دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد رمز و کد

مطالعه برخی کدهای دوری خاص بر روی حلقه‌های ناجابه‌جایی

نگارنده: افسانه عرب احمدی

استاد راهنما

دکتر عبدالله آل‌هوز

استاد مشاور

دکتر ابراهیم هاشمی

بهمن‌ماه ۱۴۰۰

تقدیم به ...

این پایان‌نامه را ضمن تشکر و سپاس بیکران و در کمال افتخار تقدیم می‌نمایم به محضر ارزشمند خانواده عزیزم به خاطر همه تلاش‌های محبت‌آمیزی که در دوران مختلف زندگی‌ام انجام داده‌اند و با مهربانی چگونه زیستن را به من آموخته‌اند و به محضر استادان فرزانه و فرهیخته‌ای که در راه کسب علم و معرفت مرا یاری نمودند.

سپاس‌گزاری...

منت خدای را عزوجل که طاعتش موجب قربت است و به شکراندرش مزید نعمت.
بعد از حمد و سپاس خدای متعال قدردانی می‌کنم از زحمات بی‌دریغ پدر و مادر بزرگوارم که همواره مشوق و پشتیبان من بوده‌اند و دلگرمی و دعاهای خیرشان تحمل مشکلات را برایم مقدور می‌گرداند. همچنین از استاد ارجمندم جناب آقای دکتر آل‌هوز که با راهنمایی‌های دلسوزانه خود بنده را در نوشتن این پایان‌نامه بسیار یاری نمودند، کمال سپاسگزاری را دارم. امید به اینکه شایستگی شاگردی ایشان را دارا بوده باشم و برای ایشان از خداوند منان عمر با عزت خواستارم. از استاد مشاورم جناب آقای دکتر ابراهیم هاشمی تشکر فراوان دارم. در پایان از دوستان خوبم که برای من بهترین بودند و مایه‌ی دلگرمی من بودند، بسیار سپاسگزارم و برای همگی آن‌ها بهترین‌ها را آرزو دارم.

افسانه عرب احمدی
بهمن‌ماه ۱۴۰۰

تعهد نامه

اینجانب **افسانه عرب احمدی** دانشجوی کارشناسی ارشد رشته **ریاضی کاربردی علوم ریاضی** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان **مطالعه برخی کدهای دوری خاص بر روی حلقه‌های ناجابه‌جایی** ، تحت راهنمایی 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.

افسانه عرب احمدی

بهمن‌ماه ۱۴۰۰

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

پایان نامه حاضر به مطالعه نظریه کدهای دوری اریب بر روی حلقه‌های چند جمله‌ای اریب از نوع اتومورفیسم می‌پردازد. حلقه‌های چندجمله‌ای اریب توسط اور (۱۹۳۳) معرفی و مورد بحث قرار گرفتند. ارزیابی چندجمله‌ای اریب و مجموعه‌ای از ریشه‌های (راست) آن ابتدا توسط لام (۱۹۸۶) مورد بررسی قرار گرفت و بعد از آن توسط لام و لروی با جزئیات بیشتر مورد مطالعه قرار گرفت. پس از بیان برخی از خواص چند جمله‌ای‌های اریب که مرتبط با بحث ما می‌باشند، نظریه جبری کدهای دوری اریب را که توسط بوچر و اولمر (۲۰۰۷) معرفی شده است، بررسی می‌کنیم. در بحث کدهای دوری اریب که مد نظر ما می‌باشند، ماتریس‌های دوری اریب نقش اساسی را ایفا می‌کنند. در نهایت، در مورد کدهای دوری اریب با کمترین فاصله طراحی شده بحث می‌شود و ما دو نوع مختلف کدهای BCH اریب که از سال ۲۰۱۴ به بعد طراحی شدند را مورد مطالعه قرار می‌دهیم.

کلمات کلیدی: کد دوری اریب، حلقه چندجمله‌ای اریب، ماتریس‌های دوری اریب، ماتریس مولد، ماتریس کنترل توازن، چندجمله‌ای مولد، کمترین فاصله طراحی شده، کد BCH اریب، کد RS.

فهرست مطالب

پیشگفتار

در نظریه کدهای بلوکی کلاسیک، کدهای دوری از جمله کدهایی هستند که بیشتر مورد مطالعه قرارگرفته‌اند و ساختار جبری اضافی دارند، که ساختار جبری این کدها از لحاظ کدگذاری بسیار مفید می‌باشد. نه تنها امکان طراحی کدهای با حداقل فاصله بزرگ را فراهم می‌کند، همچنین الگوریتم‌های کدگشایی جبری بسیار کارآمد را نیز ایجاد می‌کند. در طی دهه گذشته مفهوم دوری بودن به روش‌های مختلف به دوری اریب تعمیم یافته است که توسط اولمر و بوچر شروع شد. به عبارت دقیق‌تر فضای خارج‌قسمتی $\mathbb{F}[x]/(x^n-1)$ که فضای کاری برای کدهای دوری معمولی است، با $\mathbb{F}[x;\sigma]/^{\bullet}(x^n-1)$ جایگزین می‌شود، جایی که $\mathbb{F}[x;\sigma]$ حلقه چندجمله‌ای اریب تولید شده توسط یک اتومورفیسم σ از میدان $\mathbb{F}$ است و $^{\bullet}(x^n-1)$ ایده‌آل چپ تولید شده توسط x^n-1 است. تعمیم بیشتر با جایگزینی پیمانه x^n-1 با x^n-a به دست می‌آید که منجر به تولید کدهای دوری‌ـ ثابت اریب یا حتی چندجمله‌ای‌های کلی f از درجه n می‌شود. در همه حالات، خارج‌قسمت به عنوان یک $\mathbb{F}$ـ فضای برداری با $\mathbb{F}^n$ یکریخت می‌باشد و بنابراین ما می‌توانیم کدهای خطی در را زیرفضایی از خارج‌قسمت در نظر بگیریم.

این موضوع به ما این امکان را می‌دهد که کدهای دوری اریب را تعریف کنیم. یک کد خطی در $\mathbb{F}^n$، (σ,f)ـ دوری اریب است هرگاه یک زیرمدول چپ از $\mathbb{F}[x;\sigma]/^{\bullet}(f)$ باشد. همانطور که در حالت معمولی، هر زیرمدول از این دست توسط یک مقسوم‌علیه راست مدول f تولید می‌شود. اگر $f=x^n-a$ یا حتی $f=x^n-1$، به ترتیب کدهای به دست آمده را (σ,σ)ـ دوری اریب یا σـ دوری اریب می‌نامند. اولین تفاوت قابل‌توجه در حالت معمولی این است که پیمانه x^n-1 به طور کلی مقسوم‌علیه‌های راست بسیار بیشتری در $\mathbb{F}[x;\sigma]$ نسبت به $\mathbb{F}[x]$ دارد. در نتیجه، یک چندجمله‌ای ممکن است ریشه‌های بیشتری نسبت به درجه خود داشته باشد. همه این‌ها بیان می‌کند که خانواده کدهای دوری اریب از طول داده شده، بسیار بزرگ‌تر از کدهای دوری هستند.

در حالی که این تعاریف اساسی ساده هستند، یک مطالعه با جزئیات جبری و نظریه کدی کدهای دوری اریب نیاز به فهم دقیق حلقه چندجمله‌ای اریب $\mathbb{F}[x;\sigma]$ دارد. در بخش‌های ۱.۲ و ۳.۲ و فصل ۳ ما نظریه چندجمله‌ای‌های اریب را به اندازه‌ای که برای مطالعه کدهای دوری اریب نیاز داریم، مطالعه می‌کنیم، که این موضوع شامل خواص تقسیم در حلقه $\mathbb{F}[x,\sigma]$، ارزیابی‌های چندجمله‌ای‌های اریب و ریشه‌های (راست) آن‌ها و مجموعه‌های جبری با نسخه

اریب ماتریس‌های واندرموند می‌باشد. خواص تجزیه و تقسیم توسط اور مورد مطالعه قرار گرفت که حلقه‌های چندجمله‌ای اریب را در سال ۱۹۳۰ در مقاله پیشرو خود معرفی کرد. ارزیابی چندجمله‌ای‌های اریب ابتدا توسط لام در دهه ۱۹۸۰ مطرح شد و سپس توسط لام و لروی مورد بررسی بیشتر قرار گرفت. مثال‌های زیادی را مطرح خواهیم کرد که تفاوت‌ها را در حلقه‌های چندجمله‌ای جابجایی نشان می‌دهد. در بخش ۲.۲ به طور خلاصه رابطه موجود بین چندجمله‌ای‌های اریب روی یک میدان متناهی و چندجمله‌ای‌های تجزیه شده که نقش اساسی در بحث کدهای رتبه متریک را دارند ارائه خواهیم داد.

مطالب موجود در بخش‌های ۱.۲ و ۳.۲ و فصل ۳، مقدمات خوبی را برای مطالعه کدهای دوری اریب و تعمیم آن‌ها برای ما فراهم می‌کند. در فصل‌های ۵ و ۶ نظریه جبری کدهای دوری (σ, f)ـ اریب را مطرح کرده و همچنین به کدهای دوری‌ـ ثابت اریب اختصاص خواهیم داد. این کار را با معرفی ماتریس‌های دوری اریب شروع خواهیم کرد؛ زیرا فضاهای سطری آن‌ها کدهای مورد بحث ما هستند. به عنوان یک راهنما برای دوری‌های اریب، در فصل ۴ یک بررسی کوتاه به کدهای دوری معمولی از طریق ماتریس‌های دوری ارائه می‌دهیم. از جمله اینکه در فصل ۶ خواهیم دید که دوگان یک کد دوری‌ـ ثابت $(\sigma, x^n - a)$ـ اریب، کد دوری‌ـ ثابت $(\sigma, x^n - a^{-1})$ـ اریب است و یک چندجمله‌ای مولد آن به عنوان یک نوع مشخص از معکوس چندجمله‌ای مولد کد اولیه ایجاد می‌شود. در فصل ۷، نحوه ساختن کدهای دوری اریب با مینیمم فاصله طراحی شده را خواهیم دید. آن‌ها اساساً به دو نوع از کدهای BCHـ دوری تبدیل می‌شوند. برای نوع اول چندجمله‌ای مولد دارای ریشه‌های راست است که به عنوان توان‌های متوالی از یک عنصر دلخواه در یک توسیع میدان قرار دارد (مشابه کدهای BCH معمولی)، در حالی که نوع دوم، دارای ریشه‌های راست است که توان‌های متوالی فروبینیوس از یک عنصر مشخص هستند. هر دو مورد را می‌توان از کدهای دوری به هارتمن تزنگ[1] تعمیم داد. نظریه ماتریس‌های واندرموند اریب یک ابزار اساسی مورد استفاده در بحث ما خواهند بود.

و نکته پایانی این که در این پایان‌نامه ما بحث خودمان را به کدهای دوری اریب به دست آمده از چندجمله‌ای‌های اریب از نوع اتومورفیسم روی میدان‌ها محدود خواهیم کرد.

[1] Hartmann-Tzeng

فصل ۱

تعاریف مقدماتی

در این فصل، به بیان بعضی مفاهیم و قضایا از جبر و نظریه کد برای ورود به مفاهیم بعدی، به شکل نسبتاً مختصر می‌پردازیم.

۱.۱ مفاهیم جبری

تعریف ۱.۱.۱. فرض کنیم $\star$ یک عمل دوتایی روی مجموعه G باشد. در این صورت ساختمان جبری $(G, \star)$ یک **گروه** [۱] است، اگر شرایط زیر برقرار باشد:

۱. $\star$ شرکت‌پذیر باشد،

۲. عضوی چون $e \in G$ وجود داشته باشد به طوری که برای $x \in G$ داشته باشیم:

$$x \star e = e \star x = x\,.$$

۳. برای هر $x \in G$ عنصر $x' \in G$ وجود داشته باشد به طوری که:

$$x \star x' = x' \star x = e\,.$$

به علاوه اگر خاصیت زیر نیز برقرار باشد، گروه $(G, \star)$ یک گروه **آبلی** [۲] نامیده می‌شود.

[1] Group
[2] Abelian

۴. جابه‌جایی باشد، یعنی داشته باشیم:

$$\forall x, y \in G, \quad x \star y = y \star x \,.$$

عنصر e را عنصر همانی (یا همان عنصر خنثی) گروه و x' را یک وارون x می‌نامیم.

تعریف ۲.۱.۱. فرض کنید G یک گروه باشد. در این صورت زیرمجموعه‌ی H از G (همراه با عمل دوتایی تعریف شده در G) یک **زیرگروه**[۱] G است، اگر:

۱. H تحت عمل دوتایی گروه G بسته باشد،

۲. H همراه با عمل تحدید شده از عمل G بر H یک گروه باشد.

تعریف ۳.۱.۱. فرض کنیم R یک مجموعه باشد و دو عمل دوتایی با نام‌های جمع و ضرب روی R داشته باشیم. در این صورت R همراه با این دو عمل یک **حلقه**[۲] است، اگر:

۱. R همراه با عمل جمع یک گروه آبلی باشد،

۲. عمل ضرب شرکت‌پذیر باشد، به عبارت دیگر برای هر $a, b, c \in R$ داشته باشیم:

$$(ab)c = a(bc)\,.$$

۳. عمل ضرب نسبت به جمع توزیع‌پذیر باشد، به عبارت دیگر برای هر $a, b, c \in R$ داشته باشیم:

$$(a+b)c = ac + bc \quad \text{و} \quad a(b+c) = ab + ac\,.$$

بنا به بند ۲ تعریف حلقه، ساختمان $(R, +, .)$ یک گروه آبلی است و در نتیجه یک عنصر خنثی دارد. در اینجا عنصر خنثی را با نماد $\circ$ نمایش خواهیم داد. بنابراین برای هر $a \in R$ داریم:

$$a + \circ = \circ + a = a\,.$$

اگر علاوه بر شرط های ۱، ۲ و ۳ تعریف حلقه، شرط زیر نیز برقرار باشد، آنگاه می‌گوییم R یک حلقه‌ی جابه‌جایی است.

۴. عمل ضرب جابه‌جایی باشد، به عبارت دیگر برای هر $a, b \in R$ داشته باشیم:

$$ab = ba\,.$$

همچنین اگر علاوه بر شرط‌های ۱، ۲ و ۳ شرط زیر نیز برقرار باشد، آنگاه می‌گوییم که R یک حلقه‌ی با عنصر همانی (یا یکه) است.

---

[1] Subgroup
[2] Ring

۵. R نسبت به ضرب همانی داشته باشد. در اینجا عنصر همانی R نسبت به عمل ضرب را با نماد ۱ نمایش می‌دهیم و آن را یکه‌ی R می‌نامیم. بنابراین برای هر $a \in R$ داریم:

$$1a = a1 = a\,.$$

اگر هر دو شرط ۴ و ۵ برای حلقه‌ی R برقرار باشند، آنگاه R را یک حلقه‌ی جابه‌جایی با یکه می‌نامیم.

تعریف ۴.۱.۱. فرض کنید R یک حلقه باشد. در این صورت زیرمجموعه‌ی S از R یک **زیرحلقه**[1] R است، اگر:

۱. S تحت اعمال جمع و ضرب R بسته باشد،

۲. S با اعمال القا شده از R خود یک حلقه باشد.

تعریف ۵.۱.۱. زیرمجموعه‌ی I از حلقه‌ی R یک **ایده‌آل**[2] است، اگر:

۱. I یک زیرگروه جمعی R باشد،

۲. برای هر $a \in R$ و $i \in I$ داشته باشیم:

$$ai, ia \in I\,.$$

۳. I را یک **ایده‌آل چپ**[3] R گویند، اگر به ازای هر $a \in R$ و هر $i \in I$، داشته باشیم: $ia \in I$.

۴. I را یک **ایده‌آل راست**[4] R گویند، اگر به ازای هر $a \in R$ و هر $i \in I$، داشته باشیم: $ai \in I$.

۵. I را یک **ایده‌آل (دوطرفه‌ی)** [5] R می‌گویند، اگر هم یک ایده‌آل چپ و هم یک ایده‌آل راست R باشد.

تعریف ۶.۱.۱. فرض کنیم X زیر مجموعه‌ای از یک حلقه‌ی R باشد. در این صورت اشتراک تمام ایده‌آل‌های R که شامل X باشند را **ایده‌آل تولید شده** توسط X نامند و آن را با $\langle X \rangle$ نمایش می‌دهند. عناصر X را مولدهای ایده‌آل $\langle X \rangle$ می‌نامند. اگر $X = \{x\}$، ایده‌آل $\langle X \rangle$ تولید شده توسط X را **ایده‌آل اصلی**[6] تولید شده توسط x می‌نامند. یک **حلقه‌ی ایده‌آل اصلی** حلقه‌ای است که در آن هر ایده‌آل، اصلی باشد.

---

[1] Subring
[2] Ideal
[3] Left ideal
[4] Right ideal
[5] Two-sided ideal
[6] Principal ideal

تعریف ۷.۱.۱. اگر I یک ایده‌آل از حلقه‌ی R باشند، R/I را **حلقه خارج‌قسمتی**[1] R بر I می‌نامیم و داریم:

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

تعریف ۸.۱.۱. یک ایده‌آل M در یک حلقه‌ی R را **ماکزیمال** گویند اگر $M \neq R$ باشد و به ازای هر ایده‌آل N در R اگر $M \subseteq N \subseteq R$ باشد، آنگاه داشته باشیم: $N = M$ یا $N = R$.

تعریف ۹.۱.۱. فرض کنید $(R, +, \cdot)$ و $(R, \oplus, \circ)$ دو حلقه باشند و $f : R \to R'$ تابع باشد. در این صورت f را یک **همریختی**[2] **(حلقه‌ای)** از R به R' گویند، اگر به ازای هر $a, b \in R$ داشته باشیم:

۱. $f(a + b) = f(a) \oplus f(b)$.

۲. $f(a \cdot b) = f(a) \circ f(b)$.

تعریف ۱۰.۱.۱. فرض کنید f یک همریختی از یک حلقه‌ی R به یک حلقه‌ی R' باشد. در این صورت **هسته** f عبارت است از:

$$\ker(f) = \{a \in R | f(a) = \circ\}.$$

تعریف ۱۱.۱.۱. فرض کنیم $f : R \to R'$ یک همریختی از یک حلقه‌ی R به یک حلقه‌ی R' باشد. در این صورت:

۱. f را یک **تکریختی (حلقه‌ای)** (مونومورفیسم) نامند اگر f یک‌به‌یک باشد.

۲. f را یک **برونریختی (حلقه‌ای)** (اتومورفیسم) گویند اگر f پوشا باشد.

۳. f را یک **یکریختی (حلقه‌ای)** (ایزومورفیسم) گویند اگر f هم یک‌به‌یک و هم پوشا باشد.
وقتی $f : R \to R'$ یک یکریختی حلقه ای باشد، گوییم که حلقه‌ی R با حلقه‌ی R' یکریخت است و می‌نویسیم $R \cong R'$.

۴. هر همریختی $f : R \to R$ را یک **درونریختی** از R می‌نامند.

۵. هر یکریختی $f : R \to R$ را یک **خودریختی**[3] از R می‌نامند.

تعریف ۱۲.۱.۱. فرض کنید $(R, +, \cdot)$ یک حلقه باشد. اگر یک کوچکترین عدد صحیح مثبت m وجود داشته باشد به طوری که به ازای هر $a \in R$، $ma = \circ$ باشد،گوییم R دارای **مشخصه‌ی** m است و اگر چنین عدد صحیح مثبتی وجود نداشته باشد،گوییم R دارای **مشخصه‌ی صفر** است. مشخصه‌ی یک حلقه‌ی R را با $\mathrm{Char}(R)$ نشان می‌دهیم.

[1] Quotient ring
[2] Homomorphism
[3] Automorphism

تعریف ۱.۱.۱۳. فرض کنیم R یک حلقه باشد. یک دنباله‌ی نامتناهی $(a_0, a_1, a_2, \dots, a_n, \dots)$ از عناصر R که در آن فقط تعداد متناهی از جملات غیر صفرند، را یک **چندجمله‌ای**[1] روی R می‌نامند. مجموعه‌ی تمام چندجمله‌ای‌های روی R را با $R[X]$ نشان می‌دهند.

تعریف ۱.۱.۱۴. فرض کنیم R یک حلقه باشد. جمع و ضرب را روی $R[X]$ چنین تعریف می‌کنیم. به ازای هر $\alpha = (a_0, a_1, \dots, a_n, \dots)$ و $\beta = (b_0, b_1, \dots, b_n, \dots)$،

$$\alpha + \beta = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_b, \dots) \quad \text{و} \quad \alpha \cdot \beta = (c_0, c_1, \dots, c_n, \dots)$$

باشد که در آن به ازای هر $k \in N$ (N_0 مجموعه اعداد صحیح نامنفی است)، $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. متذکر می‌شویم که $c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j$ که اغلب آن را به‌صورت $\sum_{i+j=k} a_i b_j$ می‌نویسیم.

مجموعه $R[X]$ به همراه جمع و ضرب فوق، تشکیل یک حلقه می‌دهد که آن را **حلقه چندجمله‌ای‌ها** روی R می‌نامند.

تعریف ۱.۱.۱۵. اگر $\alpha(x) = \sum_{i=0}^{n} a_i x^i \neq 0$، **درجه‌ی** α که آن را با $\deg(\alpha)$ نشان می‌دهیم چنین تعریف می‌شود: فرض کنید $a_n \neq 0$ در این صورت a_n را **ضریب پیشرو** چندجمله‌ای $\alpha(x)$ می‌نامیم و در این حالت n را درجه چندجمله‌ای $\alpha(x)$ گوییم. اگر $\alpha(x) = 0$ آنگاه تعریف می‌کنیم $\deg(\alpha) = -\infty$. در صورتی $\deg(\alpha) = -\infty$ یا 0 باشد، می‌گوییم که $\alpha(x)$ یک **چندجمله‌ای ثابت** است.

اگر ضریب پیشرو یک چندجمله‌ای برابر ۱ باشد، در این صورت آن **چندجمله‌ای را تکین** (مونیک) می‌نامیم. چندجمله‌ای تکینی با کمترین درجه که در چندجمله‌ای صدق می‌کند را چندجمله‌ای مینیمال گویند.

تعریف ۱.۱.۱۶. فرض کنیم R یک حلقه‌ی جابجایی باشد و $a, b \in R$ باشند، گوییم که b بر a **بخش‌پذیر** است یا a **عاد می‌کند** b را و می‌نویسیم $a|b$ اگر عنصری مانند $x \in R$ وجود داشته باشد به قسمی که $ax = b$. عناصر a و b از R را **وابسته** گویند اگر $a|b$ و $b|a$.

تعریف ۱.۱.۱۷. فرض کنید F یک مجموعه ناتهی از عناصر مجهز به دو عمل دوتایی جمع $(+)$ و ضرب $(.)$ باشد، در این صورت گوییم $(F, +, .)$ یک **میدان**[2] می‌باشد، هرگاه دارای شرایط زیر باشد: ۱. $(F, +)$ یک گروه آبلی باشد. ۲. $(F, .)$ یک گروه آبلی باشد. ۳. عمل ضرب نسبت به عمل جمع توزیع‌پذیر باشد، یعنی:

$$\forall a, b, c \in F \quad a \cdot (b + c) = a \cdot b + a \cdot c\,.$$

تعریف ۱.۱.۱۸. تعداد عناصر میدان را **مرتبه**[3] میدان گوییم. یک میدان با تعداد عناصر متناهی را یک **میدان متناهی**[4] می‌نامند.

[1] Polynomial
[2] Field
[3] Order
[4] Finite field

تعریف ۱.۱.۱۹. فرض کنید F یک میدان باشد، زیرمجموعه K از F که تحت اعمال F خود یک میدان باشد را یک **زیرمیدان** F می‌نامند. همچنین F را **توسیع میدان** K گویند.

تعریف ۱.۱.۲۰. فرض کنیم F یک میدان باشد و $f(X) \in F[X]$ باشد. یک عنصر $s \in F$ را یک **ریشه** از چندجمله‌ای $f(X)$ یا از f گویند، اگر $f(s) = ۰$ در این صورت می‌گویند s در معادله‌ی چندجمله‌ای $f(X)$ صدق می‌کند.

تعریف ۱.۱.۲۱. فرض کنید $\alpha(x) \in R[x]$ از درجه مثبت را **تحویل‌پذیر** روی میدان R گوییم هرگاه موجود باشند دو چندجمله‌ای $h(x)$ و $g(x)$ به گونه‌ای که $\deg(h), \deg(g) \leq \deg(\alpha)$ و $\alpha(x) = g(x) \cdot h(x)$، در غیر این صورت یعنی اگر $h(x)$ و $g(x)$ با ویژگی‌های فوق موجود نباشند آنگاه $\alpha(x)$ را **تحویل‌ناپذیر** روی میدان R می‌نامیم.

