شناسایی کور کدهای ضربی BCH

مهدی تیموری[۱]، استادیار؛ حمیدرضا کاکایی مطلق[۲]، مربی؛ مرتضی حدادی[۳]، دانشجوی کارشناسی ارشد

۱- دانشکده علوم و فنون نوین - دانشگاه تهران - تهران - ایران - mehditeimouri@ut.ac.ir
۲- دانشکده جنگ الکترونیک و دفاع سایبری - دانشگاه جامع امام حسین (ع) - تهران - ایران - hkakaei@ihu.ac.ir
۳- دانشکده جنگ الکترونیک و دفاع سایبری - دانشگاه جامع امام حسین (ع) - تهران - ایران - mhadadi@ihu.ac.ir

چکیده: با توجه به کاربردهای روزافزونی که کدهای ترکیبی به‌خصوص کدهای ضربی در سامانه‌های مخابرات بی‌سیم نظامی و ارتباطی دارند، توانایی شناسایی کور این کدها در سامانه‌های جنگ الکترونیک یکی از نیازهای دانش‌بنیان است. تاکنون روش‌های مختلفی برای شناسایی کدهای تشخیص خطای کانال ارائه گردیده است، اما در زمینه شناسایی کور کدهای ضربی هیچ روشی معرفی نشده است. در این مقاله با معرفی کدهای ضربی دوبعدی، تلاش نموده‌ایم با استفاده از توسعه روش‌های موجود شناسایی کدهای کانال جهت شناسایی کور کدهای ضربی اقدام نماییم. به همین منظور از دو روش شناخته‌شده بزرگ‌ترین شمارنده مشترک (GCD) و رتبه ماتریس (MR) برای شناسایی این نوع کدها استفاده نموده‌ایم. با استفاده از این روش‌ها پارامترهای کد (طول کد و طول پیام) و ساختار آن استخراج می‌شوند. نتایج شبیه‌سازی نشان می‌دهند که روش‌های پیشنهادی کارایی مناسبی در شناسایی این کدها دارند.

واژه‌های کلیدی: کد ضربی، شناسایی کور، روش GCD، روش MR.

Blind Recognition of BCH Product Codes

M. Teimouri[1], Assistant Professor; H. R. Kakaei Motlagh[2], Instructor; M. Haddadi[3], MSc Student

1- Faculty of New Sciences and Technologies, University of Tehran, Tehran, Iran, Email: mehditeimouri@ut.ac.ir
2- Faculty of Electronic Warfare and Cyber Defense, Imam Hossein Comprehensive University, Tehran, Iran, Email: hkakaei@ihu.ac.ir
3- Faculty of Electronic Warfare and Cyber Defense, Imam Hossein Comprehensive University, Tehran, Iran, Email: mhadadi@ihu.ac.ir

Abstract: As a result of growing application of concatenated codes such as product codes in military wireless communication systems, the ability of blind recognition and reconstruction of such codes in electronic warfare (EW) systems is one of the important necessities. So far, diverse methods for recognition of forward error correction (FEC) codes have been suggested; however, in terms of blind recognition of TPCs no method has been introduced yet. In this paper, we have tried to generalize the existing methods for recognition of two-dimensional TPCs. We apply two well-known methods of blind recognition, i.e. greatest common divisor (GCD) and matrix rank (MR), for recognition of these codes. Based on these methods, code parameters, i.e. code word length, message length, and the structure of code are determined. Simulation results are presented and analyzed which prove the effectiveness of the proposed method.

Keywords: Product codes, blind recognition, GCD method, MR method.

تاریخ ارسال مقاله: ۱۳۹۴/۱۰/۰۲
تاریخ اصلاح مقاله:۱۳۹۴/۱۲/۱۳
تاریخ پذیرش مقاله: ۱۳۹۵/۰۱/۱۷
نام نویسنده مسئول: مهدی تیموری
نشانی نویسنده مسئول: ایران - تهران - خیابان کارگر شمالی - دانشگاه تهران - دانشکده علوم و فنون نوین.

۱- مقدمه

سامانه‌های شنود مخابراتی بخشی اساسی از جنگ الکترونیک محسوب می‌گردند. این سامانه‌ها وظیفه شناسایی، مدوله‌زدایی و کدگشایی سیگنال‌های مخابراتی دریافتی از منطقه تحت پوشش را بر عهده دارند. به‌دلیل این‌که در سامانه‌های ارتباطی دیجیتالی معمولاً از چند نوع کدگذاری کانال استفاده می‌شود شناسایی کور نوع کدگذاری به‌کاررفته درصورتی‌که هیچ‌گونه اطلاعاتی از سیگنال وجود نداشته باشد، بسیار مهم است. این مسئله در کنار مسائل دیگر مانند حمله جهت یافتن کلید مورداستفاده در رمزگذاری [۱] و یا تشخیص گره‌های کپی در یک شبکه حسگر بی‌سیم [۲]، از اهمیت بالایی در مقوله امنیت شبکه‌های مخابراتی برخوردار است.

