
بسم الله الرحمن الرحیم

دانشکده علوم ریاضی

رشته ریاضی کاربردی، گرایش گراف و ترکیبیات

پایان‌نامه کارشناسی ارشد

کدهای دوری روی حلقه‌های چندجمله‌ای اریب ناجابه‌جایی

نگارنده: ناهید باقری هاشم‌آباد

استادان راهنما

دکتر صادق رحیمی شعرباف
دکتر عبدالله آل‌هوز

استاد مشاور

دکتر ابراهیم هاشمی

مهر ۱۳۹۷

به پاس عاطفه سرشار و گرمای امید بخش وجودشان که در این سردترین روزگاران بهترین پشتیبان است

به پاس قلب‌های بزرگشان که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می‌گراید

و به پاس محبت‌های بی‌دریغشان که هرگز فروکش نمی‌کند

این مجموعه را به پدر و مادر عزیزم تقدیم می‌کنم.

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 اساتید ارجمندم آقای دکتر صادق رحیمی شعرباف و آقای دکتر عبدالله 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.
با تشکر و درود فراوان خدمت آقای دکتر ابراهیم هاشمی ریاست محترم دانشکده که زحمت مشاوره این پایان‌نامه را تقبل فرمودند و اینجانب را مورد راهنمایی قرار دادند.
در پایان از دوستان خوبم که در این دو سال برای من بهترین بودند، بسیار سپاسگزارم و برای همگی آنها بهترین‌ها را آرزو دارم.

تعهد نامه

اینجانب **ناهید باقری هاشم‌آباد** دانشجوی کارشناسی ارشد رشته **ریاضی کاربردی علوم ریاضی** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان **کدهای دوری روی حلقه‌های چندجمله‌ای** تحت راهنمایی دکتر **اریب ناجابه‌جایی** ، و دکتر **صادق رحیمی شعرباف** و **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.

ناهید باقری هاشم‌آباد

مهر ۱۳۹۷

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

به موازات تعریف کدهای دوری، ما کدهای خطی روی میدان‌های متناهی که به وسیله ایده‌آل‌های چپ حلقه خارج‌قسمتی چندجمله‌ای‌های اریب ناجابه‌جایی به دست می‌آیند را مورد مطالعه قرار می‌دهیم.

در این پایان‌نامه نشان می‌دهیم که چطور وجود و خواص این کدها به خواص ریاضی چندجمله‌ای‌های اریب ارتباط پیدا می‌کند.

این رده از کدها تعمیمی از θـ کدهای دوری معرفی شده می‌باشد. به هرحال θـ کدهای دوری یک نمایش ارزنده‌تر از این خانواده از کدها بوده و ما نشان می‌دهیم که دوگان θـ کدهای دوری نیز یک کد دوری می‌باشد.

با استفاده از مفهوم پایه‌های گروبنر، تمام θـ کدهای دوری خوددوگان هرمیتی و اقلیدسی روی میدان $\mathbb{F}_4$ از طول کمتر از ۴۰ را محاسبه می‌کنیم، که شامل $[۳۶, ۱۸, ۱۱]$ـθـ کد دوری خود دوگان اقلیدسی است که نتایج قبلی موجود برای کدهای خوددوگان با طول۳۶ روی میدان $\mathbb{F}_4$ را بهبود می‌بخشد.

کلمات کلیدی: ایده‌آل چپ، ایده‌آل دوطرفه، چندجمله‌ای تکین، حلقه چندجمله‌ای‌های اریب، حلقه خارج قسمتی، خودریختی، فاصله همینگ، کد خوددوگان اقلیدسی، کد خوددوگان هرمیتی، کدهای دوری، ماتریس کنترل توازن، ماتریس مولد، میدان متناهی.

مقدمه

نظریه کدگذاری شاخه‌ای از ریاضیات است که روش‌های کنترل خطاهای به وجود آمده در انتقال اطلاعات را بررسی می‌کند. این نظریه با وجود جوان بودن یکی از شاخه‌های پر کاربرد در ریاضیات محسوب می‌شود که به سرعت در حال گسترش است. نظریه‌ی کدگذاری با مقاله‌ای کلاسیک از شانون در سال ۱۹۴۸ متولد شد که در آن ثابت کرد ساختارهایی وجود دارد که با استفاده از آنها می‌توان اثر خطاهای به وجود آمده در انتقال اطلاعات را به دلخواه کم کرد. از آنجا که قضیه‌ی او به هیچ پرسشی در مورد نحوه‌ی ساخت این ساختارها پاسخ نمی‌داد، مطالعه در مورد کدهای کنترل کننده‌ی خطا به یک شاخه‌ی فعال تحقیق به نام نظریه‌ی کدگذاری منجر شد. این نظریه مثال بسیار جالبی از قدرت کاربردی شاخه‌های گوناگون ریاضیات مانند جبر، ترکیبیات و هندسه است که مورد توجه ریاضیدانان، متخصصان علوم کامپیوتر و مهندسان است. نظریه‌ی کدگذاری با استفاده از ابزارهای جبری و همچنین ریاضیات ترکیبی در صدد ایجاد ساختارهایی برای تبادل اطلاعات می‌باشد. مبحث اصلی این نظریه مطالعه‌ی روش‌هایی برای انتقال اطلاعات به صورت دقیق و کارآمد از محلی به محل دیگر است. چنین روش‌هایی می‌توانند کاربردهای بسیار متنوعی داشته باشند. انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر یا از یک حافظه به پردازشگر مرکزی و ارسال تصاویر و اطلاعات از فضا، تنها چند نمونه از این کاربردها هستند. این انتقال می‌تواند در زمان صورت گیرد، مانند زمانی که بخواهیم داده‌ای را ذخیره کنیم. بنابراین، کدگذاری در ذخیره‌ی داده روی دیسک‌های فشرده و DVD ها انجام می‌شود به طوری که حتی اگر خراشی روی دیسک به وجود آید بتوان از آن استفاده کرد. در این راستا کدهای بسیاری، از جمله کدهای خطی و در حالت خاص آن کدهای دوری، معرفی و مورد مطالعه قرار گرفته‌اند. یکی دیگر از انواع کدهای شناخته شده، کدهای شبه‌دوری می‌باشند که از دهه‌ی ۶۰ میلادی مورد مطالعه و بررسی قرار گرفته‌اند. کدهای دوری دارای خواص بسیار غنی می‌باشند، زیرا ارتباط نزدیکی با ایده‌آل‌های حلقه‌های خارج‌قسمتی از حلقه‌های چندجمله‌ای‌ها دارند. از این رو مورد مطالعه و بررسی بسیاری از محققان قرار گرفته‌اند.

مقالات زیادی در زمینه کدگذاری وجود دارند که از حلقه‌ی چندجمله‌ای‌های اریب استفاده کرده‌اند. انگیزه‌ی اصلی برای مطالعه‌ی کدها در این زمینه این است که چندجمله‌ای‌هایی که در حلقه‌ی چندجمله‌ای‌های اریب در معرض نمایش گذاشته می‌شوند از خواص بیشتری برخوردارند و بنابراین تعداد بیشتری ایده‌آل در حلقه‌ی چندجمله‌ای‌های اریب وجود دارد.

کدهای دوری دارای تعمیم‌های زیادی می‌باشند، یکی از مهمترین آنها کدهای دوری اریب می‌باشند که متناظر با ایده‌آل‌های حلقه‌ی چندجمله‌ای اریب هستند.

بوچر و همکارانش در مراجع [۱۰] و [۱۳]، کدهای دوری اریب را با استفاده از حلقه‌ی چندجمله‌ای‌های اریب با یک خودریختی θ روی یک میدان متناهی با q عضو تعریف کردند.

پس از آن، در خیلی از مقالات علمی، این مبحث از نظریه‌ی کدگذاری مورد تحقیق قرار گرفته است.

در این پایان‌نامه، کدهای دوری روی حلقه‌های چندجمله‌ای اریب ناجابجایی در نظر گرفته شده‌اند. در فصل اول این پایان‌نامه به بیان بعضی از مفاهیم و قضایا از جبر و نظریه کد که در فصل‌های بعد از آن استفاده خواهیم کرد می‌پردازیم. در فصل دوم کلیاتی از θـ کدها (دوری) را بیان می‌کنیم. در فصل سوم دوگان θـ کدها را مورد بررسی قرار می‌دهیم و در فصل آخر به بررسی کدهای دوری اریب روی حلقه‌ی $\mathbb{F}_p + u\mathbb{F}_p$ می‌پردازیم.

فهرست مطالب

فهرست جداول

فصل ۱

تعاریف و قضایای مقدماتی

۱.۱ مقدمه

در فصل اول این پایان‌نامه، به بیان بعضی مفاهیم و قضایا از جبر و نظریه کد برای ورود به مفاهیم بعدی، به شکل نسبتا مختصر می‌پردازیم. در بخش ۲.۱ مفاهیم جبر که شامل گروه[۱]، حلقه[۲]، حلقه چندجمله‌ای‌های اریب[۳]، میدان[۴]، میدان متناهی[۵] و ... می‌باشد مطرح می‌شود. بخش ۳.۱ شامل مفاهیم مقدماتی نظریه کدگذاری، مانند کدهای خطی[۶] ، ماتریس مولد[۷] ، ماتریس کنترل توازن[۸] ، کدگذاری کدهای خطی، کدهای دوری[۹]، کدهای خوددوگان اقلیدسی[۱۰] و کدهای خوددوگان هرمیتی[۱۱] را تعریف کردیم. در پایان این فصل، به بیان قضایای مورد نیاز پرداخته‌ایم.

---

[۱] Group
[۲] Ring
[۳] Skew polynomial ring
[۴] Field
[۵] Finite field
[۶] Linear codes
[۷] Generating matrix
[۸] Parity check matrix
[۹] Cyclic codes
[۱۰] Euclidean self-dual code
[۱۱] Hermitian self-dual code

منابع مورد استفاده در این فصل شامل [۱] و [۲] می‌باشند.

۲.۱ مفاهیم جبری

در این بخش تعریف گروه و حلقه را آورده و با استفاده از این تعاریف، تعریف میدان ارائه می‌شود.

تعریف ۱.۲.۱. فرض کنیم $*$ یک عمل دوتایی روی مجموعه‌ی G باشد. در این صورت ساختمان جبری $(G;*)$ یک **گروه** است اگر شرایط زیر برقرار باشد:

۱. $*$ شرکت‌پذیر باشد،

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

$$x * e = e * x = x$$

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

$$x * x' = x' * x = e$$

به علاوه اگر خاصیت زیر نیز برقرار باشد، گروه $(G;*)$ یک گروه **آبلی**[۱۲] یا جابه‌جایی نامیده می‌شود.

۴. $*$ جابه‌جایی باشد یعنی داشته باشیم:

$$\forall x, y \in G, x * y = y * x$$

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

تعریف ۲.۲.۱. فرض کنید G یک گروه باشد. در این صورت زیرمجموعه‌ی H از G یک **زیرگروه**[۱۳] G است اگر همراه با عمل دوتایی تعریف شده در G خود یک گروه باشد.

تعریف ۳.۲.۱. 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** 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:

$$(ab)c = a(bc)$$

---

[۱۲] Abelian

[۱۳] Subgroup

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

$$a(b+c) = ab + ac$$

و

$$(a+b)c = ac + bc$$

بنا به بند ۲ تعریف حلقه، ساختمان $(R, +, \cdot)$ 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:

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

مانند بخش قبل اگر R همراه با دو عمل جمع و ضرب یک حلقه باشد آنگاه به طور خلاصه‌تر می‌گوییم که R یک حلقه است. اگر علاوه بر شرط‌های ۱، ۲ و ۳ تعریف حلقه، شرط زیر نیز برقرار باشد، آنگاه می‌گوییم که 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.

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:

$$a\mathbb{1} = \mathbb{1}a = a.$$

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

تعریف ۴.۲.۱. فرض کنید R یک حلقه باشد. در این صورت زیرمجموعه‌ی S از R یک **زیرحلقه**[۱۴] 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 ۵.۲.۱. فرض کنیم R یک حلقه باشد و $a \in R$. در این صورت:

۱. a را یک **مقسوم‌علیه صفر چپ** می‌نامیم اگر عنصر $b \neq \circ$ در R وجود داشته باشد به طