Karafan

Quarterly Scientific Journal of Technical and Vocational University

Autumn 2022, Vol. 19, No. 3, p. 647-661

Journal Homepage: https://karafan.tvu.ac.ir/?lang=en

TVU

doi:10.48301/KSSA.2021.283956.1505

On the Generating Function and Minimum Free Distance for a Class of Convolutional Codes

Reza Kahkeshani[1*]

[1]Assistant Professor, Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran.

ARTICLE INFO

Article Type:
Original Research

Received: 06.26.2021
Revised: 08.26.2021
Accepted: 09.02.2021

Keyword:
Convolutional Encoder
Convolutional Code
State Diagram
Modified State Diagram
Generating Function
Minimum Free Distance

***Corresponding Author:**
Reza Kahkeshani
Email:
kahkeshanireza@kashanu.ac.ir

ABSTRACT

It is common knowledge that convolutional coding is one of the two main types of channel coding widely used to detect and correct errors. In convolutional coding, the encoder output is in the form of a code sequence generated from an input information sequence. In this paper, an important class of convolutional encoders, the convolutional encoders $C_{conv}(2,1,2)$ were considered. The transfer function matrix for this class of encoders were computed and their state diagram drawn. Moreover, the general form of the generating function for this class was obtained using the modified state diagram. Degenerate states and catastrophic convolutional codes appeared for some multipliers. Then, the minimum free distance for all non-catastrophic convolutional codes which are obtained from non-degenerate states were computed. As it is shown, the maximum value of the minimum free distance for this class of encoders is equal to five and it is obtained only in two situations.

E-ISSN: 2538-4430
ISSN: 2382-9796

EXTENDED ABSTRACT

Introduction

In convolutional coding, message sequences are blocks of length k that are converted into code sequences of length n under the coding process, where $k < n$. This assignment between messages and codewords should be a bijective function to enable unique decoding for each message. Each output code sequence is generated by the current and previous input elements. Each given message sequence simultaneously enters the encoder and produces a specific code sequence such that there is a one-to-one correspondence between message sequences and code sequences. In linear cases, source alphabet is the finite field $GF(q)$ and the message sequences and code sequences belong to the vector spaces $GF(q)^k$ and $GF(q)^n$, respectively. Unlike block coding, each code sequence is dependent on the message sequence at the same instant i and on the previous inputs at the instants $i-1, \cdots, i-K$, where K is the level of memory. A convolutional code with parameters n, k and K is denoted by $C_{conv}(n,k,K)$.

A significant part of convolutional encoders is linear sequential circuits, which are constructed using memory units, adders and scalar multipliers. Such circuits are called as finite state sequential machines (or FSSMs). The FSSMs are analyzed usually by the rational transfer functions $G(D) = C(D)/M(D)$, where $M(D)$ and $C(D)$ are polynomials corresponding to the messages and codewords, respectively. The rate of $C_{conv}(n,k,K)$ is $R_c = k/n$. In this paper, the convolutional encoder shown in Figure 1 was considered. At each instant, one bit m was entered into the encoder and the pair $(c^{(1)}, c^{(2)})$ was produced as output. This encoder represented a class of convolutional encoders. The transfer functions, state diagram and modified state diagram were obtained. The generating function was computed and it is seen that the largest minimum free distance, which appears only in two situations, was equal to 5.

Methodology

Consider the encoder $C_{conv}(2,1,2)$ shown in Figure 1. If an input sequence is the unit impulse $= (1,0,0)$, then the resulting outputs are $g^{(1)} = (a_0, a_1, a_2)$ and $g^{(2)} = (f_0, f_1, f_2)$. In addition, if the message sequence $m = (m_0, m_1, m_2, \dots)$ is represented and its code sequences $c^{(1)} = (c_0^{(1)}, c_1^{(1)}, c_2^{(1)}, \cdots)$ and $c^{(2)} = (c_0^{(2)}, c_1^{(2)}, c_2^{(2)}, \cdots)$ by the polynomials $M(D) = m_0 + m_1 D + m_2 D^2 + \cdots$, $C^{(1)}(D) = c_0^{(1)} + c_1^{(1)} D + c_2^{(1)} D^2 + \cdots$ and $C^{(2)}(D) = c_0^{(2)} + c_1^{(2)} D + c_2^{(2)} D^2 + \cdots$, respectively then $C(D) = M(D)G(D)$, where $C(D) = \left[C^{(1)}(D)\ \ C^{(2)}(D)\right]$ and $G(D) = \left[G^{(1)}(D)\ \ G^{(2)}(D)\right]$. Here, $G(D)$ is transfer function matrix, $G^{(1)}(D) = a_0 + a_1 D + a_2 D^2$ and $G^{(2)}(D) = f_0 + f_1 D + f_2 D^2$. The matrix $G(D)_{1\times 2}$ is invertible if there exists an inverse matrix $G^{-1}(D)_{2\times 1}$ such that $G(D)G^{-1}(D) = D^l$ for a $l \geq 0$. It is proved that $G^{-1}(D)$ exists if and only if $\left(G^{(1)}(D), G^{(2)}(D)\right) = D^l$ for a $l \geq 0$. A convolutional code is non-catastrophic if $G^{-1}(D)$ exists.

The state diagram of $C_{conv}(2,1,2)$ is shown in Figure 2. There are four states $S_a = 00$, $S_b = 10, S_c = 01$ and $S_d = 11$ and moreover, input values are either 0 or 1. It is not possible

to move from a given state to any desired state. This is useful in the error correction and decoding process because it causes some transmissions to be ignored. The modified state diagram is obtained by making changes to the state diagram. The modified state diagram starts from S_a and ends at the same state. Arrows entering and exiting states are denoted by X^i, where i is the weight of the corresponding code vector. The weight of each path between states is equal to the sum of powers of the variables. Hence, the paths with the smallest weight yield the minimum free distance. Set $\alpha_i = a_i + f_i$, $\alpha_{ij} = (a_i \oplus a_j) + (f_i \oplus f_j)$ and $\alpha_{012} = (a_0 \oplus a_1 \oplus a_2) + (f_0 \oplus f_1 \oplus f_2)$ and see Figure 3.

