
بسم الله الرحمن الرحیم

دانشکده علوم ریاضی

رشته ریاضی کاربردی، گرایش گراف و ترکیبیات

پایان‌نامه کارشناسی ارشد

ماتریس‌های مولد و ماتریس‌های بررسی توازن کدهای صحیح تعمیم‌یافته

نگارنده: گلشن گلعلی‌زاده شیری

استادان راهنما

دکتر نادر جعفری‌راد
دکتر عبدالله آل‌هوز

دی‌ماه ۱۳۹۵

فرم شماره ۷: صورتجلسه دفاع از پایان نامه تحصیلی دوره کارشناسی ارشد

با تأییدات خداوند متعال و با استعانت از حضرت ولی عصر (عج) ارزیابی جلسه دفاع از پایان نامه کارشناسی ارشد خانم **گلشن گلعلی زاده شیری** به شماره دانشجویی **۹۳۱۴۷۵۴** رشته **ریاضی کاربردی** گرایش **گراف و ترکیبات** تحت عنوان **ماتریس های مولد و ماتریس های بررسی توازن کدهای صحیح تعمیم یافته** که در تاریخ **۱۳۹۵/۱۰/۲۷** با حضور هیأت محترم داوران در دانشگاه صنعتی شاهرود برگزار گردید به شرح ذیل اعلام می‌گردد:

قبول (با درجه بسیار خوب و امتیاز ۱۸/۸۸) ☐ دفاع مجدد ☐ مردود ☐

نوع تحقیق: نظری ☑ عملی ☐

۱ـ عالی (۲۰ ـ ۱۹)
۲ـ بسیار خوب (۱۸/۹۹ ـ ۱۸)
۳ـ خوب (۱۷/۹۹ ـ۱۶)
۴ـ قابل قبول (۱۵/۹۹ ـ ۱۴)
۵- نمره کمتر از ۱۴ غیر قابل قبول

عضو هیأت داوران	نام ونام خانوادگی	مرتبهٔ علمی	امضاء
۱ـ استادراهنمای اول	دکتر نادر جعفری راد	دانشیار	
۲- استادراهنمای دوم	دکتر عبدالله آل هوز	استادیار	
۳- استاد مشاور			
۴- نماینده شورای تحصیلات تکمیلی	دکتر ابراهیم هاشمی	استاد	
۵- استاد ممتحن اول	دکتر میثم علیشاهی	استادیار	
۶ـ استاد ممتحن دوم	دکتر صادق رحیمی شعرباف	استادیار	

رئیس دانشکده: دکتر ابراهیم هاشمی

تقدیمی کوچک و بضاعتی مزجات به محضر:

آسمان (تعالی اسمه)، بلندای رفیعش و مهربانی بی‌مانندش
حضرت باران (سلام الله علیها) و پدر و بعل و خاندانش
حضرت عشق (علیه السلام) و برادر و یاران باوفایش
حضرت بهار (عجل الله فرجه) و ظهور باطراوتش
حضرت روح خدا (رحمه الله علیه) و شهدایش
حضرت نائب (حفظه الله) و سربازانش

و همچنین

پدر و مادر عزیزم
که ذکر و دعاهای آن‌ها، فرش مسیر تلاشم شد.

سپاس گزاری...

اولین چکه ناودان بلندیک احساس را، در قالب کلامی از جنس تنفس باغنچه های معصوم یاس، بر روی حجم سپیدیک برگه می ریزم و آن را به لهجه های همه پروانه صفتهای این گیتی بی انتها به آستان نیلوفری دلهای زلال هدیه می کنم.

ای یزدان پاک تو را سپاس می گویم،

که به حکمت بی انتهایت مرا یاری کردی،

و به رحمت نعمتهایت را بر من تمام کردی،

خانواده ای خوب به من عطا کردی که در همه حال پشتیبانی ام کنند و استادانی سر راهم نهادی تا دانش و علمشان را بی ریا در اختیارم بگذارند.

بر خود لازم می دانم از همه عزیزانی که در جهت به سرانجام رساندن این رساله مرا یاری نمودند، قدردانی کنم. مراتب قدردانی خود را از زحمات بی دریغ استادان، دکتر نادر

جعفری رادو دکتر عبدالله آل هوز ابراز می نمایم.

گلشن گلعلی‌زاده شیری
دی‌ماه ۱۳۹۵

تعهد نامه

اینجانب **گلشن گلعلی‌زاده شیری** دانشجوی کارشناسی ارشد رشته **ریاضی کاربردی علوم ریاضی** دانشگاه صنعتی شاهرود، نویسنده پایان‌نامه با عنوان **ماتریس‌های مولد و ماتریس‌های بررسی توازن کدهای صحیح تعمیم‌یافته** ، تحت راهنمایی **دکتر نادر جعفری راد** و **دکتر عبدالله آل‌هوز** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های دیگر پژوهش‌گران، به مرجع مورد استفاده استناد شده است.
- مطالب این پایان‌نامه، تا کنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ‌جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود تعلق دارد، و مقالات مستخرج با نام‘‘ دانشگاه صنعتی شاهرود‘‘ یا ‘‘ Shahrood University of Technology ‘‘ به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آوردن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده شده است)، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

گلشن گلعلی‌زاده شیری
دی‌ماه ۱۳۹۵

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان‌نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

کدهای شبه‌دوری تعمیم‌یافته به عنوان یک زیرمدول روی حلقه چندجمله‌ای‌ها مورد بحث قرارمی‌گیرد. ماتریس مولد و ماتریس بررسی توازن کد شبه‌دوری تعمیم‌یافته، به عنوان یک کد خطی، می‌تواند به صورت ترکیبی از ماتریس‌های گردشی با تعداد ستون‌های متفاوت نمایش داده شود. مشابه کدهای دوری، کدهای شبه‌دوری تعمیم‌یافته می‌توانند توسط ماتریس‌های چندجمله‌ای معرفی شوند.
کدهای صحیح تعمیم‌یافته نمونه‌ای از کدها روی حلقه اعداد صحیح به پیمانه n می‌باشند که در آنها به طور کلی پیمانه‌های مختلف نماد کدهای منحصر به‌فرد است. در این پایان نامه، با استفاده از معادلات ماتریسی، شرایط لازم و کافی برای اینکه یک ماتریس با درایه‌هایی از اعداد صحیح، ماتریس مولد کدهای صحیح تعمیم یافته باشد را به‌دست می‌آوریم. علاوه براین نشان می‌دهیم که معادلات ماتریسی فوق برای به‌دست آوردن ماتریس بررسی توازن این کدها نیز استفاده می‌شود و کارایی دارد. در نهایت، الگوریتم‌های کارا و بهینه برای شمارش تمام ماتریس‌های چندجمله‌ای مولد کدهای شبه‌دوری تعمیم‌یافته و همچنین برای شمارش همه‌ی ماتریس‌های مولد کدهای صحیح تعمیم‌یافته، ارائه می‌دهیم.

کلمات کلیدی: ماتریس مولد، ماتریس بررسی توازن، ماتریس چندجمله‌ای، ماتریس گردشی، کد صحیح تعمیم یافته، کد شبه‌دوری تعمیم‌یافته، الگوریتم بوخ‌برگر، مقسوم‌علیه‌های اولیه، الگوریتم اقلیدسی تعمیم یافته.

پیشگفتار

هرچند به نظر می‌رسد نظریه کدگذاری در کشور ایران موضوعی جدید است اما شروع کلاسیک آن به سال ۱۹۴۸ و انتشار مقاله **کلودشانون**[۱] برمی‌گردد. وی مقاله‌ای با عنوان **نظریه ریاضی ارتباطات** را منتشر کرد که در آن نشان داد برای یک کانال پارازیت‌دار، عددی به عنوان ظرفیت کانال وجود دارد که در صورت به‌کارگیری روش‌های مناسب کدگذاری و کدگشایی، ارتباط معتبر با هر سرعت کمتر از ظرفیت کانال قابل دستیابی است. این مقاله تولدی شد برای نظریه کدگذاری که حوزه‌ای از مطالعات درباره انتقال داده‌ها از طریق کانال‌های پارازیت‌دار و کشف پیام‌های خطادار است. این نظریه در بیشتر حوزه‌ها، از سیستم ارتباطی و پخش‌کننده‌های لوح فشرده گرفته تا فناوری ذخیره‌سازی بسیار کاربرد داشته‌است.
در حالی که مسائل نظریه کدگذاری اغلب از کاربردهای مهندسی نشأت می‌گیرند، جالب است به نقش تعیین کننده‌ای که ریاضیات در توسعه موضوع داشته‌است توجه شود. اهمیت جبر، ترکیبات و هندسه در نظریه کدگذاری، حقیقتی تأییدشده توسط نتایج عمیق ریاضی است که با روش‌هایی ظریف برای پیشرفت نظریه کدگذاری مورد استفاده قرار گرفته‌اند.
طراحی کدهای خوب، از هر دو دیدگاه نظری و کاربردی مسأله‌ای بسیار مهم در نظریه کدگذاری است. از زمان پیدایش نظریه کدگذاری پژوهشگران در این راستا بسیار تلاش کرده، در جریان این تلاش گونه‌های جالب زیادی از این کدها را تولید کرده‌اند. این پایان نامه تا حدودی حول این زمینه‌ها نگاشته شده است.
در فصل اول این پایان‌نامه تعاریف و مفاهیم مقدماتی را که در فصول بعدی به کار گرفته شده‌اند، بیان می‌کنیم. در فصل دوم به معرفی مقدماتی کدهای شبه‌دوری تعمیم‌یافته می‌پردازیم. یک رابطه بین ماتریس چندجمله‌ای مولد و ماتریس چندجمله‌ای بررسی توازن کدهای شبه دوری تعمیم‌یافته بیان می‌کنیم. برخی نتایج کدهای شبه‌دوری در مرجع [18] را به کدهای شبه‌دوری تعمیم‌یافته تعمیم می‌دهیم. به کمک قضیه دوگانگی ادعا می‌کنیم که ماتریس چندجمله‌ای بررسی توازن به کمک ماتریس چندجمله‌ای مولد که در رابطه ماتریسی $AG = \mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$ صدق می‌کند، بدست می‌آید و بالعکس. در فصل سوم کدهای صحیح تعمیم‌یافته را معرفی می‌کنیم و با استفاده از نظریه گروههای آبلی، ماتریس مولد کدهای صحیح تعمیم‌یافته را بدست می‌آوریم. به کمک رابطه ماتریسی

$$AG = \mathrm{diag}[n_1, \ldots, n_l]. \qquad (1)$$

خصوصیات ماتریس مولد و همچنین رابطه بین ماتریس مولد و ماتریس بررسی توازن کدهای صحیح تعمیم یافته را بیان می‌کنیم. در فصل چهارم با توجه به ساختار جبری آشکار کدهای شبه‌دوری تعمیم‌یافته و کدهای صحیح تعمیم‌یافته الگوریتم هایی را برای بدست آوردن ماتریس‌های مولد این کدها ارائه می‌دهیم.

[۱] Claud Shannon

فهرست مطالب

فصل ۱

تعاریف و قضایای مقدماتی

در این فصل مفاهیم مقدماتی مورد نظر پایان‌نامه را بیان کرده و تقریباً تمامی تعاریف و قضایای مهمی که پیش نیاز فصل‌های بعد می‌باشند را ذکر می‌نماییم.

۱.۱ مفاهیم جبری

۱.۱.۱ گروه، حلقه و میدان

تعریف ۱.۱.۱. *مجموعه ناتهی G را به همراه عمل دوتایی $(*)$ روی آن، **گروه** گویند اگر شرایط زیر برقرار باشد:*

۱. *G تحت عمل $*$ بسته باشد، یعنی، برای هر عنصر $a, b \in G$ ، عنصر $a * b$ در G باشد.*

۲. *عمل $*$ شرکت پذیر باشد، یعنی برای هر عنصر $a, b, c \in G$ ، داشته باشیم: $a*(b*c) = (a*b)*c$.*

۳. *G شامل یک عنصر e است به طوری که برای هر عنصر $a \in G$ داشته‌باشیم: $a * e = e * a = a$.*

۴. *برای هر عنصر $a \in G$ عنصر a' در G موجود است به گونه‌ای که $a * a' = a' * a = e$ برقرار باشد. عنصر a' را وارون عنصر a گویند.*

تعریف ۲.۱.۱. *زیر مجموعه ناتهی H از گروه G را تحت عمل $(*)$ یک **زیرگروه** از G نامیم هرگاه، H به همراه عمل $(*)$ خود یک گروه باشد و آن را با نماد $H \leqslant G$ نمایش می‌دهیم. به عبارت دیگر زیر مجموعه ناتهی H از گروه G زیر گروهی از مجموعه ناتهی $(G, *)$ است هرگاه در شرایط زیر صدق کند:*

۱. برای هر دو عنصر $a, b \in H$ داشته باشیم: $a * b \in H$.

۲. اگر $a \in H$ موجود باشد آنگاه داشته باشیم: $a^{-1} \in H$.

تعریف ۳.۱.۱. گروه $(G, *)$ **آبلی** است اگر برای هر دو عنصر $a, b \in G$ رابطه $a * b = b * a$ برقرار باشد.

تعریف ۴.۱.۱. اگر $(G, \circ)$ و $(H, \star)$ دو گروه باشند، آنگاه تابع $f : G \longrightarrow H$ را یک **همریختی**[۱] گوییم هرگاه برای هر دو عنصر $a, b \in G$ داشته باشیم :

$$f(a \circ b) = f(a) \star f(b).$$

همچنین تابع f را یک **یکریختی**[۲] گوییم هرگاه f یک‌به‌یک و پوشا باشد.

تعریف ۵.۱.۱. مجموعه ناتهی R را به همراه دو عمل جمع $(+)$ و ضرب $(\cdot)$ **حلقه** نامیم هرگاه شرایط زیر برقرار باشد:
برای هر $a, b, c \in R$:

۱. R تحت عمل جمع $(+)$ یک گروه آبلی است.

۲. R تحت عمل ضرب $(\cdot)$ بسته و شرکت پذیر است، لذا رابطه $a.(b.c) = (a.b).c$ برقرار است.

۳. ضرب $(\cdot)$ نسبت به جمع $(+)$ توزیع‌پذیر است، ازاین‌رو داریم: $a.(b + c) = a.b + a.c$.

تعریف ۶.۱.۱. زیر مجموعه ناتهی S از حلقه R را یک **زیرحلقه** از R می‌گوییم هرگاه، S با عمل‌های تعریف‌شده روی R خود یک حلقه باشد.

تعریف ۷.۱.۱. زیر مجموعه I از حلقه R را یک **ایده‌آل** نامیم هرگاه شرایط زیر برقرار باشد:

۱. برای هر $a, b \in I$، آنگاه $a - b \in I$ باشد.

۲. برای هر عنصر $a \in R$ و $i \in I$، عناصر ia و ai در I موجود باشند.

تعریف ۸.۱.۱. اگر I یک ایده‌آل از حلقه‌ی R باشد، R/I را **حلقه خارج‌قسمتی** R بر I می‌نامیم و داریم:

$$R/I = \{x + I | x \in R\}.$$

تعریف ۹.۱.۱. فرض کنید K حلقه‌ای جابجایی و یکدار باشد، $K-$**جبر** A حلقه‌ای است که:

۱. $(A, +)$ یک $K-$ مدول یکانی باشد.

۲. برای هر $k \in K$ و $a, b \in A$ داشته‌باشیم:

$$k(ab) = (ka)b = a(kb).$$

[۱] Homomorphism
[۲] Isomorphism

تعریف ۱.۱.۱۰. *مجموعه ناتهی $\mathbb{F}$ را به همراه دو عمل دوتایی جمع $(+)$ و ضرب $(\cdot)$* **میدان** *نامیم هرگاه در شرایط زیر صدق کند:*

۱. *$\mathbb{F}$ نسبت به عمل جمع، بسته و یک گروه آبلی است. عنصر همانی نسبت به عمل جمع را عنصر صفر $\mathbb{F}$ می‌نامیم و با ۰ نشان می‌دهیم؛*

۲. *مجموعه عناصر ناصفر $\mathbb{F}$ تحت عمل ضرب، بسته و یک گروه آبلی است، عنصر همانی نسبت به عمل ضرب را عنصر یکه $\mathbb{F}$ می‌نامیم و با ۱ نشان می‌دهیم؛*

۳. *عمل ضرب نسبت به عمل جمع توزیع پذیر است؛ یعنی رابطه $a.(b+c) = a.b + a.c$ برقرار است.*

تعریف ۱.۱.۱۱. *تعداد عناصر میدان را* **مرتبه** *میدان گوییم. یک میدان با تعداد عناصر متناهی را یک* **میدان متناهی** *می‌نامیم .*

تعریف ۱.۱.۱۲. ۱. *فرض کنید $\mathbb{F}$ یک میدان باشد، زیرمجموعه K از $\mathbb{F}$ که تحت عمل‌های $\mathbb{F}$ یک میدان باشد را یک* **زیرمیدان** *$\mathbb{F}$ می‌نامند. همچنین $\mathbb{F}$ را* **توسیع میدان** *$\mathbb{K}$ گویند.*

۲. *اگر $\mathbb{K}$ زیرمیدانی از $\mathbb{F}$ باشد و داشته باشیم $\mathbb{K} \neq \mathbb{F}$، آنگاه $\mathbb{K}$* **زیرمیدان سره** *از $\mathbb{F}$ نامیده می‌شود.*

تعریف ۱.۱.۱۳. *فرض کنید $\mathbb{F}$ یک میدان باشد. مجموعه*

$$\mathbb{F}[x] = \{a_۰ + a_۱x + \cdots + a_nx^n \quad , \quad a_i \in \mathbb{F}, n \geq ۰\}$$

حلقه چندجمله‌ای *روی $\mathbb{F}$ نامیده می‌شود.*

یادآوری برخی از حقایق شناخته شده در مورد $\mathbb{F}_q[x]$ لازم به نظر می‌رسد.

تعریف ۱.۱.۱۴. *چندجمله‌ای $f(x)$ با درجه مثبت را روی $\mathbb{F}$* **تحویل‌پذیر** *می‌نامیم اگر دو چندجمله‌ای $h(x)$ و $g(x)$ روی $\mathbb{F}$ چنان موجود باشند که $\deg h(x) < \deg f(x)$، $\deg g(x) < \deg f(x)$ و همچنین $f(x) = g(x)h(x)$ باشد. در غیر این صورت چندجمله‌ای $f(x)$ از درجه مثبت را* **تحویل‌ناپذیر** *(روی $\mathbb{F}$) نامیم.*

تعریف ۱.۱.۱۵. *فرض کنید $f(x) \in \mathbb{F}[x]$، چندجمله‌ای از درجه $n \geq ۱$ باشد. دراین صورت، برای هر چندجمله‌ای $g(x) \in \mathbb{F}[x]$، چندجمله‌ایهای $r(x)$ و $s(x)$ با شرط $\deg r(x) \leq \deg f(x)$ یا $r(x) = ۰$ وجود دارند به‌طوری که داشته‌باشیم: $q(x) = s(x)f(x) + r(x)$. چندجمله‌ای $r(x)$، باقیمانده‌ی $g(x)$ در تقسیم بر $f(x)$ نامیده می‌شود.*

تعریف ۱.۱.۱۶. *فرض کنید $f(x), g(x) \in \mathbb{F}[x]$ دو چندجمله‌ای غیرصفر باشند.* **بزرگترین مقسوم علیه مشترک** *$f(x)$ و $g(x)$ را با $\gcd(f(x), g(x))$[۳] نشان می‌دهند که برابر است با چندجمله‌ای منحصر به فرد با بیشترین درجه به طوری که $f(x)$ و $g(x)$ را عاد می‌کند. و اگر $f(x)$ و $g(x)$ نسبت به هم اول باشند، آنگاه*

[۳] Greatest common divisor

$\gcd(f(x),g(x))=۱$. همچنین **کوچکترین مضرب مشترک** $f(x)$ و $g(x)$ را با $\operatorname{lcm}(f(x),g(x))$[۴] *نشان می‌دهیم و برابر است با چندجمله‌ای منحصر به فرد با کمترین درجه به طوری که* $f(x)$ *و* $g(x)$ *هر دو آن را عاد می‌کنند.*

قضیه ۱.۱.۱. *فرض کنید* $f(x)$ *یک چندجمله‌ای با درجه* $n \geqslant ۱$ *روی میدان* $\mathbb{F}$ *باشد. در این صورت* $\mathbb{F}_q[x]/(f(x))$ *یک حلقه است. همچنین* $\mathbb{F}_q[x]/(f(x))$ *یک میدان است اگر و فقط اگر* $f(x)$ *تحویل ناپذیر باشد.*

برهان. به مرجع [24] مراجعه شود. □

تعریف ۱۷.۱.۱. *یک گروه آبلی* V *به همراه عمل دوتایی جمع* $(+)$ *روی آن را در نظر بگیرید. فرض کنید* $\mathbb{F}$ *یک میدان بوده و یک عمل ضرب اسکالر* $(\cdot)$ *از* $\mathbb{F}\times V$ *به* V *تعریف شده باشد. مجموعه* V *را یک* **فضای برداری** *روی* $\mathbb{F}$ *نامند اگر در شرایط زیر صدق کند:*

۱. *قانون توزیع پذیری بین* $\mathbb{F}$ *و* V *برقرار باشد. یعنی اگر* $a,b\in\mathbb{F}$ *و* $u,v\in V$ *موجود باشند آنگاه داشته باشیم:*

(آ) $a(u+v)=au+av$.

(ب) $(a+b)v=av+bv$.

۲. *قانون شرکت پذیری بین* $\mathbb{F}$ *و* V *برقرار باشد. یعنی برای هر* $a,b\in\mathbb{F}$ *و* $v\in V$ *داشته‌باشیم:* $(ab)v=a(bv)$.

۳. *اگر ۱ عضو خنثی ضربی در* $\mathbb{F}$ *باشد، در این صورت برای هر* $v\in V$ *رابطه* $۱\cdot v=v$ *برقرار باشد.*

تعریف ۱۸.۱.۱. *یک دنباله مرتب شده با* n *مؤلفه* $a_۰,a_۱,\ldots,a_{n-۱}$ *که هر مؤلفه آن عنصری از* $\mathbb{F}_q$ *است را در نظر بگیرید. این دنباله را یک* $n-$*تایی روی* $\mathbb{F}_q$ *می‌نامیم.* q *روش برای انتخاب هر* a_i *وجود دارد. بنابراین* q^n*،* $n-$*تایی متفاوت موجود است. مجموعه* $(\mathbb{F}_q)^n$ *همه* $n-$*تایی‌های مرتب روی* $\mathbb{F}_q$ *است که آن را با* $\mathbb{F}_q^n$ *نشان می‌دهیم. عناصر* $\mathbb{F}_q^n$ *را بردار می‌نامیم .*

تعریف ۱۹.۱.۱. *دو عمل روی* $\mathbb{F}_q^n$ *تعریف می‌کنیم:*

الف) جمع دو بردار: برای هر $V=(v_۰,v_۱,\ldots,v_{n-۱})$ *و* $U=(u_۰,u_۱,\ldots,u_{n-۱})$ *در* $\mathbb{F}_q^n$ *بردار* $U+V$ *به فرم زیر است:*

$$U+V=(u_۰+v_۰,u_۱+v_۱,\ldots,u_{n-۱}+v_{n-۱})\in\mathbb{F}_q^n.$$

ب) حاصلضرب یک بردار در یک اسکالر: اگر $V=(v_۰,v_۱,\ldots,v_{n-۱})\in\mathbb{F}_q^n$ *و* $a\in\mathbb{F}_q$ *موجود باشد، داریم:*

$$a(v_۰,v_۱,\ldots,v_{n-۱})=(av_۰,av_۱,\ldots,av_{n-۱})\in F_q^n.$$

جمع برداری و ضرب اسکالر تعریف شده در (الف) و (ب) به ترتیب در قوانین توزیع‌پذیری و شرکت‌پذیری صدق می‌کنند. بنابراین مجموعه $\mathbb{F}_q^n$ *یک* **فضای برداری** *روی* $\mathbb{F}_q$ *است.*

[۴] Least common multiple

تعریف ۱.۱.۲۰. *یک زیرمجموعه از $\mathbb{F}_q^n$ یک* **زیرفضای** *$\mathbb{F}_q^n$ است هرگاه تحت عمل جمع و ضرب تعریف شده روی $\mathbb{F}_q^n$ یک فضای برداری باشد.*

تعریف ۱.۱.۲۱. *فرض کنید V یک فضای برداری روی $\mathbb{F}_q$ باشد و فرض کنید $S = \{v_1, v_2, \ldots, v_k\}$ زیرمجموعه‌ای ناتهی از V باشد.* **زیرفضای (خطی) تولید شده توسط** *S به شکل زیر تعریف می‌شود:*

$$\langle S\rangle = \{\lambda_1 v_1 + \cdots + \lambda_k v_k : \lambda_i \in \mathbb{F}_q\}.$$

اگر $S = \phi$ باشد، تعریف می‌کنیم: $\langle S\rangle = \{0\}$.

تعریف ۱.۱.۲۲. *فرض کنید V یک فضای برداری روی میدان $\mathbb{F}_q$ باشد. آنگاه زیرمجموعه غیر تهی مانند $B = \{v_1, v_2, \ldots, v_k\}$ از V را یک* **پایه** *برای V می‌نامیم اگر $V = \langle B\rangle$ و B مستقل خطی باشد.*

نکته ۱.۱.۱. *اگر $B = \{v_1, v_2, \ldots, v_k\}$ یک پایه برای V باشد، آنگاه هر بردار $v \in V$ را می‌توان به صورت ترکیب خطی منحصر به فردی از اعضای پایه بیان کرد. به عبارت دیگر، عناصر یکتای $\lambda_1, \lambda_2, \ldots, \lambda_k \in F_q$ وجود دارند به طوری که داشته‌باشیم:*

$$v = \lambda_1 v_1 + \cdots + \lambda_k v_k.$$

تعریف ۱.۱.۲۳. *فضای برداری V روی میدان متناهی $\mathbb{F}_q$ می‌تواند چندین پایه داشته‌باشد، اما تعداد اعضای پایه‌ها باهم برابر است. این تعداد را،* **بعد** *V روی $\mathbb{F}_q$ می‌نامیم و با $\dim_{\mathbb{F}_q}(V)$ نشان‌می‌دهیم.*

قضیه ۱.۱.۲. *فرض کنید V یک فضای برداری روی $\mathbb{F}_q$ باشد؛ اگر $\dim_{\mathbb{F}_q}(V) = k$ باشد، آنگاه:*

۱. *V دارای q^k عضو می‌باشد؛*

۲. *V دارای $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$ پایه متفاوت است.*

برهان. به مرجع [24] مراجعه شود. □

تعریف ۱.۱.۲۴. *فرض کنید $V = (v_1, \ldots, v_n), W = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ موجود باشند.*

۱. *دو بردار V و W برهم عمودند اگر داشته‌باشیم $V \cdot W = 0$.*

۲. *فرض کنید S یک زیرمجموعه‌ی غیرتهی از $\mathbb{F}_q^n$ باشد، دوگان S به‌صورت زیر تعریف می‌شود:*

$$S^\perp = \{v \in \mathbb{F}_q^n : v \cdot s = 0, s \in S \text{ برای هر}\}.$$

اگر $S = \phi$ باشد، در این صورت تعریف می‌کنیم: $S^\perp = \mathbb{F}_q^n$.

لم ۱.۱.۱. *$S^\perp$ برای هر زیرمجموعه S از $\mathbb{F}_q^n$ همواره یک زیرفضا از فضای برداری $\mathbb{F}_q^n$ می‌باشد، و داریم: $\langle S\rangle^\perp = S^\perp$.*

قضیه ۱.۱.۳. *فرض کنید S زیرمجموعه‌ای از $\mathbb{F}_q^n$ باشد، در این صورت داریم:*

$$\dim\langle S\rangle + \dim S^\perp = n.$$

برهان. به مرجع [24] مراجعه شود. □

۲.۱.۱ مدول

تعریف ۲۵.۱.۱. *فرض کنید R یک حلقه بوده و $(M,+)$ یک گروه آبلی و $f : R \times M \longrightarrow M$ یک تابع باشد. (برای سهولت $f(r,m)$ را با $r \cdot m$ نشان می‌دهیم. توجه کنید $r \cdot m$ را ضرب اسکالر r در m گویند) و در ضمن خواص زیر برقرار باشند:*

۱. *به‌ازای هر $r \in R$ و $m_۱, m_۲ \in M$ داشته‌باشیم:*

$$r \cdot (m_۱ + m_۲) = r \cdot m_۱ + r \cdot m_۲.$$

۲. *به‌ازای هر $r_۱, r_۲ \in R$ و $m \in M$ داشته‌باشیم:*

$$(r_۱ + r_۲)m = r_۱ \cdot m + r_۲ \cdot m.$$

۳. *به‌ازای هر $r_۱, r_۲ \in R$ و $m \in M$ داشته‌باشیم:*

$$r_۱ \cdot (r_۲ \cdot m) = (r_۱ \cdot r_۲).m.$$

*دراین‌صورت M را یک $R-$**مدول چپ**گویند. به‌طریق مشابه $R-$**مدول راست** نیز تعریف‌می‌شود.*

تعریف ۲۶.۱.۱. *$R-$مدول چپ M را **یکانی**گوییم هرگاه R یکدار باشد و به‌ازای هر $m \in M$ داشته‌باشیم:*

$$۱ \cdot m = m.$$

تعریف ۲۷.۱.۱. *فرض کنید M یک $R-$مدول باشد، در این صورت زیرمجموعه ناتهی N از M را یک **زیرمدول** M نامیم هرگاه N با همان جمع و ضرب اسکالر M خود یک مدول باشد.*

تعریف ۲۸.۱.۱. *فرض کنید M و N دو $R-$مدول باشند دراین‌صورت تابع $f : M \longrightarrow N$ را یک **همریختی** $R-$مدولی گوییم هرگاه دو شرط زیر برقرار باشد:*

۱. *برای $m_۱, m_۲ \in M$ ، داشته‌باشیم: $f(m_۱ + m_۲) = f(m_۱) + f(m_۲)$.*

۲. *برای هر $m \in M$ و $r \in R$ ، داشته‌باشیم: $f(rm) = rf(m)$.*

*اگر f به‌ترتیب پوشا و یک‌به‌یک باشد آن را به‌ترتیب یک **برووریختی**[۵] و **تکریختی**[۶] می‌نامیم. در صورتی‌که f هم یک‌به‌یک و هم پوشا باشد، f را یک **یکریختی** $R-$مدولی می‌نامند.*

تعریف ۲۹.۱.۱. *فرض کنید A ، B و C سه $R-$مدول بوده و $f : A \longrightarrow B$ و $g : B \longrightarrow C$ دو همریختی $R-$مدولی باشند، در این صورت رشته‌ی $A \xrightarrow{f} B \xrightarrow{g} C$ را یک **رشته دقیق**[۷] گوییم هرگاه:*

$$\ker g = \mathrm{Im} f.$$

[۵] Epimorphism
[۶] Monomorphism
[۷] Exact sequence

بنابراین اگر $A \xrightarrow{f} B \xrightarrow{g} C$ *یک رشته دقیق باشد، آنگاه* $\mathrm{gof} = ۰$ *خواهدبود. به همین ترتیب رشته* $A_۰ \xrightarrow{f_۰} A_۱ \xrightarrow{f_۱} A_۲ \xrightarrow{f_۲} \cdots \xrightarrow{f_n} A_{n+۱}$ *از* $R-$*مدول‌ها و همریختی‌های* $R-$*مدولی را یک رشته‌ی دقیق گویند، هرگاه به ازای هر* i *داشته‌باشیم:* $\mathrm{Im} f_i = \ker f_{i+۱}$.