تعریف ۱.۱.۲۲. فرض کنید $\alpha : R \to R$ همریختی حلقه‌ای باشد. در این صورت **حلقه‌ی چندجمله‌ای‌های اریب**[1] $R[x;\alpha]$ به صورت زیر تعریف می‌شود:

$$R[x;\alpha] = \left\{ \sum_{i=۰}^{n} a_i x^i | a_i \in R, xr = \alpha(r),\ \forall r \in R \right\}.$$

در حلقه‌ی $R[x,\alpha]$ هر چندجمله‌ای به صورت $f(x) = \sum_{i=۰}^{n} a_i x^i$ را یک **چندجمله‌ای چپ** و هر چندجمله‌ای به صورت $g(x) = \sum_{i=۰}^{n} x^i a_i$ را یک **چندجمله‌ای راست** می‌نامیم.

تعریف ۱.۱.۲۳. فرض کنید $f(x), g(x) \in F[x]$ دو چندجمله‌ای دلخواه غیرصفر باشند.
بزرگترین مقسوم‌علیه مشترک $f(x)$ و $g(x)$ را با $\gcd(f(x), g(x))$ نمایش می‌دهند برابر است با چندجمله‌ای منحصر به فرد تکین با بیشترین درجه به طوری که $f(x)$ و $g(x)$ را عاد کند و اگر $f(x)$ و $g(x)$ نسبت به هم اول باشند، آنگاه $\gcd(f(x), g(x)) = ۱$ خواهد بود. همچنین **کوچکترین مضرب مشترک** $f(x)$ و $g(x)$ را با $\operatorname{lcm}(f(x), g(x))$ نمایش می‌دهند و برابر است با چندجمله‌ای منحصر به فرد تکین با کمترین درجه به طوری که $f(x)$ و $g(x)$ هردو آن را عاد می‌کنند.

تعریف ۱.۱.۲۴. یک گروه آبلی V به همراه عمل دوتایی جمع و ضرب 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**[2] روی $\mathbb{F}$ نامند اگر در شرایط زیر صدق کند:

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

(آ) $a(u+v) = au + av$.

(ب) $(a+b)v = av + bv$.

[1] Skew polynomial ring
[2] Vector space

۲. قانون شرکت‌پذیری بین $\mathbb{F}$ و V برقرار باشد. یعنی برای هر $a,b \in F$ و $u \in V$ داشته باشیم:

$$(ab)v = a(bv)\,.$$

۳. اگر ۱ عضو خنثی ضربی در $\mathbb{F}$ باشد، در این صورت برای هر $u \in V$ رابطه $u = u۱$ برقرار باشد.

تعریف ۱.۱.۲۵. 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 nـ تایی روی $\mathbb{F}_q$ می‌نامیم. q روش برای انتخاب هر a_i وجود دارد. بنابراین q^n، nـ تایی متفاوت موجود است. مجموعه $(\mathbb{F})_q^n$ همه nـ 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 ۱.۱.۲۶. یک زیر مجموعه از $\mathbb{F}_q^n$ یک **زیرفضای**[۱] $\mathbb{F}_q^n$ است هرگاه تحت عمل جمع و ضرب تعریف شده روی $\mathbb{F}_q^n$ یک فضای برداری باشد.

تعریف ۱.۱.۲۷. فرض کنید V یک فضای برداری روی $\mathbb{F}_q$ باشد و فرض کنید $S = \{v_۱, v_۲, \ldots, v_k\}$ زیرمجموعه‌ای ناتهی از V باشد. زیرفضای (خطی تولید شده توسط S) به شکل زیر تعریف می‌شود:

$$\langle S\rangle = \{\lambda_۱ v_۱ + \cdots + \lambda_k v_k | \forall i; \lambda_i \in \mathbb{F}_q\}\,.$$

اگر $S = \emptyset$ باشد، تعریف می‌کنیم: $\langle S\rangle = \{۰\}$.

تعریف ۱.۱.۲۸. فرض کنید V یک فضای برداری روی میدان $\mathbb{F}_q$ باشد، آنگاه زیرمجموعه غیرتهی مانند $B = \{v_۱, v_۲, \ldots, v_k\}$ از V را یک **پایه** برای V می‌نامیم هرگاه $V = \langle B\rangle$ و B یک مجموعه مستقل خطی باشد.

تعریف ۱.۱.۲۹. فرض کنید $u = (u_۱, u_۲, \ldots, u_n)$ و $r = \{r_۱, r_۲, \ldots, r_k\}$ دو عنصر از $\mathbb{F}_q^n$ باشند.

۱. **ضرب داخلی** (ضرب اقلیدسی) بردارهای u و v که با نماد $u \cdot r$ نمایش داده می‌شود:

$$u \cdot r = \sum_{i=۱}^{n} u_i r_i = u_۱ r_۱ + \cdots + u_n r_n \in \mathbb{F}_q\,.$$

۲. بردارهای u و r **را** متعامد گوییم هرگاه $u \cdot r = ۰$.

تعریف ۱.۱.۳۰. فضای برداری V روی میدان متناهی $\mathbb{F}_q$ می‌تواند چندین پایه داشته باشد، اما تعداد اعضای پایه‌ها با هم برابر است. این تعداد را **بُعد** V روی $\mathbb{F}_q$ می‌نامیم و با $\dim_{\mathbb{F}_q}(V)$ نشان می‌دهیم.

[۱] Subspace

تعریف ۳۱.۱.۱. فرض کنید S یک زیر مجموعه‌ی غیرتهی از $\mathbb{F}_q$ باشد، **دوگان**[1] S به صورت زیر تعریف می‌شود:

$$S^{\perp} = \{v \in \mathbb{F}_q^n : v \cdot s = ۰, \forall s \in S\}.$$

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

تعریف ۳۲.۱.۱. فرض کنید R یک حلقه بوده و $(M, +)$ یک گروه آبلی و $f : R \times M \to M$ 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.) همچنین خواص زیر برقرار باشند:

۱. به ازای هر $r \in R$ و $m_۱, m_۲ \in M$ داشته باشیم:

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

۲. به ازای هر $r_۱, r_۲ \in R$ و $m \in M$ داشته باشیم:

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

۳. به ازای هر $r_۱, r_۲ \in R$ و $m \in M$ داشته باشیم:

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

در این صورت M را یک **$\mathbf{R}$ـ مدول چپ** گویند. به طریق مشابه **$\mathbf{R}$ـ مدول راست** نیز تعریف می‌شود.

تعریف ۳۳.۱.۱. عنصر α در میدان متناهی $\mathbb{F}_q$ را **عنصر اولیه** می‌نامند، هرگاه داشته باشیم:

$$\mathbb{F}_q = \{۰, \alpha, \alpha^۲, \ldots, \alpha^{q-۱}\}.$$

تعریف ۳۴.۱.۱ (قضیه الگوریتم تقسیم اقلیدسی)**.** به ازای اعداد صحیح a و b که b مخالف صفر باشد، اعداد صحیح یکتایی مانند q و r موجودند به طوریکه $a = bq + r$ برای $۰ \leq r < b$ برقرار است.

تعریف ۳۵.۱.۱. ماتریس واندرموند[2] به ماتریسی گویند که دارای یک تصاعد هندسی در هر سطر به صورت زیر می‌باشد:

$$V = \begin{bmatrix} ۱ & \alpha_۱ & \alpha_۱^۲ & \ldots & \alpha_۱^{n-۱} \\ ۱ & \alpha_۲ & \alpha_۲^۲ & \ldots & \alpha_۲^{n-۱} \\ ۱ & \alpha_۳ & \alpha_۳^۲ & \ldots & \alpha_۳^{n-۱} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ ۱ & \alpha_m & \alpha_m^۲ & \ldots & \alpha_m^{n-۱} \end{bmatrix}$$

[1] Dual
[2] Vandermonde matrix

یا می‌توان گفت: $V_{ij} = \alpha_i^{j-1}$

این ماتریس، ضرایب یک چندجمله‌ای $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ را به مقدارهایی که چندجمله‌ای در نقطه α_i اتفاق بیفتد، تبدیل می‌کند.

۲.۱ مفاهیم مقدماتی لازم از نظریه کدگذاری

در این قسمت به مفاهیم اولیه از نظریه کدگذاری می‌پردازیم.

تعریف ۱.۲.۱. فرض کنید $A = \{a_1, a_2, \ldots, a_q\}$ یک مجموعه q عضوی باشد. در این 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 $W = w_1 w_2 \cdots w_n$ است که در آن، به ازای هر $1 \leq i \leq n$ ،$w_1 \in A$ به طور معادل، می‌توان W را به صورت بردار $(w_1, w_2, \ldots, w_n)$ در نظر گرفت.

۲. به مجموعه ناتهی C، متشکل از واژه‌های qتایی به طول n روی A، یک **کد بلوکی** qتایی به طول n روی A می‌گویند.در نتیجه، $C \subseteq A^n$ خواهد بود. گاهی اوقات، کد بلوکی qتایی C را کد qتایی یا به طور خلاصه‌تر کد می‌گویند.

۳. A^n را **فضای کد** و اعضای کد C را **کدواژه**[1] می‌نامند.

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

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

معمولاً میدان متناهی $\mathbb{F}$ را به عنوان الفبای کد درنظر 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)**[2] از x تا y که با $d(x, y)$ نمایش داده می‌شود، تعداد جایگاه‌هایی است که x و y با هم تفاوت دارند. به عبارت دیگر $x = x_1, x_2, \ldots, x_n$ و $y = y_1, y_2, \ldots, y_n$ آنگاه داریم:

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

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

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

[1] Code word
[2] Hamming distance

کد به طول n و فاصله d را (n, M, d)ـ کد می‌نامیم. به علاوه اعداد M، n 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.

تعریف ۶.۲.۱. فرض کنید α یک عنصر اولیه از میدان $\mathbb{F}_q^n$ باشد. در این صورت **چندجمله‌ای مینیمال** α^i نسبت به میدان $\mathbb{F}_q$ به صورت زیر می‌باشد:

$$M^{(i)}(x) = \prod_{j \in c_i} (x - \alpha^j)$$

جایی که c_i همدسته دایره بر منحصربه‌فرد است که به صورت زیر تعریف می‌شود:

$$c_i = \{i \cdot q^j \in \mathbb{Z}_n \mod n | j = ۰, ۱, ۲, \dots\}.$$

تعریف ۷.۲.۱. کد خطی[1] C از طول n روی $\mathbb{F}_q$ یک زیرفضا از $\mathbb{F}_q^n$ می‌باشد.

تعریف ۸.۲.۱. فرض کنید C یک کد خطی در $\mathbb{F}_q^n$ باشد. در این 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:

$$C^\perp = \{\alpha \in \mathbb{F}_q^n | \forall c \in C,\ \alpha \cdot c = ۰\}.$$

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

۳. کد C را یک **کد خود-دوگان**[2] گوییم هرگاه داشته باشیم: $C = C^\perp$.

تعریف ۹.۲.۱. فرض کنید زیرمجموعه غیر تهی S از $\mathbb{F}_q^n$ داده شده است. ابتدا ماتریس A را که سطرهای آن از کلمات S تشکیل می‌شود با استفاده از عملیات سطری مقدماتی به ماتریس تحویل شده پلکانی تبدیل می‌کنیم. فرض کنید G یک ماتریس $k \times n$ است که شامل تمام سطرهای غیر صفر بدست آمده در ماتریس سطری پلکانی تحویل شده A باشد یعنی

$$A \to \begin{pmatrix} G \\ ۰ \end{pmatrix}$$

[1] Linear code
[2] Self dual code

ماتریس G شامل k ستون اصلی می‌باشد. با جابجایی 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 در آن X^T ترانهاده X می‌باشد. حال معکوس جایگشت‌هایی که برای ستون‌های G به کار بردیم را برای ستون‌های H' استفاده می‌کنیم تا ماتریس H حاصل شود.

ماتریس مولد[1] کد خطی C ماتریس G است که سطرهای آن یک پایه برای کد C تشکیل می‌دهند. **ماتریس کنترل توازن**[2] H برای کد خطی C ماتریس مولدی برای کد دوگان C است که سطرهای آن پایه ای برای کد $C^\perp$ می‌باشند.

تعریف ۱.۲.۱۰. ماتریس مولدی به شکل $(I_k|X)$، **ماتریس مولد به استاندارد** گفته می‌شود. ماتریس کنترل توازن به شکل $(Y|I_{n-k})$ **ماتریس کنترل توازن به شکل استاندارد** گفته می‌شود.

تعریف ۱.۲.۱۱. فرض کنید C یک کد خطی به طول n و بعد k باشد و $\{r_1, r_2, \ldots, r_k\}$ 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 $\{r_1, r_2, \ldots, r_k\}$ انتخاب شده است. برای بردار $u = (u_1, u_2, \ldots, u_k) \in \mathbb{F}_q^n$ 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 $u \in \mathbb{F}_q^n$ است. جریان نمایش اعضای $u \in \mathbb{F}_q^n$ به صورت کدواژه‌های $v = uG$ در C، **کدگذاری** کدخطی نامیده می‌شود.

تعریف ۱.۲.۱۲. کد خطی C به طول n روی $\mathbb{F}_q$ را یک **کد دوری**[3] گوییم هر شیفت دوری از کدواژه‌های کد C، خود نیز کدواژه‌ای از کد C باشد. به عبارت دیگر، اگر $(c_0, c_1, \ldots, c_{n-1}) \in C$ آنگاه داشته باشیم $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. 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.

[1] Generator code
[2] Parity check matrix
[3] Cyclic code

تعریف ۱.۲.۱. فرض کنید α یک عنصر اولیه از میدان $\mathbb{F}_q^m$ و $M^{(i)}(x)$ چندجمله‌ای مینیمال α^i نسبت به میدان $\mathbb{F}_q$ باشد. دراین صورت یک **کد BCH** روی میدان $\mathbb{F}_q$ از طول $n = q^m - ۱$ و با فاصله طراحی شده δ، یک کد دوری qـ تایی با چندجمله‌ای مولد
$g(x) = lcm\ (M^{(a)}(x), M^{(a+۱)}(x), \ldots, M^{(a-\delta-۲)}(x)$ برای یک عدد صحیح a می‌باشد.

تعریف ۱.۲.۱. هر کد $[n, k, d]$ـ کدخطی که پارامترهای در شرط $k + d = n + ۱$ صدق کند یک **کد MDS** می‌باشد.

تعریف ۱.۲.۱. یک **کد q ـ تایی RS** یا رید ـ سالومون[1] یک کد qـ تایی BCH از طول $q - ۱$ و با چندجمله‌ای مولد $g(x) = (x - \alpha^{a+۱}) \ldots (x - \alpha^{a+\delta-۱})$ می‌باشد که $a \geq ۰$ و $۲ \leq \delta \leq q - ۲$ جایی که α عنصری اولیه از میدان $\mathbb{F}_q$ می‌باشد.

[1] Reed-Solomon

فصل ۲

کلیات حلقه‌های چندجمله‌ای اریب

در این فصل ما حلقه‌های چندجمله‌ای اریب روی یک میدان را مورد مطالعه قرار می‌دهیم. این حلقه‌ها اولین بار توسط اور[1] مورد بررسی و مطالعه قرار گرفت و پس از آن در شاخه‌های مختلفی از جمله نظریه کدگذاری مورد استفاده قرار گرفتند. ما بیان مختصری از نتایج نظری حلقه را تا جایی که آن‌ها برای بررسی‌های بعدی ما درباره کدهای دوری اریب مهم هستند، بیان خواهیم کرد.

۱.۲ خصوصیات اصلی حلقه‌های چندجمله‌ای اریب

تعریف ۱.۱.۲. فرض کنید F یک میدان و $\sigma \in \mathrm{Aut}(F)$ باشد. حلقه چندجمله‌ای اریب $F[x;\sigma]$ به صورت $\{\sum_{i=0}^{N} f_i x^i | N \in \mathbb{N}_0, f_i \in F\}$ با عمل جمع معمولی و قاعده ضربی زیر تعریف می‌شود:

$$xa = \sigma(a)x \tag{۱.۲}$$

که برای هر $a \in F$ همراه با قوانین توزیع‌پذیری و شرکت‌پذیری برقرار است. لذا $(F[x;\sigma],+,\cdot)$ یک حلقه با عنصر همانی $x^0 = 1$ است. عناصر آن چندجمله‌ای‌های اریب یا به طور ساده چندجمله‌ای نامیده می‌شوند.

اگر $\sigma = id$ آنگاه $F[x;\sigma] = F[x]$، حلقه چندجمله‌ای معمولی روی میدان F است. ما از این مورد خاص به عنوان قضیه جابه‌جایی و چندجمله‌ای‌های جابه‌جایی استفاده می‌کنیم. در

[1] Ore

حالت کلی گروه‌های جمعی $F[x;\sigma]$ و $F[x]$ یکسان هستند در حالی که ضرب در حلقه چند جمله‌ای‌های اریب $F[x;\sigma]$ از رابطه زیر به دست می‌آید:

$$\left(\sum_{i=0}^{N} f_i x^i\right)\left(\sum_{j=0}^{M} g_j x^j\right) = \sum_{i,j} f_i \sigma^i(g_j) x^{i+j}.$$

توجه داشته باشید که مجموعه چندجمله‌ای‌های اریب ممکن است به صورت $\{\sum_{i=0}^{N} x^i f_i | N \in \mathbb{N}_0, f_i \in F\}$ نیز نوشته شوند، یعنی ضرایب در سمت راست نوشته شود. تنها قانونی که باید از آن پیروی کنیم استفاده کردن از σ است وقتی که می‌خواهیم ضرایب x را از راست به چپ جابه‌جا کنیم و بنابراین σ^{-1} برای جهت دیگر است. همیشه چندجمله‌ای‌ها را به صورت $\sum_{i=0}^{N} f_i x^i$ خواهیم نوشت یعنی ضرایب همیشه در سمت چپ x در نظر گرفته می‌شوند. در نتیجه، ضریب پیشرو از یک چندجمله‌ای همان ضریب پیشرو چپ آن است. توجه داشته باشید که $F[x;\sigma]$ یک فضای برداری چپ و راست روی F است. اما این دو ساختار فضای برداری یکسانی نیستند.

ملاحظه ۱.۱.۲. حلقه‌های چندجمله‌ای اریب معمولاً با کلیت بیشتری معرفی و مطالعه می‌شوند. ممکن است فردی ضریب میدان F را توسط یک جبر تقسیمی یا حتی حلقه ناجابه‌جایی جایگزین کند، ممکن است درونریختی حلقه‌ای σ را به جای خودریختی در نظر بگیرد و فردی ممکن است یک σـ مشتق تعریف کند، مثلاً δ که در این صورت رابطه (۱.۲) به $xa = \sigma(a)x + \delta(a)$ تبدیل شود. همه این‌ها در مباحث حلقه‌های چندجمله‌ای اریب استاندارد هستند. در این پایان‌نامه ما از حلقه‌های چندجمله‌ای اریب در تعریف ۱.۱.۲ استفاده می‌کنیم. در حالی که در مقاله [۶] مثال‌هایی آورده شده است که نشان می‌دهد استفاده از تعریف σـ مشتق می‌تواند کدهای دوری اریب با مینیمم فاصله بهتری از آنچه که می‌توان با کمک یک اتومورفیسم بدست آورد.

ملاحظه ۲.۱.۲. حلقه چندجمله‌ای اریب $F[x;\sigma]$ را در نظر بگیرید و فرض کنید $K \subseteq F$ میدان ثابت‌های F از σ باشد. اگر σ دارای مرتبه متناهی m باشد، مرکز $F[x;\sigma]$ توسط حلقه چندجمله‌ای جابه‌جایی $K[x^m]$ به‌دست می‌آید. این به راحتی با استفاده از این واقعیت که هر f در مرکز موجب $xf = fx$ و $af = fa$ برای هر $a \in F$ دیده می‌شود. اگر σ دارای مرتبه نامتناهی باشد، K مرکز است.

مثال ۱.۱.۲. میدان $\mathbb{C}$ از اعداد مختلط را در نظر بگیرید و σ مزدوج مختلط باشد. پس مرکز $\mathbb{C}[x;\sigma]$ حلقه چندجمله‌ای جابه‌جایی $\mathbb{R}[x^2]$ است. علاوه بر این، $\mathbb{R}[x]$ یک زیرحلقه از $\mathbb{C}[x;\sigma]$ و $\mathbb{C}[x]$ است که نشان می‌دهد یک حلقه چندجمله‌ای اریب ممکن است یک زیرحلقه از حلقه‌های چندجمله‌ای اریب با اتومورفیسم‌های مختلف باشد.

در ادامه ما خودمان را به حلقه‌های چندجمله‌ای اریب روی میدان‌های متناهی محدود می‌کنیم. حالت زیر کاملاً همه حالت‌ها را پوشش می‌دهد، چون هر اتومورفیسم یک توان از

اتومورفیسم فروبینیوس در میدان اول است. به طور کلی، اتومورفیسم $\mathbb{F}_q m \to \mathbb{F}_q m$ داده شده توسط $c \to c^q$ است ک به سادگی qـ فروبینیوس[1] نامیده می‌شود.

مثال ۲.۱.۲. حلقه چندجمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ را در نظر بگیرید جایی که $\mathbb{F} = \mathbb{F}_q m$ و σ یک خودریختی qـ فروبینیوس باشد. پس σ از مرتبه m و $\mathbb{F}_q$ میدان ثابت‌ها و مرکز $\mathbb{F}[x;\sigma]$، $\mathbb{F}_q[x^m]$ است.

در ادامه به بیان چند نمادگزاری استاندارد در $F[x;\sigma]$ می‌پردازیم.

تعریف ۲.۱.۲. درجه چندجمله‌ای اریب مطابق معمول بزرگترین توان از x که در چندجمله‌ای وجود دارد تعریف می‌شود و $\deg(\circ) := -\infty$. این به جایی که ضرایب را در کدام سمت قرار می‌دهیم بستگی ندارد زیرا σ یک اتومورفیسم است و داریم:

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\},\ \deg(fg) = \deg(f) + \deg(g).$$

در نتیجه، گروه یکه‌ها از $F[x;\sigma]$، توسط $F^* = F \setminus \{\circ\}$ به دست می‌آید. یک چندجمله‌ای ناصفر، تکین است اگر ضریب پیشرو آن ۱ باشد. باز هم، این به مکان ضرایب بستگی ندارد زیرا $\sigma(1) = 1$. می‌گوییم g یک مقسوم علیه راست از f است و می‌نویسیم $g|_r f$ اگر $f = hg$ برای $h \in F[x;\sigma]$ برقرار باشد. یک چندجمله‌ای $f \in F[x;\sigma]\backslash F$ تحویل‌ناپذیر است اگر همه مقسوم‌علیه‌های راست آن (از این رو) یکه باشند یا چندجمله‌ای‌هایی از درجه f باشند. واضح است که چندجمله‌ای‌های از درجه ۱ تحویل‌ناپذیر هستند.

مثال ۳.۱.۲. فرض کنید $F = \mathbb{F}_4 = \{\circ, 1, \omega, \omega^2\}$ جایی که $\omega^2 = \omega + 1$ و σ خودریختی ۲ـ فروبینیوس باشد. در این صورت $\sigma = \sigma^{-1}$. در $\mathbb{F}_4[x;\sigma]$ داریم:

۱.

$$x^2 + 1 = (x+1)(x+1) = (x+\omega^2)(x+\omega) = (x+\omega)(x+\omega^2)$$

بنابراین ممکن است یک چندجمله‌ای اریب دارای عامل‌های خطی بیشتری نسبت به درجه‌ای که دارد باشد.

۲.

$$(x^2 + \omega x + \omega)(x+\omega) = x^3 + \omega^2 x + \omega^2$$

و بنابراین $x+\omega$ یک مقسوم‌علیه راست از $x^3 + \omega^2 x + \omega^2$ است. آن یک مقسوم‌علیه چپ نیست. این به راحتی با استفاده از محاسبات و مقایسه ضرایب آن‌ها با $x^3 + \omega^2 x + \omega^2$ مشاهده می‌شود:

$$(x+\omega)(f_2 x^2 + f_1 x + f_\circ) = f_2^2 + f_1 x + f_\circ) = f_2^2 x^3 + (\omega f_2 + f_1^2)x^2 + (\omega f_1 + f_\circ^2)x + \omega f_\circ.$$

[1] Frobenius

همان‌طور که برای چندجمله‌ای‌های جابه‌جایی، اگر جایگاه ضرایب را در محاسبه در نظر بگیریم، می‌توان مقسوم علیه آن‌ها در $F[x;\sigma]$ محاسبه کرد. اثبات کاملاً مشابه حالت جابه‌جایی است. در واقع اگر $\deg(f)=m\geq\deg(g)=\ell$ و ضرایب پیشرو از f و g به ترتیب f_m و g_ℓ باشند آنگاه چندجمله‌ای $f-f_m\sigma^{m-\ell}(g_\ell^{-1})x^{m-\ell}g$ دارای درجه کمتر از m می‌باشد. این اجازه می‌دهد تا آنجا که یک باقی‌مانده از درجه کمتر از ℓ به دست آید، ادامه یابد.

قضیه ۱.۱.۲. حلقه چندجمله‌ای‌های اریب $F[x;\sigma]$ یک دامنه اقلیدسی چپ و همچنین یک دامنه اقلیدسی راست است. به بیان دقیق‌تر داریم:

الف) مقسوم‌علیه راست: برای هر $f,g\in F[x;\sigma]$ و $g\neq 0$ چندجمله‌ای‌های منحصربه‌فرد s,r در $F[x;\sigma]$ موجودند به طوری که $f=sg+r$ و $\deg(r)<\deg(g)$. اگر $r=0$ آنگاه g یک مقسوم‌علیه راست از f است.

ب) برای چندجمله‌ای‌های ناصفر $f_1,f_2\in\mathcal{R}$، یک چندجمله‌ای تکین منحصربه‌فرد $d\in F[x;\sigma]$ موجود است به طوری که $d|_r f_1$ و $d|_r f_2$ و هرگاه $h\in F[x;\sigma]$ موجود باشد که $h|_r f_1$ و $h|_r f_2$ برقرار باشد آنگاه $h|_r d$. چندجمله‌ای d را بزرگترین مقسوم علیه راست مشترک f_1 و f_2 نامیده و با $\operatorname{gcrd}(f_1,f_2)$ نمایش داده می‌شود. در واقع همچنین d در تساوی بزو[1] راست صدق می‌کند، به این معنا که $d=uf_1+vf_2$ برای u,v در حلقه $F[x;\sigma]$ برقرار است.

ممکن است u و v را به گونه‌ای انتخاب کنیم که $\deg(u)<\deg(f_2)$ و $\deg(v)<\deg(f_1)$ باشد. این یک نتیجه از الگوریتم تقسیم اقلیدسی (تعریف ۳۵.۱.۱ را ببینید) است. اگر $d=1$، f_1 و f_2 را نسبت به هم اول‌ـراست[2] می‌نامیم.

ج) برای چندجمله‌ای‌های ناصفر f_1 و f_2 در حلقه چندجمله‌ای اریب $F[x;\sigma]$، یک چندجمله‌ای تکین منحصربه فرد $\ell\in F[x;\sigma]$ وجود دارد به طوری که $f_i|_r h,\ i=1,2$ و هرگاه $h\in F[x;\sigma]$ موجود باشد که $f_i|_r h,\ i=1,2$ برقرار باشد، آنگاه $\ell|_r h$. چندجمله‌ای ℓ را کوچکترین مضرب چپ مشترک f_1 و f_2 نامیده و با $\operatorname{lclm}(f_1,f_2)$ نمایش داده می‌شود. علاوه براین، $u,v\in F[x;\sigma]$ وجود دارند به گونه‌ای که $\ell=uf_1+vf_2$ با $\deg(u)<\deg(f_2)$ و $\deg(v)<\deg(f_1)$.

د) برای دو چندجمله‌ای ناصفر f_1 و f_2 در حلقه چندجمله‌ای اریب $F[x;\sigma]$ داریم:

$$\deg\left(\operatorname{grcd}(f_1,f_2)\right)+\deg\left(\operatorname{lclm}(f_1,f_2)\right)=\deg(f_1)+\deg(f_2).$$

بیان مشابه برای حالت چپ نیز صدق می‌کند.

[1] Bezout
[2] Relatively right-prime

دقیقاً مشابه حالت جابه‌جایی، مطلب فوق منجر به قضیه زیر می‌شود:

قضیه ۲.۱.۲. فرض کنید $I \subseteq F[x;\sigma]$ یک ایده‌آل چپ باشد در این صورت I ایده‌آل اصلی است. برای راحتی از نماد $(f)^\bullet$ برای نمایش ایده‌آل چپ تولید شده توسط f یعنی $F[x;\sigma]f$ استفاده خواهیم کرد. بیان مشابه برای ایده‌آل راست نیز درست است. بنابراین حلقه چندجمله‌ای اریب $F[x;\sigma]$ یک حلقه ایده‌آل اصلی چپ و یک حلقه ایده‌آل اصلی راست می‌باشد.

با توجه به تعریفی که از مرکز حلقه چندجمله‌ای‌های اریب $F[x;\sigma]$ داشتیم (ملاحظه ۲.۱.۲ را ببینید)، واضح است که برای هر چندجمله‌ای f در مرکز حلقه، ایده‌آل چپ اصلی $(f)^\bullet$ ایده‌آل دوطرفه است یعنی یک ایده‌آل چپ و یک ایده‌آل راست. چندجمله‌ای‌هایی که ایده‌آل‌های دوطرفه را تولید می‌کنند با عناصر مرکزی رابطه دارند.

تعریف ۳.۱.۲. فرض کنید σ دارای مرتبه m باشد. عنصر $f \in F[x;\sigma]$ را دوطرفه گوییم اگر ایده‌آل $(f)^\bullet$ ایده‌آلی دو طرفه باشد، یعنی $(f)^\bullet = {}^\bullet(f)^\bullet$.

قضیه ۳.۱.۲. عناصر دوطرفه از حلقه چندجمله‌ای‌های اریب $F[x;\sigma]$ دقیقاً چندجمله‌ای‌هایی به صورت $\{cx^tg | c \in F, t \in \mathbb{N}, g \in Z\}$ هستند جایی که، $Z = K[x^m]$ مرکز $F[x;\sigma]$ می‌باشد. در حالت خاص، برای هر $a \in F^*$، چندجمله‌ای $x^n - a$ دوطرفه است اگر و تنها اگر مرکزی باشد.

با توجه به بسیاری از خواصی که تاکنون بیان شده است، حلقه چندجمله‌ای‌های اریب $F[x;\sigma]$ مانند حلقه چندجمله‌ای‌های جابه‌جایی $F[x]$ رفتار می‌کند. با این وجود، تفاوت اصلی $F[x;\sigma]$ در $\sigma \neq id$ می‌باشد که چندجمله‌ای‌های با عامل منحصربه‌فرد به چندجمله‌ای‌های تحویل‌ناپذیر تبدیل نمی‌شوند.

تعریف ۴.۱.۲. فرض کنید f و g چند جمله‌ای‌هایی در حلقه چند جمله‌ای‌های اریب $F[x;\sigma]$ باشند. در این صورت موارد زیر معادل هستند:

۱. $h, k \in F[x;\sigma]$ وجود دارند به طوری که $\gcrd(f,h) = ۱$ و $\gcld(g,k) = ۱$ و $gh = kf$.

۲. $h \in F[x;\sigma]$ وجود دارد به طوری که $\gcrd(f,h) = ۱$ و $\lclm(f,h) = gh$.

۳. $F[x;\sigma]$ـ مدول‌های چپ $F[x;\sigma]/{}^\bullet(f)$ و $F[x;\sigma]/{}^\bullet(g)$ یکریخت هستند.

اگر ۱ برقرار باشد، بنابراین ۲ و ۳ صدق می‌کنند و چندجمله‌ای‌های f و g را متشابه می‌نامند. در حلقه جابه‌جایی $F[x]$، دو چندجمله‌ای متشابه هستند اگر و تنها اگر آن‌ها در یک عامل ثابت تفاوت داشته باشند. به طور کلی، چندجمله‌ای‌های متشابه دارای درجه یکسانی هستند (قضیه ۱.۱.۲ (د) را ببینید). قسمت ۳ نشان می‌دهد که تشابه در واقع یک رابطه هم‌ارزی در $F[x;\sigma]$ بوده و به یک طرفه بودن بستگی ندارد، یعنی f و g راست متشابه هستند اگر و تنها اگر چپ متشابه باشند. قسمت ۳ مفهوم تشابه برای ایده‌آل چپ می‌باشد که توسط

کوهن[1] معرفی و مورد بحث قرار گرفته است، منجر به یک قاعده ساده برای تشابه شده است که در ادمه ارائه خواهیم داد.

برای چندجمله‌ای تکین $f = \sum_{i=۰}^{n-۱} f_i x^i + x^n \in F[x;\sigma]$ ماتریس همراه[2] به صورت زیر تعریف می‌شود:

$$C_f = \begin{pmatrix} & ۱ & & & \\ & & \ddots & & \\ & & & ۱ & \\ & & & & ۱ \\ -f_۰ & -f_۱ & \dots & -f_{n-۲} & -f_{n-۱} \end{pmatrix} \in \mathrm{Mat}_{n,n}(F). \qquad (۲.۲)$$

نگاشت L_x را در نظر بگیرید که توسط ضرب چپ x در $F[x,\sigma]$ـ مدول چپ $\mathcal{M}_f := F[x;\sigma]/{}^{\bullet}(f)$ به‌دست می‌آید. این نگاشت σـ نیمه‌خطی می‌باشد یعنی $L_x(at) = \sigma(a)L_x(t)$ برای هر $a \in F$ و $t \in \mathcal{M}_f$ برقرار است. از این گذشته، سطرهای C_f بردارهای ضربی $L_x(x^i)$ برای $i = ۰,\dots,n-۱$ هستند. همه این‌ها نشان می‌دهند که $L_x(\sum_{i=۰}^{n-۱} a_i x^i) = \sum_{i=۰}^{n-۱} b_i x^i$ جایی که

$$(b_۰,\dots,b_{n-۱}) = (\sigma(a_۰),\dots,\sigma(a_{n-۱}))C_f \ .$$

به این معنا که C_f نمایش ماتریسی از نگاشت نیمه‌خطی L_x نسبت به پایه $\{۱, x, \dots, x^{n-۱}\}$ است.

اگر g چندجمله‌ای تکین دیگری از درجه n باشد، آنگاه هر دوی $\mathcal{M}_f$ و $\mathcal{M}_g$ روی F مدول‌هایی n بعدی هستند و بنابراین Fـ فضای برداری یکریخت است. $F[x;\sigma]$ـ مدول‌های چپ یکریخت هستند اگر بتوانیم یک ایزومورفیسم $F[x;\sigma]$ـ خطی چپ را پیدا کنیم.

گزاره ۱.۱.۲. فرض کنید f, g چندجمله‌ای‌های تکین از درجه n در حلقه چند جمله‌ای‌های اریب $F[x;\sigma]$ باشند. f و g متشابه هستند اگر و تنها اگر وجود داشته باشد یک ماتریس $B \in GL_n(F)$ به طوری که $C_g = \sigma(b)C_f B^{-۱}$.

قضیه ۴.۱.۲. فرض کنید $f_۱,\dots,f_r,g_۱,\dots,g_s$ چندجمله‌ای‌های تحویل‌ناپذیر در حلقه چند جمله‌ای‌های اریب $F[x;\sigma]$ باشند به طوری که $f_۱\dots f_r = g_۱\dots g_s$. در این صورت $r = s$ و جایگشت π از $\{۱,\dots,r\}$ وجود دارد به طوری که $g_{\pi(i)}$ با f_i برای هر $i = ۱,\dots,r$ متشابه باشد و $\forall i \quad \deg(f_i) = \deg(g_{\pi(i)})$.

توجه داشته باشید که معکوس قضیه بالا درست نیست. فرض کنید چندجمله‌ای‌های تکین $f_i, g_i,\ i = ۱,۲$ به طوری که f_i و g_i متشابه هستند اما $f_۱f_۲$ و $g_۱g_۲$ متشابه نیستند (و بنابراین مطمعناً برابر نیستند).

[1] Cohn
[2] Companion Matrix

مثال ۴.۱.۲. حلقه چند جمله‌ای‌های اریب $\mathbb{F}_۴[x;\sigma]$ را در مثال ۳.۱.۲ در نظر بگیرید. در قسمت (۱) دیدیم $x^۲+۱=(x+\omega)(x+\omega^۲)$ می‌باشد. ضرب راست عامل اول توسط $\omega^۲$ و ضرب چپ عامل دوم توسط ω حاصلضرب را تغییر نمی‌دهد و بنابراین:

$$x^۲+۱=(x+\omega)(x+\omega^۲)=(\omega x+۱)(\omega x+۱).$$

در نتیجه دو تجزیه از $x^۲+۱$ در چندجمله‌ای‌های خطی داریم. در تجزیه اول دو عامل نسبت به هم اول‌ـراست هستند، دو عامل تجزیه دوم همانی هستند. در تجزیه اول عامل‌های خطی، تکین هستند در حالی که در تجزیه دوم آن‌ها نرمال شده هستند به طوری که ضرایب ثابت آن‌ها ۱ است. با انتخاب $\pi=id$ ، $h_۱=\omega$ و $h_۲=\omega x$ می‌توان درستی قضیه ۳.۱.۲ را بررسی کرد.

یکی از مهمترین نتایج در تجزیه چندجمله‌ای‌های اریب، چندجمله‌ای‌های کاملاً تحویل‌پذیرند، یعنی چندجمله‌ای‌هایی وجود دارند که کوچکترین مضرب مشترک چپ از چندجمله‌ای‌های تحویل‌ناپذیر هستند و بنابراین چندجمله‌ای‌های جابه‌جایی بدون توان دوم را تعمیم می‌دهد.

۲.۲ چندجمله‌ای‌های اریب و چندجمله‌ای‌های خطی

در این بخش رابطه بین حلقه‌های چندجمله‌ای اریب و حلقه‌ای از چندجمله‌ای‌های خطی روی میدان‌های متناهی را بررسی می‌کنیم. حلقه‌های چندجمله‌ای‌های خطی نقش مهمی در مطالعه کدهای رتبه متریک[1] ایفا می‌کند.

حلقه چندجمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ را در نظر بگیرید جایی که $\mathbb{F}=\mathbb{F}_q m$ و σ خودریختی qـفروبینیوس است، (مثال ۲.۱.۲ را ببینید). در حلقه چندجمله‌ای جابه‌جایی $\mathbb{F}[y]$ زیرمجموعه زیر را تعریف می‌کنیم:

$$\mathcal{L}:=\mathcal{L}_{q^m,q}:=\left\{\sum_{i=۰}^{N} f_i y^{q^i} \mid N\in\mathbb{N}_۰, f_i\in\mathbb{F}\right\}.$$

چندجمله‌ای‌های از این نوع qـخطی نامیده می‌شوند چون برای هر $f\in\mathcal{L}$ تابع متناظر $\mathbb{F}\to\mathbb{F}, a\mapsto f(a)$ وجود دارد که $\mathbb{F}_q$ـخطی است و $(\mathcal{L},+,\circ)$ یک حلقه ناجابه‌جایی است جایی که $+$ جمع معمولی و $\circ$ ترکیب چندجمله‌ای‌ها است. به طور واضح حلقه‌های $\mathbb{F}[x;\sigma]$ و $\mathcal{L}$ یکریخت هستند. واضح است که نگاشت

$$\Lambda:\mathbb{F}[x;\sigma]\to\mathcal{L},\quad \sum_{i=۰}^{N} g_i x^i\mapsto\sum_{i=۰}^{N} g_i y^{q^i} \tag{۱.۲}$$

یک حلقه ایزومورفیسم بین $\mathbb{F}[x;\sigma]$ و $\mathcal{L}$ است. کافی است همریختی حلقه‌ای Λ را نشان دهیم که برای هر $a,b\in\mathbb{F}$ و $i,j\in\mathbb{N}$ از تساوی زیر نتیجه می‌شود:

$$\Lambda(ax^i bx^j)=\Lambda(a\sigma^i(b)x^{i+j})=\Lambda(ab^{q^i}x^{i+j})=ab^{q^i}y^{q^{i+j}}=ay^{q^i}\circ by^{q^j}.$$

[1] Rank-metric codes

$\mathcal{L}$ همه ویژگی‌های چند جمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ که در بخش قبل ارائه شده را به ارث می‌برد و همچنین چندجمله‌ای $y^{q^m}-y\in\mathcal{L}$ نگاشت صفر را در $\mathbb{F}=\mathbb{F}_q m$ القا می‌کند لذا تصویر آن نسبت به Λ چندجمله‌ای $x^m-۱$ است، که در مرکز $\mathbb{F}[x;\sigma]$ قرار دارد، (مثال ۲.۱.۲ را ببینید). بنابراین ایده‌آل چپ تولید شده توسط $y^{q^m}-y$ دوطرفه است و لذا حلقه خارج‌قسمتی $\mathcal{L}/(y^{q^m}-y)$ را ایجاد می‌کند. از آنجا که حلقه دوم دارای اندازه $q^{m^۲}$ می‌باشد، نشان می‌دهد که حلقه خارج‌قسمتی آن یکریخت با فضای همه نگاشت‌های $\mathbb{F}_q$ـ‌خطی در $\mathbb{F}_q m$ هستند، بنابراین:

$$\mathbb{F}[x;\sigma]/(x^m-۱)\cong\mathcal{L}/(y^{q^m}-y)\cong \mathrm{Mat}_{m,m}(\mathbb{F}_q).$$

واضح است، نگاشت دوم توسط $g+(y^{q^m}-y)\mapsto [g]_B^B$، جایی که $[g]_B^B$ بیانگر ماتریس نمایش نگاشت g نسبت به پایه B از $\mathbb{F}_q m$ به $\mathbb{F}_q$، داده شده است. پایه $B=(b_۰,\dots,b_{m-۱})$ در نظر بگیرید و ماتریس مور[1] $S=\left(b_j^{q^i}\right)_{i,j=۰}^{m-۱}$ را تعریف کنید. از استقلال خطی $b_۰,\dots,b_{m-۱}$ نتیجه می‌گیریم که S در $GL_m(\mathbb{F}_q)$ قرار دارد. علاوه بر این، برای هر $g=\sum_{i=۰}^{m-۱}g_i y^{q^i}$ داریم $S[g]_B^B S^{-۱}=D_g$ جایی که

$$D_g=\begin{pmatrix} g_۰ & g_۱ & \cdots & g_{m-۲} & g_{m-۱}\\ g_{m-۱}^q & g_۰^q & \cdots & g_{m-۳}^q & g_{m-۲}^q\\ \vdots & \vdots & & \vdots & \vdots\\ g_۱^{q^{m-۱}} & g_۲^{q^{m-۱}} & \cdots & g_{m-۱}^{q^{m-۱}} & g_۰^{q^{m-۱}}\end{pmatrix} \tag{۲.۲}$$

ماتریس دیکسون[2] g است. این ماتریس همچنین qـ‌دوری و مفهوم ماتریس دوری معمولی را تعمیم می‌دهد. با استفاده از ایزومورفیسم‌های فوق می‌توان ماتریس دیکسون $g\in\mathbb{F}[x;\sigma]$ را به صورت $D_g:=D_{\Lambda(g)}$ تعریف کرد به طوری که حلقه ایزومورفیسم زیر به دست می‌آید:

$$\mathbb{F}[x;\sigma]/(x^m-۱)\to\mathrm{Mat}_{m,m}(\mathbb{F}_q),\quad g+(x^m-۱)\mapsto D_g. \tag{۳.۲}$$

توجه داشته باشید که i^{th} سطر از D_g توسط بردار ضریب $x^i g\in\mathbb{F}[x;\sigma]$ با تجزیه به پیمانه $x^m-۱$ از طریق مقسوم علیه راست به دست می‌آید. چندجمله‌ای‌های خطی و هسته آن‌ها نقش مهمی در مطالعه مرتبه فاصله ایفا می‌کنند.

۳.۲ ارزیابی چندجمله‌ای‌های اریب و ریشه‌ها

در این بخش مروری بر ارزیابی چندجمله‌ای‌های اریب بر حسب عناصر میدانی و ریشه‌های چندجمله‌ای‌های اریب ارائه می‌دهیم. اور در مقاله اصلی خود این مفاهیم را تعریف نکرده

[1] Moore matrix
[2] Dickson matrix

است. آن‌ها در حقیقت بعداً در سال ۱۹۸۶ توسط لام[1] تعریف شدند و این مطالب و بخش بعدی از اثر لام و لروی [2] (مراجع [۲۴] ، [۲۵] ، [۲۶] ، [۲۷]) گرفته شده است.

در این بخش حلقه چندجمله‌ای‌های اریب $F[x;\sigma]$ مد نظر ماست. چندجمله‌ای $f=\sum_{i=0}^{N} f_i x^i \in F[x;\sigma]$ را در نظر بگیرید. واضح است اگر $\sigma \neq id$، مفهوم معمول ارزیابی f در یک نقطه $a \in F$، به عبارت دیگر $f(a)=\sum_{i=0}^{N} f_i a^i$ به خوبی تعریف نشده است چون x با عناصر میدان جابه‌جا نمی‌شود. به عنوان مثال، برای چندجمله‌ای $f=bx=x\sigma^{-1}(b)$ که σ بر b اعمال نمی‌شود، جایگزین کردن عنصر ناصفر a به جای x منجربه تضاد در $ba=a\sigma^{-1}(b)$ می‌شود.

برای رفع این موضوع با نیاز به آن که ضرایب در سمت چپ باشند با جایگزین کردن a به جای x مشکل را حل نمی‌کند زیرا آن منجربه باقی‌مانده خوب نمی‌شود. به عنوان مثال، $f=x^3+\omega \in \mathbb{F}_4[x;\sigma]$ جایی که $\mathbb{F}_4[x;\sigma]$ مانند مثال ۳.۱.۲ است. با جایگزین کردن ω به جای x، ω^2 را خواهیم داشت و بنابراین ω ریشه نیست. با این حال نشان می‌دهد که $x-\omega$ یک مقسوم‌علیه راست (و یک مقسوم‌علیه چپ) از f است.

تعریف ۱.۳.۲. فرض کنید $f \in F[x;\sigma]$ و $a \in F$ باشد. $f(a)=r$ را تعریف می‌کنیم جایی که $r \in F$ باقی‌مانده تقسیم راست f توسط $x-a$ می‌باشد. به عبارت دیگر، $g \in F[x;\sigma]$ موجود است به طوری که $f=g\cdot(x-a)+r$. اگر $f(a)=0$ آنگاه a را ریشه‌ای (راست) از f می‌نامیم. بنابراین a ریشه f است اگر و تنها اگر $(x-a)|_r f$.

مثال ۱.۳.۲. چندجمله‌ای $(x+\alpha^2)(x-\alpha) \in \mathbb{F}_8[x;\sigma]$ جایی که $\alpha^3+\alpha+1=0$ و σ یک خودریختی ۲ـ فروبینیوس است، فقط ریشه α را در $\mathbb{F}_8$ دارد. گسترش σ به خودریختی ۲ـ فروبینیوس در $\mathbb{F}_{8^2}$ منجربه ۲ ریشه اضافی از $f \in \mathbb{F}_{8^2}[x;\sigma]$ در $\mathbb{F}_{8^2}\backslash\mathbb{F}_8$ می‌شود.

تعریف ۲.۳.۲. برای هر $i \in \mathbb{N}_0$ تعریف کنید $N_i : F \to F$ به طوری که $N_0(a)=1$ و برای $i>0$ داشته باشیم $N_i(a)=\prod_{j=0}^{i-1}\sigma^j(a)$. N_i را نرم i^{th} در F می‌نامیم. بنابراین $N_1(a)=a$ و $N_{i+1}(a)=N_i(a)\sigma^i(a)$ برای هر $a \in F$ برقرار است.

برای $\mathbb{F}=\mathbb{F}_{q^m}$ و σ خودریختی qـ فروبینیوس N_m نرم میدان $\mathbb{F}$ روی $\mathbb{F}_q$ است. توجه داشته باشید که در حالت جابه‌جایی یعنی $\sigma=id$، داریم $N_i(a)=a^i$ و بنابراین گزاره زیر ارزیابی چندجمله‌ای‌های جابه‌جایی را تعمیم می‌دهد.

گزاره ۱.۳.۲. فرض کنید $f=\sum_{i=0}^{N} f_i x^i \in F[x;\sigma]$ و $a \in F$ باشد. در این صورت:

$$f(a)=\sum_{i=0}^{N} f_i N_i(a).$$

[1] Lam
[2] Leroy

اکنون مفهومی از ریشه‌ها را برای چندجمله‌ای‌های اریب $f \in F[x;\sigma]$ داریم و ریشه‌های مرتبط به چندجمله‌ای خطی $\Lambda(f)$ که در بخش ۲ معرفی شده است، در حقیقت چندجمله‌ای‌های جابه‌جایی هستند و بنابراین مفهوم معمولی از ریشه‌ها به کار برده می‌شود.