Results and discussion

The generating function for a code C is defined as $T(X) = \sum_{i=0}^{\infty} A_i X^i$, where A_i is the number of sequences of weight i in C. Again, consider the code $C_{conv}(2,1,2)$. If a convolutional code is non-catastrophic then its generating function can be obtained using Mason's rule. Using the modified state diagram, we have

$$S_b = X^{a_0+f_0} + X^{(a_0\oplus a_2)+(f_0\oplus f_2)} S_c,$$

$$S_c = X^{a_1+f_1} S_b + X^{(a_1\oplus a_2)+(f_1\oplus f_2)} S_d,$$

$$S_d = X^{(a_0\oplus a_1)+(f_0\oplus f_1)} S_b + X^{(a_0\oplus a_1\oplus a_2)+(f_0\oplus f_1\oplus f_2)} S_d,$$

$$T(X) = X^{a_2+f_2} S_c,$$

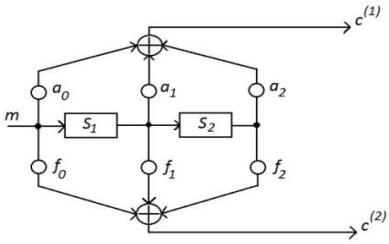


Figure 1. The convolutional encoder $C_{conv}(2,1,2)$ in general case.

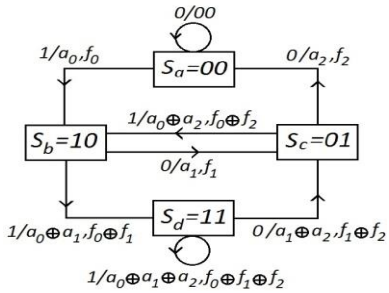


Figure 2. The state diagram of $C_{conv}(2,1,2)$.

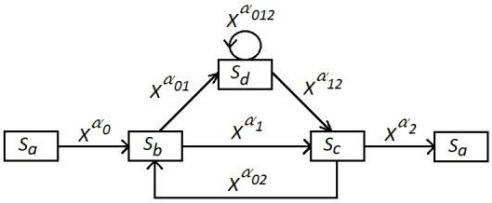


Figure 3. The modified state diagram for $C_{conv}(\mathbf{2},\mathbf{1},\mathbf{2})$.

where $+$ and $\oplus$ denote addition and addition in modulo 2, respectively. By solving the above system of equations, we have

$$T(X)=\frac{X^{\alpha_0+\alpha_2}(X^{\alpha_1}+X^{\alpha_{01}+\alpha_{12}}-X^{\alpha_1+\alpha_{012}})}{1-X^{\alpha_{012}}-X^{\alpha_1+\alpha_{02}}-X^{\alpha_{01}+\alpha_{02}+\alpha_{12}}+X^{\alpha_1+\alpha_{02}+\alpha_{012}}}.$$

Theorem. Let $C_{conv}(2,1,2)$ be a convolutional code shown in Figure 1. For different multipliers a_1, a_2, a_3, f_1, f_2, f_3, we have the generating functions

$X+2X^2+4X^3+\cdots,$

$X^2+2X^4+4X^6+\cdots,$

$X^3+X^4+X^5+\cdots,$

$2X^4+5X^6+13X^8+\cdots,$

$X^4+2X^5+2X^6+\cdots,$

$X^5+2X^6+4X^7+\cdots,$

where the first three terms of which are mentioned. In cases where only one of the multipliers a_1 and f_1 is equal to 0 and the other multipliers are equal to 1, the largest minimum free distance, which is equal to 5, is obtained.

Conclusion

In this paper, first, a significant class of convolutional encoders, namely $C_{conv}(2,1,2)$ were considered and their transfer functions and state diagrams obtained. Then, the generating function was computed in general for this class using the modified state diagram. For non-catastrophic and non-degenerate states, a table containing the generating functions and minimum free distances was presented. As it is shown, the largest minimum free distance, which is achieved in only two situations, was equal to 5.

فصلنامه علمی دانشگاه فنی و حرفه‌ای

پاییز ۱۴۰۱، دوره ۱۹، شماره ۳، ۶۶۱-۶۴۷

آدرس نشریه: https://karafan.tvu.ac.ir/

doi:10.48301/KSSA.2021.283956.1505

دربارهٔ تابع مولد و فاصلهٔ آزاد کمینه برای رده‌ای از کدهای پیچشی

رضا کهکشانی[1*]

۱- استادیار، گروه ریاضی محض، دانشکدهٔ علوم ریاضی، دانشگاه کاشان، کاشان، ایران.

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

دریافت مقاله: ۱۴۰۰/۰۴/۰۵

بازنگری مقاله: ۱۴۰۰/۰۶/۰۴

پذیرش مقاله: ۱۴۰۰/۰۶/۱۱

کلید واژگان:
کدگذار پیچشی
کد پیچشی
نمودار حالت
نمودار حالت اصلاح‌شده
تابع مولد
فاصلهٔ آزاد کمینه

***نویسنده مسئول:** رضا کهکشانی

پست الکترونیکی:
kahkeshanireza@kashanu.ac.ir

چکیده

همان‌طور که می‌دانیم، کدگذاری پیچشی یکی از دو نوع اصلی کدگذاری کانال است که به طرز گسترده‌ای برای تشخیص و تصحیح خطا مورد استفاده قرار می‌گیرد. در کدگذاری پیچشی، خروجی کدگذار به صورت یک کددنباله است که توسط یک دنبالهٔ اطلاعاتی ورودی تولید می‌شود. در این مقاله، رده‌ای مهم از کدگذارهای پیچشی، یعنی کدگذارهای پیچشی $C_{conv}(2,1,2)$، را در نظر می‌گیریم. ماتریس تابع انتقال را برای این رده از کدگذارها محاسبه نموده و نمودار حالت آنها را ترسیم می‌کنیم. به علاوه، با استفاده از نمودار حالت اصلاح‌شده، صورت کلی تابع مولد را برای این رده به دست می‌آوریم. حالت‌های تباهیده و نیز کدهای پیچشی فجیع به ازای برخی از ضرب‌کننده‌ها ظاهر می‌شوند. سپس، فاصلهٔ آزاد کمینه را برای همه کدهای پیچشی غیر فجیع، که به دست آمده از حالت‌های ناتباهیده باشند، محاسبه می‌کنیم. چنان که نشان داده می‌شود، بیشترین فاصلهٔ آزاد کمینه برای این رده از کدگذارهای پیچشی برابر پنج است و تنها در دو موقعیت حاصل می‌گردد.