تعریف ۳۰.۱.۱. رشته‌ی دقیق $۰ \to A \xrightarrow{f} B \xrightarrow{g} C \to ۰$ را یک **رشته‌ی دقیق کوتاه** می‌نامند.

قضیه ۴.۱.۱. *فرض کنید* R *یک حلقه بوده و* A ، B *و* C *سه* $R-$*مدول باشند. اگر رشته دقیق کوتاه* $۰ \to A \xrightarrow{f} B \xrightarrow{g} C \to ۰$ *را داشته‌باشیم، در این صورت گزاره‌های زیر معادلند:*

۱. *همریختی* $R-$*مدولی* $h : C \to B$ *وجود دارد به طوری که،* $gh = ۱_C$.

۲. *همریختی* $R-$*مدول* $k : B \to A$ *وجود دارد به طوری که،* $kf = ۱_A$.

برهان. به مرجع [37] مراجعه شود. □

تعریف ۳۱.۱.۱. *گوییم رشته‌ی دقیق کوتاه* $۰ \to A \xrightarrow{f} B \xrightarrow{g} C \to ۰$ *شکافته است یا شکافته می‌شود هرگاه یکی از شرایط قضیه ۴.۱.۱ برقرار باشد.*

قضیه ۵.۱.۱. *اگر رشته‌ی دقیق کوتاه* $۰ \to A \xrightarrow{f} B \xrightarrow{g} C \to ۰$ *شکافته شده باشد در این صورت داریم:*

$$B \simeq A \oplus C.$$

برهان. به مرجع [37] مراجعه شود. □

۳.۱.۱ ماتریس

تعریف ۳۲.۱.۱. ماتریس قطری *یک ماتریس* $n \times n$ *است که هر مؤلفه روی قطر اصلی غیر صفر بوده و دیگر مؤلفه‌ها صفر باشند، و به شکل* $A = \mathrm{diag}(a_{۱۱}, \ldots, a_{nn})$ *نمایش داده‌می‌شود. دترمینان ماتریس* A *به شکل زیر تعیین می‌شود:*

$$\det A = \prod_{i=۱}^{n} a_{ii}.$$

تعریف ۳۳.۱.۱. *در یک ماتریس مربعی، اگر تمام درایه‌های بالای قطر اصلی صفر باشند، ماتریس را* **پایین‌مثلثی** *یک ماتریس و هرگاه همه درایه‌های زیر قطر اصلی صفر باشند ماتریس را* **بالامثلثی** *یک ماتریس می‌نامیم.*

تعریف ۳۴.۱.۱. *حداکثر تعداد سطرها و یا ستونهای مستقل خطی ماتریس* A ، **رتبه ماتریس** A *نامیده می‌شود و با* $\mathrm{rank}(A)$ *نمایش می‌دهیم و همواره داریم :*

$$۱ \leq r(A) \leq \min\{m, n\}.$$

تعریف ۳۵.۱.۱. *فرض کنید* A *یک ماتریس روی میدان* $\mathbb{F}_q$ *باشد؛* **عملیات سطری مقدماتی** *روی ماتریس* A *یکی از سه عمل زیر است:*

۱. *جابه‌جا کردن دو سطر.*

۲. *ضرب یک سطر در یک اسکالر غیرصفر.*

۳. *جایگزین کردن یک سطر با مجموع آن سطر و مضربی از سطر دیگر.*

تعریف ۳۶.۱.۱. *دو ماتریس هم‌ارز سطری‌اند اگر یکی از آنها به‌وسیله دنباله‌ای از عملیات سطری مقدماتی از ماتریس دیگر حاصل شود.*

تعریف ۳۷.۱.۱. *یک ماتریس را* **سطری پلکانی** *(REF)*[۸] *نامیم هرگاه:*

۱. *سطرهای صفر پایین بقیه سطرها باشد.*

۲. *اولین عنصر غیرصفر هر سطر غیرصفر، یک باشد.*

۳. *یک مقدم هر سطر، در سمت راست یک مقدم سطرهای بالایی باشد.*

تعریف ۳۸.۱.۱. *ماتریس سطری پلکانی (REF) را* **تحویل شده سطری پلکانی** *(RREF)*[۹] *نامیم هرگاه، درایه‌های دیگر هر ستون حاوی یک مقدم، صفر باشند.*

تعریف ۳۹.۱.۱. *دو ماتریس A و B را در نظر بگیرید. دراین صورت B* **متشابه** *با A است اگر ماتریس نامنفردی مانند P وجود داشته‌باشد به طوری که داشته‌باشیم: $P^{-1}AP = B$.*

تعریف ۴۰.۱.۱. *ماتریس A را* **قطری‌شدنی** *گویند هرگاه متشابه با یک ماتریس قطری باشد. به عبارت دیگر، ماتریس نامنفردی مانند P وجود داشته‌باشد به طوری که داشته‌باشیم،*

$$P^{-1}AP = D = \operatorname{diag}(d_1, \ldots, d_n).$$

تعریف ۴۱.۱.۱. *برای هر ماتریس $A_{n\times m}$، دو زیرفضای مهم تحت عنوان* **فضای برد**[۱۰] *و* **فضای پوچ**[۱۱] *تعریف می‌گردد، که آنها را به‌ترتیب با $R(A)$ و $N(A)$ نمایش می‌دهیم:*

$$R(A) = \{\bar{b} \in \mathbb{R}^m | \bar{b} = A\bar{x}, \bar{x} \in \mathbb{R}^n\};$$

$$N(A) = \{\bar{x} \in \mathbb{R}^n | A\bar{x} = \bar{0}\}.$$

تعریف ۴۲.۱.۱. *برای ماتریس $A_{n\times m}$ زیرفضای تولید شده توسط سطرها و ستون‌های A، به هر ترتیب فضای سطری و فضای ستونی A می‌باشد. و همچنین رتبه A برابر با بعد $R(A)$ است. یعنی:*

$$rank(A) = \dim R(A).$$

---

[۸] Row Echelon Form
[۹] Reduced Row Echelon Form
[۱۰] Range space
[۱۱] Null space

۲.۱ مفاهیم کدگذاری

تعریف ۱.۲.۱. فرض کنید $A = \{a_1, a_2, \ldots, a_q\}$ یک مجموعه q عضوی باشد دراین صورت A را **الفبای کد** و هر عضو آن را **نماد کد** می‌نامند.

۱. یک **واژه** q تایی به طول n روی A، رشته‌ای به شکل $W = w_1 w_2 \ldots w_n$ است که در آن، به‌ازای هر $1 \leq i \leq n$، $w_i \in A$ می‌باشد. به‌طور معادل، می‌توان W را به‌صورت بردار $(w_1, w_2, \ldots, w_n)$ نیز درنظر گرفت.

۲. به مجموعه ناتهی C، متشکل از واژه‌های q تایی به‌طول n روی A، یک **کد بلوکی** q تایی به طول n روی A می‌گویند. در نتیجه، $C \subseteq A^n$ خواهدبود.

گاهی اوقات، کد بلوکی q تایی C را کد q تایی یا به‌طور خلاصه‌تر کد می‌گویند.

۳. A^n را فضای کد و اعضای کد C را **کد واژه** می‌نامند.

۴. تعداد کدواژه‌ها در C که با $|C|$ نمایش داده‌می‌شود، **اندازه** C نامیده می‌شود.

۵. کد به طول n و با اندازه M را $(n, M)-$کد می‌نامند.

معمولاً میدان متناهی $\mathbb{F}_q$ را به عنوان الفبای کد در نظر می‌گیرند. یک کد، با الفبای کد $\mathbb{F}_2 = \{0, 1\}$ را کد دودویی می‌نامند.

تعریف ۲.۲.۱. فرض کنید x و y دو واژه به طول n روی الفبای A باشند. در این صورت **فاصله (همینگ)** از x تا y که با $d(x, y)$ نمایش داده‌می‌شود، تعداد جایگاه‌هایی است که x و y با هم تفاوت دارند. به عبارت دیگر اگر $x = x_1, x_2, \ldots, x_n$ و $y = y_1, y_2, \ldots, y_n$ آنگاه:

$$d(x, y) = |\{i | x_i \neq y_i\}|$$

تعریف ۳.۲.۱. فرض کنید C کدی با اندازه حداقل ۲ باشد، دراین صورت **فاصله کد** C، که با $d(C)$ نشان داده‌می‌شود، عبارت است از :

$$d(C) = \min\{d(x, y) | x, y \in C, x \neq y\}$$

کد به طول n، اندازه M و فاصله d را $(n, M, d)-$کد می‌نامیم. به علاوه اعداد n، M و d را پارامترهای کد می‌گوییم.

تعریف ۴.۲.۱. فرض کنید x یک کلمه در $\mathbb{F}_q^n$ باشد. در این صورت **وزن همینگ** x که با $wt(x)$ نشان داده می‌شود، برابر با تعداد مؤلفه‌های ناصفر x تعریف می‌شود.

تعریف ۵.۲.۱. فرض کنید C یک کد باشد. **مینیمم وزن همینگ** کد C که با $wt(C)$ نمایش داده می‌شود، کمترین وزن کدواژه‌های ناصفر C است.

۱.۲.۱ کدهای خطی

تعریف ۶.۲.۱. *کد خطی C از طول n روی $\mathbb{F}_q$ یک زیرفضا از $\mathbb{F}_q^n$ است.*

تعریف ۷.۲.۱. *فرض کنید C یک کد خطی در $\mathbb{F}_q^n$ باشد. دراین صورت:*

۱. **دوگان** *C را با $C^\perp$ نشان می‌دهیم، که مجموعه‌ی عناصری از $\mathbb{F}_q^n$ می‌باشد که بر C عمود است و $C^\perp$ یک زیرفضای $\mathbb{F}_q^n$ است و به صورت زیر بیان می‌شود:*

$$C^\perp = \{\alpha \in \mathbb{F}_q^n | \alpha \cdot c = 0 \ , \forall c \in C\}.$$

۲. *بعد کد خطی $C^\perp$ همان بعد C به عنوان یک فضای برداری روی $\mathbb{F}_q$ می‌باشد.*

قضیه ۱.۲.۱. *فرض کنید C یک کد خطی به طول n روی $\mathbb{F}_q$ باشد. در این صورت*

الف) $|C| = q^{\dim C}$ و $\dim C = \log_q |C|$.

ب) $C^\perp$ *یک کد خطی است و* $\dim C + \dim C^\perp = n$.

ج) $(C^\perp)^\perp = C$

برهان. به مرجع [24] مراجعه شود. □

۲.۲.۱ ماتریس مولد و ماتریس بررسی توازن

فرض می‌کنیم زیرمجموعه غیرتهی S از $\mathbb{F}_q^n$ داده‌شده‌است. ابتدا ماتریس A را که سطرهای آن از کلمات S تشکیل می‌شود با استفاده از عملیات سطری مقدماتی به ماتریس تحویل‌شده پلکانی تبدیل می‌کنیم. فرض می‌کنیم G یک ماتریس $k \times n$ است که شامل تمام سطرهای غیرصفر بدست آمده در ماتریس سطری پلکانی تحویل‌شده A باشد. یعنی

$$A \longrightarrow \begin{pmatrix} G \\ 0 \end{pmatrix}.$$

ماتریس G شامل k ستون اصلی می‌باشد. با جابه‌جایی ستون‌های G ماتریس زیر را خواهیم داشت:

$$G' = (I_k | X),$$

که I_k ماتریس همانی $k \times k$ می‌باشد. در ادامه ماتریس H' را به صورت زیر تشکیل می‌دهیم:

$$H' = (-X^T | I_{n-k}),$$

که X^T ترانهاده X می‌باشد. حال معکوس جایگشت‌هایی که برای ستون‌های G به‌کار بردیم را برای ستون‌های H' ا ستفاده می‌کنیم تا ماتریس H حاصل شود.

تعریف ۱.۸.۲.۱. ۱. **ماتریس مولد** *کد خطی C ماتریس G است که سطرهای آن یک پایه برای کد C تشکیل می‌دهند.*

۲. **ماتریس بررسی توازن** *H برای کد خطی C ماتریس مولدی برای کد دوگان C است که سطرهای آن یک پایه برای کد $C^{\perp}$ می‌باشد.*

تعریف ۱.۹.۲.۱. ۱. *ماتریس مولدی به شکل $(I_k|X)$ ، ماتریس مولد به شکل استاندارد گفته‌می‌شود.*

۲. *ماتریس بررسی توازن به شکل $(Y|I_{n-k})$ ، ماتریس بررسی توازن به شکل استاندارد گفته‌می‌شود.*

قضیه ۱.۲.۲.۱. ۱. *فرض کنید C یک $[n,k]-$کد خطی روی $\mathbb{F}_q$، با ماتریس مولد G باشد. دراین‌صورت، $v \in \mathbb{F}_q^n$ متعلق به $C^{\perp}$ است اگر و فقط اگر v بر همه سطرهای G عمود باشد؛ به عبارت دیگر داریم: $v \in C^{\perp} \iff vG^T = 0$.*

۲. *برای ماتریس $(n-k) \times n$ داده شده H داریم، H ماتریس بررسی توازن برای C است اگر و فقط اگر سطرهای H مستقل خطی باشند و داریم: $HG^T = 0$.*

برهان. به مرجع [24] مراجعه شود. □

۳.۲.۱ کدگذاری کدهای خطی

فرض کنید C یک کد خطی به طول n و بعد k باشد و $\{r_1, \ldots, r_k\}$ پایه‌ای برای کد C باشد. در این صورت برای هر کدواژه v ترکیب خطی یکتای $v = \sum_{i=1}^{k} u_i r_i$ برای $u_i \in \mathbb{F}_q$ موجود است. به صورت معادل، اگر G را ماتریس مولد کد C در نظر بگیریم که i امین سطر آن بردار $\{r_1, \ldots, r_k\}$ انتخاب شده است. برای بردار $u = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$، واضح است که

$$v = uG = \sum_{i=1}^{k} u_i r_i$$

یک کدواژه در C است. برعکس ، هر کدواژه در C می‌تواند به صورت یکتای uG بیان شود که در آن G ماتریس مولد و $u \in \mathbb{F}_q^k$ است.

جریان نمایش اعضای $u \in \mathbb{F}_q^k$ به صورت کدواژه‌های $v = uG$ در C، **کدگذاری** کد خطی نامیده‌می‌شود.

۴.۲.۱ کدهای دوری و کدهای شبه‌دوری

تعریف ۱.۱۰.۲.۱. *کد خطی C به طول n روی $\mathbb{F}_q$ را یک* **کد دوری** [۱۲] *گوییم هرگاه هر انتقال دوری (یک مکان به راست) از یک کد واژه در C ، کد واژه دیگری در C حاصل شود، به عبارت دیگر، هرگاه $(c_0, c_1, \ldots, c_{n-1})$ کد واژه‌ای در C باشد، آنگاه $(c_{n-1}, c_0, \ldots, c_{n-2})$ نیز به کد C تعلق داشته‌باشد. فرض کنید C ، یک کد*

[۱۲] Cyclic codes

دوری به طول n روی $\mathbb{F}_q$ باشد، به هر کدواژه $(c_0, c_1, \ldots, c_{n-1}) \in C$، چندجمله‌ای $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ را نظیر می‌کنیم. طبق این تناظر به سادگی ثابت می‌شود که هر کد دوری به طول n نظیر یک ایده‌آل از حلقه $R = \mathbb{F}_q[x]/(x^n - 1)$ است.

کدهای شبه‌دوری[۱۳] تعمیمی از کدهای دوری هستند که زیررده مهمی از کدهای خطی را تشکیل می‌دهند.

تعریف ۱.۱۱.۲.۱. *کد خطی C را* **کد شبه‌دوری** *می‌نامیم اگر، عدد صحیح n_0 وجود داشته‌باشد به طوری که کد C تحت چرخش n_0-تایی پایا باشد.*

در حالت $n_0 = 1$ کدهای شبه‌دوری به کدهای دوری تبدیل می‌شوند. اگر کد دارای طول n باشد، آنگاه n_0، عدد n را عاد می‌کند.

۵.۲.۱ ماتریسهای مولد و بررسی توازن در کدهای دوری

قضیه ۳.۲.۱. *فرض کنید $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ چندجمله‌ای مولد کد دوری C در $\mathbb{F}_q^n$ باشد. در این صورت ماتریس*

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

ماتریس مولد C است.

برهان. به مرجع [24] مراجعه کنید. □

قضیه ۴.۲.۱. *فرض کنید که C یک $[n, k]-$کد دوری $q-$آرایه‌ای با چند جمله‌ای مولد $g(x)$ باشد. قراردهید $h(x) = (x^n - 1)/g(x)$. فرض کنید $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ باشد و چندجمله‌ای متقابل $h_R(x)$ از $h(x)$ به صورت $h_R(x) = x^k h(1/x)$ تعریف شود. در این صورت ماتریس*

$$H = \begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}$$

ماتریس بررسی توازن کد C است.

برهان. به مرجع [24] مراجعه کنید. □

[۱۳] Quaci-Cyclic codes

۶.۲.۱ کدهای LDPC

تعریف ۱۲.۲.۱. *کدهای LDPC[۱۴] زیررده‌ای از کدهای خطی هستند. این کدها اولین بار توسط گالاگر[۱۵] کشف و معرفی شدند. یک کد LDPC با ماتریس بررسی توازن معرفی می‌شود، که تعداد یکها در هر سطر و ستون آن به نسبت طول کد بسیار کوچک است، به همین دلیل این کدها را کدهایی با ماتریس بررسی توازن خلوت می‌نامند [17, 19].*

تعریف ۱۳.۲.۱. *کد C با ماتریس کنترل توازن H را $(\gamma, \delta)-$منظم می‌نامند هرگاه:*

۱. *وزن هر سطر برابر δ باشد.*

۲. *وزن هر ستون برابر γ باشد.*

۳. *مقادیر δ و γ به‌ترتیب نسبت به طول کد و تعداد سطرهای H کوچک باشند.*

اگر C یک کد LDPC با ماتریس بررسی توازن $H_{m\times n}$ باشد، آنگاه خواهیم‌داشت: $\delta m = \gamma n$، بنابراین نرخ کد در نامساوی زیر صدق می‌کند:

$$R = \frac{k}{n} \geq \frac{n-m}{n} = ۱ - \frac{\gamma}{\delta}.$$

حالت تساوی زمانی رخ می‌دهد که سطرهای H مستقل خطی باشند.

[۱۴] Low Density Parity Check codes
[۱۵] R.G. Gallager

فصل ۲

ماتریس‌های چندجمله‌ای مولد و بررسی توازن کدهای شبه‌دوری تعمیم‌یافته

در نظریه کدگذاری تحقیقات زیادی روی کدهای شبه‌دوری انجام گرفته است [5, 7, 11, 13, 18, 20, 21, 22, 23, 25, 31, 32]. کدهای شبه‌دوری (QC) به طول n به صورت $(\mathbb{F}_q[x]/x^u-1)^l$ تعریف می‌شوند که در آن u یک عدد صحیح مثبت و $\mathbb{F}_q$ یک میدان q عضوی و $\mathbb{F}_q[x]/x^u-1$ یک حلقه از چندجمله‌ای x در میدان $\mathbb{F}_q$ به پیمانه x^u-1 است و $n=ul$ می‌باشد. کد شبه‌دوری با $l=1$ برابر با کد دوری است. هر کد شبه‌دوری به کمک ماتریس مولد و یا ماتریس بررسی توازن خود معرفی می‌شود. روش دیگر برای نشان دادن کدهای شبه‌دوری استفاده از ماتریس‌های چندجمله‌ای می‌باشد [18, 32]. هر کد شبه‌دوری دارای ماتریس چندجمله‌ای مولد مخصوص خود می‌باشد که یک ماتریس بالا مثلثی است و همچنین دارای ماتریس چندجمله‌ای بررسی توازن خاص خود می‌باشد که یک ماتریس پایین مثلثی است. بخش مهمی از کدهای با ماتریس بررسی توازن خلوت $(LDPC)$ از دیدگاه کدهای شبه‌دوری بررسی می‌شود [6, 9, 12, 17, 19]. همچنین بسیاری از کدهای $LDPC$ در طبقه کدهای شبه‌دوری قرار ندارند و در یک کلاس گسترده‌تر از کدهای شبه‌دوری یعنی در کلاس کدهای **شبه‌دوری تعمیم‌یافته**[1] (GQC)، قرار می‌گیرند [4, 8, 34, 36, 38, 39]. کدهای شبه‌دوری تعمیم‌یافته به عنوان زیرمدولی از $\bigoplus_{i=1}^{l}\mathbb{F}_q[x]/x^{n_i}-1$ تعریف می‌شود، که در آن $n=\sum_{i=1}^{l}n_i$ است و $\mathbb{F}_q[x]$ یک حلقه از چندجمله‌ای‌های x در میدان $\mathbb{F}_q$ و $\bigoplus_{i=1}^{l}\mathbb{F}_q[x]/x^{n_i}-1$ یک $\mathbb{F}_q[x]-$مدول از همه $l-$تایی‌های $(c_1,\ldots,c_l)$ می‌باشد که در آن برای همه‌ی $1\leq i\leq l$، داریم: $c_i\in\mathbb{F}_q[x]/x^{n_i}-1$. در این فصل به

[1] Generalized Quaci-Cyclic code

معرفی کدهای شبه‌دوری تعمیم‌یافته می‌پردازیم. نشان می‌دهیم که هر کد شبه‌دوری تعمیم‌یافته توسط ماتریس چندجمله‌ای مولد $G = (g_{i,j})$ به فرم زیر

$$\begin{pmatrix} g_{۱۱} & g_{۱۲} & \cdots & g_{۱l} \\ ۰ & g_{۲۲} & \cdots & g_{۲l} \\ \vdots & \ddots & \ddots & \vdots \\ ۰ & \cdots & ۰ & g_{ll} \end{pmatrix} \tag{۱.۲}$$

توصیف می‌شود.یعنی، یک ماتریس چندجمله‌ای بالامثلثی از مرتبه $l \times l$، که $g_{i,j} \in \mathbb{F}_q[x]$ می‌باشد و در معادله ماتریسی زیر صدق می‌کند،

$$AG = \mathrm{diag}[x^{n_۱} - ۱, \ldots, x^{n_l} - ۱], \tag{۲.۲}$$

که در آن q عدد اول، $\mathbb{F}_q$ یک میدان متناهی با q عضو، $\mathbb{F}_q[x]$ حلقه چندجمله‌ای‌های یک متغیره x روی میدان $\mathbb{F}_q$، $A = (a_{i,j})$ یک ماتریس چندجمله‌ای بالامثلثی دیگر از مرتبه $l \times l$، $\{n_۱, \ldots, n_l\}$ یک بلوک‌بندی برای کدی به طول n است به طوری که $n = \sum_{i=۱}^{l} n_i$ باشد و $\mathrm{diag}[x^{n_۱} - ۱, \ldots, x^{n_l} - ۱]$ یک ماتریس قطری است که برای $۱ \leq i \leq l$، درایه (i,i) آن برابر $x^{n_i} - ۱$ می‌باشد. محتویات این فصل عمدتاً از مرجع [26] برداشت شده‌است. در این فصل تعاریف و اصول اولیه کدهای شبه‌دوری تعمیم‌یافته را به‌طور خلاصه بیان می‌کنیم. برای جزئیات بیشتر به مراجع [11, 25, 38] مراجعه کنید. در این فصل حلقه اعداد صحیح را با $\mathbb{Z}$ نشان می‌دهیم و ترانهاده یک ماتریس و یا بردار M را به صورت M^T تعریف می‌کنیم.

۱.۲ تعریف کدهای شبه‌دوری تعمیم‌یافته

فرض کنید C یک کد خطی به طول n و بعد k روی میدان $\mathbb{F}_q$ باشد.

تعریف ۱.۱.۲. *اگر اعداد صحیح و مثبت $n_۱, n_۲, \ldots, n_l$ به گونه‌ای موجود باشند که $\sum_{i=۱}^{l} n_i = n$ باشد و علاوه بر این، اگر همه کدواژه‌های C تحت انتقال دوری که در زیر نشان داده می‌شود، پایا باشند،*

$$(\overbrace{c_{۱,۱}, \ldots, c_{۱,n_۱-۱}, c_{۱,n_۱}}^{n_۱}, \overbrace{c_{۲,۱}, \ldots, c_{۲,n_۲-۱}, c_{۲,n_۲}}^{n_۲}, \ldots, \overbrace{c_{l,۱}, \ldots, c_{l,n_l-۱}, c_{l,n_l}}^{n_l}) \in C \tag{۳.۲}$$

$$\Longrightarrow (\overbrace{c_{۱,n_۱}, c_{۱,۱}, \ldots, c_{۱,n_۱-۱}}^{n_۱}, \overbrace{c_{۲,n_۲}, c_{۲,۱}, \ldots, c_{۲,n_۲-۱}}^{n_۲}, \ldots, \overbrace{c_{l,n_l}, c_{l,۱}, \ldots, c_{l,n_l-۱}}^{n_l}) \in C, \tag{۴.۲}$$

آنگاه C یک کد شبه‌دوری تعمیم‌یافته نامیده می‌شود.

توجه داشته‌باشید که اگر $n_۱ = n_۲ = \cdots = n_l = m$ باشد ، C تحت چرخش $m-$تایی پایاباشد. آنگاه C یک کد شبه‌دوری است. همچنین اگر $l = ۱$ باشد آنگاه C یک کد دوری می‌باشد.

اگر C یک کد شبه‌دوری تعمیم‌یافته باشد که به صورت $\sum_{i=۱}^{l} n_i = n$ بلوک بندی می‌شود، آنگاه دوگان آن نیز یک کد شبه‌دوری تعمیم‌یافته است که به همان صورت بلوک بندی می‌شود.

مثال ۱.۱.۲. *فرض کنید یک کد خطی دودویی $C_۱$ به طول ۷ به کمک ماتریس مولد زیر تعریف شود:*

$$\left(\begin{array}{ccc|ccc|c} ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۰ \\ \hline ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ \end{array}\right).$$

از آنجایی که در هر بلوک، با چرخش درایه‌ها در هر سطر، سطرهای دیگر حاصل می‌شود، در نتیجه $C_۱$ یک کد شبه‌دوری تعمیم‌یافته می‌باشد که در آن $k = ۴$، $n_۱ = n_۲ = ۳$ و $n_۳ = ۱$ است. از سوی دیگر ماتریس مولد کد $C_۱^{\perp}$، ماتریس بررسی توازن کد $C_۱$ را می‌دهد که عبارت است از:

$$\left(\begin{array}{ccc|ccc|c} ۱ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۱ \end{array}\right).$$

۲.۲ تفسیر چندجمله‌ای

چندجمله‌ای $f = \sum_{h=۰}^{d} f_h x^h \in \mathbb{F}_q[x]$ را که $f_d \neq ۰$ می‌باشد، در نظر بگیرید. درجه چندجمله‌ای f به صورت $\deg f = d$ تعریف می‌شود، برای چندجمله‌ای صفر، یعنی $f = ۰ \in \mathbb{F}_q$، درجه آن به صورت $\deg f = -\infty$، تعریف می‌شود که برای همه $w \in \mathbb{Z}$، $\deg ۰ < w$ می‌باشد. اگر C یک کد خطی به طول n باشد و به گونه‌ای بلوک بندی شود که $\sum_{i=۱}^{l} n_i = n$ باشد، آنگاه هر کدواژه (۳.۲) از این کد خطی را می‌توان به یک بردار چندجمله‌ای $(c_۱, c_۲, \ldots, c_l)$ به صورت زیر نظیر کرد.

$$c_{i,۱}, c_{i,۲}, \ldots, c_{i,n_i} \mapsto c_i = c_{i,۱} + c_{i,۲}x + \cdots + c_{i,n_i}x^{n_i - ۱} \in \mathbb{F}_q[x], \qquad (۵.۲)$$

برای $۱ \leq i \leq l$، که در آن، $\deg c_i < n_i$ می‌باشد.

برای $e, g \in \mathbb{F}_q[x]$ و $g \neq ۰$، فرض کنید $e \mod g$، چندجمله‌ای باقیمانده منحصر به فرد مانند r با درجه کمتر از g تعریف شود که حاصل تقسیم e بر g است؛ به بیان دیگر، برای $p, r \in \mathbb{F}_q[x]$ داریم: $e = pg + r$، که در آن $\deg r < \deg g$. دراین صورت بردار چندجمله‌ای کدواژه‌های (۴.۲)، از کد $c = (c_۱, c_۲, \ldots, c_l) \in C$، معادل است با

$$(xc_۱ \mod (x^{n_۱} - ۱), xc_۲ \mod (x^{n_۲} - ۱), \ldots, xc_l \mod (x^{n_l} - ۱)), \qquad (۶.۲)$$

زیرا برای $۱ \leq i \leq l$، داریم:

$$\begin{aligned} xc_i &= c_{i,۱}x + c_{i,۲}x^{۲} + \cdots + c_{i,n_i - ۱}x^{n_i - ۱} + c_{i,n_i}x^{n_i} \\ &= c_{i,n_i}(x^{n_i} - ۱) + c_i n_i + c_{i,۱}x + \cdots + c_{i,n_{i-۱}}x^{n_{i-۱}}. \end{aligned}$$

بردار چندجمله‌ای (۶.۲) را xc می‌نامیم و که سمت راست تساوی فوق جمع مستقیم از حلقه خارج قسمت $\mathbb{F}_q[x]$ بر ایده‌آل تولید شده از $(x^{n_i} - ۱)$، برای $۱ \leq i \leq l$ می‌باشد.

فرض کنید $F : \mathbb{F}_q[x]^l \longrightarrow M$ یک نگاشتی باشد که به صورت زیر تعریف می‌شود:

$$F((c_1, \ldots, c_l)) = (c_1 \mod (x^{n_1} - 1), c_2 \mod (x^{n_2} - 1), \ldots, c_l \mod (x^{n_l} - 1)),$$

که در آن $\mathbb{F}_q[x]^l$، نشان دهنده $l-$تایی $(c_1, \ldots, c_l)$ است که برای $1 \leq i \leq l$، $c_i \in \mathbb{F}_q[x]$ می‌باشد. در این صورت برای کد شبه‌دوری تعمیم‌یافته C، که $C \subset M$ می‌باشد، داریم: $D = F^{-1}(C) \subset \mathbb{F}_q[x]^l$. آنگاه برای $1 \leq i \leq l$، D شامل بردارهای چندجمله‌ای به صورت

$$(\underbrace{0, \ldots, 0}_{i-1}, x^{n_i} - 1, \underbrace{0, \ldots, 0}_{l-i}), \tag{۷.۲}$$

می‌باشد که معادل یکی از تصاویر معکوس کدواژه $(0, \ldots, 0) \in C$ است. در مقابل، فرض کنید که $D \subset \mathbb{F}_q[x]^l$ یک $\mathbb{F}_q[x]-$زیرمدول باشد که شامل l بردار چندجمله‌ای به فرم (۷.۲) است. در این صورت $F(D)$ یک کد شبه‌دوری تعمیم‌یافته را مشخص می‌کند. این تناظر بین D و C از طریق روابط $D = F^{-1}(C)$ و $F(D) = C$، یک‌به‌یک است، به عنوان مثال داریم: $F^{-1}(F(D)) = D$ و $F(F^{-1}(C)) = C$. از این پس، فرض می‌کنیم که هر کد شبه‌دوری تعمیم‌یافته C در $\mathbb{F}_q[x]^l$ قرار دارد. بنابراین ما تعریف دیگری از کدهای شبه‌دوری تعمیم‌یافته که معادل تعریف ۱.۱.۲ می‌باشد را ارائه می‌دهیم.

تعریف ۱.۲.۲. *فرض کنید C یک $\mathbb{F}_q[x]-$زیرمدول از $\mathbb{F}_q[x]^l$ باشد. اگر C شامل l بردار چندجمله‌ای به فرم (۷.۲) باشد، آنگاه C یک کد شبه‌دوری تعمیم‌یافته نامیده می‌شود.*

تعریف ۱.۲.۲ بیان می‌کند که کد شبه‌دوری تعمیم‌یافته $C \subset \mathbb{F}_q[x]^l$، چیزی جز یک شبکه منظم در $\mathbb{F}_q[x]^l$ که شامل l بردار چندجمله‌ای به فرم (۷.۲) می‌باشد، نیست.

۳.۲ ماتریس چندجمله‌ای مولد کدهای شبه‌دوری تعمیم‌یافته

یک روش برای تشکیل یک کد شبه‌دوری تعمیم‌یافته استفاده از ماتریس مولد $k \times n$، با درایه‌های متعلق به $\mathbb{F}_q$ می‌باشد. روش دیگر استفاده از ماتریس چندجمله‌ای مولد $l \times l$، با درایه‌های متعلق به $\mathbb{F}_q[x]$ است. چندجمله‌ای $f = \sum_{h=0}^{d} f_h x^h \in \mathbb{F}_q[x]$، با درجه d یا به عبارت دیگر، $\deg f = d \geq 0$، را در نظر بگیرید. آنگاه چندجمله‌ای f را تکین می‌نامیم اگر $f_d = 1$ باشد.

تعریف ۱.۳.۲. *فرض کنید C یک کد شبه‌دوری تعمیم‌یافته و $G = (g_{i,j})$ یک ماتریس $l \times l$ باشد که درایه‌های آن متعلق به $\mathbb{F}_q[x]$ و سطرهای آن کدواژه‌هایی در C باشد. اگر برای $1 \leq i, j \leq l$ و $i > j$، $g_{i,j} = 0$ داشته باشیم، یعنی، ماتریس G به‌صورت*

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{pmatrix}, \tag{۸.۲}$$

باشد و علاوه بر این، برای $۱ \leq i \leq l$ و در میان کدواژه‌های به فرم $(۰, \cdots, ۰, c_i, \cdots, c_l) \in C$ که در آن $c_i \neq ۰$ می‌باشد، $g_{i,i}$ دارای کمترین درجه باشد، آنگاه G را ماتریس چندجمله‌ای مولد کد C می‌نامیم. اگر $g_{i,i}$ برای $۱ \leq i \leq l$، تکین باشد و برای همه $۱ \leq i \neq j \leq l$، داشته باشیم: $\deg g_{i,j} < \deg g_{j,j}$، آنگاه ماتریس G را کاهنده می‌نامیم.

به‌جای ماتریس‌های مولد، ما می‌توانیم کدهای خطی را با ماتریس‌های بررسی توازن تعریف کنیم. به‌طور مشابه، به‌جای ماتریس‌های چندجمله‌ای مولد، این امکان وجود دارد که کدهای شبه‌دوری تعمیم‌یافته را توسط ماتریس‌های چندجمله‌ای بررسی توازن H تعریف کرد.

تعریف ۲.۳.۲. *فرض کنید C یک کد شبه‌دوری تعمیم‌یافته و $H = (h_{i,j})$ یک ماتریس $l \times l$ باشد که درایه‌های آن متعلق به $\mathbb{F}_q[x]$ و سطرهای آن کدواژه‌هایی در $C^{\perp}$ است. اگر برای $۱ \leq i, j \leq l$ و $i < j$، داشته باشیم: $h_{i,j} = ۰$، یعنی، ماتریس H به‌صورت*

$$H = \begin{pmatrix} h_{۱,۱} & ۰ & \cdots & ۰ \\ h_{۲,۱} & h_{۲,۲} & \ddots & \vdots \\ \vdots & \vdots & \ddots & ۰ \\ h_{l,۱} & h_{l,۲} & \cdots & h_{l,l} \end{pmatrix}, \tag{۹.۲}$$

باشد و علاوه بر این، برای $۱ \leq i \leq l$ و در میان کدواژه‌های به فرم $(c_۱, \cdots, c_i, ۰, \cdots, ۰,) \in C^{\perp}$ که در آن $c_i \neq ۰$ می‌باشد، $h_{i,i}$ دارای کمترین درجه باشد، آنگاه H را ماتریس چندجمله‌ای بررسی توازن کد C می‌نامیم. اگر $h_{i,i}$ برای $۱ \leq i \leq l$، تکین باشد و برای همه $۱ \leq i \neq j \leq l$، داشته باشیم: $\deg h_{i,j} < \deg h_{j,j}$، آنگاه ماتریس H را کاهنده می‌نامیم.

گزاره ۱.۳.۲. *ماتریس چندجمله‌ای مولد کاهنده در هر کد شبه‌دوری تعمیم‌یافته، منحصر به فرد است.*

برهان. فرض کنید که $G = (g_{i,j})$ و $G' = (g'_{i,j})$ دو ماتریس چندجمله‌ای مولد کاهنده برای کد شبه‌دوری تعمیم‌یافته باشند. اگر g_i و g'_i به‌ترتیب سطرهای i ام از ماتریس‌های چندجمله‌ای مولد G و G' باشند آنگاه $g_{i,i} = g'_{i,i}$ می‌باشد، زیرا در غیر این صورت با منحصربه‌فرد بودن چندجمله‌ای با کمترین درجه که در تعریف ۱.۳.۲ بیان شد، در تناقض است. بنابراین $d_{i+۱}, \ldots, d_l \in \mathbb{F}_q[x]$ موجوداست به طوری که $g_i - g'_i = \sum_{j=i+۱}^{l} d_j g_j$ باشد و مؤلفه j ام از $g_i - g'_i$ برای $i + ۱ \leq j \leq l$ عبارت است از: $g_{i,j} - g'_{i,j} = d_j g_{j,j}$ و چون برای $i + ۱ \leq j \leq l$، داریم: $۰ \leq \deg g_{i,j}, \deg g'_{i,j} \leq \deg g_{j,j}$، لذا خواهیم‌داشت: $d_j = ۰$. در نتیجه $g_i - g'_i = ۰$ و $G = G'$ خواهدبود. □

علاوه بر این، به طور مشابه می‌توان اثبات کرد که ماتریس چندجمله‌ای بررسی توازن کاهنده نیز منحصر به فرد است. برای هر ماتریس چندجمله‌ای مولد و ماتریس چندجمله‌ای بررسی توازن ما می‌توانیم کاهنده‌ی آنها را از طریق عملیات سطری مقدماتی روی ماتریسهای چندجمله‌ای به‌دست آوریم.

گزاره ۲.۳.۲. *(یک گزاره دو شرطی برای کدواژه‌های C). فرض کنید G ماتریس چندجمله‌ای مولد کد C باشد و برای $۱ \leq i \leq l$، سطر $i-$ام از ماتریس $G = (g_{i,j})$ برابر $g_i = (g_{i,۱}, \ldots, g_{i,l})$ باشد،*

دراین صورت بردار چندجمله‌ای $c = (c_1, \ldots, c_l) \in \mathbb{F}_q[x]^l$، *یک کدواژه از کد* C *است اگر و تنها اگر* $f = (f_1, \ldots, f_l) \in \mathbb{F}_q[x]^l$ *موجود باشد به طوری که داشته باشیم:*

$$c = fG = f_1 g_1 + \cdots + f_l g_l. \tag{۱۰.۲}$$

برهان. برای کد واژه $c = (c_1, \ldots, c_l) \in C$ و ماتریس چندجمله‌ای مولد G، طبق لم آ.۱.۰ در پیوست آ، ادعا می‌کنیم که $f = (f_1, \ldots, f_l), d = (d_1, \ldots, d_l) \in \mathbb{F}_q[x]^l$ به گونه‌ای موجودند که داشته‌باشیم: $c = fG + d$ و برای $1 \leq j \leq l$، $\deg d_j < \deg g_{j,j}$ باشد. در این صورت $d = c - fG \in C$ می‌باشد و به کمک تعریف ۱.۲.۲، نتیجه می‌گیریم که $d = (0, \ldots, 0) = 0$ خواهدبود. بنابراین رابطه (۱۰.۲) بدست می‌آید. عکس قضیه فوق بلافاصله از تعریف ۱.۲.۲، نتیجه می‌شود. □

۴.۲ الگوریتم بوخ‌برگر

وجود ماتریس چندجمله‌ای مولد برای مدولها توسط الگوریتم بوخ‌برگر[۲] در مراجع [38, 7] نشان داده شده است که مشابه عملیات سطری مقدماتی برای بالامثلثی کردن ماتریسها در روش حذفی گوس می‌باشد.

ماتریس مولد کدهای شبه‌دوری تعمیم‌یافته را توسط الگوریتم بوخ‌برگر را به صورت زیر بدست می‌آوریم. با ماتریس چندجمله‌ای

$$\begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,l} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,l} \\ \vdots & \vdots & \ddots & \vdots \\ c_{k,1} & c_{k,2} & \cdots & c_{k,l} \end{pmatrix} \tag{۱۱.۲}$$

به نمایندگی از ماتریس چندجمله‌ای مولد کدهای شبه‌دوری تعمیم‌یافته که به عنوان کدهای خطی در نظر گرفته می‌شوند شروع می‌کنیم، که در این ماتریس برای $1 \leq i \leq k$ و $1 \leq j \leq l$، $c_{i,j} \in \mathbb{F}_q[x]$ می‌باشد. فرض کنید که برای $1 \leq i \leq k$، c_i سطر $-i$ ام ماتریس (۱۱.۲) باشد. در این الگوریتم تغییراتی را به صورت استقرایی روی ماتریس چندجمله‌ای انجام می‌دهیم.

۱. اگر $c_{1,1} = c_{2,1} = \cdots = c_{k,l} = 0$ باشد، آنگاه قرار می‌دهیم: $c_1 = (x^{n_1} - 1, 0, \ldots, 0)$ و متوقف می‌شویم. اگر $c_{1,1} \neq 0$ و $c_{2,1} = \cdots = c_{k,l} = 0$ باشد باز هم عملیات را متوقف می‌کنیم.

۲. در صورت لازم سطر c_1 را با سطرهای $c_2, \ldots, c_k$ جابه‌جا می‌کنیم زیرا می‌خواهیم $c_{1,1}$ کمترین درجه را در میان $c_{1,1}, c_{2,1}, \ldots, c_{k,1}$ که غیر صفر هستند داشته باشد.

[۲] Buchberger's algorithm

۳. $p_i, r_i \in \mathbb{F}_q[x]$ را طوری محاسبه می‌کنیم که داشته‌باشیم: $c_{i,1} = p_i c_{1,1} + r_i$، که در آن برای همه $2 \le i \le k$، $\deg r_i < \deg c_{1,1}$، می‌باشد. برای $2 \le i \le k$، سطر c_i را با $c_i - p_i c_1$ جایگزین می‌کنیم و به مرحله اول بازمی‌گردیم.

با انجام عملیات فوق ما می‌توانیم $c_{2,1}, \cdots, c_{k,l}$ را صفر کنیم و سطر $c_1 = (c_{1,1}, \ldots, c_{1,l})$ را به عنوان سطر $g_1 = (g_{1,1}, \ldots, g_{1,l})$ در نظر می‌گیریم. سپس برای $c_{1,1}, c_{2,1}, \ldots, c_{k,1}$ اولیه در ماتریس (۱۱.۲)، خواهیم داشت: $g_{1,1} = \gcd(c_{1,1}, \ldots, c_{k,1})$. بنابراین ماتریس (۱۱.۲) به ماتریس

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & c_{2,2} & \cdots & c_{2,l} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{k,2} & \cdots & c_{k,l} \end{pmatrix}. \tag{۱۲.۲}$$

تبدیل می‌شود. توجه داشته‌باشید که $c_{i,j}$ در ماتریس (۱۲.۲) به طور کلی با $c_{i,j}$ در ماتریس (۱۱.۲) متفاوت است. در ادامه، عملیات بالا را برای زیرماتریس $\begin{pmatrix} c_{2,2} & \cdots & c_{2,l} \\ \vdots & \ddots & \vdots \\ c_{k,2} & \cdots & c_{k,l} \end{pmatrix}$ از ماتریس (۱۲.۲) انجام می‌دهیم. بعد از انجام عملیات بازگشتی بالا و جایگذاری l سطر بالا به عنوان سطرهای ماتریس G، در نهایت ماتریس چندجمله‌ای مولد (۸.۲) برای کد C به‌دست خواهد آمد. به طور مشابه، می‌توانیم الگوریتم مربوطه را برای محاسبه H بدست آوریم به این طریق که یک ماتریس بررسی توازن $(n-k)\times n$ را به عنوان ورودی قرار می‌دهیم و خواهیم داشت: $h_{l,l} = \gcd(c_{1,l}, \ldots, c_{(n-k),l})$. بعد از انجام عملیات بازگشتی بالا و جایگذاری l سطر پایین به عنوان سطرهای ماتریس H، در نهایت ماتریس چندجمله‌ای بررسی توازن (۹.۲) برای کد C به‌دست خواهد آمد.

مثال ۱.۴.۲. *مثال ۱.۱.۲ را در نظر بگیرید. ماتریس چندجمله‌ای در سمت چپ رابطه (۱۳.۲) به عنوان نماینده ماتریس چندجمله‌ای مولد داده شده است. از طریق انجام مراحل ۳ـ۱، ماتریس چندجمله‌ای اولیه به صورت زیر تبدیل شده است.*

$$\begin{pmatrix} 1+x^2 & 1 & 0 \\ 1+x & x & 0 \\ x+x^2 & x^2 & 0 \\ 1+x+x^2 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1+x & x & 0 \\ 0 & 1+x+x^2 & 0 \\ 0 & 0 & 0 \\ 1 & x^2 & 1 \end{pmatrix}$$

$$\longrightarrow G_1 = \begin{pmatrix} 1 & 1+x & 1 \\ 0 & 1+x+x^2 & 0 \\ 0 & 0 & 1+x \end{pmatrix}. \tag{۱۳.۲}$$

بنابراین داریم: $g_1 = (1, x^2, 1), g_2 = (0, 1+x+x^2, 0)$ و $g_3 = (0, 0, 1+x)$ *که در آن آخرین تساوی از رابطه* $(1+x, x, 0) + (1+x)g_1 = xg_2 + (0, 0, 1+x)$ *حاصل شده است. برای تبدیل آن به نوع کاهنده، $g_1 + g_2$ را جایگزین سطر g_1 می‌کنیم.*

حال به کمک الگوریتم بوخ‌برگر ماتریس چندجمله‌ای بررسی توازن آن را حساب می‌کنیم. ماتریس چندجمله‌ای در سمت چپ رابطه (۱۴.۲) به عنوان نماینده ماتریس چندجمله‌ای بررسی توازن داده شده است. سطر سوم ماتریس چندجمله‌ای بررسی توازن H_1 برابر $h_3 = (x^2, 1 + x^2, 1)$ می‌باشد. درایه‌های c_{13}, c_{23} به صورت زیر حذف می‌شوند. بنابرایم داریم: $h_2 = (x + x^2, 1 + x, 0)$ و $h_1 = (1 + x^3, 0, 0)$. برای تبدیل آن به نوع کاهنده، $h_3 + (1 + x)h_2 + h_1$ را جایگزین سطر h_3 می‌کنیم و بدست می‌آوریم:

$$\begin{pmatrix} 1 & 1+x & 1 \\ x & x+x^2 & 1 \\ x^2 & 1+x^2 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1+x^2 & x+x^2 & 0 \\ x+x^2 & 1+x & 0 \\ x^2 & 1+x^2 & 1 \end{pmatrix}$$
$$\longrightarrow H_1 = \begin{pmatrix} 1+x^3 & 0 & 0 \\ x+x^2 & 1+x & 0 \\ 1+x+x^2 & 0 & 1 \end{pmatrix}. \qquad (۱۴.۲)$$

۵.۲ معادله‌ای که ماتریس مولد کدهای شبه‌دوری تعمیم‌یافته در آن صادق است.

گزاره ۱.۵.۲. *(معادله‌ای که ماتریس مولد کدهای شبه‌دوری تعمیم‌یافته در آن صادق است). فرض کنید $G = (g_{ij})$ یک ماتریس $l \times l$ با درایه‌هایی در $\mathbb{F}_q[x]$ باشد و در آن برای $1 \leq i, j \leq l$ و $i > j$، داشته‌باشیم: $g_{ij} = 0$ و همچنین $n = \sum_{i=1}^{l} n_i$ باشد. آنگاه G، یک ماتریس چندجمله‌ای مولد برای کد شبه‌دوری تعمیم‌یافته است اگر و تنها اگر یک ماتریس $l \times l$ مانند $A = (a_{ij})$ با درایه‌هایی در $\mathbb{F}_q[x]$ موجود باشد به طوری که داشته‌باشیم:*

$$AG = \mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1], \qquad (۱۵.۲)$$

که در آن

$$\mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1] = \begin{pmatrix} x^{n_1} - 1 & 0 & \cdots & 0 \\ 0 & x^{n_2} - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x^{n_l} - 1 \end{pmatrix}.$$

می‌باشد.

برهان. اگر G یک ماتریس چندجمله‌ای مولد برای کد شبه‌دوری تعمیم‌یافته باشد، آنگاه l بردار چندجمله‌ای به فرم (۷.۲) باید توسط G بیان شود و ما (۱۵.۲) را خواهیم داشت. برای اثبات عکس مطلب، فرض کنید $C = \{fG | f \in \mathbb{F}_q[x]^l\}$ باشد. در این صورت، C یک $\mathbb{F}_q[x]-$زیرمدول از $\mathbb{F}_q[x]^l$ خواهدبود و از آنجایی که (۱۵.۲) برقرار است می‌توانیم بگوییم که C شامل l بردار چندجمله‌ای به فرم (۷.۲) می‌باشد. بنابراین طبق تعریف ۱.۲.۲، C یک کد شبه‌دوری تعمیم‌یافته می‌باشد. □

گزاره ۲.۵.۲. *(خاصیت مثلثی بودن ماتریس A)فرض کنید G ماتریس چندجمله‌ای مولد کد شبه‌دوری تعمیم‌یافته C باشد. همچنین فرض کنید که A ماتریس چندجمله‌ای باشد که در معادله (۱۵.۲) صدق کند. در این صورت ماتریس A نیز یک ماتریس بالامثلثی است، یعنی اگر $A = (a_{ij})$ و $i > j$ باشد آنگاه $a_{ij} = ۰$ خواهد بود.*

برهان. از این واقعیت نتیجه می‌شود که مجموعه ماتریس‌های بالامثلثی روی میدان خارج قسمتی $\mathbb{F}_q[x]$ تشکیل یک گروه می‌دهند و لذا حکم حاصل می‌شود. □

گزاره ۳.۵.۲. *(خاصیت جابجایی ماتریس‌های A وG در کدهای شبه‌دوری). فرض کنید G یک ماتریس چندجمله‌ای مولد برای کد شبه‌دوری C باشد و A ماتریس چندجمله‌ای باشد که در رابطه (۱۵.۲) صدق کند. در این صورت، رابطه $GA = \operatorname{diag}[x^N - ۱, \ldots, x^N - ۱]$ نیز برقرار است.*

برهان. فرض کنید میدان خارج‌قسمتی $\mathbb{F}_q[x]$ را با علامت $\mathbb{F}_q(x)$ نشان دهیم و علاوه بر این فرض کنید معادله $AG = \operatorname{diag}[x^N - ۱, \ldots, x^N - ۱]$ روی میدان $\mathbb{F}_q(x)$ صادق باشد. ماتریس قطری $M = \operatorname{diag}\left[\frac{۱}{x^N - ۱}, \ldots, \frac{۱}{x^N - ۱}\right]$ را در نظر می‌گیریم. در این صورت با ضرب M در طرفین رابطه فوق داریم: $(AG)M = A(GM) = \operatorname{diag}[۱, \ldots, ۱] = (GM)A = M(GA)$. بنابراین خواهیم داشت:

$$GA = \operatorname{diag}[x^N - ۱, \ldots, x^N - ۱].$$

□

گزاره ۴.۵.۲. *(ویژگی کاهندگی برای ماتریس A) فرض کنید G ماتریس چندجمله‌ای مولد کاهنده برای کد شبه‌دوری تعمیم‌یافته C باشد. همچنین فرض کنید که A ماتریس چندجمله‌ای باشد که در معادله (۱۵.۲) صدق کند. در این صورت در ماتریس $A = (a_{ij})$ و برای همه $۱ \leq i \neq j \leq l$ ، داریم:*

$$\deg a_{ii} > \deg a_{ij}.$$

برهان. فرض کنید $j = i + ۱$ باشد. در این صورت از معادله $a_{ii}g_{ij} + a_{ij}g_{jj} = ۰$ نتیجه می‌گیریم که $\deg a_{ii} > \deg a_{ij}$ خواهدبود. زیرا، $\deg a_{ii} = \deg a_{ij} + \deg g_{jj} - \deg g_{ij} > \deg a_{ij}$ می‌باشد. بنا به فرض استقرا برای $i \leq h < j$ داریم: $\deg a_{ii} > \deg a_{ih}$، بنابراین کافی است ثابت کنیم که $\deg a_{ii} > \deg a_{ij}$ می‌باشد. طبق رابطه $\sum_{h=i}^{j} a_{ih}g_{hj} = ۰$ داریم: $a_{ij}g_{jj} = -\sum_{h=i}^{j-۱} a_{ih}g_{hj}$. بنابراین خواهیم داشت:

$$\begin{aligned}\deg a_{ij} &= \deg\left(\sum_{h=i}^{j-۱} a_{ih}g_{hj}\right) - \deg g_{jj} \\ &\leq \max_{i\leq h<j}\{\deg a_{ih} + \deg g_{hj} - \deg g_{jj}\} < \max_{i\leq h<j}\{\deg a_{ih}\} = \deg a_{ii}.\end{aligned}$$

□

نکته ۱.۵.۲. *با توجه به گزاره ۴.۵.۲، اگر برای $۱ \leq i \leq l$ ، داشته باشیم: $g_{ii} = x^{n_i} - ۱$ ، آنگاه برای $۱ \leq i \neq j \leq l$ ، $g_{ij} = ۰$ خواهد بود؛ زیرا از آنجایی که $a_{ii}g_{ii} = x^{n_i} - ۱$ می‌باشد، در نتیجه $a_{ii} = ۱$ است و با توجه به گزاره‌های ۲.۵.۲ و ۴.۵.۲، برای $۱ \leq i \neq k \leq l$ ، خواهیم‌داشت: $a_{ik} = ۰$ ، بنابراین برای $۱ \leq i \neq j \leq l$ ، داریم: $\sum_{k=۱}^{l} a_{ik}g_{kj} = g_{ij} = ۰$.*

۶.۲ قضیه دوگانگی

در این بخش، به کمک قضیه دوگانگی[۳]، یک رابطه بین ماتریس چندجمله‌ای مولد کد C و ماتریس چندجمله‌ای مولد کد دوگان آن، $C^{\perp}$، تعریف می‌کنیم. به طور کلی روی بدست آوردن ماتریس چندجمله‌ای بررسی توازن از ماتریس چندجمله‌ای مولد متمرکز می‌شویم و نتایج معکوس آن را در بخش بعدی بدست می‌آوریم.

فرض کنید w یک عدد صحیح مثبت باشد. برای چندجمله‌ای $a \in \mathbb{F}_q[x]$ که $\deg a < w$ می‌باشد، $a^{\langle w \rangle}$ را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned} a &= a_0 + a_1 x + \cdots + a_{w-1} x^{w-1} \\ \Longrightarrow a^{\langle w \rangle} &= a_0 + a_{w-1} x + a_{w-2} x^2 + \cdots + a_1 x^{w-1} \end{aligned} \tag{۱۶.۲}$$

بردار ضرایب $(a_0, a_{w-1}, a_{w-2}, \ldots, a_1)$ از چندجمله‌ای $a^{\langle w \rangle}$، معادل است با سطر اول ماتریس $[a]^T$، که در آن $[a]$ یک ماتریس گردشی به صورت

$$[a] = \begin{pmatrix} a_0 & a_1 & \ldots & a_{w-1} \\ a_{w-1} & a_0 & \ldots & a_{w-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & \ldots & a_{w-1} & a_0 \end{pmatrix}. \tag{۱۷.۲}$$

می‌باشد. آنگاه داریم:

$$\left(a^{\langle w \rangle}\right)^{\langle w \rangle} = a$$

و

$$x^{\deg a} a(x^{-1}) = x^{\deg a} a^{\langle w \rangle} \mod (x^w - 1).$$

لم ۱.۶.۲. *برای عدد صحیح و مثبت w، فرض کنید $\xi(w)$ یک $\mathbb{F}_q-$جبر شامل همه ماتریسهای گردشی $w \times w$، با درایه‌هایی در $\mathbb{F}_q$ باشد. در این صورت،*

(i). با توجه به رابطه‌ای که بین a و $[a]$ در تساوی (۱۷.۲) وجود دارد یک یکریختی بین دو $\mathbb{F}_q-$جبر به صورت $\mathbb{F}_q[x]/(x^w - 1) \longrightarrow \xi(w)$ تعریف می‌کنیم.

(ii). به کمک نگاشت تعریف شده در بند (i) ترانهاده $[a]$ در $\xi(w)$ که به صورت $[a]^T$ نشان می‌دهیم، مطابق است با اینکه به جای a در $\mathbb{F}_q[x]/(x^w - 1)$، $a^{\langle w \rangle}$ را جاگذاری کنیم.

