تخمین پارامترهای کد کانولوشنال نرخ k/n در شرایط نویزی

احمد قلی‌زاده سوته[۱]، دانشجوی دکتری، حسین خالقی بیزکی[۲]، دانشیار

۱- مجتمع دانشگاهی برق و الکترونیک - دانشگاه صنعتی مالک اشتر - تهران - ایران - soteh.soteh@gmail.com
۲- مجتمع دانشگاهی برق و الکترونیک - دانشگاه صنعتی مالک اشتر - تهران - ایران - hbizaki@gmail.com

چکیده: این مقاله به مسئله تخمین پارامترهای کد کانولوشنال از یک رشته دریافتی نویزی می‌پردازد. از بین روش‌هایی که تاکنون برای این مسئله پیشنهاد شده‌اند، روش تخمین مبتنی بر مرتبه، بیش‌ترین قسمت تحقیقات را به خود اختصاص داده است. در این روش گیرنده رشته دریافتی را به ازای طول‌های $l=1,\ldots,l_{\max}$ به‌صورت سطری در ماتریس‌های l-ستونی $\mathbf{C}^{(l)}$ قرار داده و سپس پارامترهای کد را بر اساس مرتبه این ماتریس‌ها تعیین می‌کند. البته برای انجام این کار باید رابطه بین پارامترهای کد و مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ مشخص باشد. در کارهای پیشین یک رابطه تجربی برای این کار پیشنهاد شد که البته در حالت کلی برقرار نیست. به همین دلیل در این مقاله ابتدا رابطه بین مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ و پارامترهای کد به‌صورت تحلیلی تعیین شده و سپس بر مبنای آن الگوریتمی جامع برای تخمین پارامترهای کد کانولوشنال پیشنهاد می‌شود. در این الگوریتم از روش حذف گوسی با انتخاب رهبر سطری (GERP) برای تخمین مرتبه و فضای تهی ماتریس‌های $\mathbf{C}^{(l)}$ استفاده می‌شود. با توجه به اینکه این روش مبتنی بر حد آستانه است، در این مقاله یک حد آستانه مناسب بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه نیز پیشنهاد خواهد شد.

واژه‌های کلیدی: کد کانولوشنال، تخمین پارامتر، مخابرات غیراشتراکی، کد دوگان، قید طول.

Parameter Estimation of a Rate k/n Convolutional Code in Noisy Case

A. Gholizadeh Soteh, Ph.D. Candidate[1], H. Khaleghi Bizaki, Associate Professor[2]

1- Faculty of Electrical and Computer Engineering, Malek Ashtar University of Technology, Tehran, Iran, soteh.soteh@gmail.com
2- Faculty of Electrical and Computer Engineering, Malek Ashtar University of Technology, Tehran, Iran, bizaki@ee.iust.ac.ir

Abstract: This paper studies the problem of the convolutional code parameters estimation in noisy scenario. Among the methods that have been proposed for this problem, the rank-based method has attracted most of the research. In this method, the receiver cuts the received sequence up into vectors of length l to form the rows of matrix $\mathbf{C}^{(l)}$, for $l=1,\ldots,l_{\max}$. The code parameters are estimated based on the rank of these matrices. To this end, the relation between the code parameters and the rank of $\mathbf{C}^{(l)}$ should be known. To do this, the previous works proposed an experimental relation; however, it is not established in the general case. This paper analytically computes the rank relation and proposes a method to extract the rate k/n convolutional code parameters. The method uses the Gaussian elimination with row pivoting (GERP) algorithm to estimate the rank and null space of $\mathbf{C}^{(l)}$. The proposed algorithm is based on a threshold value. Hence, an appropriate threshold will be proposed based on the Minimax decision rule.

Keywords: Convolutional code, parameter estimation, non-cooperative communication, dual code, constraint length.

تاریخ ارسال مقاله: ۹۴/۹/۲
تاریخ اصلاح مقاله: ۹۴/۱۲/۲
تاریخ پذیرش مقاله: ۹۵/۲/۱۱
نام نویسنده مسئول: حسین خالقی بیزکی
نشانی نویسنده مسئول: ایران - تهران - تقاطع بزرگراه شهید بابایی و امام علی – دانشگاه صنعتی مالک اشتر – مجتمع دانشگاهی برق و الکترونیک

۱- مقدمه

کدهای تصحیح خطا یکی از اجزای اصلی سیستم‌های مخابراتی مدرن بوده و در بسیاری از کاربردهای عملی مورداستفاده قرار می‌گیرند. به‌عنوان‌مثال کد RS[۱] که یکی از معروف‌ترین کدهای تصحیح خطا است، به وفور در سیستم‌های ذخیره‌سازی داده استفاده می‌شود. یک کاربرد دیگر این کد در پنهان‌نگاری اطلاعات بر روی تصاویر ارسالی است. در این سیستم‌ها اطلاعات ارسالی پیش از پنهان‌نگاری توسط کد تصحیح خطا کد می‌شوند تا با تخریب‌های عمدی و یا غیرعمدی ایجادشده بر روی تصویر مقابله کند [۱]. با وجود گذشت نیم‌قرن از ابداع کدهای تصحیح خطا، کماکان تحقیقات بسیاری در زمینه کاربرد، طراحی و حتی بهینه‌سازی این کدها انجام می‌شود. به‌عنوان‌مثال محققین در [۲] الگوریتم جدیدی را برای کدگشایی کد LDPC[۲] که یکی از قدیمی‌ترین کدهای تصحیح خطا است، ارائه کرده‌اند.

در سیستم‌های مخابرات داده از کدهای تصحیح خطا برای مقابله با خطای کانال استفاده می‌شود. در این راستا فرستنده با استفاده از یک کدگذار مناسب چند بیت معنادار را به اطلاعات ارسالی اضافه می‌کند. در طرف گیرنده نیز یک کدگشای کانال مناسب از این افزونگی برای تشخیص و تصحیح خطای کانال بهره می‌برد. برای طراحی چنین کدگشایی باید پارامترهای کدگذار به‌طور کامل معلوم باشند. بااین‌حال در برخی از کاربردهای عملی مانند مخابرات غیراشتراکی[۳]، گیرنده این اطلاعات را در اختیار ندارد. در این حالت گیرنده (کور) باید ابتدا پارامترهای کدگذار را از رشته دریافتی تخمین زده و سپس کدگشای مناسب را بر مبنای این پارامترها انتخاب کند. یکی از کاربردهای مهم این سیستم در گیرنده‌های رادیو-شناختی[۴] است. گیرنده رادیو-شناختی گیرنده‌ای کور است که خود را بر اساس پارامترهای تخمینی تنظیم می‌کند. یک کاربرد دیگر این سیستم در زمینه استراق سمع است که در آن کاربری غیرمجاز قصد دارد تا اطلاعات مبادله‌شده بین دو سیستم مخابراتی را شنود کند.

کد کانولوشنال[۵] یقیناً یکی از پرکاربردترین کدهای کانال است. این کد هم به‌صورت تنها، هم به‌صورت موازی با کدهای کانولوشنال دیگر و هم به‌صورت سریال با کدهای بلوکی به کار می‌رود. لذا در این مقاله سعی بر آن است تا به مسئله تخمین پارامترهای کدگذار کانولوشنال در شرایط نویزی پرداخته شود. تاکنون روش‌های معدودی برای حل این مسئله پیشنهاد شده است. برای اولین بار در [۳] روشی جبری برای تخمین پارامترهای کد کانولوشنال نرخ $1/n$ در حالت غیرنویزی ارائه شد که محققین در [۴، ۵] آن را به نرخ k/n توسعه دادند. در [۶، ۷] از الگوریتم اقلیدسی[۶] برای تخمین ماتریس مولد کد کانولوشنال نرخ 1/2 در شرایط غیرنویزی استفاده شد. محققین در [۸] نیز یک روش مبتنی بر نسبت شبیه‌نمایی لگاریتمی[۷] را برای تخمین کد کانولوشنال در شرایط نویزی ارائه دادند. در این روش که دارای پیچیدگی بسیار زیادی است، طول کلمات کد دریافتی باید از قبل معلوم باشد. پیچیدگی این روش تا حدودی در [۹] کاهش یافته است. البته این بهبود در ازای محدود کردن فضای جستجوی پارامترهای کد حاصل شده است. درواقع این روش تنها صحت مجموعه‌ای از پارامترهای مفروض را بررسی می‌کند.

روش تخمین مبتنی بر مرتبه[۸] یکی از مؤثرترین و جامع‌ترین روش‌هایی که است که تاکنون زمینه تخمین پارامترهای کد کانولوشنال پیشنهاد شده است. علیرغم تمام روش‌هایی که در [۹-۳] پیشنهاد شده‌اند، این روش قادر است تمام پارامترهای کد کانولوشنال را با پیچیدگی بسیار پایین در شرایط نویزی تخمین بزند. این روش تاکنون بیش‌ترین قسمت تحقیقات را در زمینه تخمین پارامترهای کد کانولولشنال به خود اختصاص داده است. این روش نخستین بار در [۱۰] برای تعیین پارامترهای کد کانولوشنال نرخ $(n\text{-}1)/n$ پیشنهاد شد. در این روش رشته دریافتی به ازای طول‌های $l=1,\ldots,l_{\max}$ به‌صورت سطری در ماتریس‌های l-ستونی $\mathbf{C}^{(l)}$ قرار گرفته و سپس پارامترهای کد بر مبنای مرتبه این ماتریس‌ها محاسبه می‌شوند. البته برای انجام این کار باید رابطه بین پارامترهای کد و مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ معلوم باشد. در این راستا محققین در [۱۰] رابطه‌ای تجربی را برای مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ در کدهای نرخ $(n\text{-}1)/n$ پیشنهاد دادند. در [۱۱] نیز این رابطه تجربی بدون ارائه هیچگونه اثبات ریاضی به نرخ k/n تعمیم داده شد. در ادامه محققین در [۱۴-۱۲] روش تخمین مبتنی بر مرتبه را به حالت نویزی توسعه دادند. آن‌ها برای انجام این کار از روشی موسوم به حذف گوسی با انتخاب رهبر سطری[۹] (GERP) برای تخمین مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ در شرایط نویزی استفاده کردند. در [۱۵، ۱۶] از این روش برای تعیین پارامترهای کد کانولوشنال سوراخ‌شده[۱۰] استفاده شد. مراجع [۱۷، ۱۸] نیز عملکرد این روش را بر مبنای قاعده تصمیم‌گیری نرم بهبود دادند.

لازم به ذکر است که الگوریتم‌های پیشنهادی در [۱۸-۱۰] کاملاً بر پایه روابط تجربی ارائه‌شده در [۱۰، ۱۱] استوار هستند. بااین‌حال در [۱۹] با ارائه مثال‌های نقضی ثابت شد که این روابط تجربی برای کدهای نرخ k/n برقرار نیستند. این مسئله صحت الگوریتم‌هایی که در کارهای پیشین برای تخمین پارامترهای کد کانولوشنال نرخ k/n پیشنهاد شد را زیر سوال می‌برد.

با توجه به مطالب فوق، یافتن مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ در نرخ k/n مسئله‌ای بسیار مهم در تخمین پارامترهای کد کانولوشنال است که تاکنون به‌طور کامل حل نشده است. لذا در این مقاله ابتدا رابطه‌ای تحلیلی و جامع برای مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ پیشنهاد می‌شود. این رابطه که بر پایه خواص جبری کد کانولوشنال حاصل می‌شود [۲۲-۲۰]، وابستگی بین مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ و پارامترهای کد کانولوشنال نرخ k/n را به‌طور کامل آشکار می‌کند. به علاوه این رابطه ثابت می‌کند که رابطه مورداستفاده در کارهای پیشین تنها به ازای کدهای نرخ $(n\text{-}1)/n$ برقرار است. سپس بر مبنای این رابطه تحلیلی، الگوریتمی جامع برای تخمین پارامترهای کد کانولوشنال نرخ k/n پیشنهاد می‌شود. البته این روش نیز نیازمند تخمین مرتبه ماتریس‌های

$\mathbf{C}^{(l)}$ در شرایط نویزی است که ما برای انجام این کار از روش GERP استفاده می‌کنیم. با توجه به اینکه این روش در کارهای پیشین با اندکی ابهام ارائه شده است، این مقاله در بخشی مجزا به معرفی این روش پرداخته و شرایط لازم برای عملکرد صحیح آن را بیان می‌کند. به‌علاوه یک حد آستانه مناسب بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه[۱۱] برای این روش پیشنهاد می‌شود.

این مقاله در ادامه به این صورت تنظیم شده است؛ در بخش ۲ مهم‌ترین خواص کد کانولوشنال به طور مختصر بیان می‌شوند. سپس بخش ۳ به تشریح مسائل مطرح در زمینه تخمین پارامترهای کد کانولوشنال نرخ k/n در شرایط نویزی می‌پردازد. در بخش ۴ روش GERP به‌طور مختصر معرفی شده و یک حد آستانه مناسب برای آن پیشنهاد می‌شود. در بخش ۵ یک رابطه تحلیلی جامع برای مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ در نرخ k/n ارائه خواهد شد. سپس در بخش ۶ الگوریتمی جامع برای تخمین پارامترهای کد کانولوشنال پیشنهاد می‌شود. به‌منظور ارزیابی الگوریتم پیشنهادی، در بخش ۷ چند مثال شبیه‌سازی به همراه منحنی‌های عملکرد ارائه می‌شود. نهایتاً بخش ۸ نتایج این مقاله را به‌طور مختصر جمع‌بندی می‌کند.

۲- توصیف ریاضی کد کانولوشنال

حافظه یکی از مهم‌ترین مشخصه‌های کدگذارهای کانولوشنال است. بر خلاف کدگذارهای بلوکی، خروجی یک کدگذار کانولوشنال در هر لحظه به ورودی در لحظات قبلی بستگی دارد. به همین دلیل معمولاً کدگذارهای کانولوشنال را با ماتریس‌های چندجمله‌ای مولد نمایش می‌دهند. در این روش نمایش، یک کدگذار کانولوشنال نرخ k/n می‌تواند با ماتریس چندجمله‌ای مولد زیر توصیف شود:

$$\mathbf{G}(D)=\begin{bmatrix} g_{11}(D) & \dots & g_{1,n}(D) \\ \vdots & \ddots & \vdots \\ g_{k1}(D) & \dots & g_{kn}(D) \end{bmatrix} \quad (۱)$$

که در آن D عملگر تأخیر و $g_{ij}(D)$ تابع انتقال بین ورودی iام و خروجی jام کدگذار است. اگر بین ورودی iاُم و خروجی jام کدگذار بازخورد وجود داشته باشد، آنگاه مؤلفه $g_{ij}(D)$ کسری خواهد بود.

فرض کنید $u_i(D)$ و $c_j(D)$ به ترتیب چندجمله‌ای‌های متناظر با رشته ورودی iاُم و رشته خروجی jاُم باشند. آنگاه اگر بردارهای چندجمله‌ای ورودی و خروجی کدگذار را به ترتیب با $U(D)=\left[u_1(D)..u_k(D)\right]$ و $C(D)=\left[c_1(D)..c_n(D)\right]$ نمایش دهیم، فرآیند کدگذاری می‌تواند به‌صورت زیر نوشته شود [۲۰، ۲۱]:

$$C(D)=U(D).\mathbf{G}(D) \quad (۲)$$

مجموعه بردارهای تولیدشده توسط $\mathbf{G}(D)$ یک فضای چندجمله‌ای k-بعدی را به‌صورت زیر ایجاد می‌کند:

$$\mathcal{C}=\left\{U(D).\mathbf{G}(D)\,|\,\forall U(D)\in\mathbb{F}_2^k(D)\right\} \quad (۳)$$

که در آن $\mathbb{F}_2^k(D)$ میدان چندجمله‌ای‌های باینری k-تایی است. توجه داشته باشید که سطرهای $\mathbf{G}(D)$ در حقیقت مجموعه‌ای پایه را برای فضای کد $\mathcal{C}$ تشکیل می‌دهند. با توجه به این نکته می‌توان چندین ماتریس مولد دیگر نیز یافت که فضای $\mathcal{C}$ را تولید می‌کنند. ما مجموعه این ماتریس‌های مولد معادل را با $\mathbb{G}_{\mathcal{C}}$ نشان می‌دهیم.

فرض کنید $\mathcal{R}_{\mathbf{G}}$ مجموعه‌ای شامل تمام سطرهای ماتریس $\mathbf{G}(D)$ باشد. اگر به ازای هر ماتریس $\mathbf{G}(D)\in\mathbb{G}_{\mathcal{C}}$ رابطه زیر برقرار باشد، آنگاه به ماتریس مولد $\mathbf{G}_m(D)$ کمین-پایه[۱۲] گفته می‌شود [۲۰، ۲۱]:

$$\sum_{C(D)\in\mathcal{R}_{\mathbf{G}}}\deg(C(D))\geq\sum_{C_m(D)\in\mathcal{R}_{\mathbf{G}_m}}\deg(C_m(D)) \quad (۴)$$

در این رابطه $\deg(C(D))$ برابر با بزرگ‌ترین درجه چندجمله‌ای در بردار $C(D)$ است. ما $\mathcal{R}_{\mathbf{G}_m}$ را یک مجموعه کمین-پایه برای فضای کد $\mathcal{C}$ نامیده و بردارهای آن را به ترتیب از کم‌ترین درجه به بیش‌ترین درجه شماره‌گذاری می‌کنیم. اگر $C_m^i(D)$ iاُمین بردار در مجموعه $\mathcal{R}_{\mathbf{G}_m}$ باشد، آنگاه قیود طول[۱۳] فضای کد $\mathcal{C}$ به‌صورت زیر تعریف می‌شوند [۲۰، ۲۱]:

$$\mu_i=\deg(C_m^i(D))\quad;\quad i=1,\dots,k \quad (۵)$$

متعاقباً قید طول بیشینه و قید طول مجموع به‌صورت زیر قابل تعریف هستند:

$$\mu=\max_{i=1,\dots,k}\mu_i \quad (۶)$$

$$\nu=\sum_{i=1}^{k}\mu_i \quad (۷)$$

توجه داشته باشید که قیود طول در حقیقت جزئی از پارامترهای فضای کد بوده و به نوع کدگذار بستگی ندارند. به همین دلیل غالباً کد کانولوشنال $\mathcal{C}$ را به‌صورت $\mathcal{C}(n,k,\nu)$ نمایش می‌دهند.

فرض کنید $\mathcal{C}^{\perp}$ فضای دوگان کد $\mathcal{C}$ باشد. آنگاه $\mathcal{C}^{\perp}$ نیز یک کد کانولوشنال با ابعاد $n-k$ و قید طول مجموع ν است [۲۰، ۲۱]. درنتیجه اگر $\mu_i^{\perp}, i=1,\dots,n-k$ قیود طول فضای $\mathcal{C}^{\perp}$ باشند، خواهیم داشت:

$$\nu=\sum_{i=1}^{k}\mu_i=\sum_{i=1}^{n-k}\mu_i^{\perp} \quad (۸)$$

قید طول بیشینه در فضای $\mathcal{C}^{\perp}$ با $\mu^{\perp}$ نشان داده می‌شود؛ یعنی $\mu^{\perp}=\mu_{n-k}^{\perp}$. فرض کنید $\mathbb{H}_{\mathcal{C}}$ مجموعه تمام ماتریس‌های بررسی توازن[۱۴] فضای کد $\mathcal{C}$ (و یا مجموعه تمام ماتریس‌های مولد فضای کد $\mathcal{C}^{\perp}$) باشد. آنگاه به ازای ماتریس‌های $\mathbf{G}(D)\in\mathbb{G}_{\mathcal{C}}$ و $\mathbf{H}(D)\in\mathbb{H}_{\mathcal{C}}$ رابطه زیر برقرار است:

$$\mathbf{G}(D).\mathbf{H}^T(D)=\mathbf{0}_{k\times n-k} \quad (۹)$$

با الانویس T در این رابطه عملگر ترانهاده بوده و $\mathbf{0}_{k\times n-k}$ نیز یک ماتریس صفر با ابعاد $k\times n-k$ است. همچنین برای هر بردار $H(D)\in\mathcal{C}^{\perp}$ داریم:

$$\mathbf{G}(D).H^T(D)=0_{k\times 1} \quad (۱۰)$$

فرض کنید $\mathbf{G}(D)\in\mathbb{G}_{\mathcal{C}}$ یک ماتریس مولد با درجه بیشینه m بوده و $g_{ij}(D)=g_{ij}^0+g_{ij}^1D+\dots+g_{ij}^mD^m$ نیز مؤلفه (i,j) اُم آن باشد. آنگاه ماتریس چندجمله‌ای مولد $\mathbf{G}(D)$ می‌تواند به شکل زیر در قالب یک ماتریس نیمه-نامتناهی باینری توصیف شود [۲۲]:

$$\mathbf{G}=\begin{bmatrix}\mathbf{G}_0 & \mathbf{G}_1 & \mathbf{G}_2 & \cdots & \mathbf{G}_m & \mathbf{0} & \mathbf{0} & \cdots\\ & \mathbf{G}_0 & \mathbf{G}_1 & \cdots & \mathbf{G}_{m-1} & \mathbf{G}_m & \mathbf{0} & \cdots\\ & & \mathbf{G}_0 & \cdots & \mathbf{G}_{m-2} & \mathbf{G}_{m-1} & \mathbf{G}_m & \cdots\\ & & & \ddots & \vdots & \vdots & \vdots & \\ & & & & \mathbf{G}_0 & \mathbf{G}_1 & \mathbf{G}_2 & \cdots\\ & & & & & \mathbf{G}_0 & \mathbf{G}_1 & \cdots\\ & & \mathbf{0} & & & & \mathbf{G}_0 & \cdots\\ & & & & & & & \ddots\end{bmatrix} \qquad (۱۱)$$

که در آن $\mathbf{G}_i$ زیرماتریسی با ابعاد $k\times n$ است که به‌صورت زیر تعریف می‌شود:

$$\mathbf{G}_i=\begin{bmatrix} g_{11}^{i} & \cdots & g_{1n}^{i}\\ \vdots & \ddots & \vdots\\ g_{k1}^{i} & \cdots & g_{kn}^{i}\end{bmatrix} \quad ; \quad i=1,\ldots,m \qquad (۱۲)$$

در این شیوه نمایش، رابطه (۲) می‌تواند به شکل زیر بازنویسی شود:

$$C=U.\mathbf{G} \qquad (۱۳)$$

که در آن U و C به ترتیب بردارهای متناظر با رشته‌های سریال ورودی و خروجی کدگذار هستند.

۳- بیان مسئله

فرض کنید C بردار باینری متناظر با رشته خروجی یک کدگذار کانولوشنال نرخ k/n با ماتریس مولد $\mathbf{G}(D)$ باشد. این بردار از طریق یک کانال نویزی به کدگشای کانال در گیرنده کور وارد می‌شود (منظور از کانال مجموعه تمام بلوک‌هایی هستند که بین کدگذار در فرستنده و کدگشا در گیرنده قرار می‌گیرند، مانند مدولاتور، کانال انتقال فیزیکی، دمدولاتور و ...). لذا بردار دریافتی یک نسخه تغییر یافته بردار C است که می‌تواند به شکل زیر نوشته شود:

$$Y=C+E \qquad (۱۴)$$

در این رابطه E بردار خطای حاصل از کانال نویزی است. گیرنده باید بر مبنای بردار Y تمام پارامترهای کدگذار کانولوشنال (مانند n، k و ν) را تخمین بزند. اما پیش از آن باید نحوه تعیین پارامترهای کد از روی بردار خروجی C مشخص شود؛ زیرا رشته دریافتی Y یک نسخه تغییر یافته بردار C است. ابتدا توجه داشته باشید که هر بردار C متناظر با یک بردار چندجمله‌ای در فضای کد $\mathcal{C}(n,k,\nu)$ است. درنتیجه از خروجی کدگذار (و متعاقبا از رشته دریافتی) می‌توان حداکثر پارامترهای فضای کد $\mathcal{C}$ را تعیین کرد. این پارامترها عبارت‌اند از طول کلمات کد (n)، ابعاد فضای کد (k) و قید طول مجموع (ν). البته ماتریس مولد کدگذار در این مجموعه قرار نمی‌گیرد؛ زیرا به ازای هر کد چندین ماتریس مولد معادل وجود دارند. لذا ماتریس مولد کدگذار از روی رشته‌های دریافتی قابل تشخیص نبوده و در بهترین حالت می‌توان یک ماتریس معادل با $\mathbf{G}(D)$ را یافت؛ به‌عنوان‌مثال امکان تشخیص ماتریس مولد سیستماتیک وجود دارد. تخمین ماتریس مولد سیستماتیک به دلیل کاربرد وسیع آن از اهمیت ویژه‌ای برخوردار است.

فرض کنید L طول بردار C بوده و c_i نیز مؤلفه iام آن باشد. آنگاه به ازای هر مقدار $l=1,\ldots,l_{\max}$ ($\left\lfloor \frac{L}{l_{max}} \right\rfloor \geq 2l_{max}$) می‌توان بردار C را به شکل زیر به بردارهایی با طول l تفکیک کرد:

$$C_i^{(l)}=[c_{(i-1)l+1}\cdots c_{il}]^T \quad ; \quad i=1,2,\ldots,\left\lfloor \frac{L}{l} \right\rfloor \qquad (۱۵)$$

سپس به ازای هر یک از طول‌های $l=1,\ldots,l_{\max}$، ماتریس $\mathbf{C}^{(l)}$ با ابعاد $\left\lfloor \frac{L}{l} \right\rfloor \times l$ ساخته می‌شود:

$$\mathbf{C}^{(l)}=[C_1^{(l)}\, C_2^{(l)}\cdots C_{\left\lfloor \frac{L}{l} \right\rfloor}^{(l)}]^T \qquad (۱۶)$$

ماتریس $\mathbf{C}^{(l)}$ یک ماتریس خروجی نامیده می‌شود. برای نخستین بار در [۱۰] نشان داده شد که بین مرتبه ماتریس‌های خروجی و پارامترهای کد رابطه معناداری وجود دارد. بر این اساس ماتریس‌های خروجی می‌توانند برای تعیین پارامترهای کد استفاده شوند. البته برای انجام این کار باید ابتدا به سوال زیر پاسخ داده شود:

سوال ۱: رابطه بین پارامترهای فضای کد $\mathcal{C}$ و ماتریس‌های خروجی $\mathbf{C}^{(l)}, l=1,\ldots,l_{max}$ چیست؟

در پاسخ به این سوال رابطه‌ای تجربی در [۱۰، ۱۱] برای مرتبه ماتریس‌های خروجی پیشنهاد شد. این رابطه به‌طور مکرر در تحقیقات بعدی نیز مورداستفاده قرار گرفته است [۱۹-۱۰]. اما همان‌گونه که پیش از این نیز اشاره شد، این رابطه برای کدهای نرخ k/n برقرار نیست. به همین دلیل این رابطه به‌صورت کاملاً تحلیلی در بخش ۵ محاسبه می‌شود.

حال فرض کنید که کانال انتقال بدون نویز باشد. در این حالت گیرنده یک نسخه بدون خطا از تمام ماتریس‌های خروجی $\mathbf{C}^{(l)}$ را در اختیار دارد. لذا گیرنده به راحتی می‌تواند مرتبه تمام ماتریس‌های خروجی را تعیین کند. در این حالت تنها باید به سوال زیر پاسخ داده شود:

سوال ۲: چگونه می‌توان پارامترهای فضای کد $\mathcal{C}$ را از مرتبه ماتریس‌های خروجی $\mathbf{C}^{(l)}, l=1,\ldots,l_{max}$ تعیین کرد؟

در مراجع [۱۸-۱۰] روش‌هایی بر مبنای رابطه تجربی مرتبه در پاسخ به این سوال پیشنهاد شده است. اما تمام این روش‌ها تنها به ازای کدهای نرخ $(n\text{-}1)/n$ کارایی دارند؛ زیرا رابطه تجربی مرتبه تنها در نرخ $(n\text{-}1)/n$ برقرار است. به همین دلیل در بخش ۶ الگوریتمی جامع را برای تخمین پارامترهای کد کانولوشنال نرخ k/n پیشنهاد می‌شود.

حال یک کانال انتقال نویزی را در نظر بگیرید. در این حالت گیرنده یک نسخه تغییریافته از ماتریس‌های خروجی را به شکل زیر در اختیار دارد:

$$\mathbf{Y}^{(l)}=\mathbf{C}^{(l)}+\mathbf{E}^{(l)} \quad ; \quad l=1,\ldots,l_{\max} \qquad (۱۷)$$

در این رابطه $\mathbf{Y}^{(l)}$ و $\mathbf{E}^{(l)}$ به ترتیب ماتریس‌های متناظر با بردار دریافتی Y و بردار خطای E هستند. در این حالت یک سوال جدید مطرح می‌شود:

سوال ۳: چگونه می‌توان مرتبه ماتریس خروجی $\mathbf{C}^{(l)}$ را از ماتریس دریافتی نویزی $\mathbf{Y}^{(l)}$ تعیین کرد؟

الگوریتم GERP پاسخ بسیار مناسبی برای این سوال است. این روش برای اولین بار در [۱۰] پیشنهاد شده و در کارهای بعدی نیز مورداستفاده قرار گرفته است. این روش به‌طور مختصر در بخش ۴ معرفی می‌شود.

مسئله تخمین کدگذار کانولوشنال به‌صورت کاملاً شماتیک در شکل ۱ رسم شده است. این شکل جایگاه مسائل طرح‌شده در این بخش را به‌طور واضح مشخص می‌کند.

۴- تخمین مرتبه و فضای تهی ماتریس‌های خروجی

الگوریتمی که در این مقاله برای تخمین پارامترهای کد کانولوشنال پیشنهاد خواهد شد، نیازمند تخمین مرتبه و فضای تهی ماتریس‌های خروجی است. ما برای تخمین این پارامترها از روش GERP استفاده می‌کنیم. این روش در زیربخش‌های پیش‌رو به‌طور کامل توضیح داده شده و شرایط لازم برای عملکرد صحیح آن بیان می‌شود. همچنین یک حد آستانه مناسب بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه برای آن پیشنهاد می‌شود.

۴-۱- روش GERP

برای توضیح بهتر این روش، ابتدا حالت غیرنویزی بررسی می‌شود. در حالت بدون نویز، ماتریس دریافتی $\mathbf{Y}^{(l)}$ برابر با ماتریس خروجی $\mathbf{C}^{(l)}$ است. در روش GERP، عملیات حذف گوسی به‌صورت ستونی بر روی ماتریس $\mathbf{Y}^{(l)}$ اعمال شده و آن را به ماتریس پایین-مثلثی $\hat{\mathbf{Y}}^{(l)}$ تبدیل می‌کند. البته در این روش انتخاب عناصر رهبر[۱۵] به‌صورت سطری انجام می‌شود (یک عنصر رهبر مؤلفه‌ای است که از آن برای صفر کردن سایر مؤلفه‌های سطر استفاده می‌شود). این عملیات می‌تواند به‌صورت ماتریسی زیر نمایش داده شود [۱۰، ۱۱]:

$$\hat{\mathbf{Y}}^{(l)} = \mathbf{P}^{(l)}.\mathbf{Y}^{(l)}.\mathbf{Q}^{(l)} \qquad (۱۸)$$

در این رابطه $\mathbf{P}^{(l)}$ ماتریسی با ابعاد $L \times L$ است که جابجایی مناسب سطرهای رهبر را به بالای ماتریس انجام می‌دهد. ماتریس بالا-مثلثی $\mathbf{Q}^{(l)}$ نیز ماتریسی با ابعاد $l \times l$ است که عملیات ستونی لازم برای تبدیل $\mathbf{Y}^{(l)}$ به ماتریس پایین-مثلثی $\hat{\mathbf{Y}}^{(l)}$ را نشان می‌دهد. اگر مرتبه ماتریس $\mathbf{Y}^{(l)}$ کامل باشد، هیچکدام از ستون‌های ماتریس $\hat{\mathbf{Y}}^{(l)}$ تمام-صفر نیستند؛ ولی اگر مرتبه برابر با $r_l < l$ باشد، انتظار می‌رود که دقیقاً $l - r_l$ ستون ماتریس $\hat{\mathbf{Y}}^{(l)}$ تمام-صفر باشند. حال فرض کنید که ستون iام ماتریس $\hat{\mathbf{Y}}^{(l)}$ تمام-صفر بوده و Q_i نیز ستون iام ماتریس $\mathbf{Q}^{(l)}$ باشد. در این صورت بر طبق رابطه (۱۸) خواهیم داشت:

$$\mathbf{Y}^{(l)}.Q_i = 0_{1\times k} \qquad (۱۹)$$

با توجه به این رابطه می‌توان گفت که بردار Q_i در فضای تهی ماتریس‌های $\mathbf{Y}^{(l)}$ و $\mathbf{C}^{(l)}$ قرار دارد. لذا از این ویژگی ساده می‌توان برای تخمین مرتبه و فضای تهی ماتریس‌های خروجی در شرایط غیرنویزی استفاده کرد.

در حالت نویزی، روش فوق با چند چالش جدی روبرو می‌شود. فرض کنید رشته دریافتی نویزی بوده و بردار Q نیز متعلق به فضای تهی ماتریس $\mathbf{C}^{(l)}$ باشد. آنگاه با توجه به رابطه (۱۹) می‌توان نوشت:

$$S = \mathbf{Y}^{(l)}.Q = (\mathbf{C}^{(l)} + \mathbf{E}^{(l)}).Q = \mathbf{E}^{(l)}.Q \qquad (۲۰)$$

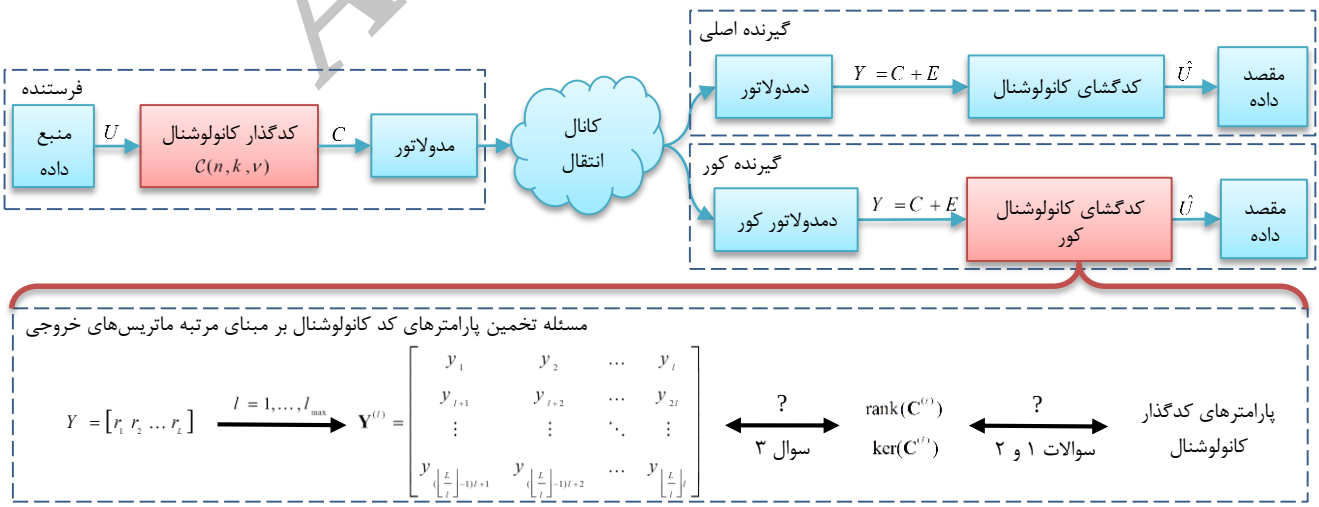
اگر s_i مؤلفه iاُم بردار S باشد، آنگاه خواهیم داشت:

$$s_i = Y_i^{(l)}Q = (C_i^{(l)} + E_i^{(l)})Q = E_i^{(l)}Q \qquad (۲۱)$$

در این رابطه $Y_i^{(l)}$ و $E_i^{(l)}$ به ترتیب سطرهای iام ماتریس‌های $\mathbf{Y}^{(l)}$ و $\mathbf{E}^{(l)}$ هستند. حال فرض کنید که w تعداد عناصر غیرصفر (وزن همینگ[۱۶]) بردار Q باشد. همچنین فرض کنید عناصر غیرصفر Q در محل‌های $j_1, j_2, \ldots, j_w$ قرار داشته باشند. در این صورت رابطه (۲۱) می‌تواند به‌صورت زیر نوشته شود:

$$s_i = e_{i,j_1}^{(l)} + e_{i,j_2}^{(l)} + \ldots + e_{i,j_w}^{(l)} \qquad (۲۲)$$

که در آن $e_{i,j}^{(l)}$ مؤلفه jاُم بردار $E_i^{(l)}$ است. درنتیجه اگر تعداد خطاها در محل‌های $j_1, j_2, \ldots, j_w$ عددی زوج باشد، مقدار s_i برابر با صفر و در غیر این صورت برابر با یک می‌شود.



شکل ۱: ترسیم مسئله تخمین پارامترهای کدگذار کانولوشنال با استفاده از روش تخمین مبتنی بر مرتبه

حال اگر کانال انتقال به‌صورت یک کانال باینری متقارن[۱۷] (BSC) با احتمال خطای ε در نظر گرفته شود، احتمال یک بودن مؤلفه s_i (و یا فرد بودن تعداد خطاها) برابر با رابطه زیر می‌شود:

$$\varepsilon_s^{(w)} = \Pr(s_i = 1) = 1 - \sum_{t=0}^{\left[\frac{w}{2}\right]} \binom{w}{2t} \varepsilon^{2t} (1-\varepsilon)^{l-2t} \qquad (۲۳)$$

با اندکی محاسبات ریاضی می‌توان این رابطه را به شکل زیر ساده کرد:

$$\varepsilon_s^{(w)} = \frac{1-(1-2\varepsilon)^w}{2} \qquad (۲۴)$$

متعاقباً با توجه به اینکه متغیرهای تصادفی $s_i, i = 1,2,\ldots,\left[\frac{L}{l}\right]$ دوبه‌دو نسبت به هم مستقل هستند، رابطه احتمال زیر حاصل می‌شود:

$$\Pr(\mathrm{wt}(S) = z) = \binom{\left[\frac{L}{l}\right]}{z} (\varepsilon_s^{(w)})^z (1-\varepsilon_s^{(w)})^{\left[\frac{L}{l}\right]-z} \qquad (۲۵)$$

که در آن $\mathrm{wt}(.)$ وزن همینگ بردار موردنظر را نشان می‌دهد. در نتیجه وزن همینگ بردار S دارای یک توزیع دوجمله‌ای[۱۸] با میانگین $m_{w,l} = \left[\frac{L}{l}\right].\varepsilon_s^{(w)}$ و واریانس $\sigma^2_{w,l} = \left[\frac{L}{l}\right].\varepsilon_s^{(w)}(1-\varepsilon_s^{(w)})$ است. توجه داشته باشید که روابط (۲۵-۲۰) تنها در صورتی برقرار هستند که بردار Q متعلق به فضای تهی ماتریس $\mathbf{C}^{(l)}$ باشد. در مقابل اگر بردار Q متعلق به فضای تهی $\mathbf{C}^{(l)}$ نباشد، می‌توان به سادگی نشان داد که $\mathrm{wt}(S)$ دارای یک توزیع دوجمله‌ای با میانگین $\hat{m}_{w,l} = \left[\frac{L}{l}\right]/2$ و واریانس $\hat{\sigma}^2_{w,l} = \left[\frac{L}{l}\right]/4$ است ($\hat{\varepsilon}_s^{(w)} = \frac{1}{2}$). لذا $\mathrm{wt}(S)$ در حالت کلی می‌تواند دارای توزیع‌های احتمال زیر باشد:

$$\mathrm{wt}(S) \sim \begin{cases} \mathcal{B}\left(\left[\frac{L}{l}\right], \varepsilon_s^{(w)}\right) & ; \quad Q \in \ker(\mathbf{C}^{(l)}) \\ \mathcal{B}\left(\left[\frac{L}{l}\right], \frac{1}{2}\right) & ; \quad Q \notin \ker(\mathbf{C}^{(l)}) \end{cases} \qquad (۲۶)$$

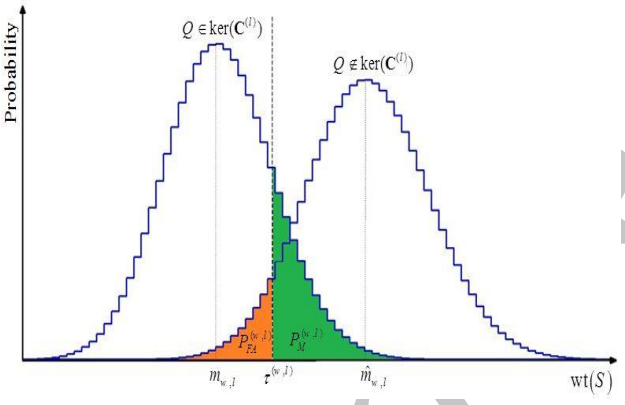
که در آن $\ker(\mathbf{C}^{(l)})$ فضای تهی ماتریس $\mathbf{C}^{(l)}$ بوده و $\mathcal{B}(.,.)$ نیز نشان‌دهنده یک توزیع دوجمله‌ای است. توزیع‌های احتمال $\mathrm{wt}(S)$ در شکل ۲ رسم شده‌اند. همان‌گونه که در این شکل نیز دیده می‌شود، از تفاوت بین توزیع‌های احتمال $\mathrm{wt}(S)$ می‌توان برای تشخیص بردارهای فضای تهی ماتریس $\mathbf{C}^{(l)}$ استفاده کرد. برای انجام این کار باید یک حد آستانه بین مقادیر $m_{w,l}$ و $\hat{m}_{w,l}$ انتخاب شده و با وزن همینگ بردار S مقایسه شود. اگر مقدار $\mathrm{wt}(S)$ کم‌تر از حد آستانه باشد، بردار Q به‌عنوان بردار تهی ماتریس $\mathbf{C}^{(l)}$ معرفی می‌شود.

در روش GERP ستون‌های ماتریس $\mathbf{Q}^{(l)}$ مورد آزمایش حد آستانه قرار می‌گیرند. لذا تشخیص صحیح هر بردار تهی مشروط به حضور آن در یکی از ستون‌های ماتریس $\mathbf{Q}^{(l)}$ است. فرض کنید $\mathbf{Y}_s^{(l)}$ زیرماتریسی شامل l سطر اول ماتریس $\mathbf{P}^{(l)}\mathbf{Y}^{(l)}$ (ماتریس $\mathbf{Y}^{(l)}$ بعد از جابجایی سطرها) باشد؛ یعنی:

$$\mathbf{P}^{(l)}\mathbf{Y}^{(l)} = \begin{bmatrix} \mathbf{Y}_s^{(l)} \\ \mathbf{Y}_t^{(l)} \end{bmatrix} \qquad (۲۷)$$

آنگاه واضح است که عملیات حذف گوسی تنها بر مبنای سطرهای زیرماتریس انجام می‌شود. پس ستون‌های ماتریس $\mathbf{Q}^{(l)}$ تنها به زیرماتریس $\mathbf{Y}_s^{(l)}$ وابسته هستند. لذا لازمه عملکرد صحیح الگوریتم GERP آن است که زیرماتریس $\mathbf{Y}_s^{(l)}$ تا حد ممکن بدون خطا باشد. البته احتمال برقراری این شرط با افزایش قدرت نویز کانال و همچنین ابعاد زیرماتریس $\mathbf{Y}_s^{(l)}$ کاهش می‌یابد. یک روش ساده برای کاهش این اثر، انتخاب زیرماتریس‌های مختلف از ماتریس $\mathbf{Y}^{(l)}$ است[۱۲، ۱۳]. برای انجام این کار می‌توان سطرهای ماتریس $\mathbf{Y}^{(l)}$ را قبل از انجام عملیات حذف گوسی به‌صورت تصادفی جابه‌جا کرد.

نهایتاً باید اشاره شود که پیچیدگی محاسباتی روش GERP برای تخمین فضای تهی $\mathbf{C}^{(l)}$ از درجه $\mathcal{O}(\left[\frac{L}{l}\right].l^2)$ است؛ زیرا ستون‌های $\left[\frac{L}{l}\right]$-بیتی ماتریس $\mathbf{Y}^{(l)}$ حداکثر $\frac{l(l+1)}{2}$ بار با هم ترکیب می‌شوند. البته برای محاسبه پیچیدگی کل باید این مقدار را در تعداد دفعاتی که الگوریتم حذف گوسی تکرار می‌شود، ضرب نمود.



شکل ۲: توزیع‌های احتمال وزن همینگ بردار S

۴-۲- پیشنهاد حد آستانه بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه

فرض کنید $P_{FA}^{(w,l)}$ احتمال این پیشامد باشد که یک بردار با وزن همینگ w اشتباهاً به‌عنوان یک بردار فضای تهی ماتریس $\mathbf{C}^{(l)}$ معرفی شود. اگر یک بردار متعلق به فضای تهی $\mathbf{C}^{(l)}$ نباشد، وزن همینگ بردار S آن دارای توزیع $\mathcal{B}(\left[\frac{L}{l}\right], \frac{1}{2})$ است. لذا احتمال $P_{FA}^{(w,l)}$ می‌تواند به‌صورت زیر نوشته شود:

$$P_{FA}^{(w,l)} = F(\tau^{(w,l)}, \left[\frac{L}{l}\right], \frac{1}{2}) = (\frac{1}{2})^{\left[\frac{L}{l}\right]} \sum_{z=0}^{\tau^{(w,l)}-1} \binom{\left[\frac{L}{l}\right]}{z} \qquad (۲۸)$$

که در آن $\tau^{(w,l)}$ حد آستانه متناظر با بردارهایی است که دارای وزن همینگ w هستند. $F(\tau^{(w,l)}, \left[\frac{L}{l}\right], \frac{1}{2})$ نیز تابع توزیع تجمعی متناظر با

توزیع دوجمله‌ای $\mathcal{B}(\left\lfloor \frac{L}{l} \right\rfloor, \frac{1}{2})$ است. در شکل ۲، ناحیه متناظر با $P_{FA}^{(w,l)}$ به‌صورت هاشور خورده در سمت چپ حد آستانه مشخص شده است.

فرض کنید $P_M^{(w,l)}$ احتمال عدم تشخیص صحیح یک بردار تهی با وزن همینگ w باشد. اگر برداری متعلق به فضای تهی ماتریس $\mathbf{C}^{(l)}$ باشد، آنگاه وزن همینگ بردار S آن دارای توزیع دوجمله‌ای $\mathcal{B}(\left\lfloor \frac{L}{l} \right\rfloor, \varepsilon_s^{(w)})$ است. لذا احتمال $P_M^{(w,l)}$ برابر خواهد بود با:

$$P_M^{(l)}(w) = F(\tau^{(w,l)}, \left\lfloor \frac{L}{l} \right\rfloor, \varepsilon_s^{(w)}) = \sum_{z=\tau^{(w,l)}}^{\left\lfloor \frac{L}{l} \right\rfloor} \binom{\left\lfloor \frac{L}{l} \right\rfloor}{z} (\varepsilon_s^{(w)})^z (1-\varepsilon_s^{(w)})^{\left\lfloor \frac{L}{l} \right\rfloor - z} \quad (۲۹)$$

در شکل ۲، ناحیه متناظر با $P_M^{(w,l)}$ به‌صورت هاشور خورده در سمت راست حد آستانه مشخص شده است.

با توجه به تعاریف فوق، احتمال خطای مجموع می‌تواند به‌صورت زیر نوشته شود:

$$P_e^{(l)} = \sum_{w=0}^{l} \lambda^{(w,l)} P_M^{(w,l)} + (1-\lambda^{(w,l)}) P_{FA}^{(w,l)} \quad (۳۰)$$

که در آن $\lambda^{(w,l)}$ نسبت بردارهایی است که متعلق به فضای تهی ماتریس $\mathbf{C}^{(l)}$ بوده و دارای وزن همینگ w هستند. برای محاسبه حد آستانه بهینه باید احتمال خطای فوق برحسب مقدار $\tau^{(w,l)}$ کمینه گردد. توجه داشته باشید که حل این مسئله بهینه‌سازی نیازمند آگاهی کامل از مقادیر $\lambda^{(w,l)}$ است. البته این شرط در مسئله تخمین فضای تهی برقرار نیست؛ زیرا وزن همینگ بردارهای تهی را نمی‌توان پیش از تخمین آن‌ها تعیین کرد. البته این یک مشکل شایع در مسائل تصمیم‌گیری بهینه است که غالباً توسط قاعده تصمیم‌گیری حداقل-بیشینه حل می‌شود. این قاعده ساده و مؤثر در مسائلی استفاده می‌شود که توزیع‌های احتمال پیشین معلوم نیستند. این قاعده درواقع بیش‌ترین احتمال خطای ممکن را حداقل می‌کند. توجه داشته باشید که در مسئله تخمین فضای تهی، مقادیر $\lambda^{(w,l)}$ و $1-\lambda^{(w,l)}$ توزیع‌های احتمال پیشین مجهول هستند. برای یافتن حد آستانه بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه باید معادله زیر برحسب پارامتر $\tau^{(w,l)}$ حل شود [۲۳]:

$$P_M^{(l)}(w) = P_{FA}^{(l)}(w) \quad ; \quad w = 1,2,\ldots,l \quad (۳۱)$$

با توجه به پیچیدگی روابط (۲۸) و (۲۹) واضح است که حل تحلیلی این معادله در حالت کلی ممکن نیست. البته از تقریب زیر می‌توان برای ساده‌سازی روابط استفاده کرد:

$$\mathcal{B}(x,p) \approx \mathcal{N}(xp, xp(1-p)) \quad (۳۲)$$

در این رابطه $\mathcal{N}(xp, xp(1-p))$ یک توزیع نرمال با میانگین xp و واریانس $xp(1-p)$ است. البته برای برقراری این تقریب باید مقدار x به اندازه کافی بزرگ باشد. یک قاعده سرانگشتی معروف برای تأیید بزرگی مقدار x این است که هر یک از مقادیر xp و $x(1-p)$ باید از مقدار ۱۰ بیش‌تر باشند (البته در برخی مسائل از مقدار ۵ نیز استفاده می‌شود). لذا در صورت برقراری شرط $\left\lfloor \frac{L}{l} \right\rfloor \varepsilon_s^{(w)} > 10$ می‌توان رابطه (۳۱) را به شکل زیر تقریب زد:

$$Q(\frac{\tau^{(w,l)} - \hat{m}_{w,l}}{\hat{\sigma}_{w,l}}) \approx 1 - Q(\frac{\tau^{(w,l)} - m_{w,l}}{\sigma_{w,l}}) \quad (۳۳)$$

که در آن تابع $Q(x)$ به‌صورت زیر تعریف می‌شود:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{x^2}{2}} dx \quad (۳۴)$$

با حل معادله (۳۳)، مقدار تقریبی حد آستانه بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه به‌صورت زیر حاصل می‌شود:

$$\tau_{MM}^{(w,l)} \approx \left\lfloor \frac{L}{l} \right\rfloor \times \left(\frac{1}{2} + \frac{\sqrt{1-(1-2\varepsilon)^w} - 1}{2.(1-2\varepsilon)^w} \right) \quad (۳۵)$$

۵- استخراج رابطه تحلیلی مرتبه ماتریس‌های خروجی

همان‌گونه که پیش از این نیز اشاره شد، رابطه مرتبه پیشنهادشده در [۱۰، ۱۱] در حالت کلی برقرار نیست. نقص این رابطه، صحت الگوریتم‌هایی را که در [۱۸-۱۰] پیشنهاد شده‌اند را زیر سوال می‌برد. لذا در این بخش سعی شده است تا مرتبه ماتریس‌های خروجی به صورت کاملاً تحلیلی محاسبه شود.

فرض کنید که U بردار سریال ورودی کدگذار بوده و U_s نیز km اُمین نسخه تأخیریافته آن باشد؛ یعنی $U_s = [0_{k\times 1}\ U]$. آنگاه به ازای طول‌های $l = pn,\ p = 1,2,\ldots,\left\lfloor \frac{l_{max}}{n} \right\rfloor$ می‌توان بردار U_s را به بردارهای lتایی زیر تقسیم کرد:

$$U_i^{(l)} = [u_s^{(i-1)l+1} \ldots u_s^{il}]^T \quad ; \quad i = 1,2,\ldots,\left\lfloor \frac{L}{l} \right\rfloor \quad (۳۶)$$

که در آن u_s^j مؤلفه jام بردار U_s است. با توجه به این تعریف، رابطه (۱۳) می‌تواند به‌صورت زیر تفکیک شود:

$$C_i^{(l)} = U_i^{(l)}.\mathbf{G}^{(p)} \quad ; \quad i = 1,\ldots,\left\lfloor \frac{L}{l} \right\rfloor \quad (۳۷)$$

که در آن ماتریس $\mathbf{G}^{(p)}$ به‌صورت زیر تعریف می‌شود:

$$\mathbf{G}^{(p)} = \begin{bmatrix} \mathbf{G}_m & & & \mathbf{0} \\ \vdots & \mathbf{G}_m & & \\ \mathbf{G}_0 & \vdots & \ddots & \\ & \mathbf{G}_0 & & \mathbf{G}_m \\ & & \ddots & \vdots \\ \mathbf{0} & & & \mathbf{G}_0 \end{bmatrix}_{(p+m)k \times pn} \quad (۳۸)$$

رابطه (۳۷) می‌تواند در قالب ماتریسی زیر بیان شود:

$$\mathbf{C}^{(l)} = \mathbf{U}^{(l)}.\mathbf{G}^{(p)} \quad (۳۹)$$

که در آن ماتریس $\mathbf{U}^{(l)}$ به‌صورت زیر تعریف می‌شود:

$$\mathbf{U}^{(l)} = [U_1^{(l)}\ U_2^{(l)} \cdots U_{\left\lfloor \frac{L}{l} \right\rfloor}^{(l)}]^T \quad (۴۰)$$

اگر ورودی کدگذار یک بردار کاملاً تصادفی باشد، آنگاه مرتبه ماتریس $\mathbf{U}^{(l)}$ با احتمال بسیار زیاد کامل است. در این حالت از رابطه (۳۹) خواهیم داشت:

$$\text{span}(\mathbf{C}^{(pn)}) = \text{span}(\mathbf{G}^{(p)}) \quad ; \quad p = 1,2,\ldots,\left\lfloor \frac{l_{max}}{n} \right\rfloor \tag{۴۱}$$

در این رابطه $\text{span}(.)$ فضای سطری ماتریس را نشان می‌دهد.

توجه کنید که روابط (۳۷) و (۳۹) تنها به ازای طول‌های مضرب n برقرار هستند. به ازای طول‌هایی که مضربی از n نیستند، ماتریس $\mathbf{C}^{(l)}$ دارای ساختار معناداری نبوده و می‌توان آن را به‌صورت یک ماتریس کاملاً تصادفی در نظر گرفت. لذا مرتبه ماتریس خروجی به ازای این طول‌ها با احتمال بسیار زیاد کامل است. به‌طورکلی، مرتبه ماتریس $\mathbf{C}^{(l)}$ می‌تواند به‌صورت زیر خلاصه شود:

$$r_l = \begin{cases} \text{rank}(\mathbf{G}^{(p)}) & ; \quad l = pn,\ p = 1,\ldots,\left\lfloor \frac{l_{max}}{n} \right\rfloor \\ l & ; \quad \text{otherwise} \end{cases} \tag{۴۲}$$

که در آن r_l مرتبه ماتریس $\mathbf{C}^{(l)}$ است. با توجه به این رابطه، مرتبه ماتریس $\mathbf{C}^{(p)}$ می‌تواند توسط ماتریس $\mathbf{G}^{(p)}$ توصیف شود. لذا در ادامه، مرتبه ماتریس $\mathbf{G}^{(p)}$ به‌صورت تحلیلی محاسبه می‌شود.