شاپای الکترونیکی: ۲۵۳۸-۴۴۳۰

شاپای چاپی: ۲۳۸۲-۹۷۹۶

مقدمه

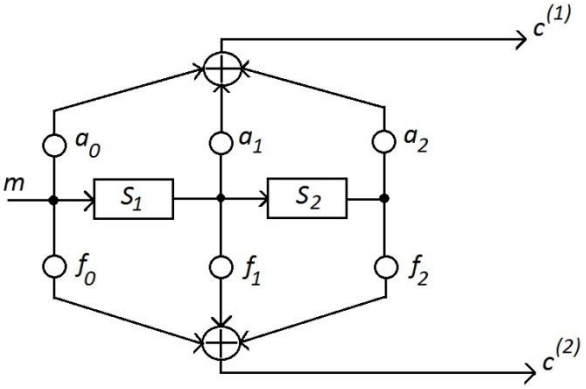
چنان که می‌دانیم، در کدگذاری مهار خطا دو نوع ساز و کار برای اضافه نمودن افزونگی وجود دارد، که عبارتند از کدگذاری بلوکی و کدگذاری پیچشی [۱]. در کدگذاری بلوکی، واژه‌های پیام بلوک‌هایی از طول k هستند که تحت فرایند کدگذاری به کدواژه‌هایی از طول n، که $n > k$، تبدیل می‌شوند. این نسبت‌دهی میان پیام‌ها و کدواژه‌ها باید به صورت یک تابع دوسویی باشد تا امکان کدگشایی یکتا را برای هر پیام فراهم نماید. روشن است که افزونگی در فرایند کدگشایی، تصحیح خطا و به‌دست آوردن دنبالهٔ پیام مفید واقع می‌شود. در کدگذاری پیچشی، خروجی کدگذار کددنباله‌ها (یا به عبارتی، کدبردارها) هستند که از دنباله‌های اطلاعاتی ورودی پدید می‌آیند. هر کد دنبالهٔ خروجی از روی عناصر ورودی حاضر و نیز پیشین در طی یک فرایند کدگذاری مستمر، که پدید آورندهٔ افزونگی است، تولید می‌شود. در اینجا نیز، هر دنبالهٔ پیام داده شده یک کددنبالهٔ خاص تولید می‌کند و در واقع، تناظری دوسویی میان دنباله‌های پیام و کددنباله‌ها برقرار است. مجموعهٔ تمامی چنین کددنباله‌هایی یک کد پیچشی C_{conv} تشکیل می‌دهند [۲]. این کدها نخستین بار در سال ۱۹۵۵ توسط الیاس معرفی شدند و نخستین الگوریتم برای کدگشایی چنین کدهایی ابتدا توسط وزنکرفت[1] و سپس، نسخهٔ اصلاح شدهٔ آن توسط فانو در ۱۹۶۳ ارائه گردید. چهار سال بعد، ویتربی الگوریتم جدیدی معرفی نمود که به‌ویژه، هنگامی که طول ثبّات تغییر مکان خیلی بزرگ نباشد، جالب است. در واقع، پیچیدگی الگوریتم ویتربی بر حسب اندازهٔ ثبّات به طور نمایی افزایش می‌یابد در حالی که پیچیدگی الگوریتم فانو تقریباً مستقل از آن است. یک الگوریتم کدگشایی مناسب این امکان را به ما می‌دهد که دنبالهٔ پیام را به عنوان تابعی از دنبالهٔ دریافتی، که احتمالاً تحت تاثیر نوفهٔ کانال بوده است، مشخص نماییم [۳].

کدهای پیچشی به طور گسترده‌ای در ارتباطات فضایی و ماهواره‌یی، تلفن همراه و پخش تصویر رقمی مورد استفاده قرار گرفته‌اند [۴]. برای پاره‌ای کاربردهای اخیر از کدهای پیچشی در قابلیت‌های ردیابی رادار و نیز، پژوهش‌هایی پیرامون الگوریتم‌های کدگشایی، فاصله‌های دوری و آزاد کمینه به [۵] ، [۶] ، [۷] و [۸] رجوع شود. در واقع، ساختار ساده و روش‌های کدگشایی تصمیم نرم، که به راحتی قابل پیاده‌سازی هستند، باعث چنین فراگیری و محبوبیتی شده‌اند. به علاوه، کدگذاری پیچشی باید به گونه‌ای طراحی گردد که فرایند کدگشایی به صورت ساده و ساختارمند انجام پذیرد. یکی از فرضیات طراحی، که کدگشایی را ساده می‌کند، خطی‌بودن کد است. لذا، کدهای پیچشی خطی در اولویت قرار می‌گیرند. در حالت خطی، دنباله‌های پیام و کددنباله‌ها به ترتیب متعلق به فضای برداری پیام و فضای برداری کد هستند. به دیگر بیان، کدبردارهای واقع در فضای برداری کد همان کددنباله‌های کد پیچشی هستند. بردارهای پیام کوتاه‌تر از کدبردارها می‌باشند و این به معنای وجود افزونگی به منظور امکان تشخیص و تصحیح خطا است. در حالت کلی، اگر الفبای منبع را میدان متناهی $GF(q)$ در نظر بگیریم آنگاه دنباله‌های پیام قطعاتی k-عنصری، یعنی اعضای $GF(q)^k$، هستند که به طور هم‌زمان به کدگذار وارد می‌شوند. کدگذار نیز قطعاتی n-عنصری تولید می‌کند، که این قطعات متعلق به فضای برداری $GF(q)^n$ هستند. در حقیقت، کدهای پیچشی خطی زیرفضاهایی k-بعدی از فضای برداری n-بعدی $GF(q)^n$ هستند. برخلاف کدگذاری بلوکی، n عنصر تشکیل دهنده قطعه کدشده نه تنها به k عنصر قطعه ورودی در همان لحظه i، بلکه به قطعات ورودی پیشین در لحظه‌های $i-1, i-2, \dots, i-K$ نیز وابسته هستند، که در اینجا K تراز حافظه است. هرچه K بیشتر باشد، پیچیدگی کدگشای پیچشی و بالطبع، قابلیت تصحیح خطا بیشتر می‌گردد. در اغلب کاربردهای عملی به جای استفاده از میدان $GF(q)$ میدان دودویی $GF(2)$، که دارای تنها دو عنصر 0 و 1 است، به کار گرفته می‌شود. به علاوه، معمول‌ترین ساختارها در میان کدهای پیچشی ساختارهایی با پارامترهای $k=1$ و $n=2$ هستند. یک کد پیچشی با پارامترهای n، k و K با نماد $C_{conv}(n,k,K)$ نشان داده می‌شود. برای دیدن جزئیات بیشتر به [۹] ، [۱۰] و [۱۱] مراجعه گردد. این نکته حائز اهمیت است که انتقال و ذخیره‌سازی اطلاعات با