(iii). فرض کنید w، عدد N را عاد کند. نگاشت $\mathbb{F}_q[x]/(x^N - 1) \longrightarrow \mathbb{F}_q[x]/(x^w - 1)$ که توسط ضرب $\frac{x^N-1}{x^w-1}$ حاصل می‌شود مطابق است با نگاشت $\xi(N) \longrightarrow \xi(w)$ که به واسطه نگاشت

[۳] Duality theorem

تعریف شده در بند (i) توسط رابطه $[a] \longmapsto \begin{pmatrix} [a] & \cdots & [a] \\ \vdots & \ldots & \vdots \\ [a] & \cdots & [a] \end{pmatrix}$ *تعریف می‌شود، که در آن ماتریس* $\begin{pmatrix} [a] & \cdots & [a] \\ \vdots & \ldots & \vdots \\ [a] & \cdots & [a] \end{pmatrix}$، *بیانگر ماتریس تکرار* $[a]$ *از مرتبه* $\frac{N}{w} \times \frac{N}{w}$ *می‌باشد. به عنوان مثال، نگاشت‌های زیر نمودار جابجایی‌اند که نگاشت‌های عمودی، توسط نگاشت تعریف شده در بند (i) بدست می‌آیند.*

$$\begin{array}{ccc} \mathbb{F}_q[x]/(x^w - ۱) & \xrightarrow{\times \frac{x^N - ۱}{x^w - ۱}} & \mathbb{F}_q[x]/(x^N - ۱) \\ \Big\downarrow (i) & & \Big\downarrow (i) \\ \xi(w) & \xrightarrow{\frac{N}{w} \times \frac{N}{w} \text{ ماتریس تکرار}} & \xi(N) \end{array}$$

$$[a] \qquad \longmapsto \qquad \begin{pmatrix} [a] & \cdots & [a] \\ \vdots & \ldots & \vdots \\ [a] & \cdots & [a] \end{pmatrix}$$

برهان. ادعای مطرح شده در بند ،(i) شناخته شده است، ادعای بند (ii) نتیجه‌ی حاصل از آن می‌باشد و بند (iii) نیز با توجه به رابطه‌ی $\frac{x^N - ۱}{x^w - ۱} = ۱ + x^w + x^{۲w} + \ldots + x^{N-w}$ به راحتی قابل محاسبه می‌باشد. □

گزاره ۱.۶.۲. *(تعامد در M). فرض کنید $(c_۱, \ldots, c_l)$ و $(d_۱, \ldots, d_l)$ متعلق به M باشند که M توسط رابطه (؟؟) تعریف شده است و $N = \operatorname{lcm}(n_۱, \ldots, n_l)$ می‌باشد. علاوه بر این فرض کنید که $c, d \in (\mathbb{F}_q)^n$ دو بردار سطری هستند که به ترتیب، توسط رابطه (۵.۲)، به $(d_۱, \ldots, d_l)$ و $(c_۱, \ldots, c_l)$ وابسته‌اند. در این صورت $c(d^T) = ۰$ می‌باشد اگر و تنها اگر*

$$x^N - ۱ \quad \Big| \quad \sum_{k=۱}^{l} c_k \frac{x^N - ۱}{x^{n_k} - ۱} d_k^{\langle n_k \rangle} . \tag{۱۸.۲}$$

برهان. طبق لم ۱.۶.۲، رابطه (۱۸.۲)، معادل است با

$$\sum_{k=۱}^{l} \begin{pmatrix} [c_k][d_k^{\langle n_k \rangle}] & \cdots & [c_k][d_k^{\langle n_k \rangle}] \\ \vdots & \ldots & \vdots \\ [c_k][d_k^{\langle n_k \rangle}] & \cdots & [c_k][d_k^{\langle n_k \rangle}] \end{pmatrix} = ۰_{N \times N}, \tag{۱۹.۲}$$

که در آن $[c_k]$ و $[d_k^{\langle n_k\rangle}]$ توسط رابطه (۱۷.۲) تعریف می‌شوند. سمت چپ تساوی فوق یک ماتریس تکرار از مرتبه $\frac{N}{n_k}\times\frac{N}{n_k}$، متشکل از ماتریس‌های $[c_k][d_k^{\langle n_k\rangle}]$ از مرتبه $n_k\times n_k$ می‌باشد و $\circ_{N\times N}$، نشان‌دهنده ماتریس صفر از مرتبه $N\times N$ است. علاوه بر این درایه $(۱,۱)$ از معادله (۱۹.۲)، معادل است با:

$$\sum_{k=۱}^{l}\begin{pmatrix}c_{k,\circ} & c_{k,۱} & c_{k,۲} & \dots & c_{k,n_k-۱}\end{pmatrix}\begin{pmatrix}d_{k,\circ}\\ d_{k,۱}\\ d_{k,۲}\\ \vdots\\ d_{k,n_k-۱}\end{pmatrix}=\circ.$$

که با $c(d^T)=\circ$ معادل است. در مقابل اگر داشته‌باشیم، $c(d^T)=\circ$، با تغییر مکان آن به اندازه m مرتبه که در آن $۱\leq m\leq N$ می‌باشد، معادله (۱۹.۲) حاصل می‌شود که می‌توان از آن رابطه (۱۸.۲) را نتیجه گرفت. □

قضیه ۱.۶.۲. *فرض کنید $G=(g_{i,j})$ یک ماتریس چندجمله‌ای مولد کاهنده کد شبه‌دوری تعمیم‌یافته C باشد و $A=(a_{i,j})$ ماتریس چندجمله‌ای باشد که در معادله $AG=\operatorname{diag}[x^{n_۱}-۱,\dots,x^{n_l}-۱]$ صدق می‌کند. تعریف می‌کنیم:*

$$A^*=\left(a_{j,i}^{\langle n_j\rangle}\right),$$

که در آن اگر $i\neq j$ و یا اگر داشته‌باشیم $a_{j,i}\neq x^{n_j}-۱$، آنگاه $a_{j,i}^{\langle n_j\rangle}$ توسط رابطه (۱۶.۲) تعریف می‌شود و در غیر این صورت خواهیم داشت: $a_{i,i}^{\langle n_i\rangle}=x^{n_i}-۱$. علاوه بر این تعریف می‌کنیم:

$$H=\operatorname{diag}[x^{\deg a_{۱,۱}},\dots,x^{\deg a_{l,l}}]A^*=\left(x^{\deg a_{i,i}}a_{j,i}^{\langle n_j\rangle}\right),$$

یعنی به عبارت دیگر داریم:

$$H=\begin{pmatrix}x^{\deg a_{۱,۱}}a_{۱,۱}^{\langle n_۱\rangle} & \circ & \dots & \circ\\ x^{\deg a_{۲,۲}}a_{۱,۲}^{\langle n_۱\rangle} & x^{\deg a_{۲,۲}}a_{۲,۲}^{\langle n_۲\rangle} & \ddots & \vdots\\ \vdots & \vdots & \ddots & \circ\\ x^{\deg a_{l,l}}a_{۱,l}^{\langle n_۱\rangle} & x^{\deg a_{l,l}}a_{۲,l}^{\langle n_۲\rangle} & \dots & x^{\deg a_{l,l}}a_{l,l}^{\langle n_l\rangle}\end{pmatrix},\qquad(۲۰.۲)$$

که در آن برای هر (i,j)، عبارت $x^{\deg a_{i,i}}a_{j,i}^{\langle n_j\rangle}$ از ستون $j-$ام ماتریس H به پیمانه $(x^{n_j}-۱)$ می‌باشد و اگر $x^{\deg a_{i,i}}a_{i,i}^{\langle n_i\rangle}$ به پیمانه $(x^{n_i}-۱)$ برابر $\circ$ باشد، عبارت $x^{\deg a_{i,i}}a_{i,i}^{\langle n_i\rangle}=(x^{n_i}-۱)$ را قرار می‌دهیم. در این صورت H یک ماتریس چندجمله‌ای بررسی توازن برای کد C می‌باشد.

برهان. در ابتدا ثابت می‌کنیم که بردار چندجمله‌ای در هر سطر A^*، متعلق به $C^\perp$ می‌باشد. از رابطه $AG=\operatorname{diag}[x^{n_۱}-۱,\dots,x^{n_l}-۱]$، ماتریس چندجمله‌ای G' را به صورت زیر تعریف می‌کنیم:

$$G'=G\operatorname{diag}\left[\frac{x^N-۱}{x^{n_۱}-۱},\dots,\frac{x^N-۱}{x^{n_l}-۱}\right]=\left(g_{i,j}\frac{x^N-۱}{x^{n_j}-۱}\right),$$

که در آن $N = \operatorname{lcm}(n_1, \dots, n_l)$ می‌باشد. از این رو خواهیم داشت:

$$AG' = \operatorname{diag}[x^N - 1, \dots, x^N - 1].$$

با توجه به گزاره ۳.۵.۲، تساوی $G'A = \operatorname{diag}[x^N - 1, \dots, x^N - 1]$ برقرار است که برای همه $1 \le i, j \le l$ معادل است با:

$$\sum_{k=1}^{l} g_{i,k} \frac{x^N - 1}{x^{n_k} - 1} a_{k,j} = \begin{cases} 0 & i \neq j, \\ x^N - 1 & i = j. \end{cases}$$

از آنجا که $\left(a_{k,j}^{\langle n_k \rangle}\right)^{\langle n_k \rangle} = a_{k,j}$ می‌باشد و با توجه به گزاره ۱.۶.۲، سطر $j-$ام بردار چندجمله‌ای $\left(a_{1,j}^{\langle n_1 \rangle}, \dots, a_{l,j}^{\langle n_l \rangle}\right)$ از A^* برای همه $1 \le j \le l$، متعلق به $C^\perp$ می‌باشد. در ادامه اثبات نشان می‌دهیم که بردارهای چندجمله‌ای سطری از ماتریس $H = (h_{i,j})$ در (۲۰.۲)، شرط مینیمم را در تعریف ۲.۳.۲ داراست. یعنی، $h_{i,i}$ دارای مینیمم درجه در میان f_i هایی است که در بردارهای چندجمله‌ای به فرم $(f_1, \dots, f_i, 0, \dots, 0) \in C^\perp$ با $f_i \neq 0$ قرار دارد. به کمک استدلال بالا داریم: $\left(a_{1,i}^{\langle n_1 \rangle}, \dots, a_{i,i}^{\langle n_i \rangle}, 0, \dots, 0\right) \in C^\perp$، $\left(x^{\deg a_{i,i}} a_{1,i}^{\langle n_1 \rangle}, \dots, x^{\deg a_{i,i}} a_{i,i}^{\langle n_i \rangle}, 0, \dots, 0\right) \in C^\perp$ و $x^{\deg a_{i,i}} a_{i,i}^{\langle n_l \rangle} \in \left(C^\perp\right)_i = \{c_i | (c_1, \dots, c_i, 0, \dots, 0) \in C^\perp\}$ می‌باشد. همچنین توجه داشته‌باشید که $h_{i,i} = x^{\deg a_{i,i}} a_{i,i}^{\langle n_i \rangle} = x^{\deg a_{i,i}} a_{i,i}(x^{-1})$ و از آنجایی که $a_{i,i} g_{i,i} = x^{n_i} - 1$ می‌باشد، می‌توانیم بگوییم که h_{ii} با چندجمله‌ای مولد کد دوگان از کد دوری $C_i = \{c_i | (0, \dots, 0, c_i, \dots, c_l) \in C\}$ معادل است. بنابراین داریم: $(C_i)^\perp \supseteq \left(C^\perp\right)_i$، همچنین بدیهی است که $\left(C^\perp\right)_i \subseteq (C_i)^\perp$ می‌باشد، بنابراین خواهیم داشت: $(C_i)^\perp = \left(C^\perp\right)_i$. ازاین رو h_{ii} با چندجمله‌ای مولد $\left(C^\perp\right)_i$ معادل است و در میان $f \in \left(C^\perp\right)_i$ و $f \neq 0$، h_{ii} دارای کمترین درجه است و اثبات کامل می‌شود. □

مثال ۱.۶.۲. *فرض کنید $q = 2$ باشد و ماتریس‌های چندجمله‌ای G و A را به‌صورت زیر داشته‌باشیم:*

$$G = \begin{pmatrix} 1 + x^4 + x^6 + x^7 & x^2 + x^3 & 1 + x + x^2 \\ 0 & 1 + x^5 & 1 + x + x^2 \\ 0 & 0 & 1 + x^3 \end{pmatrix},$$

$$A = \begin{pmatrix} 1 + x^4 + x^6 + x^7 + x^8 & x^2 + x^3 + x^6 & 1 + x + x^3 + x^7 \\ 0 & 1 + x^5 & 1 + x + x^2 + x^3 + x^4 \\ 0 & 0 & 1 + x^3 \end{pmatrix}.$$

در این صورت داریم :

$$AG = \operatorname{diag}[x^{15} - 1, x^{10} - 1, x^6 - 1].$$

فرض کنید که C یک کد شبه‌دوری تعمیم‌یافته باشد که توسط ماتریس مولد G تعریف می‌شود. دراین صورت برای بدست آوردن ماتریس H به کمک رابطه (۲۰.۲)، ابتدا ماتریس A^* را به صورت زیر محاسبه می‌کنیم:

$$A^* = \begin{pmatrix} 1 + x^7 + x^8 + x^9 + x^{11} & 0 & 0 \\ x^9 + x^{12} + x^{13} & 1 + x^5 & 0 \\ 1 + x^8 + x^{12} + x^{14} & 1 + x^6 + x^7 + x^8 + x^9 & 1 + x^3 \end{pmatrix}.$$

سپس H معادل است با:

$$H = \begin{pmatrix} ۱ + x + x^۲ + x^۴ + x^۸ & ۰ & ۰ \\ x^۲ + x^۳ + x^{۱۴} & ۱ + x^۵ & ۰ \\ ۱ + x^۲ + x^۳ + x^{۱۱} & ۱ + x + x^۲ + x^۳ + x^۹ & ۱ + x^۳ \end{pmatrix}.$$

به کمک الگوریتم بوخ‌برگر ماتریس کاهنده H' را از ماتریس H به صورت زیر بدست می‌آوریم:

$$H' = \begin{pmatrix} ۱ + x + x^۲ + x^۴ + x^۸ & ۰ & ۰ \\ ۱ + x + x^۲ + x^۷ & ۱ + x^۵ & ۰ \\ ۱ + x^۲ + x^۳ + x^۴ + x^۵ + x^۶ & ۱ + x + x^۲ + x^۳ + x^۴ & ۱ + x^۳ \end{pmatrix}.$$

مطابق با تغییر مکان، به کمک ماتریس G، می‌توان یک ماتریس مولد دودویی[۴] $\tilde{G}$، از مرتبه ۳۱×۱۶، برای کد C تولید کرد. برای مثال، از سطر اول ماتریس G، ۸ سطر از ماتریس $\tilde{G}$ به صورت زیر تولید می‌شود:

$$\left(\begin{array}{c|c|c} ۱۰۰۰۱۰۱۱۰۰۰۰۰۰۰ & ۰۰۱۱۰۰۰۰۰۰ & ۱۱۱۰۰۰ \\ ۰۱۰۰۰۱۰۱۱۰۰۰۰۰۰ & ۰۰۰۱۱۰۰۰۰۰ & ۰۱۱۱۰۰ \\ ۰۰۱۰۰۰۱۰۱۱۰۰۰۰۰ & ۰۰۰۰۱۱۰۰۰۰ & ۰۰۱۱۱۰ \\ ۰۰۰۱۰۰۰۱۰۱۱۰۰۰۰ & ۰۰۰۰۰۱۱۰۰۰ & ۰۰۰۱۱۱ \\ ۰۰۰۰۱۰۰۰۱۰۱۱۰۰۰ & ۰۰۰۰۰۰۱۱۰۰ & ۱۰۰۰۱۱ \\ ۰۰۰۰۰۱۰۰۰۱۰۱۱۰۰ & ۰۰۰۰۰۰۰۱۱۰ & ۱۱۰۰۰۱ \\ ۰۰۰۰۰۰۱۰۰۰۱۰۱۱۰ & ۰۰۰۰۰۰۰۰۱۱ & ۱۱۱۰۰۰ \\ ۰۰۰۰۰۰۰۱۰۰۰۱۰۱۱ & ۱۰۰۰۰۰۰۰۰۱ & ۰۱۱۱۰۰ \end{array}\right).$$

از سوی دیگر، به کمک ماتریس کاهنده H'، می‌توان یک ماتریس بررسی توازن دودویی $\tilde{H}$، از مرتبه ۳۱×۱۵، برای کد C تولید کرد. سپس می‌توان بررسی کرد که حاصل $\tilde{G} \times \tilde{H}^T$، معادل با ماتریس صفر است.

۷.۲ قضایایی که برای دوگان کدهای شبه‌دوری تعمیم‌یافته صادق است.

برای تکمیل بحث، در این بخش نتایج بدست آمده در بخشهای قبل را، برای دوگان کدهای شبه‌دوری تعمیم‌یافته بیان می‌کنیم. این نتایج مشابه استدلالهای قبلی نشان داده می‌شوند و ما از اثبات آنها صرف‌نظر می‌کنیم.

گزاره ۱.۷.۲. *(گزاره دوشرطی دیگر برای کدواژه‌های کد شبه‌دوری تعمیم‌یافته C)* یک بردار چندجمله‌ای $c = (c_۱, \ldots, c_l) \in \mathbb{F}_q[x]^l$ کدواژه‌ای از کد C است اگر و تنها اگر برای همه $۱ \leq i \leq l$، داشته باشیم:

$$x^N - ۱ \quad \Big| \quad \sum_{j=۱}^{l} c_j \frac{x^N - ۱}{x^{n_j} - ۱} h_{i,j}^{\langle n_j \rangle}.$$

[۴] Binary

که در آن $H = (h_{i,j})$، طبق تعریف ۲.۳.۲، یک ماتریس چندجمله‌ای بررسی توازن برای کد C می‌باشد و $N = \operatorname{lcm}(n_1, \ldots, n_l)$ است.

گزاره ۲.۷.۲. *(معادله‌ای که ماتریس چندجمله‌ای بررسی توازن کدهای شبه‌دوری تعمیم‌یافته در آن صادق است). فرض کنید که $H = (h_{i,j})$ یک ماتریس $l \times l$ با درایه‌هایی در $\mathbb{F}_q[x]$ باشد به گونه‌ای که برای همه $1 \leq i, j \leq l$، اگر $i < j$ باشد آنگاه $h_{i,j} = 0$ بوده و به گونه‌ای بلوک بندی شود که $\sum_{i=1}^{l} n_i = n$ باشد. در این صورت، H یک ماتریس چندجمله‌ای بررسی توازن برای کد شبه‌دوری تعمیم‌یافته C است اگر و تنها اگر یک ماتریس $l \times l$ مانند $B = (b_{i,j})$ با درایه‌هایی در $\mathbb{F}_q[x]$ وجود داشته باشد به گونه‌ای که رابطه زیر برقرار باشد:*

$$BH = \operatorname{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]. \qquad (۲۱.۲)$$

گزاره ۳.۷.۲. *(خاصیت مثلثی بودن ماتریس B). فرض کنید H یک ماتریس چندجمله‌ای بررسی توازن مانند ماتریس (۹.۲)، برای کد شبه‌دوری تعمیم‌یافته C باشد و B نیز ماتریس چندجمله‌ای باشد که در رابطه (۲۱.۲)، صدق می‌کند. در این صورت، ماتریس B نیز یک ماتریس پایین مثلثی است، یعنی اگر $B = (b_{i,j})$ و $i < j$ باشد، آنگاه درایه $b_{i,j} = 0$ خواهد بود.*

گزاره ۴.۷.۲. *(خاصیت جابجایی ماتریس‌های B و H در کدهای شبه‌دوری). فرض کنید که ماتریس H یک ماتریس چندجمله‌ای بررسی توازن برای کد شبه‌دوری C و $n_1 = n_2 = \ldots = n_l = N$ باشد و B نیز ماتریس چندجمله‌ای باشد که در رابطه (۲۱.۲)، صدق می‌کند. در این صورت، رابطه زیر نیز همچنین برقرار است:*

$$HB = \operatorname{diag}[x^{N} - 1, \ldots, x^{N} - 1].$$

گزاره ۵.۷.۲. *(ویژگی کاهندگی برای ماتریس B). فرض کنید که ماتریس H یک ماتریس چندجمله‌ای بررسی توازن برای کد شبه‌دوری تعمیم‌یافته C باشد و همچنین فرض کنید که ماتریس B وجود دارد که در معادله $BH = \operatorname{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$ صدق کند. در این صورت در ماتریس $B = (b_{i,j})$ و برای همه $1 \leq i \neq j \leq l$، داریم:*

$$\deg b_{i,j} < \deg b_{i,i}.$$

قضیه ۱.۷.۲. *(مرجع [38] را ببینید.) فرض کنید $H = (h_{i,j})$ یک ماتریس چندجمله‌ای بررسی توازن کاهنده برای کد شبه‌دوری تعمیم‌یافته C باشد و $B = (b_{i,j})$ یک ماتریس چندجمله‌ای باشد که در رابطه $BH = \operatorname{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$ صدق می‌کند. تعریف می‌کنیم:*

$$B^* = \left(b_{j,i}^{\langle n_j \rangle}\right),$$

که در آن اگر $i \neq j$ و یا اگر داشته‌باشیم $b_{j,i} \neq x^{n_j} - 1$، آنگاه $b_{j,i}^{\langle n_j \rangle}$ توسط رابطه (۱۶.۲) تعریف می‌شود و در غیر این صورت خواهیم داشت: $b_{i,i}^{\langle n_i \rangle} = x^{n_i} - 1$. علاوه بر این تعریف می‌کنیم:

$$G = \operatorname{diag}[x^{\deg b_{1,1}}, \ldots, x^{\deg b_{l,l}}] B^* = \left(x^{\deg b_{i,i}} b_{j,i}^{\langle n_j \rangle}\right),$$

یعنی به عبارت دیگر داریم:

$$G=\begin{pmatrix} x^{\deg b_{1,1}}b_{1,1}^{\langle n_1\rangle} & x^{\deg b_{1,1}}b_{2,1}^{\langle n_2\rangle} & \cdots & x^{\deg b_{1,1}}b_{l,1}^{\langle n_l\rangle} & \cdots \\ 0 & x^{\deg b_{2,2}}b_{2,2}^{\langle n_2\rangle} & \cdots & x^{\deg b_{2,2}}b_{l,2}^{\langle n_l\rangle} & \\ \vdots & \ddots & \ddots & \vdots & \\ 0 & \cdots & 0 & x^{\deg b_{l,l}}b_{l,l}^{\langle n_l\rangle} & \end{pmatrix}, \qquad (۲۲.۲)$$

که در آن برای هر (i,j)، عبارت $x^{\deg b_{i,i}}b_{j,i}^{\langle n_j\rangle}$ از ستون $j-$ام ماتریس G به پیمانه $(x^{n_j}-1)$ می‌باشد و اگر $x^{\deg b_{i,i}}b_{i,i}^{\langle n_i\rangle}$ به پیمانه $(x^{n_i}-1)$ برابر 0 باشد، قرار می‌دهیم: $x^{\deg b_{i,i}}b_{i,i}^{\langle n_i\rangle}=(x^{n_i}-1)$. در این‌صورت G یک ماتریس چندجمله‌ای مولد برای کد C می‌باشد.

مثال ۱.۷.۲. فرض کنید $q=2$ باشد و ماتریس‌های چندجمله‌ای H و B را به صورت زیر داشته‌باشیم:

$$H=\begin{pmatrix} 1+x+x^2+x^4+x^8 & 0 & 0 \\ 1+x+x^2+x^7 & 1+x^5 & 0 \\ 1+x^2+x^3+x^4+x^5+x^6 & 1+x+x^2+x^3+x^4 & 1+x^3 \end{pmatrix}.$$

$$B=\begin{pmatrix} 1+x+x^3+x^7 & 0 & 0 \\ 1+x^4 & 1+x^5 & 0 \\ 0 & 1+x+x^2 & 1+x^3 \end{pmatrix}.$$

در این صورت داریم :

$$BH=\mathrm{diag}[x^{15}-1, x^{10}-1, x^6-1].$$

فرض کنید که C یک کد شبه‌دوری تعمیم‌یافته باشد که توسط ماتریس بررسی توازن H تعریف می‌شود. دراین صورت برای بدست آوردن ماتریس G به کمک رابطه (۲۲.۲)، ابتدا ماتریس B^* را به صورت زیر محاسبه می‌کنیم:

$$B^*=\left(b_{j,i}^{\langle n_j\rangle}\right)=\begin{pmatrix} 1+x^8+x^{12}+x^{14} & 1+x^6 & 0 \\ 0 & 1+x^5 & 1+x^4+x^5 \\ 0 & 0 & 1+x^3 \end{pmatrix}.$$

سپس G معادل است با:

$$G=\begin{pmatrix} 1+x^4+x^6+x^7 & x^3+x^7 & 0 \\ 0 & 1+x^5 & x^3+x^4+x^5 \\ 0 & 0 & 1+x^3 \end{pmatrix}.$$

به کمک الگوریتم بوخ‌برگر ماتریس کاهنده G' را از ماتریس G به صورت زیر بدست می‌آوریم:

$$G'=\begin{pmatrix} 1+x^4+x^6+x^7 & x^2+x^3 & 1+x+x^2 \\ 0 & 1+x^5 & 1+x+x^2 \\ 0 & 0 & 1+x^3 \end{pmatrix}.$$

بنابراین، G' معادل است با ماتریس G که در مثال ۱.۶.۲، داده شده بود.

فصل ۳

کدهای صحیح تعمیم‌یافته و ماتریس مولد آنها

کدهای صحیح در بسیاری از زمینه‌های تحقیقاتی مورد مطالعه قرار گرفته‌است. [1, 2, 3, 10, 14, 15, 16, 30, 35] کدهای صحیح به طول l به عنوان زیر گروهی از $(\mathbb{Z}/N\mathbb{Z})^l$ تعریف می‌شود. که l و $\mathbb{Z}$ اعداد صحیح مثبتند. $\mathbb{Z}/N\mathbb{Z}$ یک گروه دوری از اعداد صحیح به پیمانه N می‌باشد، و $(\mathbb{Z}/N\mathbb{Z})^l$ یک گروه آبلی از همه $l-$ تایی‌های $(c_1, \ldots, c_l)$ می‌باشد که در آن برای $1 \leq i \leq l$، داریم: $c_i \in \mathbb{Z}/N\mathbb{Z}$. در نظریه کدهای شبه‌دوری چندجمله‌ای‌ها روی میدان متناهی به پیمانه $x^u - 1$ مطابق‌اند با اعداد صحیح به پیمانه N در نظریه کدهای صحیح. بنابراین کدهای صحیح قابل قیاس با کدهای QC می‌باشند. در این فصل کدهای صحیح تعمیم‌یافته معرفی و برخی خصوصیات اساسی آنها نشان داده‌می‌شود. به طور خلاصه کدهای صحیح تعمیم یافته به طول l به عنوان زیر گروهی از $\bigoplus_{i=1}^{l} \mathbb{Z}/n_i\mathbb{Z}$ معرفی می‌شوند. به عبارت دیگر، گروه‌های آبلی از برخی کدواژه‌های $(c_1, \ldots, c_l)$، که برای همه‌ی $1 \leq i \leq l$، مؤلفه‌ی $c_i \in \mathbb{Z}/n_i\mathbb{Z}$ می‌باشد و $n_1, \ldots, n_l$ اعداد صحیح مثبتند و در حالت کلی برابر نیستند. اگر داشته‌باشیم: $N = n_1 = \cdots = n_l$، آنگاه کدهای صحیح تعمیم یافته با کدهای صحیح برابرند. در ادامه نشان داده‌می‌شود که هر کد صحیح تعمیم یافته یک بیان استاندارد برای ماتریس مولدش که با $G = (g_{ij})$ معرفی می‌شود دارد که به فرم زیر است،

$$\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1l} \\ 0 & g_{22} & \cdots & g_{2l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{ll} \end{pmatrix}. \tag{۱.۳}$$

که یک ماتریس صحیح بالا مثلثی $l \times l$ است و در عملیات ماتریسی زیر صدق می‌کند.

$$AG = \mathrm{diag}[n_1, \ldots, n_l]. \tag{۲.۳}$$

که در آن A یک ماتریس صحیح $l \times l$ دیگر است و $\mathrm{diag}[n_1, \ldots, n_l]$ یک ماتریس قطری است که برای $1 \leq i \leq l$، درایه (i,i) آن برابر n_i می باشد. همچنین نشان داده می‌شود که ماتریس صحیح بالا مثلثی G، یک ماتریس مولد برای کد صحیح تعمیم‌یافته است اگر و فقط اگر G در عملیات ماتریسی (۲.۳) صدق کند. اگر در ماتریس مولد G که در روابط (۱.۳) و (۲.۳) صادق است داشته‌باشیم: $0 \leq g_{ij} < g_{jj}$ برای $1 \leq i < j \leq l$، آنگاه G یک ماتریس مولد کاهنده نامیده می‌شود. در ادامه ثابت می‌کنیم که هر کد صحیح تعمیم یافته، دارای ماتریس مولد کاهنده منحصر به فرد است. بنابراین، (۱.۳)، برای طبقه بندی کدهای صحیح تعمیم یافته مورد استفاده قرار می‌گیرد. مفهوم ارائه شده در تساوی ماتریسی (۲.۳) نخستین بار توسط لالی[۱] و فیتس پاتریک[۲] برای کدهای QC ارائه شد [18]. و توسط نویسندگان برای کدهای GQC تعمیم داده شد [28, 38]. در این فصل این مفهوم جایگاه بسیار مهمی در تولید و شمارش کدهای صحیح تعمیم‌یافته دارد، زیرا طبق رابطه (۲.۳)، داریم: $a_{ii}g_{ii} = n_i$. تساوی (۲.۳)، مفهوم شناخته‌شده $h(x)g(x) = x^n - 1$ برای کدهای دوری را تعمیم می‌دهد. که در آن $g(x)$ چند جمله‌ای مولد آن است. دوگان یک کد صحیح تعمیم‌یافته با استفاده از یک فرم خطی مناسب تعریف می‌شود. ماتریس بررسی توازن کدهای صحیح تعمیم‌یافته نیز به عنوان یک ماتریس پایین مثلثی از کد دوگان آن بدست می‌آید. محتویات این فصل عمدتاً از مرجع [27] برداشت شده‌است. در ادامه، قبل از تعریف کدهای صحیح تعمیم‌یافته به معرفی نمادهایی که در این فصل استفاده می‌شود می‌پردازیم.

