e_4^4=32,e_5^4=17,e_6^4=14,\\ &e_1^5=48,e_2^5=25,e_3^5=19,e_4^5=14,e_5^5=7,e_6^5=4,\\ &e_1^6=130,e_2^6=67,e_3^6=32,e_4^6=14,e_5^6=8,e_6^6=4.\end{aligned}$$

با حل معادله

$$-d_i=\left(b_1^ih_1+b_2^ih_4+x_ih_7\right)\left(e_2^ie_6^i-e_3^ie_5^i\right)-\left(b_1^ih_2+b_2^ih_5+x_ih_8\right)\left(e_1^ie_6^i-e_3^ie_4^i\right)+\left(b_1^ih_3+b_2^ih_6+x_ih_9\right)\left(e_1^ie_5^i-e_2^ie_4^i\right).$$

به دست می آید:

$$x_1=4,x_2=4,x_3=19,x_4=24,x_5=31,x_6=0,x_7=2,x_8=2,x_9=2.$$

جایگذاری کردن $x_i=b_3^i$ ، داریم:

$$b_3^1=4,b_3^2=4,b_3^3=19,b_3^4=24,b_3^5=31,b_3^6=0,b_3^7=2,b_3^8=2,b_3^9=2.$$

در نتیجه:

$$B_1=\begin{bmatrix}15 & 1 & 4\\ 1 & 15 & 1\\ 33 & 31 & 4\end{bmatrix},\quad B_2=\begin{bmatrix}21 & 1 & 4\\ 32 & 2 & 4\\ 13 & 15 & 2\end{bmatrix},\quad B_3=\begin{bmatrix}7 & 2 & 19\\ 18 & 7 & 2\\ 7 & 31 & 4\end{bmatrix},$$

$$B_4=\begin{bmatrix}31 & 2 & 24\\ 2 & 19 & 31\\ 1 & 13 & 2\end{bmatrix},\quad B_5=\begin{bmatrix}30 & 33 & 31\\ 4 & 15 & 2\\ 2 & 2 & 2\end{bmatrix},\quad B_6=\begin{bmatrix}2 & 5 & 0\\ 31 & 1 & 4\\ 2 & 2 & 2\end{bmatrix},$$

$$B_7=\begin{bmatrix}2 & 2 & 2\\ 2 & 2 & 2\\ 2 & 2 & 2\end{bmatrix},\quad B_8=\begin{bmatrix}2 & 2 & 2\\ 2 & 2 & 2\\ 2 & 2 & 2\end{bmatrix},\quad B_9=\begin{bmatrix}2 & 2 & 2\\ 2 & 2 & 2\\ 2 & 2 & 2\end{bmatrix}.$$

وماتریس پیام P به صورت زیراست:

$$\begin{bmatrix} 15 & 1 & 4 & 21 & 1 & 4 & 7 & 2 & 19 \\ 1 & 15 & 1 & 32 & 2 & 4 & 18 & 7 & 2 \\ 33 & 31 & 4 & 13 & 15 & 2 & 7 & 31 & 4 \\ 31 & 2 & 24 & 30 & 33 & 31 & 2 & 5 & 0 \\ 2 & 19 & 31 & 4 & 15 & 2 & 31 & 1 & 4 \\ 1 & 13 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix} := \begin{bmatrix} ش & 0 & ت & ه & ب & م & ا & ی & م \\ 0 & ت & س & ا & 0 & ا & ی & ر & ی \\ ا & م & ت & 0 & ر & د & ا & م & و \\ ه & ب & 0 & م & و & ل & ع & 0 & م \\ ا & ی & م & 0 & ر & ا & م & ش & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & د & ی \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

۴- کدگذاری وکدگشایی روی ماتریس دنباله ۳- ناسی

دراینجا، یک روش کدگذاری روی ماتریس دنباله ۳- ناسی ارائه می‌دهیم. وتوانایی تصحیح خطا دراین الگوریتم را به دست می‌آوریم.

ماتریس پیام M، یک ماتریس 3×3، با درایه‌های اعدادصحیح مثبت است. یعنی

$$M=\begin{bmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{bmatrix},\quad m_i \in \mathbb{Z}^+, 1\le i\le 9.$$

الگوریتم کدگذاری به صورت $M\times Q_n = E$، که Q_n ماتریس دنباله ۳- ناسی و E پیام کدشده است. وانتقال $E\times Q_n^{-1}=M$ الگوریتم کدگشایی می‌باشد.

اینک، با مثالی ساده روش فوق را توضیح می‌دهیم. فرض کنیم $n=3$ وماتریس پیام M، به صورت زیر باشد.

$$M=\begin{bmatrix} 7 & 2 & 4 \\ 5 & 6 & 1 \\ 3 & 2 & 1 \end{bmatrix}.$$

اگر $n=3$، آنگاه:

$$Q_3=\begin{bmatrix} F_5 & F_4 & F_3 \\ F_4 & F_3 & F_2 \\ F_3 & F_2 & F_1 \end{bmatrix}=\begin{bmatrix} 4 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

باتوجه به الگوریتم $M\times Q_n = E$، داریم:

$$\begin{bmatrix} 7 & 2 & 4 \\ 5 & 6 & 1 \\ 3 & 2 & 1 \end{bmatrix}\times\begin{bmatrix} 4 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}=\begin{bmatrix} 36 & 20 & 9 \\ 43 & 17 & 11 \\ 17 & 9 & 5 \end{bmatrix}.$$

بنابراین ماتریس کدشده $E=\begin{bmatrix} 36 & 20 & 9 \\ 43 & 17 & 11 \\ 17 & 9 & 5 \end{bmatrix}$ به کانال فرستاده می‌شود. کدگشایی الگوریتم به صورت زیر بدست می‌آید:

$$E\times Q_n^{-1}=\begin{bmatrix}36&20&9\\43&17&11\\17&9&5\end{bmatrix}\times\begin{bmatrix}4&2&1\\2&1&1\\1&1&0\end{bmatrix}^{-1}=\begin{bmatrix}7&2&4\\5&6&1\\3&2&1\end{bmatrix}.$$

حال به بررسی توانایی تصحیح خطا در روش فوق می‌پردازیم.

باتوجه با اینکه در روش فوق داریم:

$$M=\begin{bmatrix}m_1&m_2&m_3\\m_4&m_5&m_6\\m_7&m_8&m_9\end{bmatrix},\quad Q_n=\begin{bmatrix}F_{n+2}&F_{n+1}&F_n\\F_{n+1}&F_n&F_{n-1}\\F_n&F_{n-1}&F_{n-2}\end{bmatrix},$$

$$E=M\times Q_n=\begin{bmatrix}m_1&m_2&m_3\\m_4&m_5&m_6\\m_7&m_8&m_9\end{bmatrix}\begin{bmatrix}F_{n+2}&F_{n+1}&F_n\\F_{n+1}&F_n&F_{n-1}\\F_n&F_{n-1}&F_{n-2}\end{bmatrix}=\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix}.$$

ازروابط $\det E=\det(M\times Q_n)=\det M\times\det Q_n$ و $\det Q_n=-1$ بدست می آوریم $\det E=-\det M$. اگر $\det E=-\det M$ ، آنگاه خطایی در پیام کدشده وجود ندارد. درغیراینصورت ممکن است یکی از خطاهای تک، دوگانه،...،نه گانه اتفاق بیفتد.

ابتدا، حالت‌های ممکن برای خطای مفرد را در نظر می‌گیریم. یکی از نه حالت زیر اتفاق می افتد.

$$(1)\begin{bmatrix}x&e_2&e_3\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},\quad(2)\begin{bmatrix}e_1&y&e_3\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},\quad(3)\begin{bmatrix}e_1&e_2&z\\e_4&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},$$

$$(4)\begin{bmatrix}e_1&e_2&e_3\\d&e_5&e_6\\e_7&e_8&e_9\end{bmatrix},\quad(5)\begin{bmatrix}e_1&e_2&e_3\\e_4&f&e_6\\e_7&e_8&e_9\end{bmatrix},\quad(6)\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&g\\e_7&e_8&e_9\end{bmatrix},$$

$$(7)\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\h&e_8&e_9\end{bmatrix},\quad(8)\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\e_7&r&e_9\end{bmatrix},\quad(9)\begin{bmatrix}e_1&e_2&e_3\\e_4&e_5&e_6\\e_7&e_8&s\end{bmatrix}.$$

که x,y,z,d,f,g,h,r,s عناصر معیوب هستند. با توجه به (۹)- (۱) خطای مفرد برای e_1 ، ...، e_9 بصورت زیراست:

$$\begin{aligned}&x(e_5e_9-e_6e_8)-e_2(e_4e_9-e_6e_7)+e_3(e_4e_8-e_5e_7)=-\det M,\\&e_1(e_5e_9-e_6e_8)-y(e_4e_9-e_6e_7)+e_3(e_4e_8-e_5e_7)=-\det M,\\&e_1(e_5e_9-e_6e_8)-e_2(e_4e_9-e_6e_7)+z(e_4e_8-e_5e_7)=-\det M,\\&\vdots\\&e_1(e_5s-e_6e_8)-e_2(e_4e_9-e_6e_7)+e_3(e_4e_8-e_5e_7)=-\det M.\end{aligned}$$

می‌توانیم یک انتخاب از نه عنصر داشته باشیم بنابراین نه حالت بدست می‌آید به روش مشابه می‌توان خطای دوگانه، سه گانه،...، نه گانه را بررسی نمود. بنابراین ماتریس کدشده E، دارای خطای مفرد، دوگانه، سه گانه،...، نه گانه است.

داریم:

$$\binom{9}{1}+\binom{9}{2}+\cdots\binom{9}{9}=2^9-1=511.$$

ازآنجا که خطای نه گانه درست نمی باشد. بنابراین توانایی تصحیح خطا در این روش $\frac{510}{511}=0.9980=99.8\%$ خواهد بود.

۵. مراجع

1. Falcon, S. and Plaza, A. (2009), " k-Fibonacci sequences modulo m", Chaos, Solitons and Fractals 41, 497-504.
2. Prased, B. (2016), "Coding theory on Lucas p numbers", Discret Mathematics, Algorithms and Applications 8, no. 4, 17 pages.
3. Stakhov, A. Massingue, V and Sluchenkova, A. (1999), " Introduction into Fibonacci coding and cryptography", Kharkov: Osnova.
4. Stakhov, A. P. (2006), "Fibonacci matrices, a generalization of the cassini formula and new coding theory", chaos, solitions Fractals30, no. 1, 56-66.
5. Basu, M and Prased, B. (2009), " The generalized relations among the elements for Fibonacci coding theory" code,chaos,solitions Fractals 41, no. 5, 2517-2525.
6. Hoggat, V. E. (1969), "Fibonacci and Lucas number", Palo Alto, CA: Houghton-Mifflin.