[1] Wozencraft

گرایش‌های مختلفی از علوم در مرتبط است. به عنوان نمونه، برای مطالعهٔ برخی پژوهش‌های اخیر در زمینهٔ مخابرات و ارتباطات به [۱۲] و [۱۳] و نیز، برای دیدن برخی پیوندها میان کدهای پیچشی و کدهای LDPC به [۱۴] رجوع گردد.

مدارهای ترتیبی خطی[1] بخش مهمی از کدگذارهای پیچشی هستند، که با استفاده از واحدهای حافظه (یا تاخیرها)، جمع‌کننده‌ها و ضرب‌کننده‌های عددی ساخته می‌شوند. چنین مدارهایی به عنوان ماشین‌های ترتیبی حالت- متناهی[2] (یا FSSMها) نیز شناخته می‌شوند. هر واحد حافظه نظیر به حالتی از FSSM است و متغیرها بیت‌ها یا برداری از بیت‌ها هستند. هر بیت می‌تواند عنصری از یک میدان، گروه یا حلقه باشد ولی، به طور معمول، بردارها را روی میدان دودویی در نظر می‌گیرند. تحلیل FSSM معمولاً توسط تابع انتقال گویای $G(D)$ انجام می‌شود، به قسمی که در این رهیافت دنباله‌های پیام و کددنباله‌ها به ترتیب به صورت چند جمله‌یی‌های $M(D)$ و $C(D)$، که چند جمله‌یی‌هایی بر حسب حوزهٔ تاخیر D هستند، نوشته می‌شوند. ارتباط میان دنباله‌های پیام و کددنباله‌ها در FSSMهایی با ورودی‌ها و نیز خروجی‌های چندگانه توسط یک ماتریس تابع انتقال گویای $G(D)$ توصیف می‌شود. کدگذارهای پیچشی اساساً ساختارهایی هستند که توسط FSSMها به وجود می‌آیند. دو کدگذار پیچشی را هم‌ارز گوییم هرگاه هر دو کدهای پیچشی یکسانی تولید نمایند. در حالت کلی، می‌توان کدگذارهایی با ساختارهای متفاوت یافت که هم‌ارز می‌باشند. نرخ یک کد پیچشی عبارت است از خارج قسمت تعداد عناصر ورودی بر تعداد عناصر خروجی آن. یعنی، $R_c = k/n$. برای دیدن جزئیات و مثال‌های بیشتر به [۱]، [۲]، [۹] و [۱۰] مراجعه شود.



شکل ۱. کدگذار پیچشی $C_{conv}(2,1,2)$ در کلی‌ترین صورت.

در این مقاله، کدگذار پیچشی نشان داده شده در شکل ۱ را در نظر می‌گیریم. چنان که دیده می‌شود، در هر لحظه بیت m از عناصر پیام به عنوان ورودی به کدگذار وارد شده و در همان لحظه دوتایی $(c^{(1)}, c^{(2)})$ به عنوان خروجی تولید می‌گردد. از این رو، نرخ کد دودویی حاصل برابر ۱/۲ است. ساختار این کدگذار نشان می‌دهد که خروجی در هر لحظه i می‌تواند به خروجی‌های پیشین در لحظات j، که $j < i$، نیز وابسته باشد. بلوک‌های مستطیلی واحدهای حافظه یا تاخیرهای زمانی را مشخص می‌کنند. در واقع، از آنها به عنوان معرف واحد زمانی FSSM یاد می‌شود، که عبارتند از مدت زمانی که FSSM روی عنصری دلخواه از میدان $GF(۲)$ عمل می‌کند. هر دایرهٔ حاوی علامت جمع نشان‌دهندهٔ

[1] linear sequential circuits
[2] finite state sequential machines

یک جمع‌کنندهٔ دودویی و همچنین، هر دایرهٔ توخالی نشان‌دهندهٔ یک ضرب‌کننده دودویی است. همان‌طور که دیده می‌شود، می‌توان به ضرب‌کننده‌ها مقادیر صفر و یک را به دلخواه نسبت داد. از این رو، کدگذار مورد بحث نمایش‌گر رده‌ای از کدگذارهای پیچشی است. برای این رده از کدگذارهای پیچشی توابع انتقال، نمودار حالت[1] و نمودار حالت اصلاح‌شده[2] را به دست آورده و تابع مولد را در کلی‌ترین صورت ممکن محاسبه می‌کنیم. سپس، با به دست آوردن تابع مولد به‌ازای مقادیر مختلف ضرب‌کننده‌ها دیده می‌شود که بیشترین مقدار برای فاصلهٔ آزاد کمینه عدد پنج است، که تنها توسط دو کدگذار خاص ظاهر می‌گردد.