$\mathbb{Z}$ و $\mathbb{Q}$ به‌ترتیب نشان‌دهنده حلقه اعداد صحیح و اعداد گویا می‌باشند. برای عدد صحیح و مثبت l، $M_l(R)$ نشان‌دهنده یک ماتریس $l \times l$ با درایه‌هایی از R است. که در آن $R = \mathbb{Z}$ یا $R = \mathbb{Q}$ می‌باشد. ترانهاده یک ماتریس و یا بردار M را به صورت M^T تعریف می‌کنیم. علاوه براین $T_l(R)$ یک گروه از ماتریس‌های بالامثلثی است که قطر آن عناصر مثبت است، و $T_l'(R)$ نشان‌دهنده ماتریس‌های پایین‌مثلثی است. به‌عبارت دیگر داریم:

$$T_l(R) = \left\{ G = (g_{ij}) \in M_l(R) \,\middle|\, G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1l} \\ 0 & g_{22} & \cdots & g_{2l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{ll} \end{pmatrix}, \begin{array}{l} g_{ii} > 0 \\ \text{for } 1 \leq i \leq l \end{array} \right\},$$

$$T_l'(R) = \{G \in M_l(R) | G^T \in T_l(R)\}. \tag{۳.۳}$$

علاوه بر این از

$$GL_l(\mathbb{Q}) = \{G \in M_l(\mathbb{Q}) | \det(G) \neq 0\},$$

$$SL_l(\mathbb{Z}) = \{G \in M_l(\mathbb{Z}) | \det(G) = 1\},$$

[۱] Lally
[۲] Fitzpatrick

نیز استفاده می‌کنیم. برای عدد صحیح و مثبت l، $\mathbb{Z}^l$ را به‌صورت زیر تعریف می‌کنیم:

$$\mathbb{Z}^l = \{d = (d_1, \ldots, d_l) | d_1, \ldots, d_l \in \mathbb{Z}\}.$$

همچنین برای $G \in T_l(\mathbb{Z})$ و یا $G \in T_l'(R)$ تعریف می‌کنیم:

$$\mathbb{Z}^l G = \{dG | d \in \mathbb{Z}^l\}.$$

اگر $G = (g_{ij})$ و $G \in T_l(\mathbb{Z})$ و یا $G \in T_l'(\mathbb{Z})$ باشد، و اگر برای $1 \leq i, j \leq l$ داشته‌باشیم $0 \leq g_{ij} \leq g_{jj}$، آنگاه G را ماتریس کاهنده می‌نامیم. برای $G \in T_l(\mathbb{Z})$ و یا $G \in T_l'(\mathbb{Z})$، ماتریس $P \in SL_l(\mathbb{Z})$ وجود دارد به طوری که $G' = PG$ یک ماتریس کاهنده است، و $\mathbb{Z}^l G = \mathbb{Z}^l G'$ می‌باشد زیرا برای $S \in SL_l(\mathbb{Z})$ داریم:

$$\mathbb{Z}^l S = \mathbb{Z}^l.$$

تعداد عناصر در یک مجموعه متناهی مانند U را با $|U|$ و یا $\#U$ نشان می‌دهیم.

۱.۳ کدهای صحیح تعمیم‌یافته

فرض کنید که l یک عدد صحیح مثبت است و برای $1 \leq i \leq l$، $\mathbb{Z}/n_i\mathbb{Z}$ یک حلقه از اعداد صحیح به پیمانه n_i باشد که n_i نیز یک عدد صحیح مثبت است. تعریف می‌کنیم:

$$M = \bigoplus_{i=1}^{l} \mathbb{Z}/n_i\mathbb{Z} = \{c = (c_1, c_2, \ldots, c_l) | c_i = \mathbb{Z}/n_i\mathbb{Z}, 1 \leq i \leq l\}$$

برای $c = (c_1, c_2, \ldots, c_l) \in M$ و $d = (d_1, d_2, \ldots, d_l) \in M$ تعریف می‌کنیم:

$$-c = (-c_1, -c_2, \ldots, -c_l)$$

و

$$c + d = (c_1 + d_1, \ldots, c_l + d_l).$$

آنگاه خواهیم داشت:

$$-c \in M, c + d \in M.$$

و M یک گروه آبلی است.

تعریف ۱.۱.۳. *یک کد صحیح تعمیم‌یافته C به عنوان زیر گروهی از گروه آبلی M تعریف می‌شود و مؤلفه $c \in C$ را یک کدواژه از C می‌نامیم. اگر $n_1 = n_2 = \cdots = n_l$ آنگاه C یک کد صحیح است.*

به طور دقیق‌تر یک کد صحیح تعمیم‌یافته C یک زیرگروه از M است اگر شرایط زیر را برآورده کند:

$$c, d \in C \Longrightarrow c + d \in C,$$
$$c \in C \Longrightarrow -c \in C. \qquad (۴.۳)$$

با توجه به رابطه (۴.۳) می‌توانیم بگوییم که برای هر $c \in C$ و $n \in \mathbb{Z}$ داریم: $nc \in C$.

مثال ۱.۱.۳. *فرض کنیم* $l = ۱$ *و* $n_۱ = ۶$ *باشد. بنابراین،* $M = \mathbb{Z}/۶\mathbb{Z}$ *خواهدبود و کد صحیح در* M *به صورت* $g\mathbb{Z}/۶\mathbb{Z}$ *می‌باشد که در آن* $g = ۱, ۲, ۳, ۶$ *است.*

مثال ۲.۱.۳. *فرض کنید*

$$M = \mathbb{Z}/۱۰\mathbb{Z} \bigoplus \mathbb{Z}/۱۲\mathbb{Z}$$

و $C_۱ = \{(۰,۰),(۰,۴),(۰,۸),(۵,۲),(۵,۶),(۵,۱۰)\}$ *یک زیرگروه از* M *باشد، لذا* $C_۱$ *یک کد صحیح تعمیم‌یافته می‌باشد. توجه داشته‌باشید که به‌ازای* $f_۱ \in \{۰,۱\}$ *و* $f_۲ \in \{۰,۱,۲\}$ *خواهیم‌داشت:* $C_۱ = f_۱(۵,۲) + f_۲(۰,۴)$.

نکته ۱.۱.۳. *فرض کنید* $c = (c_۱, \ldots, c_l) \in M$ *و* $c' = (c'_۱, \ldots, c'_l) \in M$ *باشند. فاصله لی*[۳] *بین دو کدواژه* c *و* c' *را به‌صورت* $d_l(c, c')$ *نشان می‌دهیم و خواهیم‌داشت:*

$$d_l(c, c') = \sum_{i=۱}^{l} \min\{(c_i - c'_i) \mod n_i, (c'_i - c_i) \mod n_i\}.$$

که در آن برای $۱ \le i \le l$ *، داریم:* $۰ \le (d_i \mod n_i) \le n_i - ۱$ *. همچنین نامساوی مثلثی در* $d_l(c, c')$ *صادق است. حداقل فاصله لی در یک کد صحیح تعمیم‌یافته به‌ص ورت زیر تعریف می‌شود:*

$$d_l(C) = \min\{d_l(c, c') | c \neq c' \in C\} = \min\{d_l(c, ۰) | ۰ \neq c \in C\}.$$

شایان ذکر است که حتی در کدهای صحیح، دو کد صحیح یکریخت در یک گروه آبلی در حالت کلی دارای حداقل فاصله لی یکسان نیستند.

به عنوان مثال دو کد صحیح $C_۲, C_۳ \subset M = (\mathbb{Z}/۸\mathbb{Z})^۲$ را در نظر بگیرید:

$$C_۲ = \{(۰,۰),(۲,۰),(۴,۰),(۶,۰),(۰,۴),(۲,۴),(۴,۴),(۶,۴)\},$$

$$C_۳ = \{(۰,۰),(۲,۲),(۴,۴),(۶,۶),(۰,۴),(۲,۶),(۴,۰),(۶,۲)\}.$$

هر دو کد $C_۲$ و $C_۳$ به $\mathbb{Z}/۴\mathbb{Z} \bigoplus \mathbb{Z}/۲\mathbb{Z}$ یکریختند. بااین‌حال $d_l(C_۲) = ۲$ و $d_l(C_۳) = ۴$ می‌باشد.

۲.۳ ماتریس مولد کدهای صحیح تعمیم‌یافته

در مثال ۲.۱.۳، یک کد صحیح تعمیم‌یافته توسط فهرستی از کدواژه‌های خود معرفی گردید. روش دیگر تعیین کد صحیح تعمیم‌یافته استفاده از ماتریس مولد $l \times l$ با درایه‌هایی از حلقه اعداد صحیح می‌باشد. ما می‌توانیم با یک روش مشابه ماتریس مولد کدهای خطی در میدان متناهی و همچنین چندجمله‌ای مولد کدهای دوری در میدان متناهی، تمام کدواژه‌های کدهای صحیح تعمیم یافته را از طریق ماتریس مولدشان تولید کنیم.

[۳] Lee distance

نگاشت F را به‌صورت زیر در نظر بگیرید:

$$F : \mathbb{Z}^l \to M$$
$$(c_1, \ldots, c_l) \to (c_1 \mod n_1, \ldots, c_l \mod n_l).$$

برای هر کد صحیح تعمیم یافته $C \subset M$، $F^{-1}(C)$ زیرگروهی از $\mathbb{Z}^l$ است.

نکته ۱.۲.۳. *از این به بعد گاهی عدد صحیح $g \in \mathbb{Z}$ را با $g \in \mathbb{Z}/n_i\mathbb{Z}$، از میان $g \mod n_i$ نشان می‌دهیم. علاوه بر این بردار صحیح $c \in \mathbb{Z}^l$ نیز گاهی به‌صورت $c \in M$ در نگاشت F در نظر گرفته‌می‌شود. در حقیقت C شامل بردارهای صحیح به‌صورت*

$$(\underbrace{0, \ldots, 0}_{i-1}, n_i, \underbrace{0, \ldots, 0}_{l-i}) \qquad (۵.۳)$$

می‌باشد که در آن $1 \leq i \leq l$ است، که بیان دیگری از کدواژه $(0, 0, \cdots, 0) = 0$ می‌باشد.

تعریف ۱.۲.۳. *فرض کنید C یک کد صحیح تعمیم‌یافته و سطرهای $G \in T_l(\mathbb{Z})$ در $F^{-1}(C)$ باشد. اگر داشته‌باشیم $\mathbb{Z}^l G = F^{-1}(C)$، آنگاه G یک ماتریس مولد برای کد C می‌باشد. در این تعریف عدد صفر روی قطر اصلی ماتریس G نمی‌تواند قرار گیرد. به‌عنوان مثال ماتریس مولد $M \subset \{0\}$ برابر $\mathrm{diag}[n_1, \ldots, n_l]$ می‌باشد.*

گزاره ۱.۲.۳. *(تعریف معادل ماتریس مولد) فرض کنید C یک کد صحیح تعمیم‌یافته و سطرهای ماتریس $G = (g_{ij}) \in T_l(\mathbb{Z})$ در $F^{-1}(C)$ باشد. آنگاه $\mathbb{Z}^l G = F^{-1}(C)$ خواهدبود اگر و تنها اگر به ازای $1 \leq i \leq l$ داشته‌باشیم:*

$$g_{ii} = \min\{c_i | (0, \ldots, 0, c_i, \ldots, c_l) \in F^{-1}(C), c_i > 0\}. \qquad (۶.۳)$$

برهان. ابتدا فرض می‌کنیم که (۶.۳) برقرار باشد ثابت می‌کنیم $\mathbb{Z}^l G = F^{-1}(C)$. سطر i ام از ماتریس G را g_i می‌نامیم. برای هر $\sum_{i=1}^{l} d_i g_i$ که در $\mathbb{Z}^l G$ قرار دارد خواهیم‌داشت:

$$F(\sum_{i=1}^{l} d_i g_i) = \sum_{i=1}^{l} d_i F(g_i) \in C.$$

بنابراین ثابت کردیم $\mathbb{Z}^l G \subset F^{-1}(C)$. حال فرض می‌کنیم $c = (c_1, \ldots, c_l) \in F^{-1}(C)$ است، به کمک استقرا ثابت می‌کنیم $c \in \mathbb{Z}^l G$ می‌باشد. g_{11} باید c_1 را عاد کند، زیرا در غیر این‌صورت $c_1 \mod g_{11} < g_{11}$ خواهدبود و این با تعریف کمینگی g_{11} در (۶.۳) در تناقض است. ازاین‌رو قرار می‌دهیم $d_1 = c_1/g_{11}$ و مجدداً $c - d_1 g_1$ را توسط $c = (c_1, \ldots, c_l)$ تعریف می‌کنیم. بنابراین $c \in F^{-1}(C)$ و $c_1 = 0$ خواهدبود. فرض می‌کنیم برای $c = (c_1, \ldots, c_l) \in F^{-1}(C)$ داشته‌باشیم: $c_1 = \cdots = c_{i-1} = 0$. به‌طور مشابه قرار می‌دهیم، $d_i = c_i/g_{ii}$ و عبارت $c - d_i g_i$ را توسط $c = (c_1, \ldots, c_l) \in F^{-1}(C)$ تعریف می‌کنیم. در این صورت $c \in F^{-1}(C)$ و $c_1 = \cdots = c_i = 0$

می‌باشد. لذا $c = d_1 g_1 + \cdots + d_l g_l$ خواهدبود و خواهیم‌داشت: $c \in \mathbb{Z}^l G$. بنابراین ثابت کردیم $F^{-1}(C) \subset \mathbb{Z}^l G$ است و در نتیجه $\mathbb{Z}^l G = F^{-1}(C)$ خواهدبود. بالعکس، فرض می‌کنیم که $\mathbb{Z}^l G = F^{-1}(C)$ باشد، ثابت می‌کنیم که (۶.۳) برقرار است:

$$\begin{aligned} &\min\{c_i \mid (0, \ldots, 0, c_i, \ldots, c_l) \in F^{-1}(C), c_i > 0\} \\ &= \min\left\{ d_i g_{ii} \,\middle|\, \sum_{j=i}^{l} d_j g_j \in Z^l G, d_i > 0 \right\} = g_{ii} \,. \end{aligned}$$

□

با توجه به اثبات بالا ما می‌توانیم از ماتریس مولد پایین‌مثلثی در تعریف ۱.۲.۳ استفاده کنیم. ما در این پایان نامه ماتریس مولد را در $T_l(\mathbb{Z})$ در نظر می‌گیریم.

گزاره ۲.۲.۳. *(منحصربه‌فرد بودن ماتریس مولد کاهنده) ماتریس مولد کاهنده در هر کد صحیح تعمیم‌یافته به‌صورت یکتا تعیین می‌شود.*

برهان. فرض کنید که $G = (g_{ij})$ و $G' = (g'_{ij})$ دو ماتریس مولد کاهنده برای کد صحیح تعمیم‌یافته باشند. اگر g_i و g'_i به‌ترتیب سطرهای i ام از ماتریس مولدهای G و G' باشند آنگاه $g_{ii} = g'_{ii}$ می‌باشد، زیرا در غیر این‌صورت با منحصربه‌فرد بودن کمینگی که در (۶.۳) بیان کردیم در تناقض است. بنابراین $d_{i+1}, \ldots, d_l \in \mathbb{Z}$ موجوداست به طوری که $g_i - g'_i = \sum_{j=i+1}^{l} d_j g_j$ باشد و مؤلفه j ام از $g_i - g'_i$ برای $i+1 \leq j \leq l$ عبارت است از: $g_{ij} - g'_{ij} = d_j g_{jj}$ و چون برای $i+1 \leq j \leq l$، داریم: $0 \leq g_{ij}, g'_{ij} \leq g_{jj}$، لذا خواهیم‌داشت: $d_j = 0$. در نتیجه $g_i - g'_i = 0$ و $G = G'$ خواهدبود. □

مثال ۱.۲.۳. *باتوجه به مثال ۲.۱.۳ ماتریس مولد کاهنده C_1 عبارت است از:* $G_1 = \begin{pmatrix} 5 & 2 \\ 0 & 4 \end{pmatrix}$.

گزاره ۳.۲.۳. *(یک شرط لازم و کافی برای کدواژه‌های کد C) اگر G ماتریس مولد کد صحیح تعمیم‌یافته C باشد که در آن $C \subset M$ است، در این صورت $F(\mathbb{Z}^l G) = C$ می‌باشد. به عبارت دیگر، برای $c \in M$ و $d = (d_1, \ldots, d_l) \in \mathbb{Z}^l$ داریم $c \in C$ است، اگر و تنها اگر $c = dG = d_1 g_1 + \cdots + d_l g_l$ باشد که در آن g_i سطر i ام ماتریس مولد G از کد صحیح تعمیم‌یافته C می‌باشد و با توجه به نکته ۱.۲.۳، $dG = d_1 g_1 + \cdots + d_l g_l$ در M در نظر گرفته‌می‌شود.*

برهان. با توجه به اینکه $\mathbb{Z}^l G = F^{-1}(C)$ می‌باشد و باتوجه به پوشا بودن F می‌توان نتیجه گرفت که $F(\mathbb{Z}^l G) = F(F^{-1}(C)) = C$. □

نکته ۲.۲.۳. *عکس گزاره ۳.۲.۳ درست نیست، زیرا مواردی وجود دارد که رابطه $F(\mathbb{Z}^l G) = C$ برقرار است، اما داریم: $\mathbb{Z}^l G \subsetneq F^{-1}(C)$. به عنوان مثال، در مثال ۱.۱.۳، رابطه $F(4\mathbb{Z}) = 2\mathbb{Z}/6\mathbb{Z}$ برقرار است، اما داریم: $2\mathbb{Z} = F^{-1}(F(4\mathbb{Z})) \neq 4\mathbb{Z}$.*

در گزاره ۳.۲.۳، $d = (d_1, \dots, d_l)$ باید در $\mathbb{Z}^l$ باشد نه در M، زیرا برای $d \in M$، $dG \in C$ تعریف مناسبی نیست. به عنوان مثال، در مثال ۱.۲.۳:

$$(10, 12)\begin{pmatrix} 5 & 2 \\ 0 & 4 \end{pmatrix} = (50, 68) \neq 0 \in C.$$

با بررسی روش‌های کدگذاری برای کدهای خطی در میدان متناهی، ما می‌توانیم یک روش کدگذاری برای کدهای صحیح تعمیم‌یافته از گزاره ۳.۲.۳ بهذدست آوریم. با اطلاعات $(d_1, \dots, d_l) \in \mathbb{Z}^l$ که داریم، قرار می‌دهیم $c = (d_1, \dots, d_l)G \in C$. با این دیدگاه، G کاهنده به ما این اجازه را می‌دهد که پیچیدگی محاسباتی کاهش یابد. در ادامه، گزاره ۷.۲.۳ نشان می‌دهد که هر d_i می‌تواند محدود شود به $d_i = 0, 1, \dots, \frac{n_i}{g_{ii}} - 1$.

نکته ۳.۲.۳. *اگر ماتریس مولد G قطری باشد بدین معنا که برای $i \neq j$، $g_{ij} = 0$ داشته‌باشیم: آنگاه کد C موافق با $\bigoplus_{i=1}^{l} g_{ii}\mathbb{Z}/n_i\mathbb{Z}$ می‌باشد.*

این نکته برای تمام ماتریس‌های مولد صادق نیست. به عنوان مثال، فرض کنید که $M = (\mathbb{Z}/4\mathbb{Z})^2$ باشد و کد $C_4 = \{(0,0).(2,1),(0,2),(2,3)\}$ را در نظر بگیرید. $C_4 \subset M$ و ماتریس مولد کاهنده آن $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ می‌باشد. اگر فرض کنیم که نکته ۳.۲.۳ در مورد آن صادق باشد آنگاه داریم:

$$\bigoplus_{i=1}^{2} g_{ii}\mathbb{Z}/n_i\mathbb{Z} = 2\mathbb{Z}/4\mathbb{Z} \bigoplus 2\mathbb{Z}/4\mathbb{Z}.$$

در صورتی که C_4 با $\mathbb{Z}/4\mathbb{Z}$ به‌عنوان یک گروه آبلی یکریخت است.

۱.۲.۳ روابطی که ماتریس مولد کد صحیح تعمیم‌یافته روی آن صادق است.

اگر چه بی‌نهایت زیرگروه‌هایی به فرم $\mathbb{Z}^l G$ با $G \in T_l(\mathbb{Z})$ در $\mathbb{Z}^l$ وجود دارد، اما زیرگروه‌های خاصی که از $C \subset M$ به دست می‌آید، توسط عملیات زیر مشخص می‌شود.

گزاره ۴.۲.۳. *(عملیات ماتریسی روی ماتریس مولد کد صحیح تعمیم‌یافته) فرض کنید ماتریس $G = (g_{ij})$ متعلق به $T_l(\mathbb{Z})$ باشد. دراین صورت برای برخی کدهای صحیح تعمیم‌یافته C، که $C \subset M$ می‌باشد، رابطه $\mathbb{Z}^l G = F^{-1}(C)$ برقرار است اگر و تنها اگر $A \in M_l(\mathbb{Z})$ موجود باشد به‌قسمی که داشته‌باشیم:*

$$AG = \operatorname{diag}[n_1, \dots, n_l]. \tag{۷.۳}$$

برهان. فرض کنیم برای برخی کدهای صحیح تعمیم‌یافته $C \subset M$، رابطه $\mathbb{Z}^l G = F^{-1}(C)$ برقرار باشد. در این صورت ماتریس مولد G باید توسط بردارهای صحیح به‌فرم (۵.۳) بیان شود، و (۷.۳) به‌دست می‌آید. بالعکس: فرض کنیم که (۷.۳) برقرار باشد. اگر $C = F(\mathbb{Z}^l G)$ تعریف شود، آنگاه باید بررسی کنیم که $\mathbb{Z}^l G = F^{-1}(C) = F^{-1}(F(\mathbb{Z}^l G))$ برقرار است. اگر $c \in \mathbb{Z}^l G$ موجود باشد، آنگاه

$F(c) \in F(\mathbb{Z}^l G)$ و $c \in F^{-1}(F(\mathbb{Z}^l G))$ خواهدبود و در نتیجه داریم: $\mathbb{Z}^l G \subset F^{-1}(F(\mathbb{Z}^l G))$. علاوه براین اگر $c \in F^{-1}(F(\mathbb{Z}^l G))$ باشد آنگاه $F(c) \in F(\mathbb{Z}^l G)$ خواهدبود و $c' \in \mathbb{Z}^l G$ وجود دارد به طوری که داشته‌باشیم: $F(c) = F(c')$، درنتیجه $F(c - c') = 0$ خواهدشد، ازاین‌رو $c - c'$، مجموع بردارهایی به‌صورت (۵.۳) می‌باشند و به تبعیت از رابطه (۷.۳)، $c - c' \in \mathbb{Z}^l G$ است. بنابراین $c \in \mathbb{Z}^l G$ و $\mathbb{Z}^l G = F^{-1}(C)$ بدست می‌آید. □

نتیجه ۱.۲.۳. *در عملیات (۷.۳)، G می‌تواند به‌عنوان ماتریس مولد کاهنده درنظر گرفته شود.*

برهان. برای تبدیل ماتریس مولد G به ماتریس مولد کاهنده می‌توانیم ماتریس ابتدایی $P \in SL_l(\mathbb{Z})$ را که با عملیات سطری مقدماتی حاصل می‌شود، از سمت چپ در G ضرب کنیم آنگاه خواهیم‌داشت:

$$(AP^{-1})(PG) = \mathrm{diag}[n_1, \ldots, n_l].$$

□

طبق گزاره ۴.۲.۳، $G \in T_l(\mathbb{Z})$ یک کد صحیح تعمیم‌یافته در M تعیین می‌کند. از سوی دیگر، هر $G \in T_l(\mathbb{Z})$ یک کد صحیح در $M = (\mathbb{Z}/N\mathbb{Z})^l$ تعیین می‌کند که در آن $N = det(G)$ می‌باشد. زیرا داریم: $G^{-1}G = \mathrm{diag}[1, \ldots, 1]$، که در آن $G^{-1} \in T_l(Q)$ می‌باشد و همچنین خواهیم‌داشت:

$$N(G^{-1})G = \mathrm{diag}[N, \ldots, N],$$

که برای $N(G^{-1}) \in T_l(\mathbb{Z})$ برقرار است.

مثال ۲.۲.۳. *به مثال ۱.۱.۳ توجه کنید، هر زیرمجموعه از $\mathbb{Z}$ برای $m \in \mathbb{Z}$، به‌صورت $m\mathbb{Z}$ است. اما زیرگروهی که موافق با $F^{-1}(g\mathbb{Z}/6\mathbb{Z})$ باشد تنها $g\mathbb{Z}$ برای $g = 1, 2, 3, 6$ می‌باشد، آنگاه $ag = 6$، به ترتیب برای $a = 6, 3, 2, 1$ صادق است.*

مثال ۳.۲.۳. *مثال ۱.۲.۳ را درنظر بگیرید، معادلات ماتریسی به‌دست آمده از G_1، عبارت است از:*

$$\begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 0 \\ 0 & 12 \end{pmatrix}. \qquad (8.3)$$

قضیه ۱.۲.۳. *نگاشت کدهای صحیح تعمیم‌یافته C به ماتریس مولد کاهنده G یک‌به‌یک و پوشا است.*

$$\varphi : \{C \subset M\} \longrightarrow \{G \in T_l(\mathbb{Z}) \mid \exists A \in M_l(\mathbb{Z}) \quad \text{s.t} \quad AG = \mathrm{diag}[n_1, \ldots, n_l]\}$$

برهان. باتوجه به گزاره ۲.۲.۳، یک‌به‌یک بودن نگاشت φ از رابطه $F(\mathbb{Z}^l G) = C$ بدست می‌آید. بدین ترتیب که اگر فرض کنیم $\varphi(c_1) = \varphi(c_2)$ باشد، آنگاه $G_1 = G_2$ خواهد بود. در نتیجه خواهیم‌داشت: $Z^l G_1 = Z^l G_2$ و $F(Z^l G_1) = F(Z^l G_2)$ و در نهایت $c_1 = c_2$ حاصل می‌شود. پوشا بودن به این معناست که برای هر ماتریس G، یک کد C موجود است که رابطه $\mathbb{Z}^l G = F^{-1}(C)$ برقرار باشد. همانطور که در اثبات گزاره ۴.۲.۳ نشان داده شده‌است $F(\mathbb{Z}^l G) = C$ ویژگی مطلوب را دارد. □

گزاره ۵.۲.۳. *(مثلثی بودن ماتریس A) اگر G یک ماتریس مولد برای کد صحیح تعمیم‌یافته C باشد و اگر ماتریس $A \in M_l(\mathbb{Z})$ موجود باشد به طوری که داشته‌باشیم: $AG = \operatorname{diag}[n_1, \ldots, n_l]$، آنگاه $A = (a_{ij}) \in T_l(\mathbb{Z})$ خواهدبود.*

برهان. با توجه به بالا مثلثی بودن ماتریس G، همچنین، با توجه به اینکه $\operatorname{diag}[n_1, \ldots, n_l] \in T_l(\mathbb{Z})$ می‌باشد داریم: $A \in T_l(\mathbb{Q}) \cap M_l(\mathbb{Z}) = T_l(\mathbb{Z})$، و لذا حکم حاصل می‌شود. □

گزاره ۶.۲.۳. *(خاصیت جابجایی در کدهای صحیح)اگر G یک ماتریس مولد برای کد صحیح C باشد و اگر $A \in T_l(\mathbb{Z})$ موجود باشد به طوری که رابطه $AG = \operatorname{diag}[N, \ldots, N]$ برقرار باشد، آنگاه تساوی ماتریسی $GA = \operatorname{diag}[N, \ldots, N]$ نیز برقرار است.*

برهان. فرض کنید که $AG = \operatorname{diag}[N, \ldots, N]$ در گروه $GL_l(\mathbb{Q})$ قرار دارد، یعنی $\det G \neq 0$ می‌باشد. طبق رابطه

$$(N^{-1}A)G = \operatorname{diag}[1, \ldots, 1],$$

نتیجه می گیریم که $(N^{-1}A)$ معکوس G است. از آنجایی که معکوس یک تابع خاصیت جابجایی دارد بنابراین داریم:

$$G(N^{-1}A) = \operatorname{diag}[1, \ldots, 1].$$

در نتیجه خواهیم‌داشت: $GA = \operatorname{diag}[N, \ldots, N]$. □

درحالت کلی گزاره ۶.۲.۳، برای کدهای صحیح تعمیم یافته کاربرد ندارد. به عنوان مثال: اگر در رابطه (۸.۳) جابجایی را انجام دهیم داریم:

$$\begin{pmatrix} 5 & 2 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 10 & 1 \\ 0 & 12 \end{pmatrix}.$$

در نتیجه گزاره ۶.۲.۳ برقرار نیست. از آنجا که کوچکترین مضرب مشترک $60 = (10, 12)$ می‌باشد، ما $\operatorname{diag}[6, 5]$ را در دو طرف رابطه (۸.۳) از سمت چپ ضرب می‌کنیم و بدست می‌آوریم:

$$\begin{pmatrix} 12 & -6 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 60 & 0 \\ 0 & 60 \end{pmatrix}.$$

برای این کد صحیح حاصل، گزاره ۶.۲.۳ برقرار است و ماتریس مولد G تغییر نمی‌کند. به‌طور مشابه اگر $\operatorname{diag}[6, 5]$ را از سمت راست در دو طرف رابطه (۸.۳) ضرب کنیم خواهیم‌داشت:

$$\begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 30 & 10 \\ 0 & 20 \end{pmatrix} = \begin{pmatrix} 60 & 0 \\ 0 & 60 \end{pmatrix}.$$

در این مورد، ماتریس صحیح A تغییر نمی‌کند و گزاره ۶.۲.۳ صادق است.