در میان تحقیقاتی که تاکنون انجام شده است، روشی جبری برای بازسازی کدهای بلوکی خطی و کانولوشنی با استفاده از دوگان کد ارائه شده است که در آن از رتبه ماتریس (MR[۱])، خواص ماتریس بررسی توازن[۲] و وزن همینگ استفاده می‌شود [۳]. همچنین روشی جهت تشخیص کور کدهای تصحیح خطا ارائه شده است که از ویژگی خطی بودن این کدها استفاده کرده است و با تشکیل ماتریس داده‌ها و گرفتن رتبه ماتریس اقدام به شناسایی کور کدها می‌شود [۴]. یک روش نیز برای شناسایی کور کدهای بلوک خطی دودویی در حالت‌های نرخ پایین معرفی شده است که در شرایط نویزی عملکردی مناسب دارد اما برای کدهای با نرخ بالا مناسب نیست و علاوه بر این، نیازمند مقدار زیادی از داده‌های مشاهده‌شده است [۵]. در تحقیقی دیگر، یک الگوریتم تشخیص کور برای کدهای BCH[۳] بر اساس ریشه‌های کلمه‌های کد ارائه شده است [۶، ۷]. این الگوریتم می‌تواند در شرایط نرخ کد بالا و پایین، کد را به‌درستی تشخیص دهد؛ اما هنگامی‌که طول کد بزرگ است محاسبات پیچیده می‌شود. در سال ۲۰۱۱، وانگ به همراه همکارانش روشی جهت شناسایی طول کدهای BCH ارائه دادند که از خواص کدهای دوری بهره‌گیری می‌کند. در این روش چندجمله‌ای سازنده[۴] بر اساس کمینه وزن سندروم‌ها محاسبه می‌شود [۸]. در کاری دیگر، از تقسیم رشته بیت تصادفی دریافتی بر چندجمله‌ای‌های کمینه[۵] برای تشخیص کدهای BCH استفاده شده است که از معایب این روش پیچیدگی محاسباتی زیاد است [۹]. در روشی دیگر، بر اساس روش بزرگ‌ترین شمارنده مشترک (GCD[۶])، اقدام به شناسایی چندجمله‌ای سازنده می‌شود [۱۰]. این روش بر روی کلمات کد بدون نویز استفاده شده است و در برابر خطا مقاوم نیست.

علاوه بر روش‌های فوق، روش‌های دیگری جهت شناسایی کدهای دوری در حالت کلی ارائه شده است. در [۱۱]، نویسندگان به ارائه روشی جهت شناسایی چندجمله‌ای سازنده کدهای دوری پرداخته‌اند که باید طول کد و یا قالب طول کد از قبل مشخص شده باشد تا بتوان چندجمله‌ای سازنده را تخمین زد. در روشی دیگر، از توزیع وزنی کدها استفاده‌شده است که برای طول کدهای بزرگ (۱۲۷ به بالا) دچار خطای زیادی می‌شود و قادر به تشخیص نیست [۱۲]. در [۱۳]، روشی مبتنی بر نرم‌تصمیمی جهت شناسایی کور کدهای دوری بیان شده است که از خواص جبری کدهای دوری استفاده می‌کند. این روش دقت بالایی در تشخیص درست کدهای دوری دارد اما در برابر نویز به‌شدت تأثیرپذیر است و دارای پیچیدگی محاسباتی بالایی است. در چندین مقاله، روش‌هایی جهت شناسایی کدهای RS[۷] و نیز بهبود روش‌های شناسایی این نوع کدها ارائه‌شده است [۱۶-۱۴]. در سال‌های اخیر همچنین روش‌هایی جهت شناسایی کد LPDC معرفی شده است [۱۷]. بسیاری از این روش‌ها در حالت تصمیم‌گیری سخت و بر استفاده از خواص جبری از کدها در میدان گالوا (GF[۸]) متمرکز هستند. اشکال عمده آن‌ها این است که در برابر خطا آسیب‌پذیرند. حتی اگر تنها یک بیت خطا در یک کلمه کد رخ دهد، خواص جبری از کدهای تصحیح خطا تا حد زیادی از بین خواهد رفت؛ بنابراین، شناسایی نیاز به مقدار زیادی از داده‌های مشاهده‌شده دارد.

تا جایی که نویسندگان مقاله اطلاع دارند، تاکنون هیچ روشی برای شناسایی کدهای ضربی مطرح نشده است. با توجه به این‌که کدهای ضربی از ترکیب دو کد بلوکی ایجاد می‌شود، در این مقاله با استفاده توسعه روش‌هایی که برای شناسایی کدهای بلوکی استفاده می‌شود روش‌هایی برای شناسایی کدهای ترکیبی ضربی BCH ارائه می‌شود. در این راستا ابتدا در بخش دوم روش پیشنهادی ارائه می‌شود و سپس در بخش سوم با استفاده از نتایج شبیه‌سازی عملکرد روش پیشنهادی مورد ارزیابی قرار می‌گیرد. در پایان و در بخش چهارم هم به نتیجه‌گیری پرداخته می‌شود.

۲- روش پیشنهادی

فرض کنید C_1 (C_2) یک کد خطی به طول n_1 (n_2) و با ابعاد k_1 (k_2) باشد کد ضربی $C=C_1\otimes C_2$ مجموعه‌ای از ماتریس‌ها با اندازه $n_1\times n_2$ است، به‌طوری‌که:

- هر ردیف یک کلمه کد از C_1 است
- هر ستون یک کلمه کد از C_2 است.

چنین کدی یک کد بلوکی خطی به طول $n_1\times n_2$ و با بعد $k_1\times k_2$ است که تحت عنوان کد ضربی شناخته می‌شود. اگر کدهای تشکیل‌دهنده چنین کدی از نوع BCH باشد به آن کد ضربی BCH گفته می‌شود.

روش‌های شناسایی برای کدهای بلوکی را عموماً می‌توان به دو دسته کلی به شرح ذیل تقسیم نمود:

- شناسایی عمومی: فقط مشخصات کلی (طول کلمه کد و طول پیام) کدها را می‌دهد همانند روش رتبه.
- شناسایی دقیق: علاوه بر مشخصات کلی کد، ساختار کد (چندجمله‌ای سازنده) را نیز مشخص می‌کند همانند روش GCD.

لازم به ذکر است که علاوه بر روش‌های فوق، برخی از روش‌های شناسایی وجود دارند که فقط به بررسی استفاده از کدهای تصحیح

خطا در سامانه‌های مخابراتی می‌پردازند [۱۸]. این روش‌ها به این سؤال پاسخ می‌دهند: آیا از کدهای تصحیح خطا در رشته بیت دریافتی استفاده شده است یا نه. این روش‌ها عموماً برای تصمیم‌گیری از مقایسه مشخصه‌ای از مشاهدات جمع‌آوری‌شده با یک سطح آستانه استفاده می‌کنند.

از روش‌های موجود، برخی برای شناسایی هر دو نوع کد بلوکی و کانولوشنی استفاده‌شده و برخی دیگر فقط برای شناسایی کدهای بلوکی به‌کارگیری می‌شوند. به‌عنوان‌مثال، در [۱۹] استخراج کور ویژگی‌های کدهای کانولوشنی و بلوکی در حضور نویز موردبررسی قرار گرفته است. با توجه به این‌که کدهای ضربی از خانواده کدهای بلوکی هستند و دارای خواص جبری کدهای مذکور می‌باشند لذا می‌توان روش‌های شناسایی موجود برای کدهای بلوکی خطی را برای شناسایی کدهای ضربی توسعه داد.

تا جایی که نویسندگان مقاله اطلاع دارند، تاکنون هیچ روشی برای شناسایی کدهای ضربی ارائه نشده است و این مقاله برای اولین بار این موضوع را موردبررسی قرار می‌دهد. در این راستا و در این مقاله، ضمن توسعه دو روش شناخته‌شده GCD و رتبه ماتریس برای شناسایی کدهای ضربی، عملکرد این دو روش را مورد مقایسه قرار می‌دهیم. برای سادگی، حالتی خاص اما بسیار پرکاربرد از کدهای ضربی را در نظر می‌گیریم که در آن دو کد استفاده‌شده یکسان هستند. جایگردان[۹] مفروض در کد ضربی را جایگردان متداول ماتریسی در نظر می‌گیریم، هرچند می‌توان جایگردان‌های پیچیده‌تری نیز برای این منظور در نظر گرفت. در این صورت، یک مسئله مهم دیگر شناسایی جایگردان است که در مراجع زیادی ازجمله [۲۰] موردبررسی قرار گرفته است.

۲-۱- روش شناسایی GCD

شناسایی کور یک کد ضربی $\mathrm{BCH}(n^2,k^2)$ در تعیین این سه پارامتر خلاصه می‌شود: طول بلوک n، طول کلمه پیام k و چندجمله‌ای سازنده $g(x)$؛ اما چون درجه $g(x)$ برابر $n-k$ است، با به‌دست آمدن n و $g(x)$، k نیز خودبه‌خود به‌دست می‌آید.

در این روش ابتدا به شناسایی طول بلوک پرداخته و سپس چندجمله‌ای سازنده را شناسایی می‌کنیم و با توجه به این‌که طول بلوک و چندجمله‌ای‌های سازنده آن‌ها را یکسان فرض کردیم با شناسایی اولین طول بلوک و چندجمله‌ای سازنده، شناسایی به پایان می‌رسد.

۲-۱-۱- شناسایی طول بلوک

برای شناسایی طول بلوک فرض می‌کنیم که در حالت همزمان با کدگذار قرار داریم و طول رشته بیت دریافتی (که آن را با f_l نمایش می‌دهیم) مضربی از طول بلوک است. همچنین، فرض می‌کنیم دست‌کم دو بلوک در رشته بیت دریافتی وجود داشته باشد. در نتیجه داریم:

خاصیت ۱: f_l بر n بخش‌پذیر است ($n \mid f_l$).

خاصیت ۲: $n \in \left[3, \left\lfloor \frac{f_l}{2} \right\rfloor\right]$ که $\lfloor . \rfloor$ تابع جزء صحیح است.

از خاصیت ۱ نتیجه می‌شود که طول بلوک یکی از عامل‌های f_l است.

فرض کنید $i=n$ طول بلوک باشد. در این صورت، $N_i = \frac{f_l}{i}$ کلمه کد BCH در رشته بیت دریافتی وجود دارد. با فرض این‌که $c_p(x)$ چندجمله‌ای کد متناظر با p-امین کلمه کد باشد. متناظر با $c_p(x)$، j چندجمله‌ای $c_{p,1}(x), c_{p,2}(x), \ldots, c_{p,j}(x)$ $(j<i)$ می‌توان به‌دست آورد که $c_{p,\ell}(x)$ انتقال‌یافته دوری[۱۰] $c_p(x)$ به‌اندازه ℓ واحد به‌سمت راست است.

با توجه به خاصیت دوری این کد، اگر در $c_p(x)$ خطایی رخ نداده نباشد، بردارهای متناظر با $c_{p,1}(x), c_{p,2}(x), \ldots, c_{p,j}(x)$ و همچنین $c_{p,0}(x)=c_p(x)$ نیز متعلق به مجموعه کلمه‌های کد با چندجمله‌ای سازنده $g(x)$ هستند. لذا یک عامل مشترک بین $c_{p,0}(x), c_{p,1}(x), \ldots, c_{p,j}(x)$ وجود خواهد داشت.

$$\gcd\left[c_{p,0}(x), c_{p,1}(x), c_{p,2}(x), \ldots, c_{p,i-1}(x)\right] \neq 1. \qquad (۱)$$

هر چندجمله‌ای که در رابطه (۱) صدق کند یک چندجمله‌ای معتبر نامیده می‌شود. فرض کنید که در کل داده دریافتی به تعداد N_{ic} چندجمله‌ای معتبر وجود دارد. واضح است که اگر کانال بدون خطا باشد، در حالت $i=n$ رابطه $N_{ic}=N_i$ برقرار است. نسبت تعداد چندجمله‌ای‌های معتبر به‌کل کلمه‌های کد را با f_{ic} نشان می‌دهیم.

$$f_{ic} = \frac{N_{ic}}{N_i} \qquad (۲)$$

وقتی $i=n$ و خطایی در کانال رخ نداده باشد، رابطه $f_{ic}=1$ برقرار است. اما اگر $i \neq n$، باید تعداد چندجمله‌ای‌های معتبر کمتری داشته باشیم که در نتیجه داریم $f_{ic}<1$. در حالت وجود خطای کانال، قاعدتاً f_{ic} کمتر از یک می‌شود اما می‌توان پیش‌بینی نمود که f_{ic} مقدار بیشینه خود را در حالت $i=n$ بگیرد، زیرا تنها در این حالت است که بیشتر بلوک‌های انتخاب‌شده کلمه‌های کد سالم هستند و لذا باید رابطه (۱) برای آن‌ها برقرار باشد. اما زمانی که $i \neq n$، بلوک‌های انتخاب‌شده کلمه‌های کد مجاز نخواهند بود و لذا رابطه (۱) برای آن‌ها برقرار نخواهد بود؛ لذا انتظار داریم که در این حالت f_{ic} برابر صفر (یا بسیار نزدیک به صفر) گردد.

با توجه به این‌که برای کدهای BCH، مقدار n فرد است، می‌توان طول بلوک n را از رابطه زیر به‌دست آورد:

$$n = \underset{i \mid f_l,\, i \in \left[3, \left\lfloor \frac{f_l}{2} \right\rfloor\right],\, \mathrm{mod}(i,2)=1}{\arg\max} \left(f_{ic}\right) \qquad (۳)$$

هر چه مقدار j (تعداد انتقال‌یافته‌های دوری) و f_l بیشتر باشد، دقت تخمین طول بلوک بیشتر می‌شود. پس می‌توان مراحل یافتن طول کد را به‌شرح ذیل خلاصه نمود:

۱. $i=3$

۲. اگر f_l قابل‌تقسیم بر i نباشد به مرحله ۶ بروید

۳. N_i چندجمله‌ای به طول i را با استفاده از f_I بیت دریافتی تولید نمایید.
۴. با استفاده از رابطه (۱) تعداد چندجمله‌ای‌های معتبر N_{ic} را محاسبه نمایید.
۵. $f_{ic}=\frac{N_{ic}}{N_i}$ را محاسبه کرده و ذخیره کنید.
۶. $i \leftarrow i+2$
۷. اگر $i \le \left\lceil f_I/2 \right\rceil$ به مرحله ۲ بروید.
۸. همه f_{ic}ها ذخیره‌شده را مقایسه کرده و مقداری از i را که موجب بیشینه شدن f_{ic} می‌شود به‌عنوان طول بلوک n برگردانید.

۲-۱-۲- شناسایی چندجمله‌ای سازنده

در این بخش با فرض مشخص بودن n، نحوه یافتن چندجمله‌ای سازنده $g(x)$ بررسی می‌شود. فرض کنید که $N=\frac{f_I}{n}$ بلوک (همان کلمه کد BCH) در قالب اطلاعات کدشده توسط یک کد ضربی دریافت شده است و $c_p(x)$ چندجمله‌ای متناظر با p-امین بلوک است ($p=1,2,...,N$). با توجه به نتایج بخش قبل، اگر انتقال‌های دوری $c_p(x)$ با $c_{p,0}(x),c_{p,1}(x),...,c_{p,j}(x)$ نشان داده شوند، $g(x)$ عامل مشترک این چندجمله‌ای‌ها است. به‌عبارت‌دیگر، اگر:

$$f_p(x)=\gcd\left[c_p(x),c_{p1}(x),c_{p2}(x),....,c_{pj}(x)\right], \quad (۴)$$

آنگاه $f_p(x)$ مضربی از $g(x)$ است (توجه کنید $1\le j<n-1$).

با استفاده از N بلوک دریافتی، M ($1\le M\le N$) چندجمله‌ای متمایز از رابطه (۴) به‌دست می‌آید. با فرض وجود خطای کانال، این M چندجمله‌ای متعلق به یکی از چهار دسته زیر هست:

۱. برابر با ۱.
۲. مخالف ۱، مخالف $g(x)$ و یا مخالف مضربی از $g(x)$
۳. برابر $g(x)$
۴. برابر مضربی از $g(x)$

حالت‌های ۱ و ۲ نشان‌دهنده این هستند که در بلوک متناظر خطا وجود دارد و حالت‌های ۳ و ۴ نشانگر عدم وجود خطا هستند و یا این‌که خطا به‌صورتی بوده است که کلمه کد BCH دیگری نتیجه شده است. چندجمله‌ای سازنده $g(x)$ از M چندجمله‌ای به‌صورت زیر به‌دست می‌آید:

مرحله ۱: با توجه به خواص $g(x)$، چندجمله‌ای‌هایی که در یک یا چند شرط از سه شرط زیر صدق نمی‌کنند بایستی حذف شوند:

- $g(x)\neq 1$
- $g(x)\neq x^q+1$ که q یک عدد صحیح مثبت و $1\le q<n$.
- $g(x)\,|\,x^n+1$

مرحله ۲: فرض کنید از مرحله اول، به تعداد L چندجمله‌ای باقی‌مانده باشد. می‌گیریم:

$$h_i(x)=x^n+1/g_i(x),\quad i=1,2,....,L. \quad (۵)$$

در این صورت، سندروم بلوک jام ($j=1,2,...,N$) با استفاده از رابطه زیر محاسبه می‌شود:

$$r_{ij}(x)=\left[h_i(x)c_j(x)\right]\bmod(x^n+1) \quad (۶)$$

برای تمامی N بلوک دریافتی، وزن w_{ij} را به‌صورت $w_{ij}=\text{weigth}(r_{ij}(x))$ محاسبه کرده و سپس آن‌ها را با هم جمع کرده تا برای هر چندجمله‌ای $g_i(x)$ وزن w_i به‌دست آید.

$$w_i=\sum_{j=1}^{N}w_{ij},\quad i=1,2,...,L \quad (۷)$$

معیار شناسایی چندجمله‌ای سازنده، انتخاب چندجمله‌ای با کمترین وزن سندروم متناظر (w_i) خواهد بود.

$$g(x)=\arg\max_i(w_i) \quad (۸)$$

پس از شناسایی چندجمله‌ای سازنده، مقدار k نیز به‌صورت خودکار به‌دست می‌آید.

۲-۲- روش رتبه ماتریس

در این روش بیت‌های دریافتی به دسته‌هایی با طول یکسان تقسیم‌شده و پس از آن با زیر هم قرار دادن این دسته‌ها، یک ماتریس تشکیل داده می‌شود. ماتریس مزبور تنها در صورتی یک ماتریس با رتبه ناقص[11] خواهد بود که طول دسته برابر طول بلوک باشد. دلیل این امر را می‌توان با توجه به مفهوم فضای برداری کلمات کد توجیه نمود.

کد بلوکی خطی $c(n,k)$ را در نظر بگیرید که در آن تعداد بیت‌های اطلاعات برابر k بیت و طول کلمات کد برابر n بیت است. تعداد کل کلمات کد در این حالت برابر 2^k کلمه خواهد بود. در یک کلمه کد با طول n بیت، تعداد n-k بیتِ آن ترکیبی خطی از سایر بیت‌ها می‌باشند. به بیان ریاضی، هرگاه یک کلمه کد دلخواه مانند $v=[v_0v_1v_2...v_{n-1}]$ از یک کد بلوکی خطی را در نظر بگیریم، می‌توان نوشت:

$$\exists c_i\in\{0,1\}:v_m=\sum_{i=0}^{k-1}c_iv_i,\ k\le m<n; \quad (۹)$$

این خاصیت باعث خواهد شد تا هرگاه ماتریسی را از زیر هم قرار دادن کلمات کدی به‌عنوان سطرهای آن تشکیل دهیم، برخی از ستون‌های آن ترکیبی خطی از ستون‌های دیگر شوند که این مسئله باعث خواهد شد تا چنین ماتریسی دارای رتبه کامل نباشد.

الگوریتم رتبه ماتریس به‌عنوان ورودی، رشته‌ای از بیت‌ها را دریافت و خروجی‌های زیر را تولید می‌کند:

- میزان تأخیر (برحسب تعداد بیت) در رسیدن به ابتدای بلوک.
- نرخ و نوع کد (بلوکی یا غیر بلوکی).

در استفاده از روش رتبه ماتریس، فرض می‌شود بیت‌ها در عبور از کانال دچار خطا نشده باشند، در غیر این صورت خروجی این روش چندان معتبر نخواهند بود. فرض می‌کنیم رشته بیت‌های دریافتی

دارای طول M باشد. الگوریتم روش رتبه ماتریس برای یافتن طول به‌کاررفته در بیت‌های دریافتی را می‌توان به‌صورت زیر نوشت:

شروع: $n_\alpha = 3$.

گام اول: کل بیت‌ها را به $\left\lfloor \frac{M}{n_\alpha} \right\rfloor$ دسته (هر یک به طول n_α) تقسیم نمایید.

گام دوم: ماتریس A_α را با استفاده از زیر هم قرار دادن این دسته‌ها تشکیل دهید.

گام سوم: رتبه ماتریس A_α (مقدار r_α) را حساب کنید. درصورتی‌که $r_\alpha < n_\alpha$، مقدار r_α نشان‌دهنده مقدار k و مقدار n_α نیز نشان‌دهنده n است. اگر $r_\alpha = n_\alpha$، مقدار n_α را باید دو واحد افزایش داده و به گام اول برگردید.

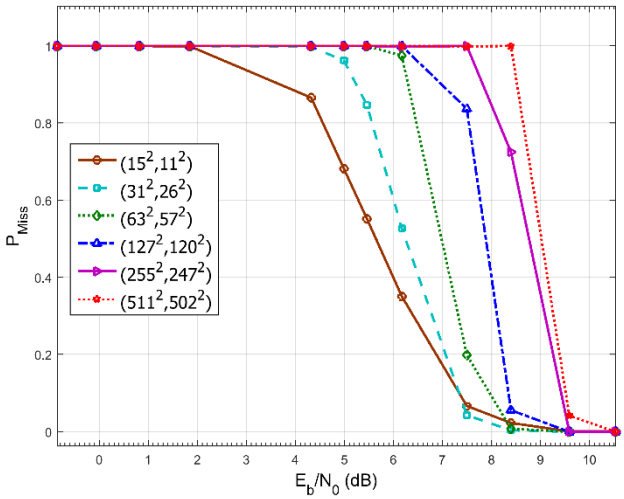
روش رتبه ماتریس تنها می‌تواند مقدار n و k را برگرداند، اما وقتی از کد BCH استفاده می‌کنیم، این مقادیر می‌توانند چندجمله‌ای سازنده را نیز مشخص نمایند.