فرض کنید $H(D) = [h_1(D) \ldots h_n(D)]$ یک بردار چندجمله‌ای تهی با درجه $p-1$ در فضای $\mathcal{C}^{\perp}$ باشد. همچنین فرض کنید $H = [h_1^{p-1}\, h_1^{p-1} \ldots h_n^{p-1} \ldots h_1^0\, h_2^0 \ldots h_n^0]$ بردار باینری متناظر با $H(D)$ باشد که در آن h_i^j ضریب جمله D^j در چندجمله‌ای $h_i(D)$ است. آنگاه رابطه (۱۰) می‌تواند به سادگی در قالب باینری زیر بازنویسی شود:

$$\mathbf{G}^{(p)}.H^T = 0_{k\times 1} \tag{۴۳}$$

حال فرض کنید که $\mathcal{C}_p^{\perp} \subset \mathcal{C}^{\perp}$ مجموعه‌ای متشکل از بردارهای تهی با درجه‌ای کم‌تر از p بوده و $\mathcal{C}_{b,p}^{\perp}$ نیز فضای باینری متناظر با آن باشد؛ یعنی:

$$\mathcal{C}_{b,p}^{\perp} = \{H \mid H(D) \in \mathcal{C}^{\perp}, \deg(H(D)) < p\} \tag{۴۴}$$

آنگاه با توجه به رابطه (۴۳) می‌توان گفت که بین بردارهای فضای $\mathcal{C}_{b,p}^{\perp}$ و بردارهای فضای تهی $\mathbf{G}^{(p)}$ تناظر یک‌به‌یک وجود دارد:

$$\ker(\mathbf{G}^{(p)}) \equiv \mathcal{C}_{b,p}^{\perp} \quad ; \quad p = 1,2,\ldots,\left\lfloor \frac{l_{\max}}{n} \right\rfloor \tag{۴۵}$$

تابع $\ker(.)$ در این رابطه فضای تهی ماتریس را نشان می‌دهد. بر طبق رابطه (۴۵)، ابعاد فضای تهی ماتریس $\mathbf{G}^{(p)}$ برابر با ابعاد فضای $\mathcal{C}_{b,p}^{\perp}$ است. لذا در ادامه ابعاد فضای $\mathcal{C}_{b,p}^{\perp}$ محاسبه می‌شود.

فرض کنید $\mathcal{R}_{\mathbf{H}_m} = \{H_1^m(D),\ldots,H_{n-k}^m(D)\}$ یک مجموعه کمین-پایه برای فضای $\mathcal{C}^{\perp}$ باشد. بردارهای این مجموعه برحسب درجه چندجمله‌ای‌ها شماره‌گذاری شده‌اند؛ یعنی درجه بردار $H_i^m(D)$ برابر با $\mu_i^{\perp}$ است. فرض کنید $\mathcal{R}_{\mathbf{H}_m}^p \subset \mathcal{R}_{\mathbf{H}_m}$ زیرمجموعه‌ای متشکل از بردارهای کمین-پایه با درجه‌ای کم‌تر از p باشد. آنگاه واضح است که $\mathcal{R}_{\mathbf{H}_m}^p$ یک مجموعه کمین-پایه را برای مجموعه باینری $\mathcal{C}_p^{\perp}$ تشکیل می‌دهد. به‌علاوه تمام نسخه‌های تأخیریافته بردارهای موجود در $\mathcal{R}_{\mathbf{H}_m}^p$ نیز متعلق به $\mathcal{C}_p^{\perp}$ هستند؛ البته مشروط به این که درجه آن‌ها کم‌تر از p باشد. مجموعه این بردارهای تأخیریافته با $\mathcal{R}_{\mathbf{H}_m,E}^p$ نشان داده می‌شود؛ یعنی:

$$\mathcal{R}_{\mathbf{H}_m,E}^p = \Big\{H_1^m(D),\ldots,D^{p-\mu_1^{\perp}}H_1^m(D),\ldots \\ \ldots,H_{\dim(\mathcal{C}_p^{\perp})}(D),\ldots,D^{p-\mu_{\dim(\mathcal{C}_p^{\perp})}^{\perp}}H_{\dim(\mathcal{C}_p^{\perp})}^m(D)\Big\} \tag{۴۶}$$

در این رابطه $\dim(\mathcal{C}_p^{\perp})$ ابعاد $\mathcal{C}_p^{\perp}$ را نشان می‌دهد (یعنی تعداد بردارهای کمین-پایه با درجه کم‌تر از p). توجه داشته باشید که $\dim(\mathcal{C}_p^{\perp})$ برابر با تعداد بردارهای زیرمجموعه $\mathcal{R}_{\mathbf{H}_m}^p$ است.

حال فرض کنید که $\mathcal{R}_{\mathbf{H}_m,E}^{b,p}$ مجموعه‌ای متشکل از بردارهای باینری متناظر با بردارهای مجموعه $\mathcal{R}_{\mathbf{H}_m,E}^p$ باشد. آنگاه $\mathcal{R}_{\mathbf{H}_m,E}^{b,p}$ یک مجموعه پایه را برای فضای $\mathcal{C}_{b,p}^{\perp}$ تشکیل می‌دهد؛ زیرا تمام بردارهای این مجموعه نسبت به هم مستقل بوده و هر بردار $\mathcal{C}_{b,p}^{\perp}$ می‌تواند به صورت ترکیبی خطی از بردارهای مجموعه $\mathcal{R}_{\mathbf{H}_m,E}^{b,p}$ نوشته شود. در نتیجه ابعاد فضای $\mathcal{C}_{b,p}^{\perp}$ برابر با تعداد بردارهای مجموعه $\mathcal{R}_{\mathbf{H}_m,E}^{b,p}$ است. به راحتی می‌توان نشان داد که این تعداد برابر با مقدار زیر است:

$$\dim(\mathcal{C}_{b,p}^{\perp}) = \sum_{i=1}^{n-k} \max(0, p - \mu_i^{\perp}) \tag{۴۷}$$

با توجه به رابطه (۴۵)، این مقدار برابر با ابعاد فضای $\ker(\mathbf{G}^{(p)})$ است. لذا مرتبه ماتریس $\mathbf{G}^{(p)}$ می‌تواند به‌صورت زیر نوشته شود:

$$\text{rank}(\mathbf{G}^{(p)}) = pn - \sum_{i=1}^{n-k} \max(0, p - \mu_i^{\perp}) \tag{۴۸}$$

نهایتاً با ادغام روابط (۴۲) و (۴۸) خواهیم داشت:

$$r_l = \begin{cases} l - \sum_{i=1}^{n-k} \max(0, p - \mu_i^{\perp}) & ; \quad l = pn,\ p = 1,\ldots,\left\lfloor \frac{l_{max}}{n} \right\rfloor \\ l & ; \quad \text{otherwise} \end{cases} \tag{۴۹}$$

برای نرخ $(n\text{-}1)/n$، این رابطه می‌تواند به شکل زیر ساده می‌شود:

$$r_l^{[\frac{n-1}{n}]} = \begin{cases} p(n-1)+\nu & ; \quad l = pn,\ p > \mu^{\perp} \\ l & ; \quad \text{otherwise} \end{cases} \tag{۵۰}$$

این رابطه مشابه با روابطی است که در [۱۰، ۱۱] پیشنهاد شده‌اند. با توجه به (۴۹)، این رابطه تنها به ازای کدهای نرخ $(n\text{-}1)/n$ برقرار است.

۶- الگوریتم پیشنهادی

تاکنون روش‌هایی در [۱۸-۱۰] برای تخمین پارامترهای کد کانولوشنال پیشنهاد شده است. اما همان‌گونه که پیش از این نیز اشاره شد، این روش‌ها تنها برای کدهای نرخ $(n\text{-}1)/n$ کارایی دارند. لذا در این بخش سعی شده است تا الگوریتمی جامع برای تخمین پارامترهای کد کانولوشنال نرخ k/n پیشنهاد شود. در این الگوریتم از روش GERP برای تخمین مرتبه و فضای تهی ماتریس‌های $\mathbf{C}^{(l)}$ استفاده می‌شود. تخمین پارامترهای کد نیز بر مبنای خواص ماتریس‌های $\mathbf{C}^{(l)}$ که در بخش ۵ حاصل شد، انجام می‌شود. این خواص به طور خلاصه در زیر لیست شده‌اند:

خاصیت ۱) با توجه به رابطه (۴۹)، مرتبه ماتریس $\mathbf{C}^{(l)}$ به ازای تمام طول‌هایی که مضربی از n نیستند، کامل است.

خاصیت ۲) با توجه به رابطه (۴۹)، مرتبه ماتریس $\mathbf{C}^{(l)}$ تنها به ازای طول‌های $l_i=(\mu_1^{\perp}+i)n, i=1,\ldots,\left\lfloor\frac{l_{max}}{n}\right\rfloor$ کامل نیست.

خاصیت ۳) تعریف $\delta_p=r_{(p-1)n}-2r_{pn}+r_{(p+1)n}$ را در نظر بگیرید. از رابطه (۴۹) می‌توان نشان داد که δ_p برابر با تعداد قیود طول دوگان $p-1$ است.

خاصیت ۴) بردارهای موجود در زیرمجموعه $\mathcal{C}_{\mu^{\perp}}^{\perp}$ یک مجموعه پایه را برای فضای $\mathcal{C}^{\perp}$ تشکیل می‌دهند.

خاصیت ۵) اگر بردار H در فضای تهی ماتریس $\mathbf{C}^{((p+1)n)}$ قرار داشته باشد، آنگاه بردار چندجمله‌ای متناظر با آن متعلق به زیرمجموعه $\mathcal{C}_p^{\perp}\subset\mathcal{C}^{\perp}$ است.

با توجه به این خواص، پارامترهای کد کانولوشنال می‌توانند به صورت زیر تخمین زده شوند:

مرحله ۱) تخمین n: با توجه به خاصیت (۲)، تفاضل طول‌های متناظر با هر دو ماتریس خروجی متوالی که مرتبه کامل ندارند، برابر با n است. در نتیجه برای تعیین پارامتر n باید تخمین مرتبه ماتریس‌های $\mathbf{C}^{(l)}$ را (با استفاده از روش GERP) تا یافتن دو ماتریس خروجی که دارای مرتبه کامل نیستند، ادامه داد. سپس مقدار پارامتر n از تفاضل طول‌های متناظر با این دو ماتریس حاصل می‌شود. با توجه به خاصیت (۲)، این ماتریس‌ها در طول‌های $l_1=(\mu_1^{\perp}+1)n$ و $l_2=(\mu_1^{\perp}+2)n$ قرار دارند. لذا پارامتر n می‌تواند در طول l_2 تخمین زده شود. بدیهی است که پس از تخمین پارامتر n می‌توان از محاسبه مرتبه ماتریس‌های خروجی در طول‌هایی که مضربی از n نیستند، صرف‌نظر نمود؛ زیرا با توجه به خاصیت (۱)، مرتبه ماتریس $\mathbf{C}^{(l)}$ در این طول‌ها کامل است. انجام این کار در کاهش پیچیدگی محاسباتی الگوریتم بسیار مؤثر است.

مرحله ۲) تخمین $\mu_1^{\perp},\ldots,\mu_{n-k}^{\perp}$: با توجه به خاصیت (۳)، از مقدار δ_p می‌توان برای تعیین قیود طول دوگان استفاده کرد. برای انجام این کار باید δ_p به ازای مقادیر مختلف $p\geq\mu_1^{\perp}$ محاسبه شود. اگر مقدار δ_p غیرصفر باشد، می‌توان نتیجه گرفت که کد موردنظر دقیقاً دارای δ_p قید طول دوگان $p-1$ است. مقدار صفر δ_p نیز شاخصی برای عدم وجود قید طول دوگان $p-1$ است.

با روش فوق می‌توان تمام قیود طول دوگان را به سادگی تعیین کرد. با توجه به خاصیت (۳)، مقدار δ_p بعد از آخرین قید طول دوگان (یعنی $p>\mu^{\perp}$) همواره برابر با صفر است. لذا توقف روند جستجوی قیود طول دوگان نیازمند تعریف یک مقدار برای تعداد تکرار است. ما این تعداد را با j_{max} نشان می‌دهیم. بر طبق این تعریف، اگر مقدار δ_p بعد از j_{max} تکرار متوالی برابر با صفر باشد، جستجوی قیود طول دوگان متوقف می‌شود. معمولاً فاصله بین قیود طول دوگان در کدهای عملی از مقدار ۵ تجاوز نمی‌کند. از این رو ما مقدار ۵ را برای j_{max} پیشنهاد می‌دهیم.

مرحله ۳) تخمین k: تعداد قیود طول دوگان برابر با $n-k$ است. در نتیجه پارامتر k می‌تواند از تفاضل مقدار n و تعداد قیود طول دوگان تعیین شود.

مرحله ۴) تخمین ν: بر طبق رابطه (۸)، پارامتر ν می‌تواند از مجموع قیود طول دوگان تعیین شود.

مرحله ۵) تخمین $\mathbf{H}_s(D)$ (ماتریس بررسی توازن سیستماتیک): تخمین ماتریس $\mathbf{H}_s(D)$ نیازمند تخمین یک مجموعه پایه برای فضای $\mathcal{C}^{\perp}$ است. با توجه به خاصیت (۴)، $\mathcal{C}_{\mu^{\perp}}^{\perp}$ چنین مجموعه‌ای را در خود جای داده است. مجموعه $\mathcal{C}_{\mu^{\perp}}^{\perp}$ نیز با توجه به خاصیت (۵) می‌تواند از فضای تهی ماتریس $\mathbf{C}^{((\mu^{\perp}+1)n)}$ تعیین شود. برای انجام این کار تنها کافی است که بردارهای فضای تهی ماتریس $\mathbf{C}^{((\mu^{\perp}+1)n)}$ به بردارهای چندجمله‌ای متناظر خود نگاشته شوند. فضای تهی ماتریس $\mathbf{C}^{((\mu^{\perp}+1)n)}$ نیز می‌تواند با استفاده از روش GERP تخمین زده شود.

پس از تعیین مجموعه $\mathcal{C}_{\mu^{\perp}}^{\perp}$ باید $n-k$ بردار مستقل از آن استخراج شود. ساده‌ترین روش برای انجام این کار، اعمال الگوریتم حذف گوس-جردن بر روی ماتریسی متشکل از بردارهای مجموعه $\mathcal{C}_{\mu^{\perp}}^{\perp}$ است. اعمال این الگوریتم، ماتریس سیستماتیک $\mathbf{H}_s(D)=[\mathbf{I}_{n-k}\,|\,\mathbf{P}]$ را نتیجه می‌دهد ($\mathbf{I}_{n-k}$ ماتریسی همانی با ابعاد $n-k\times n-k$ است).

مرحله ۶) تخمین $\mathbf{G}_s(D)$ (ماتریس مولد سیستماتیک): همان‌گونه که در بخش ۳ اشاره شد، تخمین ماتریس مولد اصلی کدگذار از رشته دریافتی میسر نیست. با این حال امکان تخمین ماتریس مولد سیستماتیک وجود دارد. اگر $\mathbf{H}_s(D)=[\mathbf{I}_{n-k}\,|\,\mathbf{P}]$ ماتریس بررسی توازن سیستماتیک باشد، آنگاه به سادگی خواهیم داشت: $\mathbf{G}_s(D)=[\mathbf{P}^T\,|\,\mathbf{I}_k]$ ($\mathbf{I}_k$ ماتریسی همانی با ابعاد $k\times k$ است).

الگوریتم پیشنهادی به‌صورت فلوچارت در شکل ۳ ارائه شده است.

۷- نتایج شبیه‌سازی

در این بخش چند مثال شبیه‌سازی برای بررسی عملکرد الگوریتم پیشنهادی ارائه می‌شود. جزئیات دقیق کدهای کانولوشنالی که در این بخش شبیه‌سازی می‌شوند، در جدول ۱ ذکر شده است. در این جدول، ماتریس‌های مولد در مبنای ۸ نمایش داده شده‌اند. در این روش نمایش، ضرایب چندجمله‌ای $g_{ij}(D)=g_{ij}^0+g_{ij}^1D+\ldots+g_{ij}^mD^m$ به صورت باینری $(g_{ij}^0\ g_{ij}^1\ldots g_{ij}^m)_2$ نوشته شده و سپس هر سه بیت متوالی به مبنای ۸ تبدیل می‌شود. اگر تعداد بیت‌ها مضربی از ۳ نباشد، چند بیت صفر از سمت چپ به عدد باینری اضافه می‌شود. به عنوان مثال معادل هشت- هشتی چندجمله‌ای $1+D+D^3+D^6$ برابر با $(151)_8$ است ($(001101001)_2$ دو بیت صفر به‌سمت چپ عدد باینری اضافه شده‌اند).

جدول ۱: جزئیات کدهای کانولوشنال شبیه‌سازی شده

Code	$\mathbf{G}(D)$	n	k	ν	$\mu_1^{\perp},\ldots,\mu_{n-k}^{\perp}$
$\mathcal{C}_1$	$[345 \quad 237]$	2	1	7	7
$\mathcal{C}_2$	$\begin{bmatrix}4 & 7 & 13\\ 0 & 16 & 2\end{bmatrix}$	3	2	4	4
$\mathcal{C}_3$	$[23 \quad 36 \quad 30]$	3	1	4	2, 2
$\mathcal{C}_4$	$\begin{bmatrix}1 & 13 & 10 & 16 & 7\\ 6 & 16 & 11 & 5 & 17\end{bmatrix}$	5	2	6	1, 2, 3

به ازای هر کدام از کدهای کانولوشنال، مراحل شبیه‌سازی زیر ۳۰۰ بار اجرا شده‌اند:

۱- تولید یک رشته تصادفی باینری

۲- کد کردن رشته تصادفی توسط کدگذار کانولوشنال

۳- انتخاب $L = ۲۰۰۰۰$ بیت اول از خروجی کدگذار

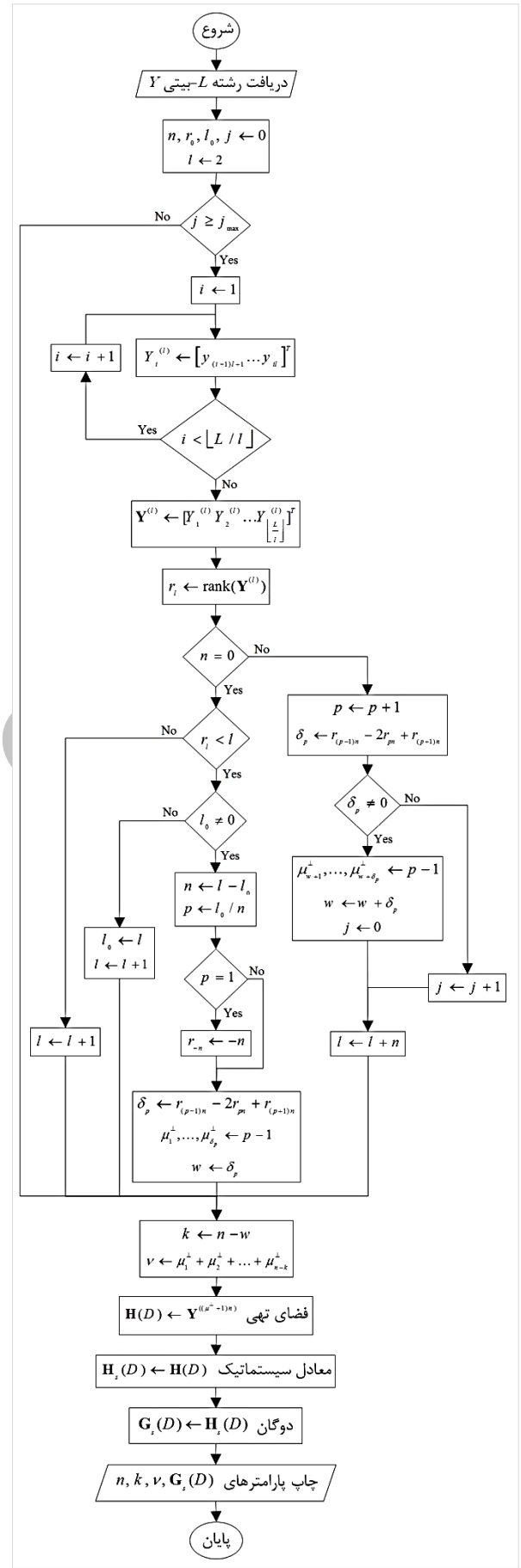
۴- عبور رشته کد از یک کانال BSC

۵- تخمین پارامترهای کد کانولوشنال توسط الگوریتم پیشنهادی

۶- مقایسه پارامترهای تخمینی با مقادیر واقعی

در شکل ۴، احتمال تخمین صحیح پارامتر n برحسب احتمال خطای کانال رسم شده است. از مرحله (مرحله ۱) بخش ۶ می‌دانیم که تخمین صحیح پارامتر n تنها به تشخیص نقصان مرتبه (و نه مقدار دقیق مرتبه) در طول‌های $(\mu_1^{\perp}+1)n$ و $(\mu_1^{\perp}+2)n$ بستگی دارد. به‌طورکلی، عملکرد روش GERP با افزایش طول ماتریس خروجی کاهش می‌یابد. لذا احتمال تخمین صحیح n با افزایش مقدار $(\mu_1^{\perp}+2)n$ کاهش خواهد یافت. البته مقدار مرتبه در طول‌های مذکور نیز بسیار تاثیرگذار است؛ زیرا تشخیص نقصان مرتبه به این معناست که حداقل یکی از بردارهای فضای دوگان به درستی تشخیص داده شوند. در نتیجه افزایش مقدار نقصان مرتبه به معنای افزایش احتمال تشخیص نقصان مرتبه است. مقدار $(\mu_1^{\perp}+2)n$ برای کدهای جدول ۱ به ترتیب برابر با ۱۸، ۱۸، ۱۲ و ۱۵ است. همان‌گونه که در شکل ۴ نیز دیده می‌شود، بهترین عملکرد متعلق به کد $\mathcal{C}_3(3,1,4)$ است؛ زیرا هم دارای کم‌ترین مقدار $(\mu_1^{\perp}+2)n$ بوده و هم از بیش‌ترین مقدار نقصان مرتبه نسبت به کدهای دیگر برخوردار است. همچنین دقت کنید که مقدار $(\mu_1^{\perp}+2)n$ برای کدهای $C_1(2,1,7)$ و $C_2(3,2,4)$ برابر با ۱۸ است. بااین‌حال کد $\mathcal{C}_2(3,2,4)$ به دلیل داشتن نقصان مرتبه بیش‌تر از احتمال تشخیص صحیح بهتری برخوردار است.

در شکل‌های ۵ تا ۷، احتمال تشخیص صحیح پارامترهای k، ν و $\mathbf{G}_s(D)$ برحسب احتمال خطای کانال رسم شده است. همان‌گونه که در این شکل‌ها دیده می‌شود، این سه پارامتر دارای احتمال تخمین تقریباً یکسانی هستند. علت اصلی این شباهت، وابستگی این سه پارامتر به قیود طول دوگان است. با توجه به مراحل تخمین (۲) تا (۶) که در بخش ۵ ارائه شد، تخمین اشتباه قیود طول دوگان منجر به تخمین اشتباه این سه پارامتر می‌شود.