توابع انتقال و نمودارهای حالت

کدگذار پیچشی $C_{conv}(2,1,2)$، نشان داده شده در شکل ۱، را در نظر می‌گیریم. اگر ورودی کدگذار ضربهٔ یکه، یعنی دنبالهٔ پیام $\boldsymbol{m} = (1,0,0)$ باشد آنگاه دیده می‌شود که پاسخ‌های ضربه، یعنی دنباله‌های خروجی متناظر، عبارتند از $\boldsymbol{g}^{(1)} = (a_0, a_1, a_2)$ و $\boldsymbol{g}^{(2)} = (f_0, f_1, f_2)$. چنان که می‌دانیم، پاسخ‌های ضربه توصیفی از اتصالات ساختاری FSSM به دست می‌دهند و به عنوان دنباله‌های مولد کد پیچشی نیز شناخته می‌شوند. به بیان دقیق، اگر به دنباله پیام $\boldsymbol{m} = (m_0, m_1, m_2, \dots)$ و کددنباله‌های متناظر $\boldsymbol{c}^{(1)} = (c_0^{(1)}, c_1^{(1)}, c_2^{(1)}, \cdots)$ و $\boldsymbol{c}^{(2)} = (c_0^{(2)}, c_1^{(2)}, c_2^{(2)}, \cdots)$ به ترتیب چندجمله‌یی‌های

$$\begin{cases} \boldsymbol{M}(D) = m_0 + m_1 D + m_2 D^2 + \cdots, \\ \boldsymbol{C}^{(1)}(D) = c_0^{(1)} + c_1^{(1)} D + c_2^{(1)} D^2 + \cdots, \\ \boldsymbol{C}^{(2)}(D) = c_0^{(2)} + c_1^{(2)} D + c_2^{(2)} D^2 + \cdots, \end{cases} \quad (۱)$$

را نظیر نماییم آنگاه در فضای D-تبدیل می‌توان نوشت $\boldsymbol{C}(D) = \boldsymbol{M}(D)\boldsymbol{G}(D)$، که در آن

$$\begin{cases} \boldsymbol{C}(D) = \left[\boldsymbol{C}^{(1)}(D) \;\; \boldsymbol{C}^{(2)}(D)\right], \\ \boldsymbol{G}(D) = \left[\boldsymbol{G}^{(1)}(D) \;\; \boldsymbol{G}^{(2)}(D)\right]. \end{cases} \quad (۱)$$

در اینجا، $\boldsymbol{G}(D)$ ماتریس تابع انتقال است و

$$\begin{cases} \boldsymbol{G}^{(1)}(D) = a_0 + a_1 D + a_2 D^2, \\ \boldsymbol{G}^{(2)}(D) = f_0 + f_1 D + f_2 D^2, \end{cases} \quad (۳)$$

چند جمله‌یی‌های مولد هستند. یک کد پیچشی با ماتریس تابع انتقال خود مشخص می‌شود. می‌گوییم ماتریس $\boldsymbol{G}(D)_{1\times 2}$ دارای وارون است هرگاه ماتریس $\boldsymbol{G^{-1}}(D)_{2\times 1}$ وجود داشته باشد به طوری که به ازای یک $l \geq 0$، $\boldsymbol{G}(D)\boldsymbol{G^{-1}}(D) = D^l$. وجود وارون برای فرایند کدگشایی و به دست آوردن دنبالهٔ ورودی امری مهم است. ثابت می‌شود چنین وارونی وجود دارد اگر و تنها اگر بزرگ‌ترین مقسوم علیه مشترک چندجمله‌یی‌های $\boldsymbol{G}^{(1)}(D)$ و $\boldsymbol{G}^{(2)}(D)$ به ازای یک $l \geq 0$ برابر D^l باشند [۱]. یک کد پیچشی را فجیع[3] گویند هرگاه ماتریس $\boldsymbol{G^{-1}}(D)$ برای آن وجود نداشته باشد.

[1] State diagram
[2] Modified state diagram
[1] Catastrophic

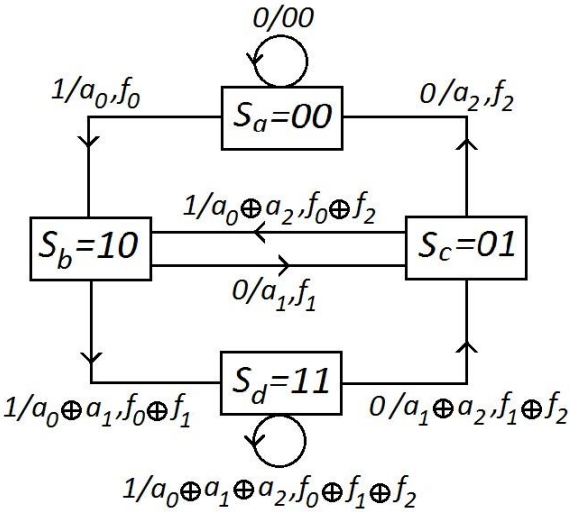
حالت یک FSSM بر اساس محتویات K طبقهٔ ثبّاتی[1]، که همان بلوک‌های مستطیلی مشخص کنندهٔ واحدهای حافظه هستند، بیان می‌گردد. هر حالت آتی با تغییر مکان محتویات طبقه‌های حاضر به اندازهٔ یک تاخیر به دست می‌آید به طوری که طبقهٔ خالی تولید شده در سمت چپ با مقدار بیت ورودی در همان لحظهٔ زمانی پر می‌گردد. در کدگذار پیچشی شکل ۱، حالت می‌تواند یکی از چهار نوع 00، 01، 10 و 11 باشد و ورودی 0 یا 1 است. از این رو، هشت وضعیت ممکن داریم که در جدول ۱ به همراه خروجی‌ها آورده شده‌اند. با استفاده از جدول ۱ نمودار حالت این کدگذار پیچشی را به صورت شکل ۲ ترسیم می‌کنیم. نمودار حالت نمایشی تصویری از تکامل دنباله‌های حالت را به دست می‌دهد. در اینجا، برای هر یک از این حالات تنها دو انتقال ورودی و دو انتقال خروجی داریم. به علاوه، این گونه نیست که بتوان از یک حالت داده شده به هر حالت دلخواهی انتقال یافت. این امر در تصحیح خطا و فرایند کدگشایی دنبالهٔ دریافتی مفید است زیرا سبب نادیده گرفتن برخی انتقال‌ها می‌گردد.