۳- نتایج شبیه‌سازی

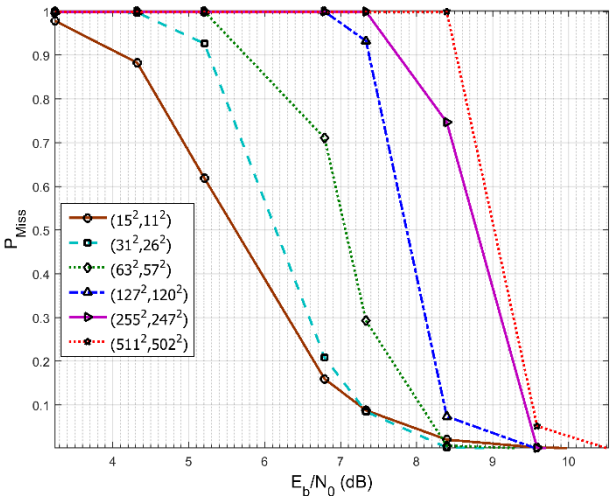
برای انجام شبیه‌سازی، فرض می‌کنیم که در فرستنده از مدولاسیون BPSK[۱۲] استفاده شده است. همچنین شبیه‌سازی هر دو روش GCD و رتبه ماتریس برای شش نوع کد مختلف انجام شده است. در هر نسبت سیگنال به نویز، ۱۰۰۰ آزمایش (شبیه‌سازی مونت‌کارلو) انجام می‌شود. در هر بار آزمایش فرض می‌کنیم که 10^5 بیت در اختیار داریم. مدل کانال را هم AWGN[۱۳] در نظر می‌گیریم و از تصمیم‌گیری سخت در خروجی کانال استفاده می‌کنیم. نسبت سیگنال به نویز E_b / N_0 را به‌شکلی تغییر می‌دهیم که احتمال خطای بیت از 10^{-6} تا 10^{-1} تغییر نماید (E_b انرژی بیت و $N_0/2$ چگالی طیف قدرت نویز است. احتمال خطای بیت نیز برابر $P_b = Q\left(\sqrt{2E_b/N_0}\right)$ است که $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$.).

در شکل ۱ احتمال عدم‌تشخیص برحسب خطای کانال برای روش GCD نمایش داده شده است. همان‌طور که انتظار داریم با افزایش طول کد، قدرت تشخیص در برابر خطاهای بالا سریع‌تر افت نموده و به‌سمت صفر می‌گراید (به‌عبارت‌دیگر، احتمال عدم‌تشخیص نسبت به افزایش خطا بیشتر می‌شود). همان‌طور که ملاحظه می‌شود، برای طول‌های کد کوچک‌تر تحمل در برابر خطا بهتر است. دلیل این موضوع این است که هرچه طول کد بزرگ‌تر باشد، برای طول مشخصی از رشته بیت دریافتی، احتمال وجود کلمات کد نویزی بیشتر می‌شود. برای مثال، برای کد $(511^2,502^2)$ احتمال عدم‌تشخیص کد در $E_b / N_0 \approx 8.4$ dB (معادل احتمال خطای حدود 10^{-4}) نزدیک به یک است. این در حالی است که برای کد $(15^2,11^2)$ در همین مقدار احتمال خطای، کمتر از ۳٪ عدم‌تشخیص درست داریم. همان‌طور که در شکل ۲ ملاحظه می‌شود، عملکرد روش رتبه ماتریس به میزان نسبتاً کمی بدتر از روش GCD است.

در هرصورت، همان‌طور که ملاحظه می‌شود، هر دو الگوریتم برای عملکرد صحیح کاملاً صحیح (یعنی رسیدن احتمال عدم‌تشخیص نزدیک به ۰٪) نیاز به مقدار E_b / N_0 حدود ۹/۵ دسی‌بل (معادل احتمال خطای بیت 10^{-5}) دارند. بااین‌حال، باید توجه شود که نسبت سیگنال به نویز لازم در مسائل شناسایی کور نسبت به شرایطی که گیرنده مجاز در حال دریافت اطلاعات است، همیشه بیشتر است.



شکل ۱: احتمال عدم‌تشخیص کد برحسب مقدار E_b / N_0 (dB) برای روش GCD.



شکل ۲: احتمال عدم‌تشخیص کد برحسب مقدار E_b / N_0 (dB) برای روش رتبه ماتریس.

۴- نتیجه‌گیری

در این مقاله دو روش مختلف برای شناسایی کدهای ضربی BCH ارائه شد: روش GCD و روش MR. این روش‌ها بر پایه شناسایی یکی از کدهای تشکیل‌دهنده پیشنهاد شدند.

همان‌طور که از نتایج شبیه‌سازی‌ها ملاحظه شد، روش GCD نسبت به نویز دارای حساسیت کمتری است. همچنین در روش رتبه ماتریس فقط طول کد و طول پیام به‌دست می‌آید، اما در روش GCD می‌توان علاوه بر استخراج مشخصات کلی کد، چندجمله‌ای سازنده کد ضربی را نیز به‌دست آورد. البته عملکرد نسبتاً بهتر روش GCD بدون

هزینه به‌دست نمی‌آیند. سرعت اجرای روش GCD نسبت به روش رتبه ماتریس کمتر است. به‌عنوان‌مثال برای شناسایی کد ضربی $(127^2,120^2)$ در نسخه ۲۰۱۲ نرم‌افزار MATLAB و بر روی کامپیوتری ۴ هسته‌ای مورداستفاده برای شبیه‌سازی، در ۱۰۰۰ بار آزمایش، روش GCD حدود ۴۲۵ ثانیه زمان برد درحالی‌که اجرای روش رتبه ماتریس در حدود ۳۲۰ ثانیه طول کشید.