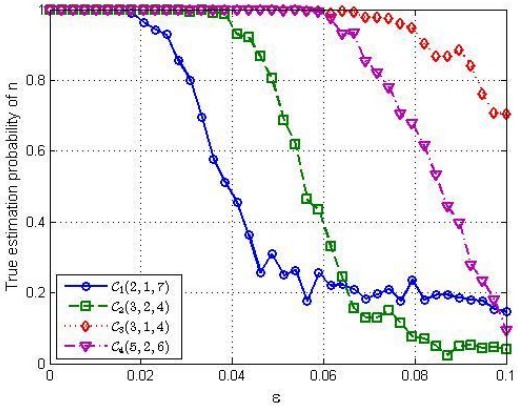


شکل ۳: الگوریتم تخمین پارامترهای کد کانولوشنال

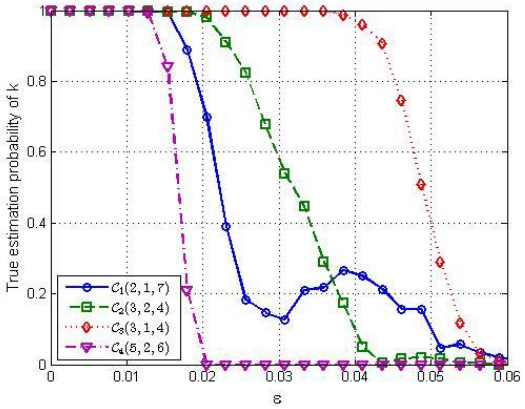
با توجه به مرحله (مرحله **۲**) در بخش ۵، تخمین صحیح قیود طول دوگان به تخمین صحیح مرتبه تا طول $l_{\max}=(\mu^{\perp}+j_{max}+1)n$ بستگی دارد. از طرف دیگر می‌دانیم که عملکرد روش GERP با افزایش طول ماتریس‌های خروجی کاهش می‌یابد. لذا احتمال تخمین صحیح پارامترهای k، ν و $\mathbf{G}_s(D)$ با افزایش مقدار $l_{\max}$ کاهش می‌یابد. به علاوه انتظار می‌رود که احتمال تخمین این پارامترها بسیار کم‌تر از پارامتر n باشد. مقدار $l_{\max}$ (به ازای $j_{max}=5$) برای کدهای جدول ۱ به ترتیب برابر با ۲۶، ۳۰، ۲۴ و ۴۵ است. همان‌گونه که در شکل‌های ۵ تا ۷ نیز دیده می‌شود، بهترین و بدترین عملکرد به ترتیب متعلق به کدهای $\mathcal{C}_3(3,1,4)$ و $\mathcal{C}_4(5,2,6)$ است. البته با توجه به تحلیل فوق انتظار می‌رفت که احتمال تخمین پارامترهای k، ν و $\mathbf{G}_s(D)$ برای کد $\mathcal{C}_1(2,1,7)$ بهتر از کد $\mathcal{C}_2(3,2,4)$ باشند؛ ولی نتایج شبیه‌سازی خلاف این را نشان می‌دهند. علت اصلی این است که تخمین صحیح قیود طول دوگان به تخمین صحیح پارامتر n وابسته است. لذا احتمال تخمین صحیح پارامترهای k، ν و $\mathbf{G}_s(D)$ همواره کم‌تر از پارامتر n است.

۸- نتیجه‌گیری

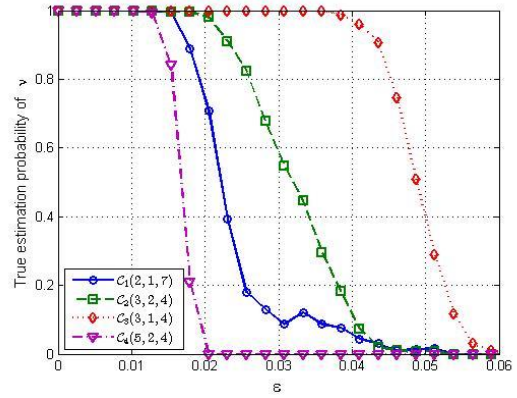
در این مقاله به مسئله تخمین پارامترهای کد کانولوشنال نرخ k/n در شرایط نویزی پرداخته شد. روش تخمین مبتنی بر مرتبه یکی از مهم‌ترین روش‌هایی است که تا کنون برای این مسئله پیشنهاد شده است. این روش بر مبنای مرتبه ماتریس‌های خروجی کدگذار عمل می‌کند. در این راستا رابطه‌ای کاملاً تجربی در [۱۰، ۱۱] برای مرتبه این ماتریس پیشنهاد شد که البته در حالت کلی برقرار نیست. لذا در این مقاله رابطه دقیق مرتبه برای نرخ k/n محاسبه شد. نتایج نشان می‌دهند که روابط پیشنهادی در [۱۰-۱۸] تنها در نرخ $(n\text{-}1)/n$ برقرار هستند. در نتیجه روش‌هایی که در کارهای پیشین پیشنهاد شده‌اند، تنها برای کدهای نرخ $(n\text{-}1)/n$ کارایی دارند. لذا در این مقاله، الگوریتمی جامع برای تخمین پارامترهای کد کانولوشنال نرخ k/n پیشنهاد شد. نتایج شبیه‌سازی نشان می‌دهند که الگوریتم پیشنهادی از عملکرد بسیار خوبی برخوردار است



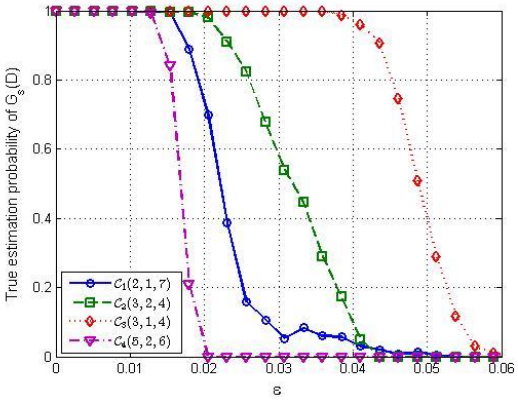
شکل ۴: احتمال تخمین صحیح پارامتر n برحسب نرخ خطای کانال



شکل ۵: احتمال تخمین صحیح پارامتر k برحسب نرخ خطای کانال



شکل ۶: احتمال تخمین صحیح پارامتر ν برحسب نرخ خطای کانال



شکل ۷: احتمال تخمین صحیح $\mathbf{G}_s(D)$ برحسب نرخ خطای کانال

مراجع

[۱] امیرمسعود مولائی کرمانی، محمدحسین صداقی و حسین ابراهیم‌نژاد، «استگانوگرافی کور مبتنی بر کدهای Reed-Solomon و جدول جانشانی بهینه با بهبود بار مفید جاسازی و مقاومت،» *مجله مهندسی برق دانشگاه تبریز*، دوره ۴۳، شماره ۲، صفحه ۴۳-۵۹، ۱۳۹۲.

[۲] احسان اولیائی ترشیزی و حسین شریفی، «ارائه دو الگوریتم دیکدینگ هیبرید جدید با عملکرد بسیار خوب و پیچیدگی بسیار

کم برای دیکدینگ کدهای LDPC،» *مجله مهندسی برق دانشگاه تبریز*، دوره ٤٥، شماره ۲، صفحه ۲۷-۳۷، ۱۳۹٤.

[3] B. Rice, "Determining the parameters of a rate 1/n convolutional encoder over GF(q)," *Proceeding of 3th International Conference on Finite Fields and Applications*, 1995.

[4] E. Filiol, "Reconstruction of convolutional encoders over GF(p)," *Proceeding of the 6th IMA Conference on Cryptography and Coding*, vol. 1355, pp. 100-110, 1997.

[5] J. Barbier, "Reconstruction of turbo-code encoders," *Proceeding of SPIE Security and Defense Space Communication Technologies*, vol. 5819, pp. 463-473, 2005.

[6] F. Wang, Z. Huang, and Y. Zhou, "A method for blind recognition of convolution code base on Euclidean algorithm," *IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, pp. 1414-1417, 2007.

[7] X. Hui, C. Xian, W. Feng, and H. Zhi, "A method for blind identification of rate 1/2 convolutional code based on improved Euclidean algorithm," *IEEE International Conference on Signal Processing (ICSP)*, vol. 2, pp. 1307-1310, 2012.

[8] J. Dingel, and J. Hagenauer, "Parameter estimation of a convolutional encoder from noisy observations," *IEEE International Symposium on Information Theory (ISIT)*, pp. 1776-1780, 2007.

[9] R. Moosavi, and E. G. Larsson, "Fast blind recognition of channel codes," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1393-1405, 2014.

[10] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of the second convolutional encoder of a turbo-code when its systematic outputs are punctured," *Journal of Military Technical Academy (MTA)*, vol. 19, no. 2, pp. 213-232, 2009.

[11] Y. Zrelli, M. Marazin, R. Gautier, and E. Rannou, "Blind identification of convolutional encoder parameters over GF(2^m) in the noiseless case," *International Conference on Computer Communications and Networks (ICCCN)*, pp. 1-5, 2011.

[12] M. Marazin, R. Gautier, and G. Burel, "Dual code method for blind identification of convolutional encoder for cognitive radio receiver design," *IEEE GLOBECOM Workshops*, pp. 1-6, 2009.

[13] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 168, pp. 1-9, 2011.

[14] Y. Wang, F. Wang, and Z. Huang, "Blind recognition of (n, k, m) convolutional code based on local decision in a noisy environment," *International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE)*, doi: 10.2991/amcce-15.2015.103, 2015.

[15] M. Marazin, R. Gautier, and G. Burel, "Algebraic method for blind recovery of punctured convolutional encoders from an erroneous bit stream," *IET Signal Processing*, vol. 6, no. 2, pp. 122-131, 2012.

[16] W. Chen, and G. Wu, "Blind recognition of (n-1)/n rate punctured convolutional encoders in a noisy environment," *Journal of Communications*, vol. 10, no. 4, 2015.

[17] Z. Jing, H. Zhiping, S. Shaojing, and Z. Yimeng, "Blind identification of convolutional codes in soft-decision situations," *International Journal of Modern Communication Technologies Research (IJMCTR)*, vol. 2, no. 4, 2014.

[18] S. Su, J. Zhou, Z. Huang, C. Liu, and Y. Zhang, "Blind identification of convolutional encoder parameters," *The Scientific World Journal*, vol. 2014, article ID: 798612, 2014.

[19] Y. Zrelli, R. Gautier, M. Marazin, E. Rannou, and E. Radoi, "Focus on theoretical properties of blind convolutional codes identification methods based on rank criterion," *Proceeding of the 9th International Conference on Communications (COMM)*, pp. 353-356, 2012.

[20] G. D. Forney, R. Johannesson, and Z. X. Wan, "Minimal and canonical rational generator matrices for convolutional codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1865-1880, 1996.

[21] G. D. Forney, "Convolutional codes I: algebraic structure," *IEEE Transactions on Information Theory*, vol. 16, no. 6, pp. 720-738, 1970.

[22] S. Lin, and D. J. Costello, *Error Control Coding: Fundamentals and Applications*, second edition, Prentice Hall, Englewood Cliffs, NJ, 2004.

[23] M. Barkat, *Signal Detection and Estimation*, second edition, Norwood, MA, Artech House Inc., 2005.

زیرنویس‌ها

[1] Reed-Solomon Code
[2] Low-Density Parity-Check Code
[3] Non-Cooperative Communication
[4] Cognitive Radio
[5] Convolutional Code
[6] Euclidean Algorithm
[7] Log-Likelihood Ratio
[8] Rank Based Estimation Method
[9] Gauss Elimination with Row Pivoting
[10] Punctured
[11] Minimax Decision Rule
[12] Minimal-Basic
[13] Constraint Lengths
[14] Parity-Check Matrix
[15] Pivot
[16] Hamming Weight
[17] Binary Symmetric Channel
[18] Binomial Distribution