نمودار حالت اصلاح‌شده با تغییراتی در نمودار حالت سنتی به دست می‌آید. نمودار حالت اصلاح‌شده از حالت تمام-صفر $S_a = 00$ آغاز و به همان حالت پایان می‌یابد. همچنین، طوقهٔ مربوط به S_a حذف می‌گردد. پیکان‌هایی که در این نمودار به حالت‌ها وارد یا از آنها خارج می‌شوند را با X^i نشان می‌دهیم، که در آن نمای i وزن کدبردار خروجی متناظر به همان پیکان است. وزن هر مسیر میان حالت‌ها برابر مجموع نماهای متغیرهای موجود در آن مسیر است و به علاوه، وزن مسیرها متناظر به وزن کددنباله‌ها هستند. از این رو، مسیرهایی با کوچک‌ترین وزن

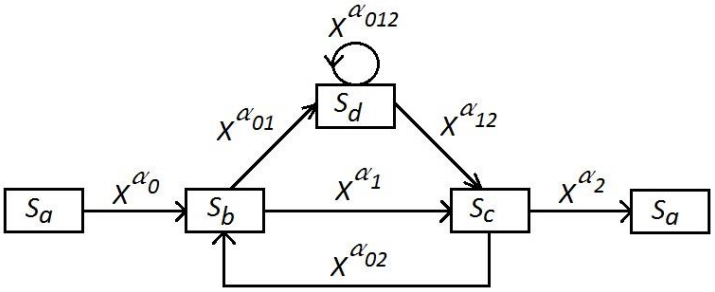
جدول ۱. تمام انتقال‌های ممکن برای ساخت نمودار حالت.

ورودی m_i	حالت در t_i	حالت در t_{i+1}	خروجی $c^{(1)}$	خروجی $c^{(2)}$
--	۰۰	۰۰	--	--
0	۰۰	۰۰	0	0
1	۰۰	۱۰	a_0	f_0
0	۰۱	۰۰	a_2	f_2
1	۰۱	۱۰	$a_0 \oplus a_2$	$f_0 \oplus f_2$
0	۱۰	۰۱	a_1	f_1
1	۱۰	۱۱	$a_0 \oplus a_1$	$f_0 \oplus f_1$
0	۱۱	۰۱	$a_1 \oplus a_2$	$f_1 \oplus f_2$
1	۱۱	۱۱	$a_0 \oplus a_1 \oplus a_2$	$f_0 \oplus f_1 \oplus f_2$

[2] Register Stage



شکل ۲. نمودار حالت کدگذار پیچشی مفروض.



شکل ۳. نمودار حالت اصلاح‌شده برای کدگذار پیچشی مفروض.

فاصلهٔ آزاد کمینهٔ کد پیچشی، یعنی d_{free}، را به دست می‌دهند. صفت « آزاد» برای فاصلهٔ کمینه از این واقعیت ناشی می‌شود که هیچ محدودیتی روی طول مسیرهای نمودار حالت متناظر وجود ندارد. در کدهای پیچشی فجیع، نمودار حالت اصلاح‌شده دارای مسیرهایی از وزن صفر میان حالت‌ها است و لذا، این امر نشان‌گر نامتناهی کددنباله با یک وزن ثابت است. در شکل ۳ نمودار حالت اصلاح‌شده برای همان کدگذار پیچشی مورد نظر ترسیم گردیده است، که در آن به ازای هر $i,j = 0,1,2$ متمایز، $\alpha_i = a_i + f_i$ و $\alpha_{ij} = (a_i \oplus a_j) + (f_i \oplus f_j)$ و به علاوه، داریم $\alpha_{012} = (a_0 \oplus a_1 \oplus a_2) + (f_0 \oplus f_1 \oplus f_2)$.

تابع مولد

چنان که می‌دانیم، تابع مولد برای یک کد مفروض عبارت است از سری صوری

$$T(X) = \sum_{i=0}^{\infty} A_i X^i, \tag{۴}$$

که در آن A_i تعداد دنباله‌ها از وزن i است. روشن است که درجهٔ کوچک‌ترین تک‌جمله‌یی غیر ۱ از $T(X)$ برابر d_{free} است. کدگذار پیچشی $C_{conv}(2,1,2)$، نشان داده شده در شکل ۱، را بار دیگر در نظر می‌گیریم. هرگاه کد پیچشی نظیر غیر فجیع باشد آنگاه تابع مولد را می‌توان به وسیلهٔ قاعدهٔ میسون[1]، که در ادامه آن را شرح می‌دهیم، به دست آورد. با استفاده از نمودار حالت اصلاح‌شده دستگاه

$$S_b = X^{a_0+f_0} + X^{(a_0\oplus a_2)+(f_0\oplus f_2)}S_c, \tag{۵}$$

$$S_c = X^{a_1+f_1}S_b + X^{(a_1\oplus a_2)+(f_1\oplus f_2)}S_d, \tag{۶}$$

$$S_d = X^{(a_0\oplus a_1)+(f_0\oplus f_1)}S_b + X^{(a_0\oplus a_1\oplus a_2)+(f_0\oplus f_1\oplus f_2)}S_d, \tag{۷}$$

$$T(X) = X^{a_2+f_2}S_c, \tag{۸}$$

را داریم، که در آنها $+$ و $\oplus$ به ترتیب جمع معمولی و جمع به پیمانه دو هستند. دیده می‌شود که تساوی‌های (۵)، (۶) و (۷) یک دستگاه سه معادله و سه مجهولی تشکیل می‌دهند. با حل این دستگاه و جایگذاری S_c در (۸)، به دست می‌آوریم:

$$T(X) = \frac{X^{\alpha_0+\alpha_2}(X^{\alpha_1} + X^{\alpha_{01}+\alpha_{12}} - X^{\alpha_1+\alpha_{012}})}{1 - X^{\alpha_{012}} - X^{\alpha_1+\alpha_{02}} - X^{\alpha_{01}+\alpha_{02}+\alpha_{12}} + X^{\alpha_1+\alpha_{02}+\alpha_{012}}}. \tag{۹}$$

به عنوان مثال، با استفاده از روابط (۳)، چند جمله‌یی‌های مولد در وضعیتی که a_0، a_1 و f_0 برابر صفر و a_2، f_1 و f_2 برابر یک باشند عبارتند از $\boldsymbol{G}^{(1)}(D) = D^2$ و $\boldsymbol{G}^{(2)}(D) = D + D^2$. از آنجا که بزرگ‌ترین مقسوم علیه مشترک این چند جمله‌یی‌ها برابر D است، کد حاصل غیر فجیع است. همچنین، با استفاده از دستور (۹)، تابع مولد عبارت است از

$$T(X) = \frac{X^3}{1 - X - X^3}$$

$$= X^3(1 + (X + X^3) + (X + X^3)^2 + \cdots) = X^3 + X^4 + X^5 + \cdots. \tag{۱۰}$$

از این رو، $d_{free} = 3$ و تنها یک کددنباله از وزن ۳ داریم.