مراجع

[۱] شهرام جمالی و عرفان آقایی کیاسرایی، «بهبود حمله مکعبی کانال جانبی بر روی الگوریتم‌های بلوکی،» *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۵، شماره ۴، صفحات ۶۹-۷۸، ۱۳۹۴.

[۲] رضا رافع و فرشته خدادادی، «ارائه یک الگوریتم شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم به‌کمک انتشارات محلی و کانال‌های کرم‌چاله قانونی،» *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۴، شماره ۴، صفحات ۲۲-۳۳، ۱۳۹۳.

[3] J. Barbier, G. Sicot, and S. Houcke, "Algebraic approach for the reconstruction of linear and convolutional error correcting codes," *Proc. CCIS 2006*, 2006.

[4] J. Barbier, and J. Letessier, "Forward error correcting codes characterization based on rank properties," *Proc. IEEE Int. Conf. Wireless Communications & Signal Processing*, pp. 1-5, 2009.

[5] J. J. Zan, and Y. b. Li, "Blind recognition of low code-rate binary linear block codes," *Radio Engineering of China*, vol. 1, pp. 1-8, 2009.

[6] W. N. Y. Xiaojing, "Recognition methods of BCH codes," *Electronic Warfare*, vol. 6, pp. 1-8, 2010.

[7] Y. Xiaojing, and W. Niancheng, "Recognition method of BCH codes on roots information dispersion entropy and roots statistic," *J. Detect. Contr.*, vol. 32, no. 3, pp. 69-73, 2010.

[8] J. Wang, Y. Yue, and J. Yao, "Statistical recognition method of binary BCH Code," *Communications and Network*, vol. 3, pp. 17-22, 2011.

[9] H. Lee, C. S. Park, J. H. Lee, and Y. J. Song, "Reconstruction of BCH codes using probability compensation," *Proc. IEEE 18th Asia-Pacific Conference on Communications*, pp. 591-594, 2012.

[10] A. U. Mustafa, and G. Murtaza, "Synthesis-by-analysis of BCH codes," *arXiv preprint arXiv:1210.7906*, 2012.

[11] J. Wang, Y. Yue, and J. Yao, "A method of blind recognition of cyclic code generator polynomial," *Proc. IEEE 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, pp. 1-4, 2010.

[12] W. Lei, H. Yihua, H. Shiqi, and Q. Lin, "The method of estimating the length of linear cyclic code based on the distribution of code weight," *Proc. IEEE 2nd International Conference on Information Science and Engineering (ICISE)*, pp. 2459-2462, 2010.

[13] Z. Jing, H. Zhiping, S. Shaojing, and Y. Shaowu, "Blind recognition of binary cyclic codes," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1-17, 2013.

[14] W. Li, J. Lei, L. Wen, and B. Chen, "An improved method of blind recognition of RS code based on matrix transformation," *Proc. 15th IEEE International Conference on Communication Technology (ICCT)*, pp. 196-200, 2013.

[15] C. Li, T. Q. Zhang, and Y. Liu, "Blind recognition of RS codes based on galois field columns Gaussian elimination," *Proc. IEEE 7th International Congress on Image and Signal Processing (CISP)*, pp. 836-841, 2014.

[16] T. Li, C.L. Miao, and J. Lv, "An improved algorithm of RS codes blind recognition," *Proc. Applied Mechanics and Materials, Trans Tech Publ.*, pp. 2308-2312, 2014.

[17] M. Cluzeau, "Block code reconstruction using iterative decoding techniques," *Proc. ISIT'06*, pp. 2269-2273, 2006.

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

[۱۹] پ. گردانی، ع. کشاورز حداد و ع. جمشیدی، «استخراج کور ویژگی‌های کدهای بلوکی خطی و کانولوشنال در حضور نویز،» *دومین کنفرانس سامانه‌های مراقبتی پسیو*، دانشگاه شیراز، شیراز، ایران، ۱۳۹۲.

[۲۰] ف. زارع، ع. جمشیدی و ع. کشاورز حداد، «تخمین کور سایز اینترلیور در کانال‌های دارای نویز گروهی،» *دومین کنفرانس سامانه‌های مراقبتی پسیو*، دانشگاه شیراز، شیراز، ایران، ۱۳۹۲.

زیرنویس‌ها

[1] Matrix Rank
[2] Parity Check Matrix
[3] Bose-Chaudhary-Hocquenghem Codes
[4] Generator Polynomial
[5] Minimal Polynomials
[6] Greatest Common Divisor
[7] Reed-Solomon
[8] Galois Field
[9] Interleaver
[10] Cyclic Shift
[11] Rank Deficient
[12] Binary Phase Shift Keying
[13] Additive White Gaussian Noise