ملاحظه ۱.۳.۲. حلقه چند جمله‌ای‌های اریب $F[x;\sigma] = \mathbb{F}[x;\sigma]$ را در مثال ۲.۱.۲ در نظر بگیرید و فرض کنید $g \in \mathbb{F}[x;\sigma]$ و $\Lambda(g) \in \mathbb{F}[y]$ مانند رابطه ۱.۲ باشند. توجه داشته باشید که $\Lambda(g)(\circ)$ همیشه صفر است.

الف) برای هر q و $b \in \mathbb{F}^*$ رابطه زیر بین ریشه‌های g و $\Lambda(g)$ برقرار است:

$$g(b^{q-1}) = \circ \Leftrightarrow \Lambda(g)(b) = \circ .$$

به منظور بررسی این موضوع برای هر $\alpha \in \mathbb{F}_q$ از $\Lambda(g)(b) = \circ$ نتیجه می‌گیریم $\Lambda(g)(\alpha b) = \circ$ بدین معنی که چندجمله‌ای خطی $y^q - b^{q-1}y$ یک مقسوم‌علیه از $\Lambda(g)$ در $(\mathbb{F}[y], +, \cdot)$ است. اما همچنین یک مقسوم‌علیه از $\Lambda(g)$ در حلقه $(\mathcal{L}, +, \circ)$ است، یعنی $G \in \mathcal{L}$ وجود دارد به طوری که $\Lambda(g) = G \circ (y^q - b^{q-1}y)$. استفاده از حلقه هوموورفیسم Λ^{-1} نشان می‌دهد که $x - b^{q-1}$ یک مقسوم‌علیه راست از g است. موارد فوق بیان می‌کند که برای $q = 2$ مجموعه ناصفر ریشه‌های $\Lambda(g)$ با مجموعه ریشه‌های ناصفر g برابر است.

ب) اگر $q \neq 2$، ریشه‌های g با ریشه‌های $\Lambda(g)$ برابر نیستند. برای بررسی این مطلب، به عنوان مثال $a \in \mathbb{F}_{q^m}$ ناصفر وجود دارد به طوری که $g = x - a$ را در نظر بگیرید. لذا a ریشه راست و چپ g است. چندجمله‌ای خطی مرتبط با g ، $\Lambda(g) = y^q - ay = y(y^{q-1} - a)$ است و ممکن است ریشه ناصفر داشته یا نداشته باشد. برای مثال، اگر $\mathbb{F}_{q^m} = \mathbb{F}_{32}$ باشد معادله $y^2 = a$ دارای دو ریشه متمایز برای ۴ مقدار a (مربعی ناصفر) و ریشه ای برای ۴ مقدار دیگر a ندارد. اختلاف بین ریشه‌های چندجمله‌ای‌های اریب و ریشه‌های چندجمله‌ای‌های خطی است. البته، همچنین مربوط به این واقعیت است که ضرب $\mathcal{L}$ ترکیب است در حالی که یک ریشه c در مفهوم عادی با عامل $y - c$ متناظر است (که حتی یک چندجمله‌ای خطی هم نیست).

رابطه‌ای واضح بین ریشه‌های راست چندجمله‌ای‌های اریب روی یک میدان متناهی و ریشه‌های چندجمله‌ای‌های جابه‌جایی متناظر مختلف وجود دارد. دوباره مانند مثال ۲.۱.۲ حلقه چندجمله‌ای اریب $\mathbb{F}[x;\sigma]$ را در نظر بگیرید. در این صورت نرم i^{th} توسط رابطه زیر به دست می‌آید:

$$N_i(a) = a^{q^\circ + q^1 + \cdots + q^{i-1}} = a^{[[i]]}; \qquad [[i]] := \frac{q^i - 1}{q - 1} \quad . \tag{۱.۲}$$

با توجه به گزاره ۱.۳.۲ می‌توان ارزیابی چندجمله‌ای‌های اریب را به ارزیابی چندجمله‌ای‌های جابجایی تبدیل کنیم.

ملاحظه ۲.۳.۲. نگاشت زیر را تعریف کنید:

$$\mathbb{F}[x;\sigma] \to \mathbb{F}[y]\,, \quad \sum_{i=0}^{n} f_i x^i \mapsto P_f := \sum_{i=0}^{n} f_i y^{[[i]]} \in \mathbb{F}[y].$$

در این صورت $f(a) = P_f(a)$.

متاسفانه، نگاشت $f \mapsto P_f$ روی ضرب به خوبی عمل نمی‌کند و بنابراین نتیجه فوق کاربرد محدودی دارد.
فرض کنید با یک میدان دلخواه F به حالت کلی برگردیم. با تعریف و تعیین ارزیابی چندجمله‌ای‌ها، ممکن است فردی ویژگی‌های نگاشت زیر را مطالعه کند:

$$\mathrm{ev}_a : F[x;\sigma] \to F, \quad f \mapsto f(a).$$

به وضوح، این نگاشت جمعی و Fـخطی چپ است، اما برخلاف حالت جابه‌جایی، نگاشت مورد نظر ضربی نمی‌باشد. به عنوان یک کران از این نگاشت غیرضربی توجه داشته باشید که $f = x - a$ در $f(a) = 0$ صدق می‌کند، در حالی که برای هر $b \in \mathbb{F}$ داریم $(fb)(a) \neq 0$ که σ روی b اعمال نمی‌شود. با این حال، ارزیابی به ضربی بودن نزدیک است. قبل از اینکه بتوانیم این موضوع را دقیق بیان کنیم به تعریف زیر نیاز داریم.

تعریف ۳.۳.۲. فرض کنید $a \in F$ باشد. برای $c \in F^*$ تعریف می‌کنیم $a^c := \sigma(c)ac^{-1}$.
$a, b \in F$ را σمزدوج گوییم هرگاه $c \in F^*$ موجود باشد به طوری که $b = a^c$. کلاس σـمزدوج a به صورت $\Delta(a) = \{a^c | c \in F^*\}$ تعریف می‌شود.
چون در سراسر پایان‌نامه اتومورفیسم مد نظر است پیشوند σ را حذف می‌کنیم. برای مثال، برای $c = -1 \in F$، نماد a^c معرف معکوس a نیست. در حقیقت $a^c = a$. به طور کلی، برای هر $c \in F^*$ داریم $a^{-c} = a^c$.

به راحتی می‌توان دید که مزدوج، یک رابطه هم‌ارزی را تعریف می‌کند و $\Delta(0) = \{0\}$ و اگر $\sigma = id$ آنگاه برای هر $a \in F$ داریم $\Delta(a) = \{a\}$. همچنین اگر $a \neq 0$ آنگاه $a^c = a$ اگر و تنها اگر c در میدانی ثابت از σ باشد. روابط مزدوج برای هر $a \neq b$ از هم‌ارزی

$$b = a^c \Leftrightarrow (x - b)c = \sigma(c)(x - a)$$

و همانی زیر ناشی می‌شود:

$$\mathrm{lclm}(x - a, x - b) = (x - b^{b-a})(x - a) = (x - a^{a-b})(x - b) \qquad (۲.۲)$$

مزدوج بالا بیان می‌کند که عامل‌های خطی می‌توانند مرتب شوند. به علاوه یک حالت خاص از گزاره ۱.۳.۲ داریم: $x - a$ و $x - b$ در مفهوم تعریف ۱.۱.۲ متشابه هستند اگر و تنها اگر a و b مزدوج باشند.

مثال ۲.۳.۲. الف) برای هر میدان متناهی $F=\mathbb{F}_{q^m}$ با σ خودریختی qـ فروبینیوس و همانی $a^c=c^{q-1}a$، داریم که کلاس‌های مزدوج ناصفر توسط همدسته‌های $\Delta(1)=\{c^{q-1}|c\in F^*\}$ در F^* به دست می‌آیند. بنابراین برای $q=2$ کلاس‌های مزدوج $\{0\}$ و $\Delta(1)=F^*$ هستند. در حالیکه برای $q=3$ دو کلاس مزدوج ناصفر وجود دارد، یکی از مربع‌های F^* و دیگری از غیرمربع‌ها تشکیل شده‌اند.
ب) برای $\mathbb{C}$ با مزدوج مختلط، کلاس‌های مزدوج ناصفر دقیقاً حلقه‌هایی مربوط به مبدأ هستند.

ملاحظه ۳.۳.۲. در حالتی که $F=\mathbb{F}_{q^m}$ و σ خودریختی qـ فروبینیوس است، کلاس‌های مزدوج ناصفر دارای اندازه $(q^m-1)/(q-1)$ هستند. این همچنین نشان می‌دهد که q تا کلاس مزدوج وجود دارد (شامل $\{0\}$).

قضیه ۱.۳.۲. فرض کنید $f,g\in F[x;\sigma]$ و $a\in F$ باشند. در این صورت:

$$(fg)(a)=\begin{cases}0 & g(a)=0\\ f(a^{g(a)})g(a) & g(a)\neq 0\end{cases}.$$

اگر a ریشه‌ای از fg باشد اما ریشه g نباشد، آنگاه مزدوج $a^{g(a)}$ ریشه f است.

قبلاً دیدیم که ممکن است تعداد ریشه‌های یک چندجمله‌ای اریب از درجه‌اش بیشتر باشد. به هر حال، محاسبه مزدوج، تعمیم زیر را در حالت جابه‌جایی ارائه می‌دهد.

قضیه ۲.۳.۲. فرض کنید $f\in F[x;\sigma]$ دارای درجه N باشد. در این صورت ریشه‌های f در حداکثر N کلاس مزدوج متمایز قرار دارند. علاوه بر این اگر برای $a_i\in F$ و $f(a)=0$ داشته باشیم $f=(x-a_1)\dots(x-a_N)$ آنگاه a مزدوج بعضی از a_iها می‌باشد.

توجه داشته باشید که برای $F=\mathbb{F}_{q^m}$ با $q=2$، قضیه صدق نمی‌کند، چون در این حالت فقط یک کلاس مزدوج وجود دارد. همچنین نشان می‌دهد که عکس قضیه ۱.۳.۲ درست نیست: همه مزدوج‌های a_iها ریشه f نمی‌باشد. (به عنوان مثال $N=1$ را در نظر بگیرید.)
همچنین قضیه فوق بیان نمی‌کند که هر کلاس مزدوج $\Delta(a_i)$ شامل یک ریشه از f است. در واقع به طور کلی این گونه نیست و مثالی را می‌توان در حلقه چندجمله‌ای‌های اریب $\mathbb{Q}(t)[x;\sigma]$ یافت، جایی که σ خودریختی $\mathbb{Q}$ـ جبری است توسط $t\mapsto t+1$ به دست می‌آید.

قضیه ۳.۳.۲. حلقه چندجمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ را مانند مثال ۲.۱.۲ در نظر بگیرید و فرض کنید $a_i\in\mathbb{F}^*$ وجود دارد به طوری که $f=(x-a_1)\dots(x-a_N)$. در این صورت هر کلاس مزدوج $\Delta(a_i)$ شامل یک ریشه از f است.

اثبات: کافی است نشان دهیم $\Delta(a_1)$ شامل یک ریشه از f است، به این معنی که $b_1,\dots,b_{N-1}$ و $c\in\mathbb{F}^*$ وجود دارند به طوری که $f=(x-b_1)\dots(x-b_{N-1})(x-a_1^c)$ است. چون $(a^{c_1})^{c_2}=a^{c_1c_2}$ حالت $N=2$ کافی است. فرض کنید برای $a,b\in\mathbb{F}^*$ داریم $f=(x-b)(x-a)$. اگر $a\in\Delta(b)$

چیزی برای اثبات وجود ندارد. بنابراین فرض کنید $a \notin \Delta(b)$. حال فرض کنید $c \in \mathbb{F}^*$. از قضیه ۱.۳.۲ نتیجه می‌گیریم $f(b^c) = \left((b^c)^{b^c-a} - b\right)(b^c - a)$ و بنابراین $f(b^c) = 0$ اگر و تنها اگر $(b^c)^{b^c-a} = b$. به راحتی می‌توان دید که قسمت دوم معادل $\sigma(\sigma(c)b - ac) = \sigma(c)b - ac$ است، که معادل $\sigma(c)b - ac \in \mathbb{F}_q$ می‌باشد. بنابراین باید وجود $c \in \mathbb{F}^*$ به طوری که $\sigma(c)b - ac \in \mathbb{F}_q$ را اثبات کنیم. نگاشت $\mathbb{F}_q$ـخطی $\Psi_{a,b} : \mathbb{F} \to \mathbb{F},\ c \mapsto \sigma(c)b - ac$ را در نظر بگیرید. اگر بتوانیم نشان دهیم که $\Psi_{a,b}$ یک به یک است آنگاه پوشا می‌باشد و اثبات تمام است. فرض کنید $d \in \ker \Psi_{a,b} \backslash \{0\}$ وجود دارد در این صورت $\sigma(d)b - ad = d^q b - ad = 0$، بنابراین $d^{q-1} = a/b$. اما از سوی دیگر

$(a/b)^{[[m]]} = (d^{q-1})^{[[m]]} = d^{q^m-1} = 1$. این نشان می‌دهد که $\Psi_{a,b}$ یک‌به‌یک است اگر $(a/b)^{[[m]]} \neq 1$. از سوی دیگر، اگر $(a/b)^{[[m]]} = 1$ آنگاه $t \in F^*$ مرتبه a/b، مقسوم‌علیه $[[m]]$ است. علاوه بر این، برای k و عنصر اولیه ω داریم $a/b = \omega^{k(q^m-1)/t}$. قرار می‌دهیم $ts = [[m]]$ و نتیجه می‌گیریم $a/b = (\omega^{ks})^{q-1}$. اما این بدین معنی است که a و b مزدوج هستند که یک تناقض است.

یک استدلال مشابه نشان می‌دهد که نتیجه قبلی در حلقه چندجمله‌ای‌های اریب $\mathbb{C}[x;\sigma]$ با σ مختلط مزدوج نیز صدق می‌کند. ■

فصل ۳

مجموعه‌های جبری و چندجمله‌ای‌های ودربرن

در این فصل با معرفی چندجمله‌ای‌های مینیمال و مجموعه‌های جبری، و ارائه برخی از خصوصیات آن‌ها، تئوری ریشه‌های راست چندجمله‌ای‌های اریب را بررسی می‌کنیم. در سرتاسر این فصل، حلقه چندجمله‌ای اریب $F[x;\sigma]$ مد نظر ما می‌باشد.

۱.۳ مجموعه‌های جبری و ریشه‌های چندجمله‌ای‌های اریب

تعریف ۱.۱.۳. برای چندجمله‌ای $f \in F[x;\sigma]$، مجموعه ریشه‌های راست f در F با $V(f)$ نشان داده می‌شود؛ بنابراین $V(f) = \{a \in F | f(a) = 0\}$ و $V(f)$ را مجموعه صفر f می‌نامیم. زیرمجموعه $A \subseteq F$، σـ جبری نامیده می‌شود به شرطی که چند جمله ای ناصفر $f \in F[x;\sigma]$ وجود داشته باشد، به گونه ای که $A \subseteq V(f)$؛ یعنی، f بر روی A صفر می‌شود. در این حالت، چندجمله‌ای تکین با کوچکترین درجه، مثل f، به گونه‌ای که $A \subseteq V(f)$ توسط A به شکلی منحصر به فرد تعیین شده و چندجمله‌ای σـ مینیمال A می‌شود که با m_A نشان داده می‌شود. درجه m_A، σـ مرتبه A نامیده شده که با $\mathrm{rk}(A)$ نشان داده می‌شود.

این بخش را با بحث راجع به مجموعه‌های صفر $V(f)$ برای چندجمله‌ای‌های داده شده شروع می‌کنیم. ابتدا توجه داریم که برای هر $f,g,h \in F[x;\sigma]$ داریم:

$$V(f) \subseteq V(g) \Rightarrow V(fh) \subseteq V(gh). \qquad (۱.۳)$$

در نگاه اول، مفهوم ممکن است دور از ذهن به نظر برسد، زیرا $V(f)$ مجموعه ریشه‌های راست را نشان می‌دهد. با این وجود، به راحتی می‌توان نشان داد که این موضوع نتیجه ساده‌ای از قضیه ۱.۳.۲ می‌باشد. از طرف دیگر، عبارت مشابه با عامل‌های چپ h در حالت کلی درست نیست؛ یعنی، $f,g,h \in F[x;\sigma]$ وجود دارند به گونه‌ای که

$$V(f) \subseteq V(g) \quad \text{و} \quad V(hf) \nsubseteq V(hg).$$

مثال ۱.۱.۳. $\mathbb{F}_۴[x;\sigma]$ از مثال ۳.۱.۲ را در نظر بگیرید. فرض کنید $f = h = x + ۱$ و $g = x^۲ + \omega^۲ x + \omega$. سپس به راحتی می‌توان بررسی کرد که $V(f) = \{۱\} = V(g)$. در مثال ۳.۱.۲ (۱)، دیده‌ایم که $hg = x^۳ + \omega^۲ x^۲ + \omega$. با این حال، $V(hf) = \{۱, \omega, \omega^۲\}$ فقط یک ریشه ۱ دارد.

حال به مجموعه‌های جبری باز می‌گردیم. بدیهی است که در حالت جابه‌جایی، به عبارتی، وقتی $\sigma = id$، مجموعه‌های جبری قطعاً مجموعه‌های متناهی هستند. طبق آنچه درست بعد از تعریف ۱.۳.۲ برای $\mathbb{C}[x;\sigma]$ جایی که σ مزدوج مختلط باشد دیدیم، این مسئله در مورد چندجمله‌ای‌های اریب صدق نمی‌کند. طبق رابطه (۲.۲)، این‌گونه استنباط می‌کنیم که هر مجموعه $A = \{a, b\}$ با اندازه ۲، دارای مرتبه ۲ است، در صورتی که از مثال ۳.۱.۲ قسمت (۱) مجموعه‌ای با اندازه ۳ و مرتبه ۲ به دست می‌آید. به‌طور کلی، مجموعه متناهی $A = \{a_۱, \ldots, a_n\}$ دارای چندجمله‌ای مینیمال $m_A = \operatorname{lclm}(x - a_۱, \ldots, x - a_n)$ است. با استفاده از استنباط مربوط به اندازه و فرمول درجه در قضیه ۱.۱.۲ (د)، بلافاصله گزاره زیر بدست می‌آید.

گزاره ۱.۱.۳. فرض کنید $A = \{a_۱, \ldots, a_n\} \subseteq F$. در این صورت، A یک مجموعه جبری است و $\operatorname{rk}(A) := r \leq |A|$. به علاوه، $b_۱, \ldots, b_r \in A$ متمایزی وجود دارند، به گونه‌ای که

$$m_A = \operatorname{lclm}(x - b_۱, \ldots, x - b_r)\,.$$

مثال ۲.۱.۳. فرض کنید $A = \mathbb{F}_{p^r}$ که p عدد اول و $r \in \mathbb{N}$ است. در این صورت داریم $m_A = \operatorname{lclm}(x - a | a \in \mathbb{F}_{p^r}) = x^{r(p-۱)+۱} - x$. بنابراین، $\operatorname{rk}(\mathbb{F}_{p^r}) = r(p-۱) + ۱$.

مثال ۳.۱.۳. فرض کنید $\mathbb{F}_{q^s}$ میدان توسیع $\mathbb{F} = \mathbb{F}_{q^m}$ باشد و $\mathbb{F}_{q^s}[x;\sigma]$ با σ خودریختی qـ فروبینیوس را درنظر بگیرید. یک عنصر $a \in \mathbb{F}_{q^s}$ را در نظر گرفته و قرار دهید $A = \{\tau(a) | \tau \in \operatorname{Aut}(\mathbb{F}_{q^s} | \mathbb{F}_{q^m})\}$. در این صورت چندجمله‌ای مینیمال m_A در $\mathbb{F}[x;\sigma]$ قرار دارد و چندجمله‌ای تکین غیرصفر با کوچکترین درجه در $\mathbb{F}[x;\sigma]$ با ریشه راست a می‌باشد که چندجمله‌ای σـ مینیمال a بر روی $\mathbb{F}$ نامیده می‌شود.

چندجمله‌ای مینیمال یک مجموعه جبری همیشه به عامل خطی تجزیه می‌شود. نتیجه زیر به حالت جابه‌جایی نزدیک‌ترین می‌باشد.

گزاره ۲.۱.۳. فرض کنید $A \subseteq F$ یک مجموعه جبری مرتبه r باشد. در این صورت، چندجمله‌ای مینیمال A به صورت $m_A = (x-a_1)\dots(x-a_r)$ است جایی که هر a_i مزدوج $a \in A$ می‌باشد.

با توجه به گزاره فوق لازم نیست ریشه‌های عامل‌های خطی در A قرار داشته باشند.

مثال ۴.۱.۳. الف) حلقه چند جمله‌ای‌های اریب $\mathbb{F}_{۳۳}[x;\sigma]$ با σ خودریختی ۳ـ فروبینیوس و عنصر اولیه β را در نظر بگیرید که در رابطه $\beta^۳ + ۲\beta + ۱ = ۰$ صدق می‌کند. فرض کنید $A = \{\beta^{۱۴}, \beta^{۲۵}\}$. در این صورت:

$$m_A = x^۲ + \beta x + \beta = (x-\beta^{۱۳})(x-\beta^{۱۴}) = (x-\beta^۲)(x-\beta^{۲۵})$$

و از این رو m_A حاصل‌ضرب ۲ عامل خطی می‌باشد که ریشه‌های این عامل‌ها در A قرار ندارند. با کمک مثال ۲.۳.۲، به این نتیجه می‌رسیم که $\beta^{۱۳}$ مزدوج $\beta^{۲۵}$ و $\beta^۲$ مزدوج $\beta^{۱۴}$ است. در نهایت، $A = V(m_A)$؛ یعنی m_A ریشه‌های بیشتری در $\mathbb{F}_{۳۳}$ ندارد.

ب) عوامل خطی $x - a_i$ در گزاره ۲.۱.۳ لازم نیست متمایز باشند. به‌طور مثال، حلقه چند جمله‌ای‌های اریب $\mathbb{F}_{۲۴}[x;\sigma]$ با σ خودریختی ۲ـ فروبینیوس و عنصر اولیه γ را در نظر بگیرید که در رابطه $\gamma^۴ + \gamma + ۱ = ۰$ صدق می‌کند. چندجمله‌ای زیر

$$f = (x-\gamma^۲)(x-\gamma^{۱۲})(x-\gamma^۲) = (x-\gamma^۳)(x-\gamma^{۱۴})(x-\gamma^{۱۴}) = x^۳ + \gamma^۷x^۲ + \gamma^۳x + \gamma$$

چندجمله‌ای مینیمال $A = \{۱, \gamma^۲, \gamma^۳, \gamma^۶, \gamma^۸, \gamma^{۱۳}, \gamma^{۱۴}\}$ یعنی $V(f) = A$ است. برای شرح گزاره ۱.۱.۳ رابطه $f = \mathrm{lclm}(x-۱, x-\gamma^۲, x-\gamma^۳)$ را عنوان می‌کنیم که نشان می‌دهد مجموعه $B = \{۱, \gamma^۲, \gamma^۳\}$ جبری است، اما مجموعه صفر محسوب نمی‌شود: هر چندجمله‌ای که برروی B صفر است در $\mathbb{F}_{۲۴}$ دارای ریشه‌های اضافی می‌باشد. از طرف دیگر، $f \neq \mathrm{lclm}(x-۱, x-\gamma^۲, x-\gamma^۸)$. چندجمله‌ای دوم از رابطه $g = x^۲ + \gamma^۵x + \gamma^{۱۰}$ به دست آمده است.

مرتبه مجموعه جبری متناهی را می‌توان از طریق نسخه اریب ماتریس معمولی واندرموند، تعیین نمود. ماتریس واندرموند اریب توسط لام معرفی شده است. برای $a_1, \dots, a_r \in F$، ماتریسی در $\mathrm{Mat}_{n,r}(F)$ می‌باشد که به صورت زیر تعریف شده است:

$$V_n^\sigma(a_1,\dots,a_r) := V_n(a_1,\dots,a_r) = \begin{pmatrix} ۱ & \dots & ۱ \\ N_۱(a_1) & \dots & N_۱(a_r) \\ \vdots & & \vdots \\ N_{n-۱}(a_1) & \dots & N_{n-۱}(a_r) \end{pmatrix}. \qquad (۲.۳)$$

ماتریس واندرموند اریب به σ وابسته است (زیرا نرم‌ها این‌گونه هستند). گزاره ۱.۳.۲ نشان می‌دهد که برای $g=\sum_{i=۰}^{n-۱} g_i x^i \in F[x;\sigma]$، داریم

$$(g(a_۱),\dots,g(a_r))=(g_۰,\dots,g_{n-۱})V_n^{\sigma}(a_۱,\dots,a_r).$$

با استفاده از رابطه (۱.۲) به این نتیجه می‌رسیم که برای حلقه چندجمله‌ای اریب $\mathbb{F}[x;\sigma]$ جایی که σ خودریختی qـ فروبینیوس است ماتریس واندرموند اریب، توان‌های $x^{[[۰]]}, x^{[[۱]]},\dots,x^{[[n-۱]]}$ را در $a_۱,\dots,a_r$ ارزیابی می‌کند. این ماتریس نبایستی با ماتریس مور $a_۱,\dots,a_r$ اشتباه گرفته شود که توان‌های $x^{q^۰}, x^{q^۱},\dots,x^{q^{n-۱}}$ را در $a_۱,\dots,a_r$ ارزیابی می‌کند (به مثال ۶.۱.۳ زیر یا بخش ۲.۲ نیز نگاه کنید).