نکته ۴.۲.۳. *تئوری مقسوم‌علیه‌های اولیه در این تحقیق ضروری است و به‌شرح زیر است:*

فرض کنید $A \in T_l(\mathbb{Z})$ موجود باشد. طبق تئوری مقسوم‌علیه‌های اولیه، (لم ۳۰۱۱ از مرجع [۳۳]) $U, V \in SL_l(\mathbb{Z})$ وجود دارند به طوری که داشته‌باشیم: $UAV^{-1} = \mathrm{diag}[b_1, \ldots, b_l]$، که در آن $b_1, \ldots, b_l$ منحصر به فرد و مثبت هستند و برای $1 \le i \le l$ ، داریم: $b_{i+1} \in b_i\mathbb{Z}$. سپس $\mathbb{Z}^l = \mathbb{Z}^l V$ و $\mathbb{Z}^l = \bigoplus_{i=1}^{l} \mathbb{Z}v_i$ و $\mathbb{Z}^l A = \mathbb{Z}^l \mathrm{diag}[b_1, \ldots, b_l]V$ خواهد بود؛ به عبارت دیگر داریم: $\mathbb{Z}^l A = \bigoplus_{i=1}^{l} \mathbb{Z}b_i v_i$، که در آن v_i سطر i ام از ماتریس V است. بنابراین، $\mathbb{Z}^l/\mathbb{Z}^l A = \bigoplus_{i=1}^{l} \mathbb{Z}/b_i\mathbb{Z}$ و خواهیم‌داشت: $|\mathbb{Z}^l/\mathbb{Z}^l A| = \prod_{i=1}^{l} b_i = \det(A)$ ، علاوه بر این اگر ماتریس A در تساوی ماتریسی $AG = \mathrm{diag}[n_1, \ldots, n_l]$ برای ماتریس مولد G در کد صحیح تعمیم‌یافته C صدق کند، آنگاه اثبات گزاره بعدی نشان می‌دهد که $\mathbb{Z}^l/\mathbb{Z}^l A$ یک یکریختی برای کد C به عنوان یک گروه آبلی است.

گزاره ۷.۲.۳. *(رابطه‌ی اندازه‌ی کد صحیح تعمیم‌یافته) اگر C یک کد صحیح تعمیم‌یافته و $G = (g_{ij})$ ماتریس مولد آن باشد، آنگاه C به‌صورت زیر بیان می‌شود:*

$$C = \left\{ (d_1, \ldots, d_l)G \,\middle|\, d_i = 0, 1, \ldots, \frac{n_i}{g_{ii}} - 1 \right\}, \tag{۹.۳}$$

که در آن باتوجه به نکته ۱.۲.۳، $(d_1, \ldots, d_l)G$ در M در نظر گرفته‌می‌شود، و $|C|$ به صورت زیر به‌دست می‌آید:

$$|C| = \prod_{i=1}^{l} \frac{n_i}{g_{ii}} = \frac{|M|}{\det(G)}. \tag{۱۰.۳}$$

برهان. با گنجاندن $\supset$ در (۹.۳) به تبعیت از گزاره ۳.۲.۳، واضح است که (۱۰.۳) $\Longleftrightarrow$ (۹.۳). ما نشان می‌دهیم که سمت راست تساوی (۹.۳) ، عناصر متمایز، $|M|/\det(G)$ را تعیین می‌کند. فرض کنید که در سمت راست (۹.۳) ، $dG = d'G$ باشد. سپس $(d - d')G = 0$ خواهدبود و خواهیم‌داشت:

$$(d - d')G = \sum_{i=1}^{l} f_i(\underbrace{0, \ldots, 0}_{i-1}, n_i, \underbrace{0, \ldots, 0}_{l-i}) = \sum_{i=1}^{l} f_i a_i G \tag{۱۱.۳}$$

برای $f = (f_1, \ldots, f_l) \in \mathbb{Z}^l$، که در آن a_i سطر i ام از ماتریس A در $AG = \mathrm{diag}[n_1, \ldots, n_l]$ می‌باشد. اگر (۱۱.۳) در $GL_l(\mathbb{Q})$ درنظر گرفته‌شود که در آن $\det(G) \neq 0$، آنگاه خواهیم داشت: $(d - d') = \sum_{i=1}^{l} f_i a_i = fA$. به یاد داشته باشید که طبق گزاره ۵.۲.۳، A یک ماتریس بالامثلثی است. سپس با توجه به این که $d_1 - d'_1 = f_1 a_{11}$ و $0 \le d_1, d'_1 < a_{11}$ می‌باشد داریم: $d_1 - d'_1 = 0$. به کمک استقرا می‌توان نشان داد که برای $1 \le i < l$ ، $d_i - d'_i = 0$ می‌باشد. بنابراین ثابت کردیم که در سمت راست (۹.۳)، اگر $dG = d'G$ باشد آنگاه $d = d'$ خواهدبود. از این‌رو ما ثابت کردیم که $|C| \ge \prod_{i=1}^{l} a_{ii} = \det(A)$. همچنین نشان دادیم که هسته نگاشت

$$\theta : \mathbb{Z}^l \longrightarrow C$$

$$d \longrightarrow dG$$

معادل است با $\mathbb{Z}^l A$. بنابراین، $\mathbb{Z}^l/\mathbb{Z}^l A$ با C به‌عنوان یک گروه آبلی یکریخت است. طبق نکته ۴.۲.۳، $|C| = \det(A) = |M|/\det(G)$ بدست می‌آید. □

نکته ۵.۲.۳. *همانگونه که در فصل ۲ بیان کردیم، در کدهای GQC که روی میدان متناهی $\mathbb{F}_q$ قرار دارند، برای ماتریس چند جمله‌ای مولد $G = (g_{ij}(x))$ ماتریس چند جمله‌ای $A = (a_{ij}(x))$ وجود دارد که در عملیات ماتریسی زیر*

$$AG = \mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$$

که مشابه رابطه (۷.۳) است صدق می‌کند، و در آن $g_{ij}(x)$ و $a_{ij}(x)$ در حلقه چندجمله‌ای‌های $\mathbb{F}_q[x]$ قرار دارند. علاوه براین اگر ماتریس چندجمله‌ای مولد G کاهنده باشد یعنی برای $1 \le i < j \le l$ ، داشته‌باشیم: $\deg g_{jj} > \deg g_{ij}$ ، آنگاه ماتریس A نیز برای $1 \le i < j \le l$ ، دارای خاصیت مشابه $\deg a_{ii} > \deg a_{ij}$ می‌باشد. اما به طور کلی، برای کدهای صحیح، ماتریس A ویژگی $|a_{ii}| > |a_{ij}|$ را ندارد.

به مثال نقض زیر توجه کنید:

$$\begin{pmatrix} 20 & -16 & -11 & 23 \\ 0 & 4 & -1 & -3 \\ 0 & 0 & 5 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4 & 3 & 1 \\ 0 & 5 & 1 & 19 \\ 0 & 0 & 4 & 16 \\ 0 & 0 & 0 & 20 \end{pmatrix} = \begin{pmatrix} 20 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 \\ 0 & 0 & 20 & 0 \\ 0 & 0 & 0 & 20 \end{pmatrix}.$$

می‌توانیم ثابت کنیم که در کدهای صحیح، تنها زمانی که $j = i + 1$ می‌باشد، رابطه $a_{ii} > -a_{ij} \ge 0$ برقرار است، زیرا از آنجایی که $a_{ii}g_{ij} + a_{ij}g_{jj} = 0$ می‌باشد، بنابراین داریم: $-a_{ij} = a_{ii}g_{ij}/g_{jj} \ge 0$ و با توجه به اینکه ماتریس مولد G کاهنده است و برای $1 \le i < j \le l$ ، داریم: $g_{jj} > g_{ij}$، در نتیجه $-a_{ij} = a_{ii}g_{ij}/g_{jj} < a_{ii}$ خواهدبود.

نکته ۶.۲.۳. *اگر یک کد صحیح تعمیم‌یافته به طول $(l = 2)2$ ، معادل با کدهای ترکیبی*

$$\{(c, c') | c \in C, c' \in C'\},$$

از دو گروههای دوری $C = g_{11}\mathbb{Z}/n_1\mathbb{Z}$ و $C' = g_{22}\mathbb{Z}/n_2\mathbb{Z}$ داشته‌باشیم و $\gcd(n_1, n_2) = 1$ باشد، آنگاه می‌توان نشان داد که برای ماتریس مولد کاهنده G ، $g_{12} = 0$ می‌باشد. زیرا درایه $(1, 2)$ از ماتریس AG برابر است با $a_{11}g_{12} + a_{12}g_{22} = 0$ و a_{11} عدد a_{12} را عاد می‌کندزیرا به‌تبعیت از $\gcd(n_1, n_2) = 1$ ، خواهیم‌داشت: $\gcd(a_{11}, g_{22}) = 1$. همانطور که فرض کردیم ماتریس مولد G کاهنده است، طبق نکته قبلی $a_{11} > -a_{12} \ge 0$ می‌باشد. بنابراین $a_{12} = 0$ بدست می‌آید. از آنجایی که داریم $a_{11} \ne 0$ ، در نتیجه $g_{12} = 0$ خواهدبود. این استدلال را می‌توان برای $l \ge 2$ نیز گسترش داد؛ اگر برای همه‌ی $1 \le i < j \le l$ ، داشته‌باشیم: $\gcd(n_i, n_j) = 1$ ، آنگاه هر ماتریس مولد کاهنده $G = (g_{ij})$ قطری است. این حقیقت در ادامه توسط لم ۲.۲.۴ نشان داده می‌شود. از سوی دیگر، وقتی $l = 3$ باشد، با وجود اینکه $\gcd(n_1, n_2, n_3) = 1$ می‌باشد، برای $i < j$ ، تعدادی g_{ij} وجود دارد که برابر 0 نیستند، برای مثال،

$$\begin{pmatrix} 5 & -4 & 1 \\ 0 & 7 & -3 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 & 1 \\ 0 & 5 & 3 \\ 0 & 0 & 7 \end{pmatrix} = \begin{pmatrix} 15 & 0 & 0 \\ 0 & 35 & 0 \\ 0 & 0 & 21 \end{pmatrix}.$$

۳.۳ دوگان کدهای صحیح تعمیم‌یافته

اگر داشته‌باشیم $N = n_۱ = n_۲ = \cdots = n_l$، آنگاه برای $c, d \in M$، یک فرم خطی به صورت، $\langle c, d\rangle = c(d^T) = \sum_{i=۱}^{l} c_i d_i \in \mathbb{Z}/N\mathbb{Z}$ تعریف می‌کنیم. در حالت کلی اگر N، کوچکترین مضرب مشترک اعداد $n_۱, n_۲, \ldots, n_l$ باشد، برای $c, d \in M = \bigoplus_{i=۱}^{l} \mathbb{Z}/n_i\mathbb{Z}$، تعریف می‌کنیم،

$$\langle c, d\rangle = c\,\mathrm{diag}[\frac{N}{n_۱}, \ldots, \frac{N}{n_l}](d^T) = \sum_{i=۱}^{l} c_i \frac{N}{n_i} d_i \in \mathbb{Z}/N\mathbb{Z},$$

که در آن $c_i N d_i/n_i \in \mathbb{Z}/N\mathbb{Z}$ از این حقیقت ناشی می‌شود که برای همه $۰ \leq i \leq ۱$ و عناصر $c_i, d_i, c_i', d_i' \in \mathbb{Z}/n_i\mathbb{Z}$ داریم:

$$c_i d_i \equiv c_i' d_i' \mod n_i \iff \frac{c_i N d_i}{n_i} \equiv \frac{c_i' N d_i'}{n_i} \mod N.$$

تعریف ۱.۳.۳. *اگر C یک کد صحیح تعمیم‌یافته باشد، تعریف می‌کنیم:*

$$C^\perp = \{d \in M | \langle c, d\rangle = ۰ \quad \forall c \in C\},$$

که بنا بر خاصیت خطی $\langle c, d\rangle$، $C^\perp$ یک زیر گروه از M است، که $C^\perp$ را کد دوگان[۴] C می‌نامیم.

مثال ۱.۳.۳. *مثال ۲.۱.۳ را مجدداً ملاحظه کنید. برای تعیین $C_۱^\perp$ یک شرط لازم و کافی به صورت زیر بدست می‌آید. طبق تعریف ۱.۳.۳ و گزاره ۳.۲.۳، $d = (d_۱, d_۲)$ در $C_۱^\perp$ قرار دارد اگر و تنها اگر برای $i = ۱, ۲$، رابطه $\langle g_i, d\rangle = ۰$ برقرار باشد. به عبارت دیگر، داشته‌باشیم :*

$$\begin{pmatrix} ۵ & ۲ \\ ۰ & ۴ \end{pmatrix} \begin{pmatrix} ۶ & ۰ \\ ۰ & ۵ \end{pmatrix} \begin{pmatrix} d_۱ \\ d_۲ \end{pmatrix} \equiv \begin{pmatrix} ۰ \\ ۰ \end{pmatrix} \mod ۶۰. \tag{۱۲.۳}$$

توجه داشته باشید که، $۲۰ d_۲ \equiv ۰ \mod ۶۰ \iff d_۲ \equiv ۰ \mod ۳$. معادله‌های دیگر در (۱۲.۳) حل می‌شوند و $C_۱^\perp$ به شرح زیر محاسبه می‌شود:

$$\begin{aligned} ۳۰ d_۱ + ۱۰ d_۲ \equiv ۰ \mod ۶۰ &\iff ۳ d_۱ + d_۲ \equiv ۰ \mod ۶ \\ &\iff d_۱ \equiv \begin{cases} ۰ \mod ۲ & \text{if} \quad d_۲ \equiv ۰ \mod ۶ \\ ۱ \mod ۲ & \text{if} \quad d_۲ \equiv ۳ \mod ۶ \end{cases}, \end{aligned}$$

$$C_۱^\perp = \left\{ \begin{matrix} (۰,۰), (۰,۶), (۱,۳), (۱,۹), (۲,۰), (۲,۶), (۳,۳), (۳,۹), (۴,۰), (۴,۶), \\ (۵,۳), (۵,۹), (۶,۰), (۶,۶), (۷,۳), (۷,۹), (۸,۰), (۸,۶), (۹,۰), (۹,۹) \end{matrix} \right\}.$$

[۴] Dual code

۱.۳.۳ ماتریس بررسی توازن کدهای صحیح تعمیم‌یافته

این امکان وجود دارد که کدهای صحیح تعمیم‌یافته را به جای ماتریس مولدشان توسط ماتریس‌های بررسی توازن آنها تعریف کنیم. در ادامه قصد داریم که به این موضوع بپردازیم.

تعریف ۲.۳.۳. *فرض کنید C کد صحیح تعمیم‌یافته باشد و $H \in M_l(\mathbb{Z})$ و سطرهای H در $F^{-1}(C^\perp)$ باشد. فرض کنید H را به صورت*

$$H = \begin{pmatrix} h_{11} & 0 & \cdots & 0 \\ h_{21} & h_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ h_{l1} & h_{l2} & \cdots & h_{ll} \end{pmatrix}$$

نشان می‌دهیم که در آن برای $0 \leq i \leq l$، $h_{ii} > 0$ می‌باشد و $H \in T'_l(\mathbb{Z})$ است. اگر تساوی $\mathbb{Z}^l H = F^{-1}(C^\perp)$ برقرار باشد آنگاه می‌توانیم بگوییم که H یک ماتریس بررسی توازن از کد C است. شرط $\mathbb{Z}^l H = F^{-1}(C^\perp)$ معادل است با رابطه زیر، که برای عناصر قطر اصلی h_{ii} و برای $0 \leq i \leq l$، خواهیم داشت:

$$h_{ii} = \min\{c_i | (c_1, \ldots, c_i, 0, \ldots, 0) \in F^{-1}(C^\perp), c_i > 0\}.$$

هر ماتریس بررسی توازن از یک کد صحیح تعمیم‌یافته، یک ماتریس بررسی توازن کاهنده منحصر به فرد می‌دهد.

مشابه ماتریس مولد، دیده می‌شود که در تعریف ۲.۳.۳، ماتریس بررسی توازن می‌تواند یک ماتریس بالامثلثی با خصوصیات بیان شده تعریف شود. ماتریس مولد G و ماتریس بررسی توازن H، یکی در $T_l(\mathbb{Z})$ و دیگری در $T'_l(\mathbb{Z})$ قرار دارند. این نکته ما را قادر می‌سازد که در قضیه ۱.۳.۳ یک رابطه بین ماتریس مولد G و ماتریس بررسی توازن H در کدهای صحیح تعمیم‌یافته بدست آوریم.

گزاره‌های ۲.۲.۳ـ۷.۲.۳ و قضیه ۱.۲.۳، بعد از اصلاحات لازم برای ماتریس بررسی توازن H معتبر هستند که ما توضیح آن را حذف می‌کنیم.

مثال ۲.۳.۳. *مثال ۱.۳.۳ درنظربگیرید. ماتریس بررسی توازن H_1 از کد صحیح تعمیم‌یافته C_1 به صورت زیر محاسبه می‌شود،*

$$h_{11} = \min\{c_1 | (c_1, 0) \in F^{-1}(C_1^\perp), c_1 > 0\} = 2$$

$$h_{22} = \min\{c_2 | (c_1, c_2) \in F^{-1}(C_1^\perp), c_2 > 0\} = 3.$$

بنابراین $H_1 = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}$ خواهد بود و عملیات ماتریسی توسط H_1 به‌صورت زیر به‌دست می‌آید:

$$\begin{pmatrix} 5 & 0 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 10 & 0 \\ 0 & 12 \end{pmatrix} \qquad (13.3)$$

نکته ۱.۳.۳. همریختی گروههای آبلی را در نظر بگیرید، فرض کنید $N = \mathrm{lcm}(n_1, \ldots, n_l)$ باشد، نگاشت φ را به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned} \varphi : M &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^l \\ (c_1, \ldots, c_l) &\longrightarrow (c_1, \ldots, c_l)\mathrm{diag}[\frac{N}{n_1}, \ldots, \frac{N}{n_l}]G^T. \end{aligned} \tag{۱۴.۳}$$

توجه داشته باشید که این نگاشت خوش تعریف است، زیرا طبق این نگاشت برای $l-$ تایی $(n_1, \ldots, n_l)$، $(n_1, \ldots, n_l)\mathrm{diag}[N/n_1, \ldots, N/n_l] = (N, \ldots, N)$. فرض کنید C' نگاره این نگاشت تعریف شود. یعنی داریم: $C' = \mathrm{Img}\varphi$. در این صورت، C' یک کد صحیح در $(\mathbb{Z}/N\mathbb{Z})^l$ است. از آنجایی که هسته نگاشت (۱۴.۳)، $C^\perp$ است، یک دنباله دقیق از گروههای آبلی به‌صورت زیر وجود دارد،

$$\{\circ\} \longrightarrow C^\perp \hookrightarrow M \longrightarrow C' \longrightarrow \{\circ\}.$$

آنگاه داریم، $|C'||C^\perp| = |M|$. علاوه بر این از عملیات $AG = \mathrm{diag}[n_1, \ldots, n_l]$ خواهیم داشت:

$$AG\mathrm{diag}[N/n_1, \ldots, N/n_l] = \mathrm{diag}[N, \ldots, N].$$

با توجه به خاصیت جابجایی در ضرب ماتریس‌های A و G در کدهای صحیح که در گزاره ۶.۲.۳ ثابت کردیم می‌توانیم بنویسیم، $G\mathrm{diag}[N/n_1, \ldots, N/n_l]A = \mathrm{diag}[N, \ldots, N]$، که ترانهاده آن برابر است با:

$$A^T\mathrm{diag}[\frac{N}{n_1}, \ldots, \frac{N}{n_l}]G^T = \mathrm{diag}[N, \ldots, N]. \tag{۱۵.۳}$$

ازاین‌رو $\mathrm{diag}[N/n_1, \ldots, N/n_l]G^T$، یک ماتریس مولد برای C' است. از رابطه (۱۰.۳) بدست می‌آوریم:

$$|C'| = \frac{N^l}{\det(G^T)\prod_{i=1}^{l}\frac{N}{n_i}} = \frac{|M|}{\det(G)} = |C|.$$

بنابراین خواهیم داشت:

$$|C||C^\perp| = |M|. \tag{۱۶.۳}$$

که این رابطه متناظر با رابطه $\dim C + \dim C^\perp = n$، برای هر کد خطی C به طول n در میدان متناهی می‌باشد.

حال نشان می‌دهیم که چگونه ماتریس کنترل توازن یک کد صحیح تعمیم‌یافته، از ماتریس مولد آن حاصل می‌شود.

قضیه ۱.۳.۳. فرض کنید G ماتریس مولد کد صحیح تعمیم‌یافته C و ماتریس $A \in T_l(\mathbb{Z})$ به گونه‌ای موجود باشد که در رابطه $AG = \mathrm{diag}[n_1, \ldots, n_l]$ صدق کند. تعریف می‌کنیم $H = A^T$. آنگاه H یک ماتریس بررسی توازن برای کد C می‌باشد.

برهان. اگر i امین سطر از ماتریس مولد G را با $g_i = (g_{i1}, \dots, g_{il})$ و j امین سطر از ماتریس $H = A^T = a_{ji}$ را با $h_j = (a_{1j}, \dots, a_{lj})$ نشان دهیم، آنگاه طبق رابطه (۱۵.۳)، در میدان $\mathbb{Z}/N\mathbb{Z}$ و برای همه $0 \leq i, j \leq 1$ داریم، $\langle g_i, h_j \rangle = 0$. بنابراین، $h_1, \dots, h_l \in F^{-1}(C^\perp)$ است و $\mathbb{Z}^l H \subset F^{-1}(C^\perp)$ بدست می‌آید. از پوشا بودن F می‌توان نتیجه گرفت که $F(\mathbb{Z}^l H) \subset C^\perp$ می‌باشد. حال برای اثبات تساوی $F(\mathbb{Z}^l H) = C^\perp$ کافی است ثابت کنیم که $|C^\perp| = |F(\mathbb{Z}^l H)|$. ترانهاده رابطه $AG = \operatorname{diag}[n_1, \dots, n_l]$ برابر است با $G^T H = \operatorname{diag}[n_1, \dots, n_l]$. ازاین‌رو $F(\mathbb{Z}^l H)$ یک کد صحیح تعمیم‌یافته در M است. که ماتریس مولد آن H می‌باشد و طبق رابطه (۱۰.۳) خواهیم‌داشت $|F(\mathbb{Z}^l H)| = |M|/\det(H)$. علاوه بر این، از رابطه‌های (۱۰.۳)،(۱۶.۳) و دترمینان از طرفین رابطه $G^T H = \operatorname{diag}[n_1, \dots, n_l]$، نتیجه می‌گیریم که $|C^\perp| = |F(\mathbb{Z}^l H)|$. بنابراین $C^\perp = F(\mathbb{Z}^l H)$ خواهد بود. مشابه اثبات گزاره ۴.۲.۳، رابطه‌های $C^\perp = F(\mathbb{Z}^l H)$ و $G^T H = \operatorname{diag}[n_1, \dots, n_l]$، نشان می‌دهند که رابطه $\mathbb{Z}^l H = F^{-1}(C^\perp)$ برقرار است. □

مثال ۳.۳.۳. *در رابطه (۸.۳) ، ترانهاده* $\begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix}$ *و افزودن سطر اول ماتریس حاصل به سطر دوم آن بدست می‌آید،* $\begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}$ *، که با ماتریس* H_1 *در مثال ۲.۳.۳ برابر است.*

اگر $N = n_1 = \cdots = n_l$ باشد آنگاه رابطه $\langle c, h_1 \rangle = \cdots = \langle c, h_l \rangle = 0$ معادل است با رابطه $cH^T \equiv 0 \mod N$. به طور کلی $\langle c, h_1 \rangle = \cdots = \langle c, h_l \rangle = 0$ معادل است با

$$c \operatorname{diag}[N/n_1, \dots, N/n_l] H^T \equiv 0 \mod N.$$

که به صورت $\langle c, H \rangle = 0$ نشان داده می‌شود.

گزاره ۱.۳.۳. *(یکی دیگر از شرایط لازم و کافی برای کدواژه‌ها) اگر H ماتریس بررسی توازن کد صحیح تعمیم یافته $C \subset M$ باشد. آنگاه داریم: $C = \{d \in M | \langle d, H \rangle = 0\}$.*

برهان. اگر $c \in C$ باشد، آنگاه طبق تعریف ۱.۳.۳، $\langle c, h_i \rangle = 0$ خواهدبود. از سوی دیگر، طبق تعریف ۱.۳.۳، داریم: $(C^\perp)^\perp = \{d \in M | \langle d, H \rangle = 0\}$. آنگاه واضح است که $C \subset (C^\perp)^\perp$ خواهدبود. اگر در رابطه (۱۶.۳) از $C^\perp$ استفاده کنیم، آنگاه خواهیم داشت: $|C| = |(C^\perp)^\perp|$. بنابراین، ما توانستیم ثابت کنیم که $C = (C^\perp)^\perp$. □

نکته ۲.۳.۳. *می‌توان نشان داد که دو رابطه هم‌ارزی زیر برقرار است.*

$$\exists\, B;\ BH = \operatorname{diag}[n_1, \dots, n_l] \iff \mathbb{Z}^l H = F^{-1}(C^\perp), \tag{۱۷.۳}$$

$$\{d \in M | \langle d, H \rangle = 0\} = C \iff \{d \in \mathbb{Z}^l | \langle F(d), H \rangle = 0\} = F^{-1}(C). \tag{۱۸.۳}$$

با قیاس گزاره ۴.۲.۳ برای $C^\perp$ رابطه (۱۷.۳) بدست می‌آید، از آنجایی که برای $d \in \mathbb{Z}^l$ ، داریم: $\langle F(d), H \rangle = 0$ ، لذا مطابق رابطه (۱۸.۳) خواهیم‌داشت: $\langle F(d), H \rangle = 0 \iff F(d) \in C$. قابل توجه است که هر

دو شرط در رابطه‌ی (۱۷.۳) *معادل نیست با دو شرط در رابطه‌ی* (۱۸.۳)*، و تنها رابطه* (۱۸.۳) $\Longrightarrow$ (۱۷.۳) *توسط گزاره* ۱.۳.۳ *برقرار است. به مثال زیر توجه کنید:*

طبق رابطه (۱۸.۳)*،* $\{d \in \mathbb{Z}/۶\mathbb{Z} | \langle d, ۴\rangle = ۰\} = ۳\mathbb{Z}/۶\mathbb{Z}$ و $\{d \in \mathbb{Z} | \langle F(d), ۴\rangle = ۰\} = ۳\mathbb{Z}$ *برقرارند، اما داریم:* $۴\mathbb{Z} \neq F^{-۱}((۳\mathbb{Z}/۶\mathbb{Z})^{\perp}) = ۲\mathbb{Z}$.

برای تکمیل بحث، قضیه زیر را که با یک روش مشابه قضیه ۱.۳.۳ اثبات می‌شود، ارائه می‌کنیم.

قضیه ۲.۳.۳. *اگر* H *یک ماتریس بررسی توازن کد صحیح تعمیم یافته* C *و* $B \in T_l'(\mathbb{Z})$ *باشد به‌طوری که رابطه* $BH = \mathrm{diag}[n_۱, \ldots, n_l]$ *برقرار باشد. آنگاه تعریف می‌کنیم،* $G = B^T$ *. در این صورت* G*، یک ماتریس مولد برای* C *است.*

در نهایت، بسیاری از نتایج به شرح زیر خلاصه شده است.

قضیه ۳.۳.۳. *چهار نگاشت زیر، همه دوسویی‌اند و دارای نمودارهای جابجایی به صورت زیر می‌باشند:*

$$\{\text{گروه } C \subset M\} \longrightarrow \left\{ G \in T_l(\mathbb{Z}) \;\middle|\; \begin{array}{l} G \text{ کاهنده است و} \\ \exists A \in M_l(\mathbb{Z}) \quad \text{s.t} \quad AG = \mathrm{diag}[n_۱, \ldots, n_l] \end{array} \right\}$$

$$\downarrow \qquad\qquad \downarrow \quad H = A^T$$

$$\{\text{گروه } C^{\perp} \subset M\} \longrightarrow \left\{ H \in T_l'(\mathbb{Z}) \;\middle|\; \begin{array}{l} H \text{ کاهنده است و} \\ \exists B \in M_l(\mathbb{Z}) \quad \text{s.t} \quad BH = \mathrm{diag}[n_۱, \ldots, n_l] \end{array} \right\}$$

برهان. نگاشت عمودی سمت چپ، همانطور که در اثبات گزاره ۱.۳.۳ نشان داده شده است دوسویی است، نگاشت عمودی سمت راست نیز دوسویی است. نگاشت‌های افقی بر اساس قضیه ۱.۲.۳ دوسویی‌اند. و طبق قضیه ۱.۳.۳، جابه‌جایی پذیرند. □

مثال ۴.۳.۳. *در عملیات* (۱۳.۳) *اگر در ترانهاده ماتریس* $\begin{pmatrix} ۵ & ۰ \\ -۲ & ۴ \end{pmatrix}$*، سطر دوم را به سطر اول آن اضافه کنیم، ماتریس* $\begin{pmatrix} ۵ & ۲ \\ ۰ & ۴ \end{pmatrix}$ *حاصل می‌شود که برابر با ماتریس مولد* $G_۱$ *در مثال* ۳.۲.۳ *می‌باشد.*

فصل ۴

الگوریتم شمارشی

۱.۴ الگوریتم شمارشی کدهای شبه‌دوری تعمیم‌یافته

در این بخش الگوریتمی را که از لحاظ نظری، همه ماتریس‌های چندجمله‌ای مولد کدهای شبه‌دوری تعمیم‌یافته را به کمک معادله (۱۵.۲)، تولید می‌کند، معرفی می‌کنیم. توجه داشته‌باشید که این معادله برابر است با:

$$AG = (a_{i,j})(g_{i,j}) = \left(\sum_{h=i}^{j} a_{i,h}g_{h,j}\right) = \begin{cases} ۰ & i \neq j \\ x^{n_i} - ۱ & i = j \end{cases}. \tag{۱.۴}$$

در حالت $i = j$، معادله فوق برابر است با $a_{i,i}g_{i,i} = x^{n_i} - ۱$. بنابراین ما می‌توانیم $a_{i,i}$ و $g_{i,i}$ را به عنوان فاکتورهای مقسوم‌علیه $x^{n_i} - ۱$ بدست آوریم.

حالت $i < j$ را در (۱.۴) در نظر بگیرید. اگر $j = i + ۱$ باشد، آنگاه (۱.۴) معادل است با: $a_{i,i}g_{i,j} + a_{i,j}g_{j,j} = ۰$، لذا برای حل این معادله دانستن لم های زیر ضروری است.

لم ۱.۱.۴. *اگر a, g چندجمله‌ای‌هایی در $\mathbb{F}_q[x]$ باشند و داشته‌باشیم: $d = \gcd(a, g)$، آنگاه هر پاسخ چندجمله‌ای $(X, Y) = (X_۰, Y_۰)$ از معادله $aX + Yg = ۰$ برای $z \in \mathbb{F}_q[x]$ به صورت زیر بیان می‌شود:*

$$(X_۰, Y_۰) = \left(\frac{g}{d}z, -\frac{a}{d}z\right). \tag{۲.۴}$$

در حالت خاص، اگر فرض کنیم $\deg X_۰ < \deg g$ باشد، $q^{\deg d}$ راه‌حل به صورت زیر به‌ازای چندجمله‌ای

$z \in \mathbb{F}_q[x]$ که درجه آن کمتر از درجه چندجمله‌ای d می‌باشد وجود دارد:

$$(X_\circ, Y_\circ) = \left(\frac{g}{d}z, -\frac{a}{d}z\right). \tag{۳.۴}$$

برهان. از آنجایی که $\frac{a}{d}X_\circ + Y_\circ\frac{g}{d} = \circ$ می‌باشد، آنگاه $X_\circ$ عدد $\frac{g}{d}$ را عاد می‌کند. ادامه بحث بدیهی است. □

فرض کنید $d_{i,j} = \gcd(a_{i,i}, g_{j,j})$ باشد. در این صورت، G کاهنده را که در آن $\deg g_{i,j} < \deg g_{j,j}$ است، در نظر می‌گیریم. بااستفاده از (۳.۴)، کاندیدهای $(g_{i,j}, a_{i,j})$ به‌ازای چندجمله‌ای $z \in \mathbb{F}_q[x]$ که درجه آن کمتر از درجه چندجمله‌ای $d_{i,j}$ می‌باشد به صورت زیر نوشته می‌شوند :

$$\left(\frac{g_{j,j}}{d_{i,j}}z, -\frac{a_{i,i}}{d_{i,j}}z\right). \tag{۴.۴}$$

سپس، اگر $i+۱ < j$ باشد، آنگاه (۱.۴) معادل است با

$$a_{i,i}g_{i,j} + \sum_{i<h<j} a_{i,h}g_{h,j} + a_{i,j}g_{j,j} = \circ. \tag{۵.۴}$$

لم ۲.۱.۴. *فرض کنید a و g چندجمله‌ای‌هایی در $\mathbb{F}_q[x]$ باشند و داشته‌باشیم: $d = \gcd(a, g)$ و همچنین فرض کنید که c یک چندجمله‌ای در $\mathbb{F}_q[x]$ باشد. در این صورت یک جواب مانند (X, Y) از معادله $aX + Yg = c$ وجود دارد اگر و تنها اگر d، چندجمله‌ای c را عاد کند. حال فرض کنید d، چندجمله‌ای c را عاد کند، در این صورت، هر جواب (X, Y) از معادله $aX + Yg = c$ به صورت $(X, Y) = (g_\circ, a_\circ) + (X_\circ, Y_\circ)$ بیان می‌شود، که درآن $(X_\circ, Y_\circ)$ جواب کلی معادله $aX_\circ + Y_\circ g = \circ$ در لم ۱.۱.۴ است و $(g_\circ.a_\circ)$ یک جواب منحصر به فرد از معادله $ag_\circ + a_\circ g = c$ می‌باشد که در آن $deg g_\circ < \deg \frac{g}{d}$ است. به طور خاص، اگر فرض کنید؛ $\deg X < \deg g$ باشد، آنگاه به‌ازای چندجمله‌ای $z \in \mathbb{F}_q[x]$ که درجه آن کمتر از درجه چندجمله‌ای d می‌باشد $q^{\deg d}$ پاسخ به صورت زیر وجود دارد:*

$$(X, Y) = \left(g_\circ + \frac{g}{d}z, a_\circ - \frac{a}{d}z\right). \tag{۶.۴}$$

برهان. اگر d، چندجمله‌ای c راعاد کند، آنگاه الگوریتم اقلیدسی قابل تعمیم، یک جواب از معادله $aX + Yg = c$ را می‌دهد. در مقابل، اگر یک جواب از معادله $aX + Yg = c$ وجود داشته‌باشد آنگاه d چندجمله‌ای c را عاد می‌کند. زیرا d، $aX + Yg$ را عاد می‌کند. فرض کنید d چندجمله‌ای c را عاد کند، از معادله $\frac{a}{d}X + Y\frac{g}{d} = \frac{c}{d}$ نتیجه می‌گیریم که $\frac{a}{d}X \equiv \frac{c}{d} \mod \frac{g}{d}$، که یک جواب منحصر به فرد به پیمانه $\frac{g}{d}$ دارد؛ زیرا $\gcd\left(\frac{a}{d}, \frac{g}{d}\right) = ۱$ می‌باشد. اگر $(g_\circ, a_\circ)$ یک جواب منحصر به فرد از معادله $\frac{a}{d}g_\circ + a_\circ\frac{g}{d} = \frac{c}{d}$ تعریف شود که در آن $\deg g_\circ < \deg \frac{g}{d}$ می‌باشد، آنگاه داریم: $ag_\circ + a_\circ g = c$. برای جواب دیگر معادله $aX + Yg = c$، بااستفاده از لم ۱.۱.۴، خواهیم داشت : $a(X - g_\circ) + (Y - a_\circ)g = \circ$، آنگاه $(X - g_\circ, Y - a_\circ)$ معادل است با (۳.۴) و ادعا ثابت می‌شود. □

گزاره ۱.۱.۴. *(شرط کافی برای عملیات ماتریسی).فرض کنید* $G = (g_{i,j})$ *و* $A = (a_{i,j})$ *دو ماتریس از مرتبه* $l \times l$ *با درایه‌هایی در* $\mathbb{F}_q[x]$ *باشند و برای* $i > j$*، درایه‌های* $g_{i,j} = a_{i,j} = 0$ *می‌باشند و فرض کنید که برای* $1 \leq i < j \leq l$ *داشته‌باشیم:* $d_{i,j} = \gcd(a_{i,i}, g_{j,j})$*. در این صورت اگر* $AG = \mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$*، باشد، آنگاه برای همه* $1 \leq i \leq l$ *داریم:* $a_{i,i}g_{i,i} = x^{n_i} - 1$*، و برای همه* $1 \leq i < j \leq l$ *داریم:*

$$d_{i,j} \Bigg| \sum_{i<h<j} a_{i,h}g_{h,j} \,. \tag{۷.۴}$$

برهان. به کمک لم ۲.۱.۴، معادله (۵.۴)، حل شدنی است اگر و تنها اگر $d_{i,j}$، عبارت $c = -\sum_{i<h<j} a_{i,h}g_{h,j}$ را عاد کند. □

فرض کنید (۷.۴) برقرار باشد، آنگاه با استفاده از رابطه (۶.۴)، کاندیدهای زوج مرتب $(g_{i,j}, a_{i,j})$ به‌ازای چندجمله‌ای $z \in \mathbb{F}_q[x]$، که درجه آن کمتر از درجه چندجمله‌ای $d_{i,j}$ می‌باشد به‌صورت زیر نوشته می‌شود :

$$\left(g_{i,j}^{(0)} + \frac{g_{j,j}}{d_{i,j}}z, a_{i,j}^{(0)} - \frac{a_{i,i}}{d_{i,j}}z\right), \tag{۸.۴}$$

که در آن $(g_{i,j}^{(0)}, a_{i,j}^{(0)})$ جواب منحصر به فرد رابطه (۵.۴) خواهد بود و $\deg g_{i,j}^{(0)} < \deg \frac{g_{j,j}}{d_{i,j}}$ می‌باشد. توجه داشته‌باشید که رابطه (۴.۴)، حالت خاص رابطه (۸.۴) می‌باشد. قبل از محاسبه $(g_{i,j}, a_{i,j})$ به کمک حل رابطه (۵.۴) و با استفاده از (۸.۴)، برای برخی از i و j ها لازم است که برای همه $i < h < j$، ابتدا

$$a_{i,h} \quad \text{و} \quad g_{h,j} \tag{۹.۴}$$

را محاسبه کنیم که با توجه به موقعیت مکانی آنها در ماتریسهای A و G به صورت زیر،

$$\begin{pmatrix} \ddots & & & & & \\ & a_{ii} & a_{i,i+1} & \ldots & a_{i,j-1} & a_{i,j}/g_{i,j} \\ & & \ddots & & & g_{i+1,j} \\ & & & \ddots & & \vdots \\ & & & & \ddots & g_{j-1,j} \\ & \circ & & & & g_{j,j} \\ & & & & & \ddots \end{pmatrix}, \tag{۱۰.۴}$$

قابل محاسبه‌اند. ما این شرط را که عناصر در (۹.۴)، باید قبل از $(g_{i,j}, a_{i,j})$ محاسبه شوند را یک پیش شرط می‌نامیم. اگر همه پیش شرط‌ها را برای محاسبه همه $(g_{i,j}, a_{i,j})$ ها انجام دهیم، آنگاه ماتریس‌های A و G در تساوی ماتریسی (۱۵.۲)، با استفاده از رابطه (۸.۴) بدست می‌آیند. الگوریتمی را معرفی می‌کنیم که همه پاسخ‌های رابطه $AG = \mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$ را تولید می‌کند.

الگوریتم ۱.۱.۴.

Input : $M = \mathrm{diag}[x^{n_1} - 1, \ldots, x^{n_l} - 1]$
Output : $A = (a_{i,j})$, $G = (g_{i,j})$ such that $AG = M$
1 : for $\iota = 1$ *to* $l(l+1)/2$ do
2 : $(i, j) := (i_\iota, j_\iota)$
3 : if $i = j$ then
4 : monic $g_{i,i}, a_{i,i} \in \mathbb{F}_q[x]$ such that $a_{i,i}g_{i,i} = x^{ni} - 1$
5 : else if $i + 1 = j$ then
6 : $d_{i,j} := \gcd(a_{i,i}, g_{j,j}), (g_{i,j}, a_{i,j})$ *given by* (4.4)
7 : else if $i + 1 < j$ then
8 : $d_{i,j} := \gcd(a_{i,i}, g_{j,j})$
9 : if $d_{i,j}$ does not divide $\sum_{i<h<j} a_{i,h}g_{h,j}$ then
10 : break
11 : end if
12 : $(g_{i,j}, a_{i,j})$ given by (8.4)
13 : end if
14 : end for

در این قسمت، سه ترتیبی که می‌توان به کمک آنها پیش شرط را محاسبه کرد، معرفی می‌کنیم. فرض کنید که $\prec_f$، $\prec_b$ و $\prec_d$ سه ترتیب روی مجموعه $\{(i,j)|۱ \le i \le j \le l\}$ باشند که برای $1 \le i, i' \le j, j' \le l$، به صورت زیر تعریف می‌شوند:

$$
\begin{aligned}
&(i,j) \prec_f (i',j') \iff j < j' \quad \text{یا} \quad [j = j' \quad \text{و} \quad i \ge i'],\\
&(i,j) \prec_b (i',j') \iff i > i' \quad \text{یا} \quad [i = i' \quad \text{و} \quad j \le j'],\\
&(i,j) \prec_d (i',j') \iff j - i < j' - i' \quad \text{یا} \quad [j - i = j' - i' \quad \text{و} \quad i \le i'], \qquad (۱۱.۴)
\end{aligned}
$$

که ما $\prec_f$، $\prec_b$ و $\prec_d$ را به ترتیب، ترتیب رو به جلو، ترتیب رو به عقب و ترتیب مورب می‌نامیم. به کمک این دستورها و با توجه به مؤلفه‌های $a_{i,j}$ $g_{i,j}$ در ماتریس‌های A و G، که توسط الگوریتم ۱.۱.۴ محاسبه می‌شوند، زوج مرتب (i,j) را می‌توان به ترتیب نوشت. به عنوان مثال فرض کنید که $l = ۳$ باشد. در این صورت داریم:

$$
\begin{aligned}
&\text{ترتیب رو به جلو} : \quad (۱,۱) \prec_f (۲,۲) \prec_f (۱,۲) \prec_f (۳,۳) \prec_f (۲,۳) \prec_f (۱,۳),\\
&\text{ترتیب رو به عقب} : \quad (۳,۳) \prec_b (۲,۲) \prec_b (۲,۳) \prec_b (۱,۱) \prec_b (۱,۲) \prec_b (۱,۳),\\
&\text{ترتیب مورب} : \quad (۱,۱) \prec_d (۲,۲) \prec_d (۳,۳) \prec_d (۱,۲) \prec_d (۲,۳) \prec_d (۱,۳).
\end{aligned}
$$

از این رو، به کمک ترتیب مورب، مجموعه $\{(i,j)|\ ۱ \le i \le j \le ۳\}$، را می‌توان به صورت زیر مرتب کرد:

$$(i_۱,j_۱)=(۱,۱),(i_۲,j_۲)=(۲,۲),\dots,(i_۶,j_۶)=(۱,۳).$$

در این سه ترتیب معرفی شده، ما می‌توانیم برای هر l، پیش شرط را بررسی کنیم. به عنوان مثال، در ترتیب مورب، برای $i<h<j$، پیش شرط معادل است با: $(i,h)\prec_d(i,j)$ و $(h,j)\prec_d(i,j)$، زیرا اگر $h<j$ باشد، آنگاه $h-i<j-i$ خواهد بود و در نتیجه داریم: $(i,h)\prec_d(i,j)$، همچنین اگر $i<h$ باشد، آنگاه $j-h<j-i$ خواهد بود لذا خواهیم داشت: $(h,j)\prec_d(i,j)$. به طور مستقیم، همه پیش شرط‌ها معتبرند زیرا، در این سه ترتیب معرفی شده، همانطور که در (۱۰.۴) نشان داده شده است، قبل از محاسبه $(g_{i,j},a_{i,j})$، مؤلفه‌های (۹.۴)، قابل محاسبه‌اند.

هرچند الگوریتم ۱.۱.۴، به کمک هر یک از سه ترتیب معرفی شده می‌تواند ماتریس‌های A و G را در عملیات ماتریسی بدست آورد، ولی کارایی آن به این نکته بستگی دارد که می‌خواهیم چه نوع جستجویی توسط الگوریتم ۱.۱.۴، انجام شود. به عنوان مثال، از آنجایی که بردارهای چندجمله‌ای سطری در ماتریس G، در الگوریتم ۱.۱.۴، توسط $\prec_b$، از پایین محاسبه می‌شوند، ترتیب رو به عقب، برای جستجو از طریق بررسی وزن همینگ سطرهای ماتریس G، مناسب خواهدبود. از سوی دیگر، از آنجایی که بردارهای چندجمله‌ای ستونی در ماتریس A، در الگوریتم ۱.۱.۴، توسط $\prec_f$، از سمت چپ محاسبه می‌شوند، ترتیب به جلو، برای جستجو از طریق بررسی سطرهای ماتریس‌های چندجمله‌ای بررسی توازن با استفاده از قضیه ۱.۶.۲ به بردارهای چندجمله‌ای ستونی در ماتریس A، مناسب خواهدبود.

در نهایت، به کمک ترتیب مورب، نیاز به محاسبات کمتری برای بدست آوردن $(g_{i,j},a_{i,j})$ داریم. توجه کنید که برای بررسی پیش‌شرط به کمک رابطه‌ی (۱۱.۴)، ما تنها از شرط $j-i<j'-i'$ استفاده می‌کنیم و شرط دوم را در نظر نمی‌گیریم. این حقیقت این امکان را به ما می‌دهد که به محاسبات خود نظم دهیم. بدین صورت که اگر فرض کنیم $j-i=h$ باشد و رابطه (۷.۴) را برای زوج مرتب‌های $(i,j)=(۱,h+۱),(۲,h+۲),\dots,(l-h,h)$ بررسی کنیم، خواهیم دید که $d_{i,j}$ که در رابطه (۷.۴) صدق کند وجود ندارد لذا می‌توانیم از این حلقه صرف‌نظر کنیم زیرا ماتریس‌های A و G با درایه‌های $(g_{i,j},a_{i,j})$ وجود ندارد. این روش الگوریتم ۱.۱.۴ را با ترتیب مورب به سمت سرعت بیشتر هدایت می‌کند. بنا براین مطابق با موضوع جستجو باید ترتیب مناسب را انتخاب کنیم.

مثال ۱.۱.۴. *فرض کنید که $l=۳$ و $q=۲$ باشد. اگر $\alpha=۱+x$ و $\beta=۱+x+x^۲$ باشد، آنگاه خواهیم داشت: $\alpha\beta=۱+x^۳$. در این مثال، به کمک الگوریتم ۱.۱.۴ و ترتیب مورب، ماتریس‌های A و G را به گونه‌ای محاسبه می‌کنیم که داشته‌باشیم:*

$$AG=\begin{pmatrix}\alpha\beta & a_{۱,۲} & a_{۱,۳}\\ ۰ & \beta & a_{۲,۳}\\ ۰ & ۰ & \alpha\end{pmatrix}\begin{pmatrix}۱ & g_{۱,۲} & g_{۱,۳}\\ ۰ & \alpha & g_{۲,۳}\\ ۰ & ۰ & \beta\end{pmatrix}=\mathrm{diag}[۱+x^۳,۱+x^۳,۱+x^۳]. \quad (۱۲.۴)$$

به کمک عملیات ماتریس بالا درایه $g_{۱,۲}$ را می‌توان محاسبه کرد، به این ترتیب که بعد از ضرب دو ماتریس A و G، معادله $a_{۱,۱}g_{۱,۲}+a_{۱,۲}g_{۲,۲}=۰$ حاصل می‌شود. با توجه به رابطه بیان شده در (۴.۴) و با توجه

به این نکته که $\gcd(a_{۱,۱}, g_{۲,۲}) = \gcd(\alpha\beta, \alpha) = \alpha$ می‌باشد، لذا خواهیم داشت:

$$(g_{۱,۲}, a_{۱,۲}) = \left(\frac{g_{۲,۲}}{\alpha}\phi_۱, \frac{a_{۱,۱}}{\alpha}\phi_۱\right) = (\phi_۱, \beta\phi_۱), \qquad \deg\phi_۱ < ۱.$$

به طور مشابه، درایه $g_{۲,۳}$ از طریق معادله $a_{۲,۲}g_{۲,۳} + a_{۲,۳}g_{۳,۳} = ۰$ محاسبه می‌شود. با توجه به رابطه (۴.۴) و اینکه $\gcd(a_{۲,۲}, g_{۳,۳}) = \gcd(\beta, \beta) = \beta$ می‌باشد، بنابراین داریم:

$$(g_{۲,۳}, a_{۲,۳}) = \left(\frac{g_{۳,۳}}{\beta}\phi_۲, \frac{a_{۲,۲}}{\beta}\phi_۲\right) = (\phi_۲, \phi_۲), \qquad \deg\phi_۲ < ۲.$$

با توجه به رابطه‌های بالا، $g_{۱,۲} = \phi_۱ = ۱$ و $g_{۲,۳} = \phi_۲ = x$ خواهدبود. همچنین خواهیم داشت: $a_{۱,۲} = \beta\phi_۱$ و $a_{۲,۳} = \phi_۲$. حال $g_{۱,۳}$ را محاسبه می‌کنیم. با توجه به عملیات ماتریسی (۱۲.۴)، درایه $g_{۱,۳}$ از طریق معادله زیر بدست می‌آید:

$$a_{۱,۱}g_{۱,۳} + a_{۱,۲}g_{۲,۳} + a_{۱,۳}g_{۳,۳} = ۰. \tag{۱۳.۴}$$

از آنجا که $a_{۱,۲}g_{۲,۳} = \beta x$ عادی‌کند $d_{۱,۳} = \gcd(a_{۱,۱}, g_{۳,۳}) = \gcd(\alpha\beta, \beta) = \beta$ را، از این رو طبق لم ۲.۱.۴، یک جفت جواب برای معادله (۱۳.۴) وجود دارد. جواب منحصر به فرد $(g_۰, a_۰)$، از معادله (۱۳.۴)، با توجه به اینکه $\deg g_۰ < \deg\frac{g_{۳,۳}}{d_{۱,۳}} = \deg\frac{\beta}{\beta} = \deg ۱ = ۰$ می‌باشد، معادل است با: $(g_۰, a_۰) = (۰, x)$، بنابراین، جواب کلی معادله (۱۳.۴) را با توجه به اینکه $\deg g_{۱,۳} < \deg g_{۳,۳} = ۲$ می‌باشد، می‌توان به صورت زیر نشان داد:

$$(g_{۱,۳}, a_{۱,۳}) = \left(g_{۱,۳}^{(۰)} + \frac{g_{۳,۳}}{d_{۱,۳}}\phi_۳, {}_{۱,۳}^{(۰)} + \frac{a_{۱,۱}}{d_{۱,۳}}\phi_۳\right) = (\phi_۳, x + \alpha\phi_۳), \qquad \deg\phi_۳ < ۲.$$

از آنجایی که چهار چندجمله‌ای با شرط $\deg\phi_۳ < ۲$ وجود دارد، در نهایت چهار جواب به صورت زیر خواهیم داشت:

$$(g_{۱,۳}, a_{۱,۳}) = (۰, x), (۱, ۱), (x, x^۲), (۱ + x, ۱ + x + x^۲).$$

۲.۴ الگوریتم شمارشی کدهای صحیح تعمیم‌یافته

در این بخش الگوریتم‌هایی را ارائه می‌دهیم که ماتریس مولدهای کدهای صحیح تعمیم‌یافته را به کمک معادله (۷.۳) تولید می‌کند. توجه داشته‌باشید که عملیات $AG = \mathrm{diag}[n_۱, \dots n_l]$ معادل است با

$$AG = (a_{ij})(g_{ij}) = \left(\sum_{h=i}^{j} a_{ih}g_{hj}\right) = \begin{cases} ۰ & i \neq j \\ n_i & i = j \end{cases}. \tag{۱۴.۴}$$

اگر $i = j$ باشد آنگاه $a_{ii}g_{ii} = n_i$ خواهدبود. برای i و j های دیگر ابتدا لم‌های زیر را بیان و اثبات می‌کنیم.

لم ۱.۲.۴. اگر a, g اعداد صحیح مثبت با $d = \gcd(a, g)$ باشند آنگاه هر پاسخ صحیح $(x_۰, y_۰)$ از معادله $ax + yg = ۰$ برای $z \in \mathbb{Z}$ به صورت زیر بیان می‌شود:

$$(x_۰, y_۰) = \left(\frac{g}{d}z, -\frac{a}{d}z\right). \tag{۱۵.۴}$$

در حالت خاص، اگر فرض کنیم $0 \leq x_0 < g$ *باشد، آنگاه تعداد* d *پاسخ به‌ازای* $z = 0, 1, \ldots, d-1$ *به صورت زیر موجود است:*

$$(x_0, y_0) = \left(\frac{g}{d}z, -\frac{a}{d}z\right). \tag{۱۶.۴}$$

برهان. از آنجایی که $\frac{a}{d}x_0 + y_0\frac{g}{d} = 0$ می‌باشد، آنگاه x_0 عدد $\frac{g}{d}$ را عاد می‌کند. ادامه بحث بدیهی است. □

لم ۲.۲.۴. *فرض کنید* a *و* g *اعداد صحیح مثبت و* $d = \gcd(a, g)$ *باشند و* c *یک عدد صحیح باشد. آنگاه یک جواب صحیح مانند* (x, y) *از معادله* $ax + yg = c$ *وجود دارد اگر و تنها اگر* d*،* c *را عاد کند. فرض کنید* d*،* c *را عاد کند، سپس هر جواب صحیح* (x, y) *از معادله* $ax + yg = c$ *به صورت* $(x, y) = (g_0, a_0) + (x_0, y_0)$ *بیان می‌شود، که درآن* (x_0, y_0) *جواب کلی معادله* $ax_0 + y_0 g = 0$ *در لم* ۱.۲.۴ *است و* $(g_0.a_0)$ *یک جواب منحصر به فرد از معادله* $ag_0 + a_0 g = c$ *می‌باشد که در آن* $0 \leq g_0 < \frac{g}{d}$ *است. به طور خاص، اگر* $0 \leq x < g$ *باشد، آنگاه به‌ازای* $z = 0, 1, \ldots, d-1$*،* d *جواب به صورت زیر وجود دارد:*

$$(x, y) = \left(g_0 + \frac{g}{d}z, a_0 - \frac{a}{d}z\right). \tag{۱۷.۴}$$

برهان. اگر d، عدد c راعاد کند، آنگاه الگوریتم اقلیدسی قابل تعمیم، یک جواب از معادله $ax+yg = c$ را می‌دهد. در مقابل، اگر یک جواب صحیح از معادله $ax + yg = c$ وجود داشته‌باشد آنگاه d عدد c را عاد می‌کند. زیرا d، $ax + yg$ را عاد می‌کند. فرض کنید d عدد c را عاد کند، از معادله $\frac{a}{d}x + y\frac{g}{d} = \frac{c}{d}$ نتیجه می‌گیریم که $\frac{a}{d}x \equiv \frac{c}{d} \mod \frac{g}{d}$ می‌باشد، که یک جواب منحصر به فرد به پیمانه $\frac{g}{d}$ دارد؛ زیرا $\gcd\left(\frac{a}{d}, \frac{g}{d}\right) = 1$ می‌باشد. اگر (g_0, a_0) یک جواب منحصر به فرد از معادله $\frac{a}{d}g_0 + a_0\frac{g}{d} = \frac{c}{d}$ تعریف شود که در آن $0 \leq g_0 < \frac{g}{d}$ است، آنگاه داریم: $ag_0 + a_0 g = c$. برای جواب دیگر معادله $ax+yg = c$، بااستفاده از لم ۱.۲.۴، خواهیم داشت : $a(x - g_0) + (y - a_0)g = 0$، آنگاه $(x - g_0, y - a_0)$ معادل است با (۱۵.۴) و ادعا ثابت می‌شود. □

حال رابطه $i < j$ *در* (۱۴.۴) *را بررسی می‌کنیم. اگر* $j = i + 1$ *باشد، آنگاه* (۱۴.۴) *معادل است با* $a_{ii}g_{ij} + a_{ij}g_{jj} = 0$*. اگر* $d_{ij} = \gcd(a_{ii}, g_{jj})$ *باشد، آنگاه* G *کاهنده را که درآن* $0 \leq g_{ij} < g_{jj}$ *است، در نظر می‌گیریم. بااستفاده از* (۱۶.۴)*، کاندیدهای* (g_{ij}, a_{ij}) *برای* $z = 0, 1, \ldots, d_{ij} - 1$ *به صورت زیر نوشته می‌شوند :*

$$\left(\frac{g_{jj}}{d_{ij}}z, -\frac{a_{ii}}{d_{ij}}z\right).$$

اگر $j > i + 1$ *باشد، آنگاه* (۱۴.۴) *معادل است با*

$$a_{ii}g_{ij} + \sum_{i<h<j} a_{ih}g_{hj} + a_{ij}g_{jj} = 0. \tag{۱۸.۴}$$

گزاره ۱.۲.۴. *(شرط معادل برای عملیات ماتریسی) اگر برای $1 \le i < j \le l$ ، داشته باشیم:*

$$A = (a_{ij}) \in T_l(\mathbb{Z}) \,,\; G = (g_{ij}) \in T_l(\mathbb{Z}),$$

و $d_{ij} = \gcd(a_{ii}, g_{jj})$ باشد، آنگاه $AG = \operatorname{diag}[n_1, \ldots, n_l]$ است اگر و تنها اگر برای $1 \le i \le l$ داشته‌باشیم: $a_{ii}g_{ii} = n_i$ و برای $1 \le i < j \le l$ داشته‌باشیم:

$$\sum_{i<h<j} a_{ih}g_{hj} \in d_{ij}\mathbb{Z}. \tag{۱۹.۴}$$

برهان. به کمک لم ۲.۲.۴، (۱۸.۴) قابل حل است اگر و تنها اگر d_{ij}، عدد $c = -\sum_{i<h<j} a_{ih}g_{hj}$ را عاد کند. □

فرض کنید (۱۹.۴) برقرار باشد، آنگاه با استفاده از رابطه (۱۷.۴)، کاندیدهای زوج مرتب (g_{ij}, a_{ij}) برای $z = 0, 1, \ldots, d_{ij} - 1$ ، به‌صورت زیر نوشته می‌شود :

$$\left(g_{ij}^{(0)} + \frac{g_{jj}}{d_{ij}}z, a_{ij}^{(0)} - \frac{a_{ii}}{d_{ij}}z\right), \tag{۲۰.۴}$$

که در آن $(g_{ij}^{(0)}, a_{ij}^{(0)})$ جواب منحصر به فرد رابطه (۱۸.۴) خواهد بود و $0 \le g_{ij}^{(0)} < \frac{g_{jj}}{d_{ij}}$ می‌باشد. برای اعداد صحیح مثبت $n_1, \ldots, n_l$، الگوریتم زیر یک روش برای تولید همه جوابهای معادله

$$AG = \operatorname{diag}[n_1, \ldots, n_l],$$

شرح می‌دهد.

الگوریتم ۱.۲.۴.

Input positive $n_1, ..., n_l \in \mathbb{Z}$
output all $A, G \in T_l(\mathbb{Z})$ such that $AG = \operatorname{diag}[n_1, ..., n_l]$
1 : for $j = 1$ to l do
2 : positive $g_{jj}, a_{jj} \in \mathbb{Z}$ such that $a_{jj}g_{jj} = n_j$
3 : for $i = j - 1$ to 1 do
4 : $d_{ij} = \gcd(a_{ii}, g_{jj})$
5 : if $\sum_{i<h<j} a_{ih}g_{hj} \in d_{ij}\mathbb{Z}$ then
6 : (g_{ij}, a_{ij}) given by (20.4)
7 : end if
8 : end for
9 : end for

در الگوریتم ۱.۲.۴، قبل از محاسبه (g_{ij}, a_{ij}) در معادله (۱۸.۴)، لازم است که برای $i < h < j$ ،

$$a_{ih} \quad \text{و} \quad g_{hj}$$

را بدست آوریم. این پیش‌شرط برای محاسبه (g_{ij}, a_{ij}) *به‌صورت زیر می‌تواند بررسی شود.*
فرض کنید $\prec$ *یک ترتیب روی مجموعه* $\{(i,j)|\ ۱ \le i \le j \le l\}$ *باشد که به صورت زیر تعریف می‌شود:*

$$(i,j) \prec (i',j') \iff j < j' \quad \text{یا} \quad [j = j' \quad \text{و} \quad i \ge i'].$$

اگر $l = ۳$ *باشد، با توجه به این تعریف خواهیم‌داشت:*

$$(۱,۱) \prec (۲,۲) \prec (۱,۲) \prec (۳,۳) \prec (۲,۳) \prec (۱,۳).$$

ترتیب $\prec$ *معادل است با ترتیب محاسبه* (g_{ij}, a_{ij}) *در الگوریتم ۱.۲.۴. بنابراین، برای* $i < h < j$*، پیش شرط* $(i,h) \prec (i,j)$ *و* $(h,j) \prec (i,j)$ *لازم است.*
از سوی دیگر، ترتیب دیگری وجود دارد که در زیر، در (۲۱.۴)، تعریف شده است که می‌توانیم به کمک آن پیش شرط را بدست آوریم. بنابراین الگوریتم دیگری که همه جوابهای $AG = \text{diag}[n_۱, \ldots, n_l]$ *را برای داده‌های* $n_۱, \ldots, n_l$ *تولید کند به شرح زیر می باشد. همان پیش شرط برای الگوریتم ۱.۲.۴ باید برای الگوریتم ۲.۲.۴ نیز بررسی شود.*
فرض کنید $\sqsubset$ *یک ترتیب روی مجموعه* $\{(i,j)|\ ۱ \le i \le j \le l\}$ *باشد که به صورت زیر تعریف می‌شود.*

$$(i,j) \sqsubset (i',j') \iff i > i' \quad \text{یا} \quad [i = i' \quad \text{و} \quad j \le j']. \tag{۲۱.۴}$$

الگوریتم ۲.۲.۴.

input positive $n_1, ..., n_l \in \mathbb{Z}$
output all $A, G \in T_l(\mathbb{Z})$ such that $AG = \text{diag}[n_1, ..., n_l]$
1 : for $i = l$ to 1 do
2 : *positive* $g_{ii}, a_{ii} \in \mathbb{Z}$ such that $a_{ii} g_{ii} = n_i$
3 : for $j = i + 1$ to l do
4 : $d_{ij} = \gcd(a_{ii}, g_{jj})$
5 : if $\sum_{i<h<j} a_{ih} g_{hj} \in d_{ij}\mathbb{Z}$ then
6 : (g_{ij}, a_{ij}) given by (20.4)
7 : end if
8 : end for
9 : end for

اگر $l = ۳$ *باشد، با توجه به این تعریف داریم:*

$$(۳,۳) \sqsubset (۲,۲) \sqsubset (۲,۳) \sqsubset (۱,۱) \sqsubset (۱,۲) \sqsubset (۱,۳).$$

ترتیب $\sqsubset$ *معادل است با ترتیب محاسبه* (g_{ij}, a_{ij}) *برای* $i < h < j$ *در الگوریتم ۲.۲.۴*
الگوریتم‌های ۱.۲.۴ و ۲.۲.۴ ویژگی‌های خاص خود را دارند. به عنوان مثال، از آنجایی که الگوریتم ۲.۲.۴ ماتریس مولد را از سطرهای پایینش می‌سازد بنابراین زمانی که به دنبال ماتریس مولدی با مینیمم

فاصله بیشتر هستیم الگوریتم ۲.۲.۴ بسیار مناسب‌تر از الگوریتم ۱.۲.۴ می‌باشد. از سوی دیگر، از آنجایی که الگوریتم ۱.۲.۴ ماتریس A و ماتریس کنترل توازن A^T را از سطرهای بالایی آن تولید می‌کند، هنگامی که به‌دنبال ماتریس کنترل توازنی هستیم که سطرهای آن دارای اجزای غیرصفر پراکنده است، الگوریتم ۱.۲.۴ بسیار مناسب‌تر از الگوریتم ۲.۲.۴ می‌باشد. بنابراین ما می‌توانیم با توجه به هدفمان بین دو الگوریتم انتخاب کنیم.

مثال ۱.۲.۴. فرض کنید $l = ۳$ و $n_۱ = n_۲ = n_۳ = ۱۲$ باشد. اگر در الگوریتم ۱.۲.۴، داشته‌باشیم: $(g_{۱۱}, g_{۲۲}, g_{۳۳}) = (۲, ۶, ۲)$. در این صورت با توجه به رابطه $a_{jj}g_{jj} = ۱۲$، خواهیم‌داشت: $(a_{۱۱}, a_{۲۲}, a_{۳۳}) = (۶, ۲, ۶)$. لذا طبق عملیات ماتریسی و همچنین بزرگترین مقسوم‌علیه مشترک (a_{ii}, g_{jj}) خواهیم داشت:

$$\begin{pmatrix} ۶ & a_{۱۲} & a_{۱۳} \\ ۰ & ۲ & a_{۲۳} \\ ۰ & ۰ & ۶ \end{pmatrix} \begin{pmatrix} ۲ & g_{۱۲} & g_{۱۳} \\ ۰ & ۶ & g_{۲۳} \\ ۰ & ۰ & ۲ \end{pmatrix} = \begin{pmatrix} ۱۲ & ۰ & ۰ \\ ۰ & ۱۲ & ۰ \\ ۰ & ۰ & ۱۲ \end{pmatrix}. \tag{۲۲.۴}$$

$$d_{۱۲} = \gcd(a_{۱۱}, g_{۲۲}) = ۶,$$

$$d_{۲۳} = \gcd(a_{۲۲}, g_{۳۳}) = ۲,$$

$$d_{۱۳} = \gcd(a_{۱۱}, g_{۳۳}) = ۲.$$

سپس کاندیدهای (g_{ij}, a_{ij}) در ترتیب $(۱,۳) \prec (۲,۳) \prec (۱,۲) = (i,j)$ توسط (۲۰.۴) محاسبه می‌شود. اولاً، برای $(g_{۱۲}, a_{۱۲})$، از رابطه‌های (۱۸.۴) یا (۲۰.۴) داریم که $۶g_{۱۲} + a_{۱۲}۶ = ۰$ می‌باشد. توسط رابطه (۲۰.۴)، کاندیدهای $(g_{۱۲}, a_{۱۲})$، عبارتند از:

$$(g_{۱۲}, a_{۱۲}) = (۰,۰), (۱,-۱), (۲,-۲), (۳,-۳), (۴,-۴), (۵,-۵). \tag{۲۳.۴}$$

دوماً، $(g_{۲۳}, a_{۲۳})$، از رابطه $۲g_{۲۳} + a_{۲۳}۲ = ۰$ بدست می‌آید. به کمک رابطه (۲۰.۴)، کاندیدهای $(g_{۲۳}, a_{۲۳})$ عبارتند از:

$$(g_{۲۳}, a_{۲۳}) = (۰,۰), (۱,-۱). \tag{۲۴.۴}$$

در نهایت، برای $(g_{۱۳}, a_{۱۳})$ که از رابطه $۶g_{۱۳} + a_{۱۲}g_{۲۳} + a_{۱۳}۲ = ۰$ بدست می‌آید، اگر در رابطه (۲۴.۴)، $(g_{۲۳}, a_{۲۳}) = (۰,۰)$ باشد، آنگاه به تبعیت از آن در شرط (۱۹.۴) داریم: $a_{۱۲}g_{۲۳} = ۰$ و برای $(g_{۱۲}, a_{۱۲})$ دلخواه در (۲۳.۴)، داریم:

$$(g_{۱۳}, a_{۱۳}) = (۰,۰), (۱,-۳).$$

اگر در رابطه (۲۴.۴)، $(g_{۲۳}, a_{۲۳}) = (۱,-۱)$ باشد، آنگاه شرط (۱۹.۴) معادل با $a_{۱۲}/۲ \in \mathbb{Z}$ می‌باشد و در رابطه (۲۳.۴)، داریم: $(g_{۱۲}, a_{۱۲}) = (۰,۰), (۲,-۲)(۴,-۴)$. برای هر $(g_{۱۲}, a_{۱۲})$، به کمک رابطه (۲۰.۴)، مقادیر $(g_{۱۳}, a_{۱۳})$ به صورت زیر بدست می‌آید:

$$(g_{۱۲}, a_{۱۲}) = (۰,۰) \Longrightarrow (g_{۱۳}, a_{۱۳}) = (۰,۰), (۱,-۳)$$

$$(g_{۱۲}, a_{۱۲}) = (۲,-۲) \Longrightarrow (g_{۱۳}, a_{۱۳}) = (۰,۱), (۱,-۲)$$

$$(g_{۱۲}, a_{۱۲}) = (۴,-۴) \Longrightarrow (g_{۱۳}, a_{۱۳}) = (۰,۲), (۱,-۱)$$

بنابراین، همه ۱۸ *پاسخ برای رابطه* (۲۲.۴) *بدست می‌آید. به عنوان مثال، یکی از آنها به صورت زیر است:*

$$\begin{pmatrix} ۶ & -۴ & -۱ \\ ۰ & ۲ & -۱ \\ ۰ & ۰ & ۶ \end{pmatrix} \begin{pmatrix} ۲ & ۴ & ۱ \\ ۰ & ۶ & ۱ \\ ۰ & ۰ & ۲ \end{pmatrix} = \begin{pmatrix} ۱۲ & ۰ & ۰ \\ ۰ & ۱۲ & ۰ \\ ۰ & ۰ & ۱۲ \end{pmatrix}.$$

پیوست آ

تقسیم اقلیدسی برای ماتریس‌های چندجمله‌ای

در این پیوست لم کاربردی را نشان می‌دهیم که تقسیم اقلیدسی از چندجمله‌ای ها را به نوع خاصی از ماتریس‌های چندجمله‌ای تعمیم می‌دهد.

لم آ.۰.۱. *فرض کنید $h, l, m \in \mathbb{Z}$ اعداد صحیح مثبتی باشند به طوری که $h \leq l$ است و فرض کنید که $F = (f_{i,j})$ یک ماتریس $m \times l$ با درایه‌هایی در $\mathbb{F}_q[x]$ و $G = (g_{i,j})$ یک ماتریس $h \times l$ با درایه‌هایی در $\mathbb{F}_q[x]$ باشد و فرض کنید که G به فرم زیر است:*

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,h} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,h} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots & \cdots & \vdots \\ 0 & \cdots & 0 & g_{h,h} & \cdots & g_{h,l} \end{pmatrix}$$

که در آن برای $i > j$، درایه $g_{i,j} = 0$ است، علاوه بر این فرض کنید که برای $1 \leq l \leq h$ درایه $g_{j,j} \neq 0$ باشد. در این صورت یک ماتریس $m \times h$ مانند $Q = (q_{i,j})$ با درایه‌هایی در $\mathbb{F}_q[x]$ و یک ماتریس $m \times l$ مانند $D = (d_{i,j})$ با درایه‌هایی در $\mathbb{F}_q[x]$ موجود است به طوری که داشته‌باشیم:

$$F = QG + D,$$

که در آن برای $1 \leq i, j \leq h$، داریم: $\deg d_{i,j} < \deg g_{j,j}$.

برهان. ابتدا فرض می‌کنیم که $R = \mathbb{F}_q[x]$ باشد و برای اعداد صحیح مثبت $r, s \in \mathbb{Z}$، مجموعه همه ماتریس‌ها از مرتبه $r \times s$ و با درایه‌هایی در R را به صورت $R^{r,s}$ نشان می‌دهیم. ما می‌توانیم فرض کنیم که $m = ۱$ باشد، زیرا در حالت کلی، اگر برای $۱ \leq i \leq m$، $F_i \in R^{۱,l}$ را به عنوان سطر $i-$ام از ماتریس F در نظر بگیریم و $Q_i \in R^{۱,h}$ و $D_i \in R^{۱,l}$ را به گونه‌ای تعریف کنیم که با استفاده از لم برای $m = ۱$، داشته باشیم: $F_i = Q_i G + D_i$، در این صورت با توجه به اینکه $Q = (Q_i) \in R^{m,h}$ و $D = (D_i) \in R^{m,l}$ می‌باشد، می‌توانیم ثابت کنیم که $F = QG + D$.

لم را برای $m = ۱$ و با استقرا روی h ثابت می‌کنیم. فرض کنید که $h = ۱$ باشد. در این صورت برای $F = (f_۱, \ldots, f_l) \in R^{۱,l}$ و $G = (g_۱, \ldots, g_l) \in R^{۱,l}$ با $g_۱ \neq ۰$، دو چندجمله‌ای $q_۱, d_۱ \in R$ موجود است به طوری که $f_۱ = q_۱ g_۱ + d_۱$ بوده و $\deg d_۱ < \deg g_۱$ باشد. سپس $Q = (q_۱)$ و $D = F - q_۱ G$ ویژگی لازم را داراست. حال فرض کنید که لم برای $h - ۱ \geq ۱$ برقرار است، کافیست لم را برای h ثابت کنیم. فرض کنید که $F = (f_۱, \ldots, f_l) \in R^{۱,l}$ و $G = (g_{i,j}) \in R^{h,l}$ باشند و $G^{(۰)} = \left(g_{i,j}^{(۰)}\right) \in R^{h-۱,l}$ یک زیرماتریس متشکل از $h - ۱$ سطر اول ماتریس G باشد. به کمک فرض استقرا، $Q^{(۰)} = \left(q_j^{(۰)}\right) \in R^{۱,h-۱}$ و $D^{(۰)} = \left(d_j^{(۰)}\right) \in R^{۱,l}$ به گونه‌ای موجودند که برای $۱ \leq j \leq h - ۱$، داریم: $F = Q^{(۰)} G^{(۰)} + D^{(۰)}$ و $\deg d_j^{(۰)} < \deg g_{j,j}^{(۰)}$. علاوه بر این، فرض می‌کنیم که $G^{(۱)} = (g_{h,h}, \ldots, g_{h,l}) \in R^{۱,l-h+۱}$ و $F^{(۱)} = \left(d_h^{(۰)}, \ldots, d_l^{(۰)}\right) \in R^{۱,l-h+۱}$ باشد. با استفاده از لم برای $m, h = ۱$، ماتریس‌های $Q^{(۱)} \in R^{۱,۱}$ و $D^{(۱)} = \left(d_h^{(۱)}, \ldots, d_l^{(۱)}\right) \in R^{۱,l-h+۱}$، به گونه‌ای موجودند که داشته‌باشیم: $F^{(۱)} = Q^{(۱)} G^{(۱)} + D^{(۱)}$ و $\deg d_h^{(۱)} < \deg g_{h,h}^{(۱)}$. سپس توجه داشته‌باشید که:

$$\begin{aligned} F &= Q^{(۰)} G^{(۰)} + D^{(۰)} \\ &= Q^{(۰)} G^{(۰)} + \left(d_۱^{(۰)}, \ldots, d_{h-۱}^{(۰)} \;\middle|\; F^{(۱)}\right) \\ &= Q^{(۰)} G^{(۰)} + \left(d_۱^{(۰)}, \ldots, d_{h-۱}^{(۰)} \;\middle|\; Q^{(۱)} G^{(۱)} + D^{(۱)}\right). \end{aligned} \tag{۱.آ}$$

با جایگذاری $Q = \left(Q^{(۰)} \;\middle|\; Q^{(۱)}\right) \in R^{۱,h}$ و $D = (d_j) = \left(d_۱^{(۰)}, \ldots, d_{h-۱}^{(۰)} \;\middle|\; D^{(۱)}\right) \in R^{۱,l}$ و همچنین $G = \begin{pmatrix} G^{(۰)} \\ \hline ۰ \;\cdots\; ۰ \;\; G^{(۱)} \end{pmatrix} \in R^{h,l}$، آنگاه معادله (۱.آ)، معادل است با:

$$F = QG + D,$$

و همچنین برای $۱ \leq j \leq h$ داریم:

$$\deg d_j < \deg g_{j,j}.$$

در نهایت ثابت می‌کنیم که ماتریس‌های Q و D منحصر به فرد هستند. با استفاده از برهان خلف، فرض کنید داشته‌باشیم: $F = QG + D = Q'G + D'$، که در آن $D = (d_j)$ و $\deg d_j < \deg g_{j,j}$، همچنین $D' = (d'_j)$ و $\deg d'_j < \deg g_{j,j}$ می‌باشد. با تفریق طرفین در تساوی فوق و با توجه به این نکته که $\deg(d_j, d'_j) \leq \max\{\deg d_j, \deg d'_j\}$، ادعا می‌کنیم که $QG + D = (۰, \ldots, ۰)$ و

$\deg d_j < \deg g_{j,j}$ خواهد بود اگر و تنها اگر Q و D هر دو برابر صفر باشند. با اثبات این ادعا منحصر به فرد بودن Q و D ثابت می‌شود. فرض کنید که $Q = (q_1, \ldots, q_h)$ و $D = (d_1, \ldots, d_l)$ باشد. در این صورت خواهیم داشت: $q_1 g_{1,1} = -d_1$، با توجه به این نکته که $\deg d_1 < \deg g_{1,1}$، نتیجه می‌گیریم که $q_1 = d_1 = 0$. □

مراجع

[1] Blake I.: Codes over certain rings. *Inf. Control* 20(4), 396–404 (1972).

[2] Blake I.: Codes over integer residue rings. *Inf. Control* 29(4), 295–300 (1975).

[3] Calderbank A.R., Sloane N.J.A.: Modular and p-adic cyclic codes. *Des. Codes Cryptogr.* 6(1), 21–35 (1995).

[4] Cao Y.: Structural properties and enumeration of 1-generator generalized quasi-cyclic codes. *Des. Codes Cryptogr.* 60(1), 67–69 (2010).

[5] Cao Y., Gao J.: Constructing quasi-cyclic codes from linear algebra theory, *Des. Codes Cryptogr.* 67(1), 59–75 (Apr. 2013).

[6] Chen L., Xu J., Djurdjevic I., Lin S.: Near-Shannon-limit quasi-cyclic low-density parity-check codes. *IEEE Trans. Commun.* 52(7), 1038–1042 (2004).

[7] Conan J., Séguin G.: Structural properties and enumeration of quasi cyclic codes, *Appl. Algebra Eng. Commun. Comput*. 4(1), 25–39 (Mar. 1993).

[8] Esmaeili M., Yari S.: Generalized quasi-cyclic codes: structural properties and code construction.*Appl. Algebra Eng. Commun. Comput.* 20(2), 159–173 (2009).

[9] Fossorier M.P.C.: Quasi-cyclic low density parity check codes from circulant permutation matrices. *IEEE Trans. Inf. Theory* 50(8), 1788–1793 (2004).

[10] Han Vinck A.J., Morita H.: Codes over the ring of integers modulo m. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E81-A(10), 2013–2018 (1998).

[11] Heegard C., Little J., Saints K.: Systematic encoding via Gröbner bases for a class of algebraic geometric Goppa codes. *IEEE Trans. Inf. Theory* 41(6), 1752–1761 (1995).

[12] Kamiya N.: High-rate quasi-cyclic low-density parity-check codes derived from finite affine planes. *IEEE Trans. Inf. Theory* 53(4), 1444–1459 (2007).

[13] Kamiya N., Fossorier M.P.C.: Quasi-cyclic codes from a finite affine plane. *Des. Codes Cryptogr.* 38(3), 311–329 (2006)

[14] Kostadinov H., Morita H., Manev N.: Integer codes correcting single errors of specific types (±e1,±e2, ...,±es). *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E86-A(7), 1843–1849 (2003).

[15] Kostadinov H., Morita H., Manev N.: Derivation on bit error probability of coded QAM using integer codes. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E87-A(12), 3397–3403 (2004).

[16] Kostadinov H., Morita H., Iijima N., Han Vinck A.J., Manev N.: Soft decoding of integer codes and their application to coded modulation. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E93-A(7), 1363–1370 (2010).

[17] KouY., Lin S., Fossorier M.P.C.: Lowdensity parity check codes based on finite geometries: a rediscovery and new results. *IEEE Trans. Inf. Theory* 47(7), 2711–2761 (2001).

[18] Lally K., Fitzpatrick P.: Algebraic structure of quasi-cyclic codes. *Discret. Appl.Math.* 111(1–2), 157–175 (2001).

[19] Ling S., Costello D.J.: Error Control Coding: *Fundamentals and Applications,* 2nd edn. Prentice-Hall, Englewood Cliffs (2004).

[20] Ling S., Solé P.: On the algebraic structure of quasi-cyclic codes I: finite fields. *IEEE Trans. Inf. Theory* 47(7), 2751–2760 (2001).

[21] Ling S., Solé P.: On the algebraic structure of quasi-cyclic codes II: chain rings. *Des. Codes Cryptogr.* 30(1), 113–130 (2003).

[22] Ling S., Solé P.: On the algebraic structure of quasi-cyclic codes III: generator theory. *IEEE Trans. Inf. Theory* 51(7), 2692–2700 (2005).

[23] Ling S., Niederreiter H., Solé P.: On the algebraic structure of quasi-cyclic codes IV: repeated roots. *Des. Codes Cryptogr.* 38(3), 337–361 (2006).

[24] Ling S., Xing C.: *Coding theory: a first course.* Cambridge University Press. .(2004)

[25] MacWilliams F.J., Sloane N.J.A.: *The Theory of Error Correcting Codes,* 9th edn. Elsevier,North Holland (1988).

[26] Matsui, Hajime. ”On generator and parity-check polynomial matrices of generalized quasi-cyclic codes. *Finite Fields and Their Applications*. 34, 280-304 .(2015)

[27] Matsui H.: On generator matrices and parity check matrices of generalized integer codes. *Designs, Codes and Cryptography*, 74(3), 681-701 (2015).

[28] Matsui H.: *On polynomial generator matrices of generalized quasi-cyclic codes.* In: 6th Asia-Europe Workshop on Information Theory, Ishigaki Island, Okinawa, Japan, 22–24 (Oct 2010).

[29] Nakamura K.: A class of error-correcting codes for DPSK channels. In:*IEEE International Conference on Communications*, Boston, MA, June 10–14 1979, pp. 45.4.1–45.4.5.

[30] Nebe G., Rains E.M., Sloane N.J.A.: *Self-Dual Codes and Invariant Theory.* Springer, Berlin (2006).

[31] Peterson W.W., Weldon E.J.: *Error Correcting Codes*, 2nd ed., MIT Press, Cambridge, MA, (1972).

[32] Séguin G.E.: Aclass of 1-generator quasi-cyclic codes.*IEEE Trans. Inf. Theory* 50(8), 1745–1753 (2004).

[33] Shimura G.: *Introduction to the Arithmetic Theory of Automorphic Functions.* PrincetonUniversity Press, Princeton (1971).

[34] Siap I., Kulhan N.: The structure of generalized quasi-cyclic codes. *Appl.Math. E-Notes* 5, 24–30 (2005).

[35] Spiegel E.: Codes over Zm. *Inf. Control* 35(1), 48–51 (1977).

[36] Tang H., Xu J., Lin S., Abdel-Ghaffar K.A.S.: Codes on finite geometries. *IEEE Trans. Inf. Theory* 51(2), 572–596 (2005).

[37] Thomas W. Hungerford.:*Algebra, volume 73 of Graduate Texts in Mathematics*, 367-369 (1980).

[38] Van V.T., Matsui H., Mita S.: Computation of Gröbner basis for systematic encoding of generalized quasicyclic codes.*IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E92-A(9), 2345–2359 (2009).

[39] Van V.T., Matsui H., Mita S.: *A class of generalized quasi-cyclic LDPC codes: high-rate and lowcomplexity encoder for data storage devices.* In: IEEE Global Communications Conference (GLOBECOM), Miami, FL, pp. 6–10 (2010).

واژه‌نامه فارسی به انگلیسی

الگوریتم بوخ‌برگر ..... Buchberger's algorithm
الگوریتم شمارشی ..... Enumeration algorithm
ایده‌آل ..... Ideal
برووریختی ..... Epimorphism
پوشایی ..... Surjectivity
ترانهاده ..... Transpose
تقسیم اقلیدسی ..... Euclidean division
تکریختی ..... Monomorphism
حلقه ..... Ring
دترمینان ..... Determinant
درجه ..... Degree
دوسویی ..... Bijection
رشته دقیق ..... Exact sequence
رتبه کامل ..... Full rank
زیرحلقه ..... Subgroup
زیرگروه ..... Subring
فاصله لی ..... Lee distance
فضای برد ..... Range space
فضای پوچ ..... Null space
قضیه همزادی ..... Duality theorem
کاهنده ..... Reduced
کد خطی ..... Linear code
کد دوری ..... Cyclic code
کد دوگان ..... Dual code
کد شبه دوری ..... Quasi cyclic code
کد شبه‌دوری تعمیم یافته ..... Generalized quasi-cyclic code
کد صحیح ..... Integer code

کد صحیح تعمیم یافته ..... Generalized integer code
گروه ..... Group
گروه آبلی ..... Abelian group
ماتریس چندجمله‌ای ..... Polynomial matrix
ماتریس کنترل توازن ..... Parity check matrix
ماتریس گردشی ..... Circulant matrix
ماتریس مولد ..... Generator matrix
مقسوم‌علیه‌های اولیه ..... Elementary divisors
همریختی ..... Homomorphism
یک به یک بودن ..... Injectivity
یکریختی ..... Isomorphism

واژه‌نامه انگلیسی به فارسی

گروه آبلی ..... Abelian group
دوسویی ..... Bijection
الگوریتم بوخ‌برگر ..... Buchberger's algorithm
ماتریس گردشی ..... Circulant matrix
کد دوری ..... Cyclic code
درجه ..... Degree
دترمینان ..... Determinant
کد دوگان ..... Dual code
قضیه همزادی ..... Duality theorem
مقسوم‌علیه‌های اولیه ..... Elementary divisors
الگوریتم شمارشی ..... Enumeration algoritm
برووریختی ..... Epimorphism
تقسیم اقلیدسی ..... Euclidean division
رشته دقیق ..... Exact sequence
رتبه کامل ..... Full rank
کد صحیح تعمیم یافته ..... Generalized integer code
کد شبه دوری تعمیم یافته ..... Generalized quasi-cyclic code
ماتریس مولد ..... Generator matrix
گروه ..... Group
همریختی ..... Homomorphism
ایده‌آل ..... Ideal
یک به یک بودن ..... Injectivity
یکریختی ..... Isomorphism
کد صحیح ..... Integer code
فاصله لی ..... Lee distance
کد خطی ..... Linear code
تکریختی ..... Monomorphism

فضای پوچ ..... Null space
ماتریس کنترل توازن ..... Parity check matrix
ماتریس چندجمله‌ای ..... Polynomial matrix
کد شبه دوری ..... Quasi-cyclic code
فضای برد ..... Range space
کاهنده ..... Reduced
حلقه ..... Ring
پوشایی ..... Surjectivity
زیرحلقه ..... Subgroup
زیرگروه ..... Subring
ترانهاده ..... Transpose

Aabstract

GQC codes are usually discussed in terms of submodules over polynomial rings. The generator matrix and parity-check matrix of a GQC code viewed as a linear code can be represented by a combination of circulant matrices with different numbers of columns. Similar to QC codes, a GQC code can also be represented by a polynomial matrix.
Generalized integer codes are defined as codes over rings of integers modulo n in which individual code symbols generally have different moduli. In this thesis, we use a certain type of matrix identities to derive a necessary and sufficient condition for integer matrices to be equal to the generator matrices of generalized integer codes. Moreover, it is shown that the parity check matrix is generated from this matrix identity of the generator matrix. Finally, an efficient algorithms which calculates all generator polynomial matrices of Generalized integer codes and also enumerates theoretically all of the generator matrices of generalized integer codes is provided.

keywords: Codes over rings, Generalized integer code,Generalized quasi-cyclic code, Buchberger's algorithm, Generator matrix, Parity check matrix, Polynomial matrix, Circulant matrix, Elementary divisors، Extended Euclidean algorithm.

Shahrood University of Technology

Faculty Of Mathematical Sciences

MSc Thesis in: Graph and Combinatorics

On generator matrices and parity check matrices of generalized integer codes

By: Golshan Golalizadeh Shiri

Supervisors

Dr. Nader Jafari Rad
Dr. Abdollah Alhevaz

January 2017