[1] Mason

جدول ۲. توابع مولد و فاصلهٔ آزاد کمینه در تمامی حالات ناتباهیدهٔ ممکن.

a_0	a_1	a_2	f_0	f_1	f_2	$T(X)$	d_{free}	A_d
0	0	1	0	0	1	$X^2/(1-2X^2)$	۲	۱
0	0	1	0	1	0	$X^2/(1-2X^2)$	۲	۱
0	0	1	0	1	1	$X^3/(1-X-X^3)$	۳	۱
0	0	1	1	0	0	$X^2/(1-2X^2)$	۲	۱
0	0	1	1	0	1	$X^3(1-X+X^3)/(1-2X+X^2-X^4)$	۳	۱
0	0	1	1	1	0	$X^3/(1-X-X^3)$	۳	۱
0	0	1	1	1	1	$X^4(2-X^2)/(1-3X^2+X^4)$	۴	۲
0	1	0	0	0	1	$X^2/(1-2X^2)$	۲	۱
0	1	0	0	1	0	$X^2/(1-2X^2)$	۲	۱
0	1	0	0	1	1	$X^3/(1-X-X^3)$	۳	۱
0	1	0	1	0	0	$X^2/(1-2X^2)$	۲	۱
0	1	0	1	0	1	$X^3(1-X+X^3)/(1-2X+X^2-X^4)$	۳	۱
0	1	0	1	1	0	$X^3/(1-X-X^3)$	۳	۱
0	1	0	1	1	1	$X^4(2-X^2)/(1-3X^2+X^4)$	۴	۲
0	1	1	0	0	1	$X^3/(1-X-X^3)$	۳	۱
0	1	1	0	1	0	$X^3/(1-X-X^3)$	۳	۱
0	1	1	0	1	1	فجیع	-	-
0	1	1	1	0	0	$X^3/(1-X-X^3)$	۳	۱
0	1	1	1	0	1	فجیع	-	-
0	1	1	1	1	0	فجیع	-	-
0	1	1	1	1	1	$X^4(1+X-X^2)/(1-X-X^2-X^3+X^4)$	۴	۱
1	0	0	0	0	1	$X^2/(1-2X^2)$	۲	۱
1	0	0	0	1	0	$X^2/(1-2X^2)$	۲	۱
1	0	0	0	1	1	$X^3/(1-X-X^3)$	۳	۱
1	0	0	1	0	0	$X^2/(1-2X^2)$	۲	۱
1	0	0	1	0	1	$X^3(1-X+X^3)/(1-2X+X^2-X^4)$	۳	۱
1	0	0	1	1	0	$X^3/(1-X-X^3)$	۳	۱
1	0	0	1	1	1	$X^4(2-X^2)/(1-3X^2+X^4)$	۴	۲
1	0	1	0	0	1	$X^3(1-X+X^3)/(1-2X+X^2-X^4)$	۳	۱
1	0	1	0	1	0	$X^3(1-X+X^3)/(1-2X+X^2-X^4)$	۳	۱
1	0	1	0	1	1	فجیع	-	-
1	0	1	1	0	0	$X^3(1-X+X^3)/(1-2X+X^2-X^4)$	۳	۱
1	0	1	1	0	1	فجیع	-	-
1	0	1	1	1	0	فجیع	-	-
1	0	1	1	1	1	$X^5/(1-2X)$	۵	۱
1	1	0	0	0	1	$X^3/(1-X-X^3)$	۳	۱
1	1	0	0	1	0	$X^3/(1-X-X^3)$	۳	۱

a_0	a_1	a_2	f_0	f_1	f_2	$T(X)$	d_{free}	A_d
1	1	0	0	1	1	فجیع	-	-
1	1	0	1	0	0	$X^3/(1-X-X^3)$	۳	۱
1	1	0	1	0	1	فجیع	-	-
1	1	0	1	1	0	فجیع	-	-
1	1	0	1	1	1	$X^4(1+X-X^2)/(1-X-X^2-X^3+X^4)$	۴	۱
1	1	1	0	0	1	$X^4(2-X^2)/(1-3X^2+X^4)$	۴	۲
1	1	1	0	1	0	$X^4(2-X^2)/(1-3X^2+X^4)$	۴	۲
1	1	1	0	1	1	$X^4(1+X-X^2)/(1-X-X^2-X^3+X^4)$	۴	۱
1	1	1	1	0	0	$X^4(2-X^2)/(1-3X^2+X^4)$	۴	۲
1	1	1	1	0	1	$X^5/(1-2X)$	۵	۱
1	1	1	1	1	0	$X^4(1+X-X^2)/(1-X-X^2-X^3+X^4)$	۴	۱
1	1	1	1	1	1	فجیع	-	-

اینک، تابع مولد $T(X)$ را برای کلیهٔ کدهای پیچشی غیر فجیع محاسبه نموده و جدول ۲ را تشکیل می‌دهیم. توجه نمایید که وضعیت‌هایی مانند $a_0 = a_1 = a_2 = 0$ یا $f_0 = f_1 = f_2 = 0$ حالت‌هایی تباهیده هستند و لذا، آنها را از جدول حذف نموده‌ایم. در این جدول، ستون‌های مشخص شده با d_{free} و A_d به ترتیب مقدار فاصلهٔ آزاد کمینه و تعداد کددنباله‌ها از وزن کمینه را نشان می‌دهند. همچنین، برخی طراحی‌ها منجر به ایجاد کدهای پیچشی فجیع می‌شوند و همان‌طور که می‌دانیم، از جهت کدگشایی کدهای مناسبی نیستند. لذا، پارامترهای مربوطه برای آنها با علامت «-» مشخص شده است. با استفاده از نتایج به دست آمده، قضیهٔ زیر را داریم:

قضیه ۱. گیریم $C_{conv}(2,1,2)$ کدگذار پیچشی نشان داده شده در شکل ۱ باشد. بـه ا ز ا ی ضرب‌کننده‌های مختلف a_1، a_2، a_3، f_1، f_2 و f_3، یا معادلاً به‌ازای طراحی‌های مختلف، توابع مولد

$$X + 2X^2 + 4X^3 + \cdots, \quad (۱۱)$$

$$X^2 + 2X^4 + 4X^6 + \cdots, \quad (۱۲)$$

$$X^3 + X^4 + X^5 + \cdots, \quad (۱۳)$$

$$۲X^4 + 5X^6 + 13X^8 + \cdots, \quad (۱۴)$$

$$X^4 + 2X^5 + 2X^6 + \cdots, \quad (۱۵)$$

$$X^5 + 2X^6 + 4X^7 + \cdots, \quad (۱۶)$$

به دست می‌آیند، که نخستین سه جملهٔ آنها ذکر شده است. در حالاتی که تنها یکی از ضرب‌کننده‌های a_1 یا f_1 برابر با صفر و دیگر ضرب‌کننده‌ها برابر با یک باشند، بیشترین فاصلهٔ کمینه، که مساوی ۵ است، حاصل می‌شود

نتیجه‌گیری

در این مقاله، ابتدا یک ردهٔ مهم از کدگذارهای پیچشی، یعنی $C_{conv}(2,1,2)$، را در نظر گرفته و به محاسبهٔ توابع انتقال و نمودارهای حالت آنها پرداخته‌ایم. سپس، با بهره گرفتن از نمودار حالت اصلاح‌شده تابع مولد را به طور کلی برای این رده از کدگذارها به دست آورده‌ایم. همچنین، جدولی از توابع مولد و فاصلهٔ آزاد کمینهٔ کدهای حاصل برای حالت‌های غیر فجیع و ناتباهیده ارائه گردیده است. چنان که نشان داده شده است، بیشترین فاصلهٔ آزاد کمینه برابر پنج است و تنها در دو موقعیت حاصل می‌گردد.

تقدیر و تشکر

این پژوهش توسط دانشگاه کاشان تحت پژوهانهٔ شماره ۱۰۷۳۲۱۱/۱ به طور جزئی مورد حمایت قرار گرفته است. از داوران محترم، که با ارائه پیشنهادهای ارزشمند خود سبب بهبود کیفی مقاله شده‌اند، کمال سپاسگزاری را دارم.

References

[1] Moreira, J. C., & Farrell, P. G. (2006). *Essentials of error-control coding*. John Wiley & Sons. https://doi.org/10.1002/9780470035726

[2] Lin, S., & Costello, D. J. (2001). *Error control coding* (2 ed.). Pearson Education International. https://www.amazon.com/Error-Control-Coding-2nd-Shu/dp/0130426725

[3] Berrou, C. (2010). *Codes and turbo codes*. Springer. https://doi.org/10.1007/978-2-8178-0039-4

[4] Vucetic, B., & Yuan, J. (2002). *Turbo codes: principles and applications*. Springer Scienc e & Business Media. https://doi.org/10.1007/978-1-4615-4469-2

[5] Alfarano, G. N., & Lieb, J. (2021). On the left primeness of some polynomial matrices with applications to convolutional codes. *Journal of Algebra and Its Applications*, *20*(11), 1-13. https://doi.org/10.1142/s0219498821502078

[6] Enma, L. P., Liu, J., & Wang, J. (2021). Improvement of radar detection capabilities for fluctuating targets using convolutional error control coding technique. *Journal of P hysics: Conference Series*, *1792*(1), 1-6. https://doi.org/10.1088/1742-6596/1792/1/012042

[7] Gómez-Torrecillas, J., Lobillo, F. J., & Navarro, G. (2021). Cyclic distances of idempoten t convolutional codes. *Journal of Symbolic Computation*, *102*, 37-62. https://doi.org/10.1016/j.jsc.2019.10.008

[8] Raviv, T., Schwartz, A., & Be'ery, Y. (2021). Deep ensemble of weighted viterbi decoders for tail-biting convolutional codes. *Entropy*, *23*(1), 1-13. https://doi.org/10.3390/e23010093

[9] Huffman, W. C., Kim, J-L., & Solé, P. (2021). *Concise Encyclopedia of Coding Theory*. Chapman and Hall/CRC. https://www.taylorfrancis.com/books/edit/10.1201/9781315147901/concise-encyclopedia-coding-theory-cary-huffman-jon-lark-kim-patrick-sol%C3%A9

[10] Moon, T. K. (2020). *Error correction coding: mathematical methods and algorithms* (2 ed.). John Wiley & Sons. https://doi.org/10.1002/0471739219

[11] MacWilliams, F. J., & Sloane, N. J. A. (1977). *The theory of error correcting codes*. No rth Holland. https://www.amazon.com/Theory-Error-Correcting-North-Holland-Mathematical-Library/dp/0444851933

[12] Hashemi Talkhouncheh, S. A., & Shahbazi, A. (2020). Design, Simulation and Fabrication of a Mobile Jammer in GSM Bands. *Karafan Quarterly Scientific Journal*, *17*(1), 27-41. https://doi.org/10.48301/kssa.2020.112755

[13] Talkhouncheh, S. A. H., & Basafa, A. (2021). Design of a Microstrip Bandpass Filter Using Metamaterials. *Karafan Quarterly Scientific Journal*, *17*(4), 271-280. https://doi.org/10.48301/kssa.2021.128406

[14] Esmaeili, M., & Gholami, M. (2009). Geometrically-structured maximum-girth LDPC block and convolutional codes. *IEEE Journal on Selected Areas in Communications*, *27*(6), 831-845. https://doi.org/10.1109/JSAC.2009.090802