قضیه ۱.۱.۳. فرض کنید $A=\{a_۱,\dots,a_n\}\subseteq F$ باشد. در این صورت $\mathrm{rk}(A)=\mathrm{rk}(V_n(a_۱,\dots,a_n))$. در نتیجه، اگر $\mathrm{rk}(A)=|A|$ (چنین مجموعه‌ای Pـ مستقل نامیده می‌شود)، آنگاه برای هر زیرمجموعه $B\subseteq A$ داریم $\mathrm{rk}(B)=|B|$.

مثال ۵.۱.۳. الف) حلقه‌ی چندجمله‌ای‌های اریب $\mathbb{C}[x;\sigma]$ ، جایی که σ مزدوج مختلط می‌باشد، را در نظر بگیرید. فرض کنید $A=\{a_۱,\dots,a_n\}\subseteq\mathbb{C}$ که $a_۱,\dots,a_n$ همگی برابر نیستند و $|a_۱|=\cdots=|a_n|=:c$. در این صورت برای هر i، رابطه $N_۲(a_i)=a_i\sigma(a_i)=c^۲$ برقرار می‌باشد. لذا $V_n(a_۱,\dots,a_n)$ از مرتبه ۲ است و با $m_A=x^۲-c^۲=(x+a_i)(x-\overline{a_i})$ سازگاری دارد.

ب) مثال ۴.۱.۳ قسمت (ب) را در نظر بگیرید. در نتیجه

$$V_۳(۱,\gamma^۲,\gamma^۸)=\begin{pmatrix}۱ & ۱ & ۱\\ ۱ & \gamma^۲ & \gamma^۸\\ ۱ & \gamma^۶ & \gamma^۹\end{pmatrix}$$

دارای مرتبه ۲ است و با این موضوع سازگاری دارد که $\mathrm{lclm}(x-۱,x-\gamma^۲,x-\gamma^۸)$ از درجه ۲ می‌باشد.

مثال ۶.۱.۳. حلقه‌ی چندجمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ را مانند مثال ۲.۱.۲ در نظر بگیرید. فرض کنید $\gamma\in\mathbb{F}_{q^m}$ به‌گونه‌ای باشد که $\{\gamma,\sigma(\gamma),\dots,\sigma^{m-۱}(\gamma)\}$ پایه نرمال $\mathbb{F}_{q^m}$ بر روی $\mathbb{F}_q$ باشد قرار دهید $b=\sigma(\gamma)\gamma^{-۱}=\gamma^{q-۱}$. به راحتی می‌توان دید که $N_i(\sigma^j(b))=\sigma^j(\gamma^{-۱})\sigma^{i+j}(\gamma)$، یعنی برای هر $j=۰,\dots,m-۱$ ، $\sigma^j(b)$ ریشه راست $x^m-۱\in\mathbb{F}[x;\sigma]$ می‌باشد. علاوه بر این،

$$V_m(b,\sigma(b),\dots,\sigma^{m-۱}(b))\begin{pmatrix}\gamma & & & \\ & \sigma(\gamma) & & \\ & & \ddots & \\ & & & \sigma^{m-۱}(\gamma)\end{pmatrix}=\begin{pmatrix}\gamma & \sigma(\gamma) & \dots & \sigma^{m-۱}(\gamma)\\ \sigma(\gamma) & \sigma^۲(\gamma) & \dots & \sigma^m(\gamma)\\ \vdots & \vdots & & \vdots\\ \sigma^{m-۱}(\gamma) & \sigma^m(\gamma) & \dots & \sigma^{۲m-۲}(\gamma)\end{pmatrix}.$$

ماتریس سمت راست، ماتریس مور $\{\gamma, \sigma(\gamma), \dots, \sigma^{m-1}(\gamma)\}$ است (به بخش ۲.۲ نگاه کنید). به دلیل استقلال خطی $\gamma, \sigma(\gamma), \dots, \sigma^{m-1}(\gamma)$ بر روی $\mathbb{F}_q$، ماتریس مور وارون‌پذیر است و از این رو، با توجه به مطالب بیان شده در بالا و قضیه ۱.۱.۳ داریم:

$$x^m - 1 = \mathrm{lclm}(x-b, x-\sigma(b), \dots, x-\sigma^{m-1}(b)) \ .$$

توجه داشته باشید که ریشه ۱ راست $x^m - 1$ در $b, \sigma(b), \dots, \sigma^{m-1}(b)$ قرار ندارد. قضیه ۱.۱.۳ همچنین نشان می‌دهد برای هر زیرمجموعه $\{j_1, \dots, j_r\} \subseteq \{0, \dots, m-1\}$، چندجمله‌ای $\mathrm{lclm}(x-\sigma^{j_1}(b), \dots, x-\sigma^{j_r}(b))$ دارای درجه r است. در نهایت، چندجمله‌ای $x^m - a \in \mathbb{F}[x;\sigma]$، جایی که $a \in \mathbb{F}^*$ را در نظر بگیرید و فرض کنید $c \in \mathbb{F}$ ریشه $x^m - a$ باشد. با استفاده از چندگانگی نگاشت‌های N_i می‌توان به راحتی این‌گونه دید که

$$x^m - a = \mathrm{lclm}(x-cb, x-c\sigma(b), \dots, x-c\sigma^{m-1}(b)).$$

حال به چندجمله‌ای‌هایی بر می‌گردیم که به صورت چندجمله‌ای مینیمال یک مجموعه جبری A رخ می‌دهند.

تعریف ۲.۱.۳. چندجمله‌ای تکین $f \in F[x;\sigma]$، چندجمله‌ای ودربرن[1] بر روی F یا به بیان ساده، Wـ‌چندجمله‌ای نامیده می‌شود، به شرطی که $A \subseteq F$ موجود باشد به گونه‌ای که $f = m_A$.

چندجمله‌ای $x^2 + 1$، یک Wـ‌چندجمله‌ای بر روی $\mathbb{F}_4$ می‌باشد، زیرا برابر $m_{\{1,\omega,\omega^2\}}$ است. (به مثال ۳.۱.۲ (۱) نگاه کنید)، اما یک Wـ‌چندجمله‌ای بر روی $\mathbb{F}_2$ نیست. بنابراین میدان F در تعریف Wـ‌چندجمله‌ای، مهم تلقی می‌شود. همیشه این‌گونه فرض می‌کنیم که میدان مورد نظر، میدان ضرایب حلقه چندجمله‌ای اریب است.

چندجمله‌ای $x^2 - 1 \in \mathbb{C}[x;\sigma]$ که در آن σ مزدوج مختلط است، چندجمله‌ای مینیمال دایره واحد (یا مجموعه $\{1, -1\}$) است و از این رو به عنوان یک Wـ‌چندجمله‌ای شناخته می‌شود. در $\mathbb{F}_4[x;\sigma]$، چندجمله‌ای $f = (x+1)(x+\omega)$، یک W–چندجمله‌ای محسوب نمی‌شود زیرا $V(f) = \{\omega\}$. اگر مجموعه جبری A متناهی باشد، یعنی $A = \{a_1, \dots, a_N\}$، آنگاه قضیه ۱.۳.۲ نشان می‌دهد که $f = m_A = \mathrm{lclm}(x-a_1, \dots, x-a_N)$. این رابطه نشان می‌دهد که در مورد حالت جابه‌جایی، Wـ‌چندجمله‌ای‌ها، چندجمله‌ای‌های تحویل‌پذیری هستند که به عوامل خطی تجزیه می‌شوند. همچنین توجه کنید که از نظر اور، Wـ‌جمله‌ای‌ها حالت خاصی از چندجمله‌ای‌های کاملاً تحویل‌پذیر محسوب می‌شوند، جایی که اصطلاح دوم به صورت کوچک‌ترین مضرب مشترک چپ چندجمله‌ای‌های تحویل‌ناپذیر تعریف شده است.

از آنجایی که برای هر $f \in F[x;\sigma]$، داریم $m_{V(f)} | _r f$، لذا مشاهده می‌کنیم که f یک Wـ‌چندجمله‌ای است اگر و تنها اگر $m_{V(f)} = f$. اگر $\deg(f) = N$، آنگاه داریم:

[1] Wedderburn

f ودربرن است اگر و فقط اگر $\mathrm{rk}(V(f)) = N$ باشد.

گزاره ۳.۱.۳. فرض کنید $A, B \subseteq F$ مجموعه‌های جبری هستند. در این صورت داریم:

الف)

$$m_{A\cup B} = \mathrm{lclm}(m_A, m_B) \Rightarrow \mathrm{rk}(A \cup B) \leq \mathrm{rk}(A) + \mathrm{rk}(B).$$

ب)

$$\mathrm{rk}(A \cup B) = \mathrm{rk}(A) + \mathrm{rk}(B) \Leftrightarrow \mathrm{gcrd}(m_A, m_B) = ۱ \Leftrightarrow V(m_A) \cap V(m_B) = \emptyset.$$

قسمت (الف) و همچنین هم‌ارز آن در قسمت (ب) واضح هستند؛ (به قضیه ۱.۱.۲ قسمت (د) نیز نگاه کنید). قسمت دوم (ب) به توضیح و واکاوی بیشتری نیاز دارد.

حال برخی از خصوصیات Wـ‌چندجمله‌ای‌های را مطرح می‌کنیم.

قضیه ۲.۱.۳. ۱. فرض کنید $f \in F[x;\sigma]$ یک چندجمله‌ای تکین از درجه N باشد. موارد زیر هم‌ارز هستند:

(i) f یک Wـ‌چندجمله‌ای است.

(ii) $f = \mathrm{lclm}(x - a_۱, \ldots, x - a_N)$ برای هر عنصر متمایز $a_i \in F$ برقرار است.

(iii) f کاملاً تجزیه شده و هر عامل تکین از f، یک Wـ‌چندجمله‌ای است.

۲. فرض کنید $f, g \in F[x;\sigma]$ چندجمله‌ای‌های تکین متشابه و f یک Wـ‌چندجمله‌ای باشد. در این صورت، g یک Wـ‌چندجمله‌ای می‌باشد.

۳. فرض کنید g و h دو تا W ـ‌چندجمله‌ای باشند. در این صورت موارد زیر هم‌ارز هستند:

(i) gh یک Wـ‌چندجمله‌ای است.

(ii) $۱ \in {}^\bullet(g) + (h)^\bullet$.

(iii) ${}^\bullet(g) + (h)^\bullet \subseteq \{k \in F[x;\sigma] | gk \in {}^\bullet(g)\}$.

مجموعه سمت چپ (iii) (۳)، ایده‌آل‌ساز ${}^\bullet(g)$ نامیده می‌شود. این مجموعه بزرگترین زیرحلقه از $F[x;\sigma]$ می‌باشد که در آن ${}^\bullet(g)$ یک ایده‌آل دوطرفه باشد.

این بخش را با بحث مختصری راجع به تعدد و چندگانگی ریشه‌ها و میدان‌های شکافنده برای چندجمله‌ای‌های اریب، به پایان می‌رسانیم.

تعریف چندگانگی ریشه a از چندجمله‌ای اریب $f \in F[x;\sigma]$ به عنوان بزرگ‌ترین توان r که $(x-a)^r$ مقسوم‌علیه راست f است، جالب توجه می‌باشد. با این حال، این رابطه، چندگانگی را بر مبنای عامل خطی تکین با ریشه a تعریف می‌کند. متأسفانه، تعریف مجدد یک عامل

خطی با ریشه از چپ (یا از راست)، می‌تواند توان مقسوم‌علیه راست f را تغییر دهد. در واقع، در مثال ۴.۱.۲ دیدیم که $x+\omega^۲$ با توان ۱ به عنوان مقسوم‌علیه راست $x^۲+۱$ ظاهر می‌شود، در حالی که $\omega(x+\omega^۲)=\omega x+۱$ با توان ۲ ظاهر می‌شود. به همین دلیل، تعریف چندگانگی ریشه‌ها به این طریق معنادار نیست.

با توجه به توسیع میدان F، لازم است خودریختی σ نیز توسعه و تعمیم داده شود. اما حتی اگر qـ‌فروبینیوس $\mathbb{F}_{q^m}$ را به qـ‌فروبینیوس بر روی توسیع میدان $\mathbb{F}_{q^M}$ تعمیم و توسعه دهیم، باز هم این سؤال را مطرح می‌کنیم که آیا به دنبال میدان شکافنده با کوچک‌ترین توسیع هستیم که چندجمله‌ای داده شده تقسیم می‌شود یا به دنبال کوچک‌ترین حالت هستیم که چندجمله‌ای دارای کلیه ریشه‌هایش است؟ مثال ۱.۳.۲ قبلاً نشان داده است که این دو هدف یکسان نیستند. دستیابی به هدف دوم از مورد میدان متناهی $\mathbb{F}_{q^m}[x;\sigma]$، راحت‌تراست؛ ملاحظه ۲.۳.۲ نشان می‌دهد که میدان شکافنده چندجمله‌ای جابه‌جایی $P_f\in\mathbb{F}_{q^m}[y]$، کوچکترین میدانی است که شامل کلیه ریشه‌های f می‌باشد. از طرف دیگر، چندجمله‌ای $x^۲-i\in\mathbb{C}[x;\sigma]$، جایی که σ مزدوج مختلط می‌باشد، در $\mathbb{C}$ ریشه ندارد (زیرا $N_۲(c)=|c|^۲$ برای هر $c\in\mathbb{C}$ حقیقی است) و از این رو، در صورت وجود میدان شکافنده، بایستی توسیع میدان $\mathbb{C}$ باشد.

فصل ۴

رویکرد دوری در راستای کدهای دوری بلوکی

در این فصل، با کمک ماتریس‌های دوری به طور مختصر نظریه جبری کدهای بلوک دوری را بیان می‌کنیم که در اینجا به این دلیل مطرح شده است تا در بخش‌های بعدی به عنوان راهبردی برای حالت اریب عمل کند.

۱.۴ نظریه جبری کدهای دوری بلوکی

فرض کنید $\mathbb{F} = \mathbb{F}_q$ یک میدان متناهی و با طول n باشد. معمولاً q و n باید نسبت به هم اول باشند، اما در نظریه جبری نیازی به آن نیست. این مسئله فقط زمانی صادق است که بحث درمورد فاصله باشد. در اینجا حلقه خارج‌قسمتی $\mathcal{R} = \mathbb{F}[x]/(x^n - ۱)$ را در نظر می‌گیریم که به عنوان یک $\mathbb{F}$ـ فضای برداری از طریق نگاشت زیر با $\mathbb{F}^n$ همریخت می‌شود:

$$\mathfrak{p} : \mathbb{F}^n \to \mathcal{R}, \quad (g_۰, \ldots, g_{n-۱}) \mapsto \overline{\sum_{i=۰}^{n-۱} g_i x^i} \tag{۱.۴}$$

جایی که $\bar{\cdot}$ هم مجموعه‌ها را نشان می‌دهد. قرار دهید $\mathfrak{b} := \mathfrak{p}^{-۱}$.

طبق تعریف، یک کد دوری در $\mathbb{F}^n$ زیرفضایی به شکل $\mathcal{C} = \mathfrak{b}(I)$ است، که I به عنوان یک ایده‌آل در $\mathcal{R}$ تلقی می‌گردد. این بدان معناست که $\mathcal{C}$ تحت شیفت دوری،

$(a_۰,\dots,a_{n-۱}) \mapsto (a_{n-۱},a_۰,\dots,a_{n-۲})$ ثابت است. معمولاً کد با ایده‌آل نظیرش شناسایی می‌شود، به گونه‌ای که کدواژه‌ها چندجمله‌ای‌هایی با درجه کمتر از n هستند. جبر پایه نشان می‌دهد که $\mathcal{R}$ یک حلقه ایده‌آل اصلی است و هر ایده‌آل به صورت $(\overline{g})$ می‌باشد جایی که g مقسوم‌علیه تکین $x^n-۱$ است. چنین مولدی منحصر به فرد بوده و چندجمله‌ای مولد کد دوری $(\overline{g})$ نامیده می‌شود. لذا به این نتیجه می‌رسیم که تعداد کدهای دوری به طول n بر روی فضای برداری $\mathbb{F}$ با تعداد مقسوم‌علیه‌های $x^n-۱$ برابر می‌باشد. اگر $gh=x^n-۱$، آنگاه h چندجمله‌ای کنترل توازن $\mathcal{C}$ می‌باشد.

قبل از جمع‌بندی ویژگی‌های کدهای دوری، ماتریس‌های دوری را معرفی می‌کنیم. برای هر $g=(g_۰,\dots,g_{n-۱})\in\mathbb{F}^n$، ماتریس دوری به صورت زیر را تعریف می‌شود:

$$\Gamma(g):=\begin{pmatrix} g_۰ & g_۱ & \cdots & g_{n-۲} & g_{n-۱}\\ g_{n-۱} & g_۰ & \cdots & g_{n-۳} & g_{n-۲}\\ \vdots & \vdots & & \vdots & \vdots\\ g_۲ & g_۳ & \cdots & g_۰ & g_۱\\ g_۱ & g_۲ & \cdots & g_{n-۱} & g_۰ \end{pmatrix}. \qquad (۲.۴)$$

با اندیس‌گذاری $i=۰,\dots,n-۱$، می‌بینیم که iامین ردیف از $\Gamma(g)$ با رابطه $\mathfrak{b}(\overline{x^i\sum_{j=۰}^{n-۱}g_jx^j})$ به‌دست می‌آید. مجموعه $\mathrm{Circ}:=\{\Gamma(g)|g\in\mathbb{F}^n\}$ یک زیرفضای nـبعدی از $\mathrm{Mat}_{n,n}(\mathbb{F})$ است. رابطه زیر را تعریف می‌کنیم:

$$\rho:\mathbb{F}[x]\to\mathbb{F}[x],\quad g=\sum_{i=۰}^{r}g_ix^i\mapsto x^rg(x^{-۱})=\sum_{i=۰}^{r}g_ix^{r-i}\quad (g_r\neq ۰) \qquad (۳.۴)$$

جایی که تصویر $\rho(g)$، معکوس g نامیده می‌شود.

ملاحظه ۱.۱.۴. الف) نگاشت $\mathrm{Circ}\to\mathcal{R},\ \Gamma(g_۰,\dots,g_{n-۱})\mapsto\overline{\sum_{i=۰}^{n-۱}g_ix^i}$ یک ایزومورفیسم $\mathbb{F}$ـجبر است. ازاین پس از نماد $\Gamma\left(\overline{\sum_{i=۰}^{n-۱}g_ix^i}\right)$ برای $\Gamma(g_۰,\dots,g_{n-۱})$ استفاده می‌کنیم. با توجه به مطالب بیان شده در بالا داریم:

$$\Gamma(\overline{g}\overline{h})=\Gamma(\overline{g})\Gamma(\overline{h})=\Gamma(\overline{h})(\overline{g})$$

ب) $\mathrm{rk}\Gamma(\overline{g})=\deg\dfrac{x^n-۱}{\gcd(g,x^n-۱)}:=k$ (که خارج‌قسمت در $\mathbb{F}[x]$ ارزیابی شده است) و هر مجموعه از k سطر متوالی از $\Gamma(\overline{g})$ از نظر خطی مستقل است.

ج) نگاشت $\phi:\mathcal{R}\to\mathcal{R},\ \overline{g}\mapsto\overline{g(x^{n-۱})}$ یک اوتومورفیسم $\mathbb{F}$ـجبر خوش تعریف متناظر با ترانهاده Circ می‌باشد به عبارتی $\Gamma(\overline{g})^T=\Gamma(\phi(\overline{g}))$ است.

د) فرض کنید $g=\sum_{i=۰}^{r}g_ix^i$ از درجه r باشد. در این صورت $\overline{x^r}\phi(\overline{g})=\overline{\rho(g)}$ یا معادل آن $\phi(\overline{g})=\overline{x^{n-r}\rho(g)}$ برقرار می‌باشد. بنابراین داریم:

$$\Gamma(\overline{\rho(g)})=\Gamma(\overline{x^r})\Gamma(\phi(\overline{g}))=\Gamma(\phi(\overline{g}))\Gamma(\overline{x^r})$$

و چون $\overline{x^r}$ یکه است، ماتریس‌های دوری $\Gamma(\phi(\overline{g}))$ و $\Gamma(\overline{\rho(g)})$ دارای فضای سطری و ستونی یکسان هستند. در واقع، عامل چپ (راست) $\Gamma(\overline{x^r})$ به سادگی سطرهای (ستون‌ها) $\Gamma(\phi(\overline{g}))$ را جابه‌جا می‌کند.

ه) اگر g مقسوم‌علیه x^n-1 باشد، آنگاه $\rho(g)$ نیز مقسوم‌علیه x^n-1 می‌باشد. اما عامل $\phi(\overline{g})$ با درجه کمتر از n، به طور کلی مقسوم‌علیه x^n-1 نیست. بنابراین، در حالی که به توان رساندن $\overline{g(x)} \mapsto \overline{g(x^{n-1})}$ نگاشت مناسبی برای ترانهاده ماتریس‌های دوری است، اما در مورد مقسوم‌علیه‌های x^n-1 صدق نمی‌کند.

ملاحظه ۲.۱.۴. فرض کنید $x^n-1 = hg$ جایی که $h = \sum_{i=0}^{k} h_i x^i$ و $g = \sum_{i=0}^{r} g_i x^i$ چندجمله‌ای‌های تکین از درجه k و r هستند. فرض کنید $\mathcal{C}$ کد دوری $\mathcal{C} = \mathfrak{b}((\overline{g})) \subseteq \mathbb{F}^n$ باشد.

الف) ایده‌آل $(\overline{g})$ دارای بعد $k := n-r$ به عنوان یک $\mathbb{F}$ـفضای برداری است و $\overline{g}, \ldots, \overline{x^{k-1}g}$ پایه $(\overline{g})$ می‌باشد. ایزومورفیسم $\mathfrak{b}$ نشان می‌دهد که $\mathcal{C}$ فضای سطری ماتریس دوری $\Gamma(g)$ و در حقیقت k سطر اول $\Gamma(g)$ می‌باشد (به ملاحظه ۱.۱.۴ قسمت (ب) نگاه کنید). از آنجایی که $\deg(g) = r$، پس سطرهای اول به صورت زیر نشان داده می‌شود:

$$G = \begin{pmatrix} \mathfrak{b}(\overline{g}) \\ \mathfrak{b}(\overline{xg}) \\ \vdots \\ \mathfrak{b}(\overline{x^{k-1}g}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \ldots & g_r & & \\ & g_0 & g_1 & \ldots & g_r & \\ & & \ddots & \ddots & \ddots & \\ & & & g_0 & g_1 & \ldots & g_r \end{pmatrix} \in \mathrm{Mat}_{k,n}(\mathbb{F}) \qquad (۴.۴)$$

جایی که ماتریس مولد کد دوری که توسط g تولید شده است را نشان می‌دهد.

ب) از ملاحظه ۱.۱.۴ قسمت (الف) برای نگاشت ϕ داریم:
$\Gamma(\overline{g})\Gamma(\overline{h}) = 0$ و بنابراین $\Gamma(\overline{g})\Gamma(\phi(\overline{h}))^T = 0$ که نتیجه‌ای از ملاحظه ۱.۱.۴ قسمت (ج) است لذا کد $\mathcal{C} = \mathfrak{b}((\overline{g}))$ در رابطه زیر را صدق می‌کند:

$$\mathcal{C} = \{v \in \mathbb{F}^n | \Gamma(\phi(\overline{h}))v^T = 0\}$$

از آنجایی که $\deg(\phi(h)) = \deg(h) = k$، $n-k$ سطر آخر از ماتریس دوری $\Gamma(\phi(\overline{h}))$ ، پایه فضای سطری ماتریس $\Gamma(\overline{h})$ را تشکیل می‌دهند. برای $h = \sum_{i=0}^{k} h_i x^i$ داریم $\mathcal{C} = \{v \in \mathbb{F}^n | Hv^T = 0\}$ است جایی که

$$H = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & & \\ & h_k & h_{k-1} & \ldots & h_0 & \\ & & \ddots & \ddots & & \ddots \\ & & & h_k & h_{k-1} & \ldots & h_0 \end{pmatrix} \in \mathrm{Mat}_{n-k,n}(\mathbb{F}) \qquad (۵.۴)$$

معروف به ماتریس کنترل توازن $\mathcal{C}$ است. همچنین زیرماتریسی متشکل از $n-k$ سطر اول از $\Gamma(\overline{\rho(h)})$ نیز می‌باشد جایی که $\rho(h)$ معکوس h می‌باشد.

ج) $\rho(h)\rho(g) = x^n - ۱$ و کد دوگان $\mathcal{C}^{\perp}$ با چندجمله‌ای مولد و کنترل توازن $\rho(h)/h_{\circ}$ و $\rho(g)/g_{\circ}$ دوری می‌باشد.

فصل ۵

رویکرد جبری نسبت به کدهای دوری اریب

در این فصل، مفهوم کدهای دوری اریب را در کلی ترین حالت ممکن معرفی نموده و برخی از خواص جبری مهم این کدها را بیان خواهیم کرد، سپس بحث خود را به برخی حالت های خاص این کدها محدود کرده و نتایجی در این خصوص بیان خواهیم کرد. مطالب این فصل برگرفته از مراجع [۴] ، [۸] و [۱۴] می‌باشد.

۱.۵ مفهوم کدهای دوری اریب در حالت کلی

از این به بعد حلقه چندجمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ را در نظر می‌گیریم جایی که $\mathbb{F}=\mathbb{F}_{q^m}$ و σ خودریختی qـفروبینیوس است. برای تعمیم بخش آخر، ابتدا باید حلقه خارج‌قسمتی $\mathcal{R}=\mathbb{F}[x]/(x^n-1)$ را تعمیم دهیم. برای این کار، برای هر $f\in\mathbb{F}[x;\sigma]$ باید $\mathbb{F}[x;\sigma]$ـمدول چپ $\mathbb{F}[x,\sigma]/{}^{\bullet}(f)$ را به دست می‌آوریم (قطعاً می‌توانیم ایده‌آل‌های راست و مدول‌های راست را نیز در نظر بگیریم). نظریه مدول پایه نشان می‌دهد که این مدول یک حلقه محسوب می‌شود اگر و تنها اگر f یک چندجمله‌ای دوطرفه باشد؛ (به تعریف ۳.۱.۲ نگاه کنید).

فرض کنید $f\in\mathbb{F}[x;\sigma]$ یک چندجمله‌ای تکین درجه n باشد که پیمانه نامیده می‌شود و

$\mathbb{F}[x;\sigma]$ـ مدول چپ زیر را در نظر می‌گیریم:

$$\mathcal{R}_f = \mathbb{F}[x;\sigma]/{}^{\bullet}(f)$$

توجه داشته باشید که ساختار مدول چپ به این معناست که برای هر $z, g \in \mathbb{F}[x;\sigma]$ داریم $z\overline{g} = \overline{zg}$ جایی که $\overline{g}$ هم مجموعه ${}^{\bullet}(f) + g$ در $\mathcal{R}_f$ را نشان می‌دهد. همانند بخش قبل، نگاشت زیر را در نظر می‌گیریم:

$$\mathfrak{p}_f : \mathbb{F}^n \to \mathcal{R}_f, \quad (c_0, \ldots, c_{n-1}) \mapsto \overline{\sum_{i=0}^{n-1} c_i x^i}. \tag{۱.۵}$$

مهم است که ضرایب c_i در سمت چپ x ظاهر شوند، به این طریق $\mathfrak{p}_f$ به یک ایزومورفیسم از $\mathbb{F}$ ـ فضاهای برداری (چپ) تبدیل می‌شود، به عبارت دیگر کدها در $\mathbb{F}^n$ را به زیرمدول‌ها در $\mathcal{R}_f$ تبدیل می‌کند. مجدداً قرار می‌دهیم[۱] $\mathfrak{b}_f = \mathfrak{p}_f^{-1}$. نگاشت $\mathfrak{b}_f$ با نگاشت ϕ منطبق است، جایی که با کمک نگاشت نیمه‌خطی بر اساس ماتریس همراه f تعریف شده است؛ به رابطه ۲.۲ نگاه کنید.

مطالب زیر در مورد زیرمدول‌های $\mathcal{R}_f$، تعمیم‌های ساده‌ای از حالت جابه‌جایی هستند و قطعاً به شیوه‌ای یکسان اثبات می‌شوند (با کمک مقسوم علیه راست در $\mathbb{F}[x;\sigma]$). از نماد ${}^{\bullet}(\overline{g})$ برای زیرمدول چپ $\{z\overline{g} | z \in \mathbb{F}[x;\sigma]\}$ از $\mathcal{R}_f$ استفاده می‌کنیم که توسط $\overline{g}$ تولید شده است.

گزاره ۱.۱.۵. فرض کنید M زیرمدول چپ $\mathcal{R}_f$ باشد. در این صورت، ${}^{\bullet}(\overline{g}) = M$ جایی که $g \in \mathbb{F}[x;\sigma]$ چندجمله‌ای تکین منحصر به فرد با کوچک‌ترین درجه است، به طوری که $\overline{g} \in M$. متناوباً g مقسوم‌علیه راست تکین منحصر به فرد f است، به طوری که ${}^{\bullet}(\overline{g}) = M$. و همچنین، برای هر $h \in \mathbb{F}[x;\sigma]$ داریم $g|_r h$ به طوری که $\overline{h} \in M$.

تعریف کدهای دوری اریب برای اولین بار این‌گونه مطرح گردید که f یک چندجمله‌ای مرکزی به شکل $f = x^n - 1$ است، به عبارتی $\sigma^n = id$.

تعریف ۱.۱.۵. ۱. زیرفضای $\mathcal{C} \subseteq \mathbb{F}^n$، دوری (σ, f)ـ اریب نامیده می‌شود اگر $\mathfrak{p}_f(\mathcal{C})$ زیرمدولی از $\mathcal{R}_f$ باشد.

۲. برای $a \in \mathbb{F}^*$، کد $\mathcal{C} \subseteq \mathbb{F}^n$ دوری‌ـ ثابت (σ, a)ـ اریب[۱] نامیده می‌شود اگر دوری $(\sigma, x^n - a)$ـ اریب باشد.

۳. کد σـ دوری نامیده می‌شود، اگر دوری‌ـ ثابت $(\sigma, 1)$ـ اریب باشد. همچنین تصویر $\mathfrak{p}_f(\mathcal{C})$ را یک کد دوری می‌نامیم.

بنابراین، در مورد ایزومورفیسم $\mathfrak{p}_f$، کدهای دوری اریب زیرمدول‌هایی از $\mathcal{R}_f$ هستند. کدهای فوق‌الذکر اغلب ایده‌آل σـ کدها نامیده می‌شوند اگر f یک ایده‌آل دوطرفه تولید کند و

[1] Skew-constanceyclic

در غیر این صورت مدول σـ کدها خوانده می‌شوند. کدهای qـ دوری، کدهای دوری‌ـ ثابت $(\sigma,۱)$ـ اریب برای حالت $m=n$ هستند.

کدهای دوری‌ـ ثابت اریب به راحتی در $\mathbb{F}^n$ توصیف می‌شوند. درست مانند حالت جابه‌جایی، مشاهده می‌شود که زیرفضای $\mathcal{C}\subseteq\mathbb{F}^n$، دوری‌ـ ثابت (σ,a)ـ اریب است اگر و تنها اگر

$$(c_۰,\dots,c_{n-۱})\in\mathcal{C}\Rightarrow(a\sigma(c_{n-۱}),\sigma(c_۰),\dots,\sigma(c_{n-۲}))\in\mathcal{C}. \qquad (۲.۵)$$

واضح است، سمت راست رابطه با $\overline{\mathfrak{b}_{x^n-a}(x\sum_{i=۰}^{n-۱}c_ix^i)}$ برابر است. به عبارت دیگر، کد دوری‌ـ ثابت (σ,a) ـ اریب تحت نگاشت σـ نیمه‌خطی القا شده با ماتریس همراه C_{x^n-a} در نظر گرفته می‌شود(به رابطه (۲.۲) و پاراگراف بعد از آن نگاه کنید). این ویژگی‌ها به کدهای دوری (σ,f)ـ اریب نیز تعمیم می‌یابد.

با توجه به گزاره ۱.۱.۵ داریم هر کد دوری (σ,f)ـ اریب توسط یک عنصر در $\mathcal{R}_f$ تولید می‌شود (مشابه ایده‌آل‌های اصلی)، به عبارتی دارای یک چندجمله‌ای مولد می‌باشد. در نتیجه، تعداد کدهای دوری (σ,f)ـ اریب با تعداد مقسوم‌علیه‌های راست تکین f برابر است. به طور کلی این مسئله منجر به تعداد بسیاری از کدهای دوری اریب نسبت به کدهای دوری معمولی می‌گردد. به‌طور مثال، در حالت دوری‌ـ ثابت برای $f=x^{۱۵}-\omega$ و $\omega\in\mathbb{F}_۴$ داریم $\omega^۲+\omega+۱=۰$ جایی که چندجمله‌ای f در حلقه جابه‌جایی $\mathbb{F}_۴[x]$، دارای ۸ مقسوم‌علیه تکین می‌باشد، در صورتی که در حلقه چندجمله‌ای اریب $\mathbb{F}_۴[x;\sigma]$، ۳۲ مقسوم علیه راست تکین دارد.

گزاره ۱.۱.۵ به ما امکان می‌دهد تا ماتریس‌های مولد را درست مانند حالت جابه‌جایی مطرح کنیم. مجدداً این کار را با استفاده از ماتریس‌های دوری انجام می‌دهیم.

تعریف ۲.۱.۵. برای $\overline{g}\in\mathcal{R}_f$، ماتریس (σ,f)ـ دوری زیر را تعریف می‌کنیم:

$$\Gamma_f^\sigma(\overline{g}):=\begin{pmatrix}\mathfrak{b}_f(\overline{g})\\ \mathfrak{b}_f(x\overline{g})\\ \vdots\\ \mathfrak{b}_f(x^{n-۲}\overline{g})\\ \mathfrak{b}_f(x^{n-۱}\overline{g})\end{pmatrix}\in\mathrm{Mat}_{n,n}(\mathbb{F}). \qquad (۳.۵)$$

در حالت $a\in\mathbb{F}^*$ و $f=x^n-a$ به جای $\Gamma^\sigma_{x^n-a}$ از نماد Γ^σ_a استفاده می‌کنیم. هر ماتریس به صورت $\Gamma_f^\sigma(\overline{g})$ را دوری اریب می‌نامیم.

$\Gamma_f^\sigma(\overline{g})$ را می‌توان به عنوان نمایش ماتریسی نگاشت $\mathbb{F}$ـ خطی چپ بر روی $\mathcal{R}_f$ در نظر گرفت که از ضرب راست روی $\overline{g}$ نسبت به پایه $\{\overline{x^۰},\dots,\overline{x^{n-۱}}\}$ به‌دست می‌آید. اگر $f=x^n-a$، آنگاه

ماتریس دوری اریب $\overline{g}$ را می‌توان به راحتی تعریف کرد. برای $g=\sum_{i=0}^{n-1} g_i x^i$، داریم:

(۴.۵)

$$\Gamma_a^\sigma(\overline{g})=\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-2} & g_{n-1} \\ a\sigma(g_{n-1}) & \sigma(g_0) & \sigma(g_1) & \cdots & \sigma(g_{n-3}) & \sigma(g_{n-2}) \\ a\sigma^2(g_{n-2}) & \sigma(a)\sigma^2(g_{n-1}) & \sigma^2(g_0) & \cdots & \sigma^2(g_{n-4}) & \sigma^2(g_{n-3}) \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ a\sigma^{n-2}(g_2) & \sigma(a)\sigma^{n-2}(g_3) & \sigma^2(a)\sigma^{n-2}(g_4) & \cdots & \sigma^{n-2}(g_0) & \sigma^{n-2}(g_1) \\ a\sigma^{n-1}(g_1) & \sigma(a)\sigma^{n-1}(g_2) & \sigma^2(a)\sigma^{n-1}(g_3) & \cdots & \sigma^{n-2}(a)\sigma^{n-1}(g_{n-1}) & \sigma^{n-1}(g_0) \end{pmatrix}.$$

اگر $f=x^n-1$، آنگاه $\Gamma_1^\sigma(\overline{g})=D_g$ ماتریس دیکسون در رابطه (۲.۲) می‌باشد و اگر $\sigma=id$، ماتریس دوری معمولی $\Gamma(g)$ در رابطه (۲.۴) به دست می‌آید. علاوه بر این، برای هر f تکین، ماتریس دوری اریب $\Gamma_f^\sigma(\overline{g})$ برابر با C_f یعنی ماتریس همراه f در رابطه (۱.۲) است. همچنین توجه داشته باشید که به پیمانه x^n-a داریم:

$$\Gamma_a^\sigma(\overline{x})=\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ a & & & \end{pmatrix} \quad \text{و} \quad \Gamma_a^\sigma(\overline{x^2})=\begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ a & & & \\ & \sigma(a) & & \end{pmatrix}. \qquad (۵.۵)$$

مثال ۱.۱.۵. فرض کنید $f=x^7+\alpha\in\mathbb{F}_8[x;\sigma]$ جایی که $\alpha^3+\alpha+1=0$ و σ خودریختی ۲ـ‌فروبینیوس و $g=x^4+\alpha x^3+\alpha^5x^2+\alpha$ باشد. در این صورت g مقسوم‌علیه راست f است و

$$\Gamma:=\Gamma_f^\sigma(\overline{g})=\begin{pmatrix} \alpha & 0 & \alpha^5 & \alpha & 1 & 0 & 0 \\ 0 & \alpha^2 & 0 & \alpha^3 & \alpha^2 & 1 & 0 \\ 0 & 0 & \alpha^4 & 0 & \alpha^6 & \alpha^4 & 1 \\ \alpha & 0 & 0 & \alpha & 0 & \alpha^5 & \alpha \\ \alpha^3 & \alpha^2 & 0 & 0 & \alpha^2 & 0 & \alpha^3 \\ 1 & \alpha^6 & \alpha^4 & 0 & 0 & \alpha^4 & 0 \\ 0 & 1 & \alpha^5 & \alpha & 0 & 0 & \alpha \end{pmatrix}.$$

سطر اول، بردار ضرایب چپ g است. سطرهای دوم و سوم Γ شیفت دوری سطر قبل هستند که با استفاده از نگاشت σ اعمال می‌شود. بنابراین سه سطر اول، به f وابسته نیستند. در ۴ سطر آخر که $\deg(x^ig)$ حداقل ۷ است به پیمانه $\bullet(f)$ کاهش می‌یابد.

حال بیان مشابهی از ملاحظه ۲.۱.۴ (الف) را بیان می‌کنیم. هر کد دوری (σ,f)ـ‌اریب دارای یک ماتریس مولد است که ساختار دوری اریب را نشان می‌دهد. پیمانه‌های عمومی f

با درجه n را در نظر بگیرید. برای هر ماتریس G، از نماد $\mathrm{rs}(G)$ برای اندازه سطری G استفاده می‌کنیم.

گزاره ۲.۱.۵. فرض کنید $\mathcal{M} = {}^{\bullet}(\overline{g}) \subseteq \mathcal{R}_f$ جایی که $g = \sum_{i=0}^{r} g_i x^i \in \mathbb{F}[x;\sigma]$ از درجه r باشد. در این صورت داریم:

الف) برای هر $u \in \mathbb{F}^n$ داریم $\mathfrak{p}_f(u\Gamma_f^\sigma(\overline{g})) = \mathfrak{p}_f(u)\overline{g}$.

ب) $\mathfrak{b}_f(\mathcal{M}) = \mathrm{rs}(\Gamma_f^\sigma(\overline{g}))$.

ج) فرض کنید g مقسوم‌علیه راست f از درجه r باشد. در این صورت $\mathcal{M}$، $\mathbb{F}$ـفضای برداری چپ با بعد $k := n - r$ و پایه $\{\overline{g}, \overline{xg}, \ldots, \overline{x^{k-1}g}\}$ است. در نتیجه $\mathrm{rk}(\Gamma_f^\sigma(\overline{g})) = k$ و $\mathfrak{b}_f(\mathrm{M}) = \mathrm{rs}(G)$ جایی که $G \in \mathrm{Mat}_{k,n}(\mathbb{F})$ از k سطر اول ماتریس دوری اریب $\Gamma_f^\sigma(\overline{g})$ تشکیل می‌شود:

(۶.۵)

$$G = \begin{pmatrix} \mathfrak{b}_f(\overline{g}) \\ \mathfrak{b}_f(\overline{xg}) \\ \vdots \\ \mathfrak{b}_f(\overline{x^{k-1}g}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & & & \\ & \sigma(g_0) & \sigma(g_1) & \cdots & \sigma(g_r) & & \\ & & \ddots & \ddots & & \ddots & \\ & & & \sigma^{k-1}(g_0) & \sigma^{k-1}(g_1) & \cdots & \sigma^{k-1}(g_r) \end{pmatrix}.$$

علاوه بر این، اگر g تکین باشد، آنگاه آن را چندجمله‌ای مولد کد دوری (σ, f)ـاریب $\mathcal{M}$ می‌نامیم.

د) فرض کنید $z \in \mathbb{F}[x;\sigma]$ و $g = \mathrm{gcrd}(z, f)$ باشد. در این صورت ${}^{\bullet}(\overline{g}) = {}^{\bullet}(\overline{z})$ و از این رو $\mathrm{rs}(\Gamma_f^\sigma(\overline{z})) = \mathrm{rs}(\Gamma_f^\sigma(\overline{g}))$.

اثبات:

الف) برای هر $u_i \in \mathbb{F}$ داریم:

$$(u_0, \ldots, u_{n-1})\Gamma_f^\sigma(\overline{g}) = \sum_{i=0}^{n-1} u_i \mathfrak{b}_f(\overline{x^i g}) = \mathfrak{b}_f\left((\sum_{i=0}^{n-1} u_i x^i)\overline{g}\right).$$

بنابراین $(\sum_{i=0}^{n-1} u_i x^i)\overline{g} = \mathfrak{p}_f((u_0, \ldots, u_{n-1})\Gamma_f^\sigma(\overline{g}))$ که عبارت را اثبات می‌کند.

ب) $\supseteq$ از (الف) پیروی می‌کند. برای $\subseteq$، $\overline{zg} \in {}^{\bullet}(g)$ را در نظر بگیرید جایی که $z \in \mathbb{F}[x;\sigma]$. با توجه به قضیه ۱.۱.۲ قسمت (ج)، $u, v \in \mathbb{F}[x;\sigma]$ وجود دارند، به طوری که $ug = vf = \mathrm{lclm}(g, f)$ و $\deg(u) \leq n$. تقسیم راست z بر u چندجمله‌ای‌های $t, r \in \mathbb{F}[x;\sigma]$ را حاصل می‌کند به طوری که $z = tu + r$ و $\deg(r) < \deg(u) \leq n$. حال داریم $\overline{zg} = \overline{tvf + rg} = \overline{rg}$ و $r = \sum_{i=0}^{n-1} r_i x^i$، در نتیجه رابطه زیر به دست می‌آید:

$$\mathfrak{b}_f(\overline{zg}) = \mathfrak{b}_f(\overline{rg}) = (r_0, \ldots, r_{n-1})\Gamma_f^\sigma(\overline{g}).$$

ج) فرض کنید $hg = f$ باشد. کافی است که نشان دهیم هر $\overline{zg} \in {}^{\bullet}(\overline{g})$ به صورت $\overline{rg}$ است جایی که $\deg(r) < k$. اما این حالت دنباله بخش قبلی است زیرا $hg = f = \mathrm{lclm}(g, f)$.

د) ${}^{\bullet}(\overline{g}) \subseteq {}^{\bullet}(\overline{z})$ برقرار است، زیرا $g|_r z$. برای $\supseteq$ ، از تساوی (همانی) بزو $g = uf + vz$ جایی که $u, v \in \mathbb{F}[x;\sigma]$ استفاده کرده (به قضیه ۱.۱.۲ قسمت (ب) نگاه کنید) و هم مجموعه‌ها را انتخاب کنید.

همان گونه که در مثال ۱.۱.۵ اشاره شد، ماتریس G در رابطه (۶.۵) به پیمانه‌های f وابسته نیست. وابستگی در صورتی تحقق می‌یابد که کد $\mathcal{M}$، دوری (σ, f)ـاریب باشد. در نتیجه، زیرفضای داده شده $\mathbb{F}^n$، برای پیمانه‌های مختلف f می‌تواند دوری (σ, f)ـاریب باشد.

۲.۵ نگاشت القاء شده توسط کد دوری اریب

گزاره ۱.۲.۵. نگاشت $\Gamma_f^\sigma : \mathcal{R}_f \to \mathrm{Mat}_{n,n}(\mathbb{F}),\ \overline{g} \mapsto \Gamma_f^\sigma(\overline{g})$ را در نظر بگیرید. در این صورت داریم:

الف) Γ_f^σ یک‌به‌یک و جمع پذیر است.

ب) برای هر $g \in \mathcal{R}_f$، $c \in \mathbb{F}$ و $f' \in \mathbb{F}[x;\sigma]$ تکین از درجه n، رابطه $\Gamma_f^\sigma(c\overline{g}) = \Gamma_{f'}^\sigma(\overline{c})\Gamma_f^\sigma(\overline{g})$ برقرار است و داریم:

$$\Gamma_{f'}^\sigma(\overline{c}) = \begin{pmatrix} c & & & \\ & \sigma(c) & & \\ & & \ddots & \\ & & & \sigma^{n-1}(c) \end{pmatrix} \qquad (۱.۵)$$

جایی که برای هر f' تکین از درجه n برقرار است. در نتیجه Γ_f^σ ماتریسی $\mathbb{F}$ـخطی نیست (مگر اینکه $\sigma = id_{\mathbb{F}}$)، بلکه $\mathbb{F}_q$ـخطی است (به خاطر داشته باشید که $\mathbb{F}_q$ میدان ثابتی از σ است).

ج) Γ_f^σ ضربی نیست، یعنی به طور کلی $\Gamma_f^\sigma(\overline{gg'}) \neq \Gamma_f^\sigma(\overline{g})\Gamma_f^\sigma(\overline{g'})$. این مسئله بازتابی از این مطلب است که $\mathcal{R}_f$ حلقه نیست.

قضیه ۱.۲.۵. فرض کنید $f \in \mathbb{F}[x;\sigma]$ دوطرفه باشد. در این صورت $\mathcal{R}_f$ یک حلقه است و داریم:

$$\Gamma_f^\sigma(\overline{gg'}) = \Gamma_f^\sigma(\overline{g})\Gamma_f^\sigma(\overline{g'}), \quad \forall g, g' \in \mathbb{F}[x;\sigma]$$

از این رو Γ_f^σ یک ایزومورفیسم $\mathbb{F}_q$ـجبر بین $\mathcal{R}_f$ و زیرحلقه $\Gamma_f^\sigma(\mathcal{R}_f)$ از $\mathrm{Mat}_{n,n}(\mathbb{F})$ متشکل از ماتریس‌های (σ, f)ـدوری است.

اگر f دوطرفه نباشد، قضیه تعمیم نمی‌یابد. به طور مثال، رابطه (۱.۵) نشان می‌دهد که اگر $\sigma(a) \neq a$، آنگاه $\Gamma_a^\sigma(\overline{x^۲}) \neq (\Gamma_a^\sigma(\overline{x}))^۲$.

بلافاصله نتیجه زیر برای کدهای دوری ـ ثابت (σ, f) ـ اریب به دست می‌آید. در مرجع [۸]، ماتریس $\Gamma_f^\sigma(\overline{h'})$ که در مطالب بعدی بیان می‌شود، ماتریس کنترل کد $\mathcal{C}$ نامیده می‌شود. این ماتریس نباید با ماتریس کنترل توازن اشتباه گرفته شود که در قسمت‌های بعدی به آن خواهیم پرداخت.

نتیجه ۱.۲.۵. فرض کنید $f \in \mathbb{F}[x;\sigma]$ دوطرفه باشد و $g, h, h' \in \mathbb{F}[x;\sigma]$ وجود داشته باشند به طوری که $f = hg = gh'$. در این صورت $\Gamma_f^\sigma(\overline{g})\Gamma_f^\sigma(\overline{h'}) = ۰$ و کد $\mathcal{C} = \mathfrak{b}_f(^\bullet(\overline{g})) = \mathrm{rs}(\Gamma_f^\sigma(\overline{g}))$، هسته چپ ماتریس دوری اریب $\Gamma_f^\sigma(\overline{h'})$ است.

به راحتی می‌توان دید که دوطرفه بودن f در کنار $f = hg$ به وجود h' دلالت دارد، به طوری که $f = gh'$.

حال که مفهومی از ماتریس مولد برای کد دوری اریب داریم، باید راجع به این مسئله بحث کنیم که آیا چنین کدی دارای یک ماتریس کنترل توازن نیز می‌باشد که ساختار دوری اریب را نشان دهد. در ملاحظه ۲.۱.۴ قسمت (ب) نشان دادیم که در حالت جابه‌جایی، ماتریس کنترل توازن به دو موضوع وابسته است: (۱) حاصلضرب ماتریس‌های دوری، دوری است، (۲) ترانهاده یک ماتریس دوری، دوری است. قضیه ۱.۲.۵ نشان می‌دهد که اگر پیمانه‌ها دوطرفه باشند، آنگاه خصوصیت (۱) به حالت ناجابه‌جایی منتقل می‌شود (و از این رو برای پیمانه دلخواه f به جای $x^n - ۱$ نیز به حالت جابه‌جایی منتقل می‌شود). اما اگر f دوطرفه نباشد، آنگاه حتی در حالت دوری ـ ثابت اریب (به عبارتی، پیمانه‌ای به صورت $f = x^n - a$)، حاصلضرب دو ماتریس (σ, f) ـ دوری، به طور کلی (σ, f) ـ دوری نیست. با این حال، در بخش بعدی با خاصیت ضرب‌پذیری روبه‌رو خواهیم شد که اهداف ما را کاملاً برآورده می‌سازد.

ترانهاده ماتریس‌های (σ, f) ـ دوری، یک مسئله مهم به حساب می‌آید. برای پیمانه‌های عمومی f، ترانهاده یک ماتریس (σ, f) ـ دوری، لازم نیست برای هر اتومورفیسم σ' و پیمانه‌های f' هم درجه f، یک (σ', f') ـ دوری باشد. این مسئله زیاد تعجب آور نیست، زیرا حتی در حالت جابه‌جایی، ترانهاده یک ماتریس دوری در تعریف ۲.۱.۵ لازم نیست دوری باشد.

مثال ۱.۲.۵. چند جمله‌ای‌های $g = x^۲ + \omega x + \omega$ و $f = x^۳ + x^۲ + \omega^۲$ را در حلقه چند جمله‌ای‌های اریب $\mathbb{F}_۴[x;\sigma]$ در نظر بگیرید جایی که $\omega^۲ + \omega + ۱ = ۰$ و σ خودریختی ۲ـ فروبینیوس باشد. در این صورت، g مقسوم علیه راست f است و

$$G := \Gamma_f^\sigma(\overline{g}) = \begin{pmatrix} \omega & \omega & ۱ \\ \omega^۲ & \omega^۲ & \omega \\ \omega & \omega & ۱ \end{pmatrix}.$$

ماتریس G دارای رتبه ۱ است و به این ترتیب یک کد دوری (σ, f)ـاریب ۱ بعدی $\mathcal{C} = \mathfrak{b}_f(^\bullet(\overline{g}))$ تولید می‌کند. فرض کنید اتومورفیسم σ' و $f' \in \mathbb{F}[x;\sigma']$ از درجه ۳ موجودند به طوری که ترانهاده G^T یک ماتریس (σ', f')ـدوری باشد، یعنی $G^T = \Gamma^{\sigma'}_{f'}(\overline{g'})$. در این صورت، واضح است که g' توسط ستون اول G به دست می‌آید؛ از این رو $g' = \omega + \omega^2 x + \omega x^2$. با استفاده از SageMath، می‌بینیم که برای هر اتومورفیسم σ' از $\mathbb{F}_4$ و هر $f' \in \mathbb{F}[x;\sigma']$ از درجه ۳ (حتی غیرتکین)، رابطه $G^T \neq \Gamma^{\sigma'}_{f'}(\overline{g})$ برقرار است. علاوه براین، ماتریس دوری اریب $H = \Gamma^{\sigma'}_{f'}(\overline{h})$ برای $\mathrm{rk}(H) = 2$ و $GH^T = 0$ وجود ندارد . این بدان معناست که تشابهی از ملاحظه ۲.۱.۴ قسمت (ب) و (ج) وجود ندارد: $\mathcal{C}$ ماتریس کنترل توازن دوری اریب ندارد و $\mathcal{C}^\perp$ برای هر (σ', f')، دوری (σ', f')ـاریب نیست.

در فصل بعدی، خودمان را به کدهای دوری‌ـثابت اریب محدود کرده و می‌بینیم که در آن حالت می‌توان این مسائل را برطرف کرد.

قضیه ۲.۲.۵. فرض کنید $f \in \mathbb{F}[x;\sigma]$ پیمانه تکین از درجه n و $g \in \mathbb{F}[x;\sigma]$ مقسوم‌علیه تکین f از درجه r است. فرض کنید g، یک Wـچندجمله‌ای است. بنابراین برای $a_1, \ldots, a_r \in \mathbb{F}$ متمایز داریم $g = \mathrm{lclm}(x - a_1, \ldots, x - a_r)$ (به قضیه ۲.۱.۳ قسمت (ب) نگاه کنید). فرض کنید $M = V_n(a_1, \ldots, a_r) \in \mathrm{Mat}_{n,r}(\mathbb{F})$ ماتریس واندرموند اریب باشد. در این صورت، کد دوری $\mathcal{C} = \mathfrak{b}(^\bullet(\overline{g}))$ از رابطه زیر به دست می‌آید:

$$\mathcal{C} = \{(c_0, \ldots, c_{n-1}) | (c_0, \ldots, c_{n-1})M = 0\}.$$

فصل ۶

کدهای دوری_ ثابت اریب و دوگان آن‌ها

در این فصل بحث را به کدهای دوری_ ثابت اریب؛ یعنی به پیمانه $x^n - a$ محدود می‌کنیم. در این حالت، می‌توانیم ماتریس کنترل توازن و لذا ماتریس مولد کد دوگان را به دست بیاوریم که ساختار دوری_ ثابت اریب را نشان می‌دهد.

۱.۶ کدهای دوری_ ثابت اریب

در این بخش، پیمانه $f = x^n - a$ جایی که $a \in \mathbb{F}^*$ را در نظر می‌گیریم. برای جمع‌بندی نتایج اصلی، در حالت جابه‌جایی، به معکوس یک چندجمله‌ای نیاز داریم. در حالت ناجابه‌جایی، این کار را بسته به مکان ضرایب، به روش‌های متفاوتی می‌توان انجام داد. قسمت چپ رابطه (۳.۴)، برای این بررسی کافی است. فرض کنید برای $g_r \neq 0$ داریم:

$$\rho l : \mathbb{F}[x;\sigma] \longmapsto \mathbb{F}[x;\sigma],\ \sum_{i=0}^{r} g_i x^i \longmapsto \sum_{i=0}^{r} x^{r-i} g_i = \sum_{i=0}^{r} \sigma^i(g_{r-i}) x^i$$

در این صورت $\rho l(g)$ معکوس چپ g نامیده می‌شود. علاوه براین، اتومورفیسم σ را از طریق $\sigma(\sum_{i=0}^{r} g_i x^i) = \sum_{i=0}^{r} \sigma(g_i) x^i$ به حلقه $\mathbb{F}[x;\sigma]$ تعمیم می‌دهیم. آنگاه σ یک اتومورفیسم حلقه‌ای از $\mathbb{F}[x;\sigma]$ است که برای هر $g \in \mathbb{F}[x;\sigma]$ رابطه $xg = \sigma(g)x$ برقرار است.

دیدیم برای $f = x^n - a$ ماتریس دوری اریب Γ_f^σ را با Γ_a^σ نشان می‌دهیم. در اینجا باید با پیمانه متفاوت $x^n - a$ و $x^n - c$ سروکار داشته باشیم و قطعاً نماد $\Gamma_c^\sigma(\overline{g})$ به این معناست که هم مجموعه g به پیمانه $(x^n - c)$• را انتخاب کرده است.

قضیه ۱.۱.۶. فرض کنید $x^n - a = hg$ و قرار دهید $c = \sigma^n(g_\circ)ag_\circ^{-1}$ جایی که $g_\circ$ ضریب ثابت g باشد. در این صورت $\Gamma_a^\sigma(\overline{g'g}) = \Gamma_c^\sigma(\overline{g'})\Gamma_a^\sigma(\overline{g})$ داریم $g' \in \mathbb{F}[x;\sigma]$ و برای هر $x^n - c = \sigma^n(g)h$.

با توجه به اتومورفیسم σ^n در تعریف ۲.۳.۲ می‌بینیم c تعریف شده در قضیه، مزدوج $a^{g_\circ}$ می‌باشد. اگر $c = a$، یعنی $\sigma^n(g_\circ) = g_\circ$ آنگاه رابطه بهتر $\Gamma_a^\sigma(\overline{g'g}) = \Gamma_a^\sigma(\overline{g'})\Gamma_a^\sigma(\overline{g})$ را داریم که به عنوان تعمیم حالت دوطرفه در قضیه ۱.۲.۵ در نظر گرفته می‌شود. با این حال، نتیجه فوق فقط برای مقسوم‌علیه‌های راست g از $x^n - a$ برقرار است. به طور مثال، با کمک رابطه (۵.۵) چک کنید که برای هر $b \neq \circ$، رابطه $\Gamma_a^\sigma(\overline{x(x+1)}) \neq \Gamma_b^\sigma(\overline{x})\Gamma_a^\sigma(\overline{x+1})$ برقرار است، مگر اینکه $a = \sigma(a) = b$.

فرمول حاصلضرب فوق در قضیه زیر نقش اصلی را ایفا می‌کند و بیان می‌کند که ترانهاده ماتریس $(\sigma, x^n - a)$_ دوری، برای یک ثابت مناسب a' ماتریس $(\sigma, x^n - a')$_دوری است.

قضیه ۲.۱.۶. فرض کنید $g, h \in \mathbb{F}[x;\sigma]$ از درجه r و $k = n - r$ موجودند که رابطه $x^n - a = hg$ برقرار باشد. مجدداً قرار دهید $c = \sigma^n(g_\circ)ag_\circ^{-1}$ جایی که $g_\circ$ ضریب ثابت g باشد. در این صورت داریم:

$$\Gamma_a^\sigma(\overline{g})^T = \Gamma_{c^{-1}}^\sigma(\overline{g^\#}) = \Gamma_{\sigma^k(c^{-1})}^\sigma(\overline{g^\circ})\Gamma_{c^{-1}}^\sigma(\overline{x^k})$$

جایی که $g^\# = a\sigma^k(\rho l(g))x^k$ و $g^\circ = a\sigma^k(\rho l(g))$. به علاوه، g° مقسوم‌علیه راست پیمانه‌های $x^n - \sigma^k(c^{-1})$ است.

نتیجه به دست آمده ملاحظه ۱.۱.۴ (ج) و (د) را تعمیم می‌دهد: اگر $f = x^n - 1 = hg$ و $\sigma = id$، آنگاه $g^\circ = \rho(g)$، $c = 1$ و بنابراین $g^\# = \rho(g)x^k$. پیمانه‌های علاوه براین، به طور کلی و در مقایسه با ملاحظه ۱.۱.۴ (ه)، g° مقسوم‌علیه راست پیمانه‌های $x^n - \sigma^k(c^{-1})$ می‌باشد، در صورتی که عامل $\overline{g^\#}$ با درجه کمتر از n بطور کلی مقسوم‌علیه $x^n - c^{-1}$ نیست. به این دلیل، برای ترانهاده ماتریس دوری اریب $\Gamma_a^\sigma(\overline{g})$، دو فرمول ارائه می‌دهیم. فرمول اول فوق، جالب توجه می‌باشد زیرا بیان می‌کند که ترانهاده مجدداً یک ماتریس دوری اریب است. فرمول دوم می‌گوید که کد دوری_ثابت اریب $(\overline{g})$•، به عبارتی فضای سطری $\Gamma_a^\sigma(\overline{g})$ با فضای سطری ترانهاده ماتریس دوری اریب برابر است که نشان می‌دهد چندجمله‌ای، مقسوم‌علیه راست پیمانه‌ها می‌باشد. در همه این موارد، مهم است که g مقسوم‌علیه راست پیمانه‌های $x^n - a$ باشد، در غیر این صورت ترانهاده ماتریس $\Gamma_a^\sigma(\overline{g})$ به طور کلی یک ماتریس دوری اریب محسوب نمی‌شود.

۲.۶ دوگان کدهای دوری_ثابت اریب

در این بخش می‌خواهیم یک ماتریس کنترل توازن را به دست بیاوریم که ساختار دوری_ثابت اریب کد را نشان می‌دهد و همچنین قسمت دوری_ثابت (σ, a^{-1})_اریب کد دوگان $\mathcal{C}^{\perp}$ نیز با کمک رابطه (۲.۵) بررسی می‌شود.

قضیه ۱.۲.۶. فرض کنید $x^n - a = hg$ جایی که $\deg(g) = r$ و $\deg(h) = k = n - r$. قرار دهید $h^{\circ} := \rho l(\sigma^{-n}(h))$. در این صورت $h^{\circ}|_r(x^n - a^{-1})$. کد دوری_ثابت (σ, a)_اریب $\mathcal{C} = \mathfrak{b}_{x^n-a}(^{\bullet}(\overline{g}))$ را در نظر بگیرید. در این صورت $\Gamma^{\sigma}_{a}(\overline{g})\Gamma^{\sigma}_{a^{-1}}(\overline{h^{\circ}})^T = 0$ و $\mathrm{rk}(\Gamma^{\sigma}_{a^{-1}}(\overline{h^{\circ}})) = n-k$. بنابراین

$$\mathcal{C} = \mathrm{rs}(\Gamma^{\sigma}_{a}(\overline{g})) = \{c \in \mathbb{F}^n \mid \Gamma^{\sigma}_{a^{-1}}(\overline{h^{\circ}}))c^T = 0\}$$

و $(n-k)\times n$_زیرماتریس متشکل از $n-k$ سطر اول از $\Gamma^{\sigma}_{a^{-1}}(\overline{h^{\circ}})$، ماتریس کنترل توازن $\mathcal{C}$ است. در نتیجه، کد دوگان $\mathcal{C}^{\perp}$، دوری_ثابت (σ, a^{-1})_ اریب با چندجمله‌ای مولد (غیر تکین) h° و ماتریس مولد و کنترل توازن به ترتیب $n-k$ سطر اول از $\Gamma^{\sigma}_{a^{-1}}(\overline{h^{\circ}})$ و k سطر اول از $\Gamma^{\sigma}_{a}(\overline{g})$ به دست می‌آیند.
واضح است ماتریس کنترل توازن کد $\mathcal{C}$ متناظر رابطه ۶.۵ می‌باشد و به همین دلیل ساختار دوری_ثابت اریب کد $\mathcal{C}$ را نشان می‌دهد. همانند گزاره ۲.۱.۵، فضای سطری کد $\mathcal{C}$ برابر با فضای سطری تام ماتریس دوری اریب $\Gamma^{\sigma}_{a^{-1}}(\overline{h^{\circ}})$ است. در حالت دوری جابه‌جایی، جایی که $x^n - 1 = hg = gh$، داریم $a^{-1} = a = 1$ و $h^{\circ} = \rho(h)$ و بنابراین ملاحظه ۲.۱.۴ (ب) بازیابی می‌گردد.

با درک دوگانگی کدهای دوری_ثابت اریب، می‌توانیم خود_دوگانگی را بیان کنیم که نتیجه زیر مطرح می‌گردد.

نتیجه ۱.۲.۶. اگر کد خود_دوگان دوری_ثابت (σ, a)_اریب به طول n وجود داشته باشد، آنگاه n، زوج است و $a = \pm 1$. به ویژه، فرض کنید n زوج است و پیمانه‌های $x^n - \epsilon$ را در نظر بگیرید جایی که $\epsilon \in \{1, -1\}$. در این صورت، یک کد دوری_ثابت اریب خود_دوگان به طول n وجود دارد اگر و تنها اگر یک چندجمله‌ای $h \in \mathbb{F}[x;\sigma]$ وجود داشته باشد به طوری که $x^n - \epsilon = hh^{\circ}$. در این حالت کد خود_دوگان از رابطه $\mathcal{C} = \mathfrak{b}_{x^n-\epsilon}(^{\bullet}(\overline{h^{\circ}}))$ به دست می‌آید.

از $x^n - \epsilon = hh^{\circ}$ برای شمارش یا ساخت کدهای دوری_ثابت اریب خود_دوگان با مینیمم فاصله بسیار خوب، استفاده می‌شود.
حال به چندجمله‌ای‌های کنترل برای کدهای دوری_ثابت اریب می‌پردازیم. می‌دانیم در حلقه چند جمله‌ای‌های $\mathbb{F}[x]$ جایی که $x^n - 1 = hg$ برقرار باشد، h را چندجمله‌ای کنترل می‌نامیم به این دلیل که برای هر $z \in \mathbb{F}[x]$، رابطه $\overline{zh} = 0 \iff \overline{z} \in (\overline{g})$ برقرار می‌باشد. به عبارت دیگر $(\overline{h})$، ایده‌آل پوچ‌ساز $(\overline{g})$ است.

قضیه بعد چند جمله‌ای‌های کنترل را برای حلقه چند جمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ تعمیم می‌دهد که مبتنی بر این است که $x^n - a = hg$ می‌باشد.

قضیه ۲.۲.۶. فرض کنید $x^n - a = hg$ و قرار دهید $c = \sigma^n(g_\circ)ag_\circ^{-1}$ جایی که $g_\circ$ ضریب ثابت g باشد. $\tilde{c} = \sigma^{-n}(c)$ را تعریف کنید. در این صورت نگاشت

$$\Psi : \mathbb{F}[x;\sigma]/^\bullet(x^n - a) \longrightarrow \mathbb{F}[x;\sigma]/^\bullet(x^n - \tilde{c}),\ \overline{z} \longmapsto \overline{z\sigma^{-n}(h)}$$

یک نگاشت $\mathbb{F}[x;\sigma]$ـخطی چپ خوش تعریف با هسته $^\bullet(\overline{g})$ است و لذا $\sigma^{-n}(h)$ را چندجمله‌ای کنترل کد $\mathcal{C}$ می‌نامیم.

فصل ۷

فاصله کدهای دوری اریب

در این فصل، نحوه ساختن کدهای دوری اریب با مینیمم فاصله طراحی شده را بررسی خواهیم کرد. فاصله مدنظر در تمام نتایج این فصل، فاصله همینگ می‌باشد. (در نوشتارها، در مورد فاصله رتبه‌ای نیز معدود نتایجی وجود دارد). در سرتاسر این فصل همواره داریم، $\mathbb{F} = \mathbb{F}_{q^m}$ و σ یک خودریختی qـ فروبینیوس می‌باشد. علاوه براین، کد زیر را در نظر می‌گیریم:

$$\mathcal{C} = \mathfrak{b}((\overline{g})).$$

که برای چندجمله‌ای‌های تکین $f, g \in \mathbb{F}[x, \sigma]$ جایی که $\deg(f) = n$ و $g|_r f$ برقرار می‌باشد.

در سراسر این فصل، شرایطی برای f و g در نظر می‌گیریم که مینیمم فاصله مطلوب را تضمین می‌کنند.
در همه حالت‌های مد نظر ما، چند جمله‌ای مولد کد مورد نظر، کوچکترین مضرب مشترک چپ عوامل خطی بر روی برخی توسیع میدان‌ها می‌باشد و لذا g، یک Wـ چندجمله‌ای بر روی آن توسیع میدان می‌باشد؛ به قضیه ۲.۱.۳ (۱) نگاه کنید. در قضیه ۲.۲.۵، ماتریس کنترل توازن یک کد دوری اریب را مطرح کردیم که توسط یک Wـ چندجمله‌ای به شکل ماتریس واندرموند اریب تولید می‌شود. این ماتریس، اساس نتایجی است که در این فصل در مورد فاصله کدهای دوری اریب آورده خواهند شد.

۱.۷ کدهای BCH ـ اریب نوع اول

در این بخش شکل‌گیری کدهای BCH ـ اریب نوع اول را می‌بینیم. این دسته از کدها مبتنی بر چندجمله‌ای‌های مولدی هستند که ریشه‌های آن‌ها توان‌های عادی متوالی برخی عناصر می‌باشند.

قضیه ۱.۱.۷. فرض کنید b و δ دو عدد طبیعی باشند و $\alpha \in \overline{\mathbb{F}}$ وجود دارد به طوری که $\alpha^{[[\circ]]}, \alpha^{[[1]]}, \ldots, \alpha^{[[n-1]]}$ متمایز هستند و برای هر $i = \circ, \ldots, \delta - 2$ داریم:

$$g(\alpha^{b+i}) = \circ.$$

در این صورت، کد $\mathcal{C} = \mathfrak{b}_f(^\bullet(\overline{g}))$ دارای مینیمم فاصله δ است. اگر g کوچکترین چندجمله‌ای تکین با ریشه‌های $\alpha^b, \ldots, \alpha^{b+\delta-2}$ باشد، آنگاه $\mathcal{C}$ یک $(n, q^m, \alpha, b, \delta)$ ـ کد BCH ـ اریب اریب نوع اول نامیده می‌شود.

نتیجه ۱.۱.۷. قضیه ۱.۱.۷ و $\alpha \in \mathbb{F}$ را در نظر بگیرید. در این صورت چندجمله‌ای $g' := \mathrm{lclm}(x - \alpha^b, \ldots, x - \alpha^{b+\delta-2})$ حلقه چند جمله‌ای‌های اریب در $\mathbb{F}[x; \sigma]$ بوده و درجه آن $\delta - 1$ می‌باشد. بنابراین، برای هر مضرب چپ f' از g' با درجه n، کد دوری اریب $\mathfrak{b}_{f'}(^\bullet(\overline{g'}))$ دارای بعد $n - \delta + 1$ بوده و یک کد MDS می‌باشد و $(n, q^m, \alpha, b, \delta)$ ـ کد RS ـ اریب اریب نوع اول نامیده می‌شود.

قضیه ۱.۱.۷ حاصل این مطلب است که کد مورد نظر در هسته چپ ماتریس واندرموند اریب می‌باشد (به رابطه ۲.۳ نگاه کنید).

$$V_n(\alpha^b, \ldots, \alpha^{b+\delta-2}) = \begin{pmatrix} 1 & \ldots & 1 \\ (\alpha^{[[1]]})^b & \ldots & (\alpha^{[[1]]})^{b+\delta-2} \\ \vdots & & \vdots \\ (\alpha^{[[n-1]]})^b & \ldots & (\alpha^{[[n-1]]})^{b+\delta-2} \end{pmatrix}.$$

ستون‌های ماتریس از $[[i]]$ ـ توان‌های متوالی $\alpha^b, \ldots, \alpha^{b+\delta-2}$ تشکیل شده است در حالی‌که سطرها از توان‌های عادی متوالی $\alpha^{[[\circ]]}, \ldots, \alpha^{[[n-1]]}$ تشکیل شده است. در سطرها اینکه $\alpha^{[[\circ]]}, \alpha^{[[1]]}, \ldots, \alpha^{[[n-1]]}$ متمایز هستند، تضمین می‌کند که هر $(\delta - 1) \times (\delta - 1)$ ـ مینور ناصفر از $V_n(\alpha^b, \ldots, \alpha^{b+\delta-2})$ فاصله طراحی شده را تعیین می‌کند.

قضیه ۲.۱.۷. فرض کنید f دارای یک ضریب ثابت ناصفر می‌باشد و $b, v \in \mathbb{N}_\circ$ و $\delta, t_1, t_2 \in \mathbb{N}$ و $\alpha \in \overline{\mathbb{F}}$ وجود دارند به طوری که:

(i) $g(\alpha^{b+t_1 i+t_2 j}) = \circ$ برای هر $j = \circ, \ldots, v$ و $i = \circ, \ldots, \delta - 2$.

(ii) $(\alpha^{t_\ell})^{[[i]]} \neq ۱$ برای $\ell = ۱,۲$ و $i = ۱,\dots,n-۱$ (اگر $v = ۰$، آنگاه شرط $\alpha^{t_۲}$ حذف می‌شود).

در این صورت کد $\mathfrak{b}_f(^\bullet(\overline{g})) \subseteq \mathbb{F}^n$ دارای مینیمم فاصله $\delta+v$ می‌باشد که یک $(n, q^m, \alpha, b, t_۱, t_۲, \delta)$ ـ کد BCH ـ اریب اریب نوع اول نیز نامیده شود.

توجه داشته باشید که برای $v = ۰$ و $t_۱ = ۱$، این قضیه به قضیه ۱.۱.۷ کاهش می‌یابد، زیرا شرط (ii) هم‌ارز $\alpha^{[[۰]]}, \alpha^{[[۱]]}, \dots, \alpha^{[[n-۱]]}$ که متمایز هستند، می‌شود.

از آنجایی که کد ساخته شده دارای بعد $n-\deg(g)$ است، پس نحوه یافتن کوچکترین چندجمله‌ای تکین g با صدق کردن در شرط (i) (و با حداکثر درجه n) باید مورد بررسی قرار بگیرد. در گزاره ۲.۱.۵ (ج) دیدیم پیمانه‌های f در ماتریس مولد کد $\mathfrak{b}_f(^\bullet(\overline{g})) \subseteq \mathbb{F}^n$، نقشی ندارند. بنابراین، به محض یافتن g، هر مضرب چپ تکین f از درجه n کافی است. چندجمله‌ای g به صورت زیر به دست می‌آید که نتیجه مستقیم مثال ۳.۱.۳ می‌باشد.

ملاحظه ۱.۱.۷. قضیه ۲.۱.۷ را در نظر گرفته و فرض کنید α در توسیع میدان $\mathbb{F}_{q^{ms}}$ از $\mathbb{F} = \mathbb{F}_{q^m}$ باشد. قرار دهید:

$$A = \{\tau(\alpha^t) \mid \tau \in Aut(\mathbb{F}_{q^{ms}}|\mathbb{F}), t \in T\} \quad \text{و} \quad T = \{b+t_۱i+t_۲j \mid i = ۰,\dots,\delta-۲, j = ۰,\dots,v\}$$

در این صورت، $g := m_A$ در حلقه چند جمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ قرار دارد و کوچکترین چندجمله‌ای تکینی است که در قضیه ۲.۱.۷ شرط (i) صدق می‌کند.

مثال ۱.۱.۷. توسیع میدان $\mathbb{F}_{۲^{۱۲}} \mid \mathbb{F}_{۲^۶}$ را در نظر بگیرید. فرض کنید α عنصر اولیه $\mathbb{F}_{۲^{۱۲}}$ با چندجمله‌ای مینیمال $x^{۱۲} + x^۷ + x^۶ + x^۵ + x^۳ + x + ۱$، $\gamma = \alpha^{۶۵}$ عنصر اولیه $\mathbb{F}_{۲^۶}$ و σ خودریختی ۲ـ فروبینیوس باشد. فرض کنید $v = ۰$، $\delta = ۴$، $t_۲ = ۱$، $t_۱ = ۲۳$، $b = ۰$. چون $v = ۰$ لذا شرط (ii) قضیه ۲.۱.۷ به $(\alpha^۳)^{[[i]]} \neq ۱$ برای $i = ۰,\dots,n-۱$ می‌رسد. از آنجایی که $i = ۱۲$ کوچکترین عدد صحیح مثبت است که $(\alpha^۳)^{[[i]]} = ۱$، پس می‌توانیم کدهای BCH ـ اریب با طول ۱۲ بسازیم. شرط (i) و ملاحظه ۱.۱.۷ نشان می‌دهند که g مطلوب با $g = m_A$ به دست می‌آید جایی که

$$A = \{\alpha^۰, \alpha^{۲۳}, \alpha^{۴۶}, (\alpha^۰)^{۲^۶}, (\alpha^{۲۳})^{۲^۶}, (\alpha^{۴۶})^{۲^۶}\} \subseteq \mathbb{F}_{۲^{۱۲}}.$$

بنابراین $g = \operatorname{lclm}(x-a \mid a \in A)$ و در نتیجه $g = x^۳ + \gamma^{۴۷}x^۲ + \gamma^{۱۹}x + \gamma^{۴۰}$.

با ساخت کد برای هر مضرب چپ تکین f از g از درجه $۳ \leq n \leq ۱۲$، کد BCH ـ اریب $\mathcal{C} = \mathfrak{b}(^\bullet(\overline{g})) \subseteq \mathbb{F}^n$ دارای مینیمم فاصله ۴ و بعد $n-۳$ است لذا یک کد MDS می‌باشد. بیان این مسئله که چندجمله‌ای $f = x^{۱۲} - ۱$ مضرب چپ g است، جالب توجه می‌باشد و بنابراین برای طول $n = ۱۲$، کد σ ـ دوری است. برای هر طول بین $۳ \leq n \leq ۱۱$، کد σ ـ دوری ـ ثابت نیست. در نهایت، توجه داشته باشید که طبق تعریف، g یک W ـ چندجمله‌ای در $\mathbb{F}_{۲^{۱۲}}[x;\sigma]$ است؛ ولی در $\mathbb{F}_{۲^۶}[x;\sigma]$ یک W ـ چندجمله‌ای نیست (و چندجمله‌ای مینمال مجموعه صفر در $\mathbb{F}_{۲^۶}$ نیست).

۲.۷ کدهای BCH ـ اریب نوع دوم

در این بخش، کدهای BCH ـ اریب از نوع دوم را مطرح می‌کنیم که مبتنی بر چندجمله‌ای‌های مولدی بوده که ریشه‌های آن‌ها q ـ توان‌های متوالی از برخی عناصر می‌باشند. در انتها با دو مثال و تشریح روند ساخت، بخش را به پایان می‌رسانیم.
کدهای مطرح شده در این بخش σ ـ دوری هستند، به عبارتی با توجه به پیمانه‌های مرکزی $x^n - ۱$، دوری اریب هستند و بر روی توسیع میدان $\mathbb{F}_{q^n}$ از $\mathbb{F} = \mathbb{F}_{q^m}$ تعریف شده‌اند.

قضیه ۱.۲.۷. فرض کنید σ بر روی $\mathbb{F}_{q^n}$ خودریختی q ـ فروبینیوس باشد. فرض کنید $f = x^n - ۱$ و $g \in \mathbb{F}_{q^n}[x;\sigma]$ مقسوم‌علیه راست f و $\alpha \in \mathbb{F}_{q^n}$ وجود دارند به طوری که $\alpha, \alpha^q, \ldots, \alpha^{q^{n-۱}}$، پایه نرمال $\mathbb{F}_{q^n}$ بر روی $\mathbb{F}_q$ می‌باشد و قرار دهید $\beta = \alpha^{-۱}\sigma(\alpha) = \alpha^{q-۱}$. فرض کنید $\delta, t_۱, t_۲ \in \mathbb{N}$ و $b, v \in \mathbb{N}_۰$ وجود دارند به طوری که $\gcd(n, t_۱) = ۱$ و $\gcd(n, t_۲) < \delta$ و

$$g(\beta^{q^{b+it_۱+jt_۲}}) = ۰, \quad i = ۰, \ldots, \delta - ۲,\ j = ۰, \cdots, v.$$

در این صورت کد $\mathfrak{b}_f(^\bullet(\overline{g})) \subseteq \mathbb{F}_{q^n}^n$ دارای مینیمم فاصله $\delta + v$ است.

در مثال ۶.۱.۳ دیدیم که $x^n - ۱ = \operatorname{lclm}(x - \beta^{q^t} \mid t = ۰, \ldots, n-۱)$. بنابراین، شرط ریشه g با این شرط که g مقسوم‌علیه راست f است در تضاد نیست.
حال، فرض کنیم $n = ms$، به طوری که $\mathbb{F}_{q^n}$ توسیع میدان $\mathbb{F}_{q^m}$ باشد. در مرجع [۲۰]، نحوه ساختن کد قضیه قبل، بر روی زیرمیدان $\mathbb{F} = \mathbb{F}_{q^m}$ با مینیمم فاصله یکسان طراحی شده $\delta + s$ نشان داده شده است.
با توجه به کدهای BCH ـ اریب نوع اول، می‌خواهیم کوچکترین چندجمله‌ای تکین g در $\mathbb{F}_{q^m}[x;\sigma]$ را با ریشه‌های مطلوب به دست بیاوریم. با توجه به ملاحظه ۱.۱.۷ این چندجمله‌ای با جابه‌جایی مجموعه T و $\tilde{T}$ به دست می‌آید:

$$\tilde{T} = \{q^{b+it_۱+jt_۲} \mid i = ۰, \ldots, \delta - ۲,\ j = ۰, \ldots, v\}$$

قابل توجه است که $\operatorname{Aut}(\mathbb{F}_{q^{ms}} \mid \mathbb{F}_{q^m}) = \{\tau_۰, \ldots, \tau_{s-۱}\}$ جایی که $\tau_\ell(\alpha) = a^{q^{\ell m}}$ و در نتیجه مجموعه $A = \{\tau(\alpha^t) \mid t \in T, \tau \in \operatorname{Aut}(\mathbb{F}_{q^{ms}} \mid \mathbb{F}_{q^m})\}$ توسط مجموعه زیر به دست می‌آید:

$$A = \{\alpha^{q^{b+it_۱+jt_۲+\ell m}} \mid i = ۰, \ldots, \delta - ۲,\ j = ۰, \cdots, v,\ \ell = ۰, \ldots, s - ۱\}.$$

کل این رابطه را می‌توان به صورت q ـ توان‌ها در گروه دوری C_{ms} با مرتبه ms بیان نمود. C_s، گروه دوری مرتبه s را به عنوان زیرگروهی از C_{ms} در نظر بگیرید. علاوه براین، فرض کنید $X_۰ = C_s, X_۱, \ldots, X_{m-۱}$، هم مجموعه‌های C_s در C_{ms} باشند. در این صورت، ملاحظه ۱.۱.۷ و قضیه ۱.۲.۷ منجر به قضیه زیر می‌گردند.

قضیه ۲.۲.۷. قضیه ۱.۲.۷ را در نظر بگیرید. فرض کنید $n = ms$ و مجموعه $S = \{b + it_1 + jt_2 \mid i = 0, \dots, \delta - 2,\ j = 0, \dots, v\}$ را به عنوان زیرمجموعه‌ای از C_{ms} در نظر بگیرید (که خوش تعریف است، زیرا $\sigma^{ms} = id$). $\overline{S}$ را به عنوان کوچکترین اجتماع هم مجموعه‌های X_i شامل S تعریف کنید. در این صورت، چندجمله‌ای $g' = \mathrm{lclm}(x - \beta^{q^t} \mid t \in \overline{S})$ در حلقه چند جمله‌ای‌های اریب $\mathbb{F}[x;\sigma]$ قرار دارد. بنابراین، کد دوری (σ, f) ـ اریب $\mathcal{C} = \mathfrak{b}_f(^\bullet(\overline{g'}))$ به طول $n = ms$ بر روی $\mathbb{F}$ تعریف می‌شود. کد $\mathcal{C}$ دارای مینیمم فاصله $\delta + v$ است و یک $(n, q^m, \alpha, b, t_1, t_2, \delta)$ ـ کد BCH ـ اریب نوع دوم نامیده می‌شود.

مثال ۱.۲.۷. مانند مثال ۱.۱.۷، توسیع میدان $\mathbb{F}_{2^{12}} \mid \mathbb{F}_{2^6}$ با عنصر اولیه α و داده‌های یکسان $v = 0$، $\delta = 4$، $t_2 = 1$، $t_1 = 23$، $b = 0$ و $\gamma = \alpha^{65}$ را در نظر بگیرید. عنصر α^5 پایه نرمال $\mathbb{F}_{2^{12}}$ بر روی $\mathbb{F}_2$ را تولید می‌کند. بنابراین، $\beta = \alpha^{-5}\sigma(\alpha^5) = \alpha^5$. در اینجا باید مجموعه $S = \{b + it_1 \mid i = 0, 1, 2\} = \{0, 11, 10\}$ را در نظر گرفته و کوچکترین اجتماع هم مجموعه‌های C_2 در C_{12} شامل S را بیابیم که $\overline{S} = \{0, 6, 11, 5, 10, 4\}$ می‌باشد. لذا

$$\mathrm{lclm}(x - (\alpha^5)^{q^t} \mid t \in \overline{S}) = x^6 + \gamma^{61}x^5 + \gamma^{41}x^4 + \gamma^4 x^3 + \gamma^{20}x^2 + \gamma^{46}x + \gamma^7 \in \mathbb{F}_{2^6}[x;\sigma]$$

بر روی میدان $\mathbb{F}_{2^6}$ یک کد دوری اریب با طول ۱۲ و مینیمم فاصله طراحی شده ۴ تولید می‌کند. این کد دارای بعد ۶ و مینیمم فاصله حقیقی ۶ می‌باشد و بنابراین، یک کد MDS نمی‌باشد.

در نهایت، ارزیابی کدها را در محیط چندجمله‌ای اریب بیان می‌کنیم. به خاطر بیاورید که ارزیابی زیر، $p(\alpha_i)$، مطابق تعریف ۱.۳.۲ انجام شده است.

قضیه ۳.۲.۷. فرض کنید $k \in \{1, \dots, n-1\}$ و $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ وجود دارند به طوری که ماتریس واندرموند اریب $V_n(\alpha_1, \dots, \alpha_n) \in \mathrm{Mat}_{n,n}(\mathbb{F})$ دارای رتبه n باشد. در این صورت کد

$$\varepsilon_{\sigma,\alpha_1,\dots,\alpha_n} := \{(p(\alpha_1), \dots, p(\alpha_n)) \mid p \in \mathbb{F}[x;\sigma],\ \deg p \le k-1\} \subseteq \mathbb{F}^n$$

دارای بعد k و مینیمم فاصله $n - k + 1$ است و یک کد MDS می‌باشد.

طبق قضیه ۱.۱.۳، رتبه ماتریس واندرموند اریب با درجه چند جمله‌ای مینیمال مجموعه $\{\alpha_1, \dots, \alpha_n\}$ که $\mathrm{lclm}(x - \alpha_i \mid i = 1, \dots, n)$ می‌باشد، برابر است. بنابراین شرط رتبه‌ای فوق هم‌ارز $\deg(\mathrm{lclm}(x - \alpha_i \mid i = 1, \dots, n)) = n$ است. در حالت معمولی جایی که $\sigma = id$، این رابطه هم‌ارز $\alpha_1, \dots, \alpha_n$ که متمایز هستند، می‌باشد و کد $\varepsilon_{id,\alpha_1,\dots,\alpha_n}$ یک کد $[n,k]$ ـ رید ـ سالومون تعمیم‌یافته است.

اثبات قضیه ۳.۲.۷ همانند حالت معمولی کدهای رید ـ سالومون تعمیم یافته با کمک قضیه ۱.۱.۳ انجام می‌گیرد. کاملاً واضح است که در بسیاری از حالت‌های معمولی کدهای رید ـ سالومون تعمیم‌یافته، دوری هستند، مثلاً $\varepsilon_{id,\alpha_1,\dots,\alpha^{n-1}}$ دوری است، اگر α عنصر اولیه $\mathbb{F}$ باشد و $n \le |\mathbb{F}|$.

مراجع

[۱] ناهید باقری هاشم‌آباد، *کدهای دوری روی حلقه‌های چندجمله‌ای اریب*، پایان نامه کارشناسی ارشد، انتشارات دانشگاه صنعتی شاهرود، ۱۳۹۷.

[2] D. Boucher, Construction and number of self-dual skew codes over $\mathbb{F}_{p^2}$, *Adv. Math.Commun.*, 10 (2016), 765–795.

[3] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *AAECC*, 18 (2007), 379–389.

[4] D. Boucher and F. Ulmer, Codes as modules over skew polynomial rings, In M. G. Parker, editor, *Cryptography and Coding, 12th IMA International Conference. Lecture Notes in Computer Science*, 2009, 38–55.

[5] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.*, 44 (2009), 1644–1656.

[6] D. Boucher and F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, *Des. Codes Cryptogr.*, 70 (2014), 405–431.

[7] D. Boucher and F. Ulmer, Self-dual skew codes and factorizations of skew polynomials, *J. Symb. Comput.*, 60 (2014), 47–61.

[8] M. Boulagouaz and A. Leroy, (σ, δ)-Codes, *Adv. Math. Commun.*, 7 (2013), 463–474.

[9] X. Caruso and J. Le Borgne, A new faster algorithm for factoring skew polynomials over finite fields, *J. Symb. Comp.*, 79 (2017), 411–443.

[10] L. Chaussade, P. Loidreau and F. Ulmer, Skew codes of prescribed distance or rank, *Des. Codes Cryptogr.*, 50 (2009), 267–284.

[11] P. M. Cohn, *Free Rings and Their Relations*, Academic Press, London, 2. edition,1985.

[12] P. J. Davis, *Circulant Matrices*, A Wiley-Interscience Publication, New York,1979.

[13] N. Fogarty, *On Skew-Constacyclic Codes*, PhD thesis, University of Kentucky,2016.

[14] N. Fogarty and H. Gluesing-Luerssen, A circulant approach to skew-constacyclic codes, *Finite Fields Appl.*, 35 (2015), 92–114.

[15] E. M. Gabidulin, Theory of codes with maximal rank distance, *Probl. Inf. Transm.*, 21 (1985), 1–12.

[16] E. M. Gabidulin, Rank q-cyclic and pseudo-q-cyclic codes, *In Proceedings of the IEEE International Symposium on Information Theory ISIT 2009 (Seoul, Korea)*, 2009, 2799-2802.

[17] J. Gao, L. Shen and F.-W. Fu, A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields, *Cryptogr. Commun.*, 8 (2016), 51–66. See also: arXiv: 1309.1621 (different title).

[18] M. Giesbrecht, Factoring in skew-polynomial rings over finite fields, *J. Symb.Comput.*, 26 (1998), 463–486.

[19] J. G´omez-Torrecillas, F. J. Lobillo and G. Navarro, Peterson-Gorenstein-Zierler algorithm for skew RS codes, *Linear and Multilinear Algebra*, 66 (2018), 469-487.

[20] J. G´omez-Torrecillas, F. J. Lobillo, G. Navarro and A. Neri, Hartmann-Tzeng bound and skew cyclic codes of designed Hamming distance, *Finite Fields Appl.*, 50 (2018), 84–112.

[21] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[22] N. Jacobson, *The Theory of Rings*, American Mathematical Society, 1943.

[23] N. Jacobson, *Finite Dimensional Division Algebra over Fields*, Springer, NewYork, 1996.

[24] I. Kra and S. R. Simanca, On circulant matrices, *Not. Amer. Math. Soc.*, 59 (2012), 368–377.

[25] T. Y. Lam, A general theory of Vandermonde matrices, *Expos. Math.*, 4 (1986), 193–215.

[26] T. Y. Lam and A. Leroy, Vandermonde and Wronskian matrices over division rings, *J.Algebra*, 119 (1988), 308–336.

[27] T. Y. Lam and A. Leroy, Wedderburn polynomials over division rings, I. *J. PureAppl.Algebra*, 186 (2004), 43–76.

[28] T. Y. Lam, A. Leroy and A. Ozturk, Wedderburn polynomials over division rings, II. *Noncommutative rings, group rings, diagram algebras and their applications* (S.K. Jain, Ed.), *Contemp. Math.*, 456 (2008), 73–98.

[29] A. Leroy, Noncommutative polynomial maps, *J. Algebra Appl.*, 11(4), 2012.

[30] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[31] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, NorthHoland, 1977.

[32] U. Mart´ınez-Pe˜nas, On the roots and minimum rank distance of skew cyclic codes, *Des. Codes Cryptogr.*, 83 (2017), 639–660.

[33] O. Ore, Theory of non-commutative polynomials, *Annals Math.*, 34 (1933), 480–508.

[34] L. F. Tapia Cuiti˜no and A. L. Tironi, Some properties of skew codes over finite fields, *Des. Codes Cryptogr.*, 85 (2017), 359–380.

[35] A. E. A. Valdebenito and A. L. Tironi, On the duals codes of skew constacyclic codes, *Adv. Math. Commun.*, 12 (2018), 659–679.

[36] B. Wu and Z. Liu, Linearized polynomials over finite fields revisited, *Finite Fields Appl.*, 22 (2013), 79–100.

واژه‌نامه فارسی به انگلیسی

الگوریتم اقلیدسی ..... Euclidean algorithm
ایده‌آل ..... Ideal
ایده‌آل اصلی ..... Principal ideal
ایده‌آل چپ ..... Left ideal
ایده‌آل راست ..... Right ideal
ایده‌آل دوطرفه ..... Two-sided ideal

بزرگ‌ترین مقسوم‌علیه مشترک ..... Greatest common divisor

تجزیه ..... Factorization
تحویل‌پذیر ..... reducible
تحویل‌ناپذیر ..... Irreducible
تکین ..... Monic

چندجمله‌ای ..... Polynomial
چند جمله‌ای مولد ..... Generating polynomial

حداقل فاصله ..... Minimum distance
حلقه ..... Ring
حلقه ایده‌آل اصلی ..... Principal ideal ring
حلقه چند جمله‌ای اریب ..... Skew polynomial ring
حلقه خارج‌قسمتی ..... Quotient ring

خودریختی ..... Automorphism
خودریختی فروبنیوس ..... Frobenius automorphism

درجه ..... Degree

رتبه ..... Rank
ریشه ..... Root

فاصله همینگ ..... Hamming distance
فضای برداری ..... Vector space

کد ..... Code
کد بلوکی ..... Block code
کد خطی ..... Linear code
کد خود ـ دوگان ..... Self dual code
کد دوری ..... Cyclic code
کد دوری ـ ثابت اریب ..... Skew-Constacyclic code
کد دوگان ..... Dual code
کد واژه ..... Code word
کران ..... Bound
کوچکترین مضرب مشترک ..... Least common multiple

ماتریس دیکسون ..... Dickson matrix
ماتریس کنترل توازن ..... Parity check matrix
ماتریس مولد ..... Generator matrix
مدول ..... Module
مرتبه ..... Order
مزدوج ..... Conjugate
مقسوم‌علیه راست ..... Right divisor
مقسوم‌علیه چپ ..... Left divisor
مولد ..... Generator
میدان ..... Field
میدان متناهی ..... Finite field

یکریختی ..... Isomorphism

واژه‌نامه انگلیسی به فارسی

خودریختی ..... Automorphism

کران ..... Bound
کد بلوکی ..... Block code

کد ..... Code
کد واژه ..... Code word
مزدوج ..... Conjugate
کد دوری ..... Cyclic code

درجه ..... Degree
ماتریس دیکسون ..... Dickson matrix
کد دوگان ..... Dual code

الگوریتم اقلیدسی ..... Euclidean algorithm

تجزیه ..... Factorization
میدان ..... Field
میدان متناهی ..... Finite field
خودریختی فروبنیوس ..... Frobenius automorphism

چند جمله‌ای مولد ..... Generating polynomial
مولد ..... Generator
ماتریس مولد ..... Generator matrix
بزرگترین مقسوم‌علیه مشترک ..... Greatest common divisor

فاصله همینگ ..... Hamming distance

ایده‌آل ..... Ideal
تحویل‌ناپذیر ..... Irreducible
یکریختی ..... Isomorphism

مقسوم‌علیه چپ ..... Left divisor
ایده‌آل چپ ..... Left ideal
کد خطی ..... Linear code
کوچکترین مضرب مشترک ..... Least common multiple

حداقل فاصله ..... Minimum distance
مدول ..... Module
تکین ..... Monic

مرتبه ..... Order

ماتریس کنترل توازن ..... Parity check matrix
چند جمله‌ای ..... Polynomial
ایده‌آل اصلی ..... Principal ideal
حلقه ایده‌آل اصلی ..... Principal ideal ring

حلقه خارج‌قسمتی ..... Quotient ring

رتبه ..... Rank
تحویل‌پذیر ..... Reducible
مقسوم‌علیه راست ..... Right divisor
ایده‌آل راست ..... Right ideal
حلقه ..... Ring
ریشه ..... Root

کد خود ـ دوگان ..... Self dual code

کددوری ـ ثابت اریب ..... Skew-Constacyclic code

حلقه چند جمله‌ای اریب ..... Skew polynomial ring

ایده‌آل دوطرفه ..... Two-sided ideal

فضای برداری ..... Vector space

Abstract

In this thesis, we study skew-cyclic codes over skew-polynomial rings of automorphism type. Skew-polynomial rings have been introduced and discussed by Ore (1933), and they are one of the important classes of non-commutative rings. Evaluation of skew polynomials and sets of (right) roots were first considered by Lam (1986) and studied in great detail by Lam and Leroy thereafter. After a detailed presentation of the most relevant properties of skew polynomials, we study algebraic theory of skew-cyclic codes as introduced by Boucher and Ulmer (2007) and studied by many authors thereafter. Skew-circulant matrices playing explosion role in this study. Finally, skew-cyclic codes with designed minimum distance are discussed, and we study two different kinds of skew-BCH codes, which were designed recently.

Keywords: Cyclic code, Skew polynomial ring, Generator matrix, Parity check matrix, Generating polynomial, Minimum distance designed, BCH code, RS code.

Faculty Of Mathematical Sciences

MSc Thesis in Cryptography and Coding

Study of special cyclic codes over non-commutative rings

By: Afsane Arab Ahmadi

Supervisor:

Dr. Abdollah Alhevaz

Advisor:

Dr. Ebrahim Hashemi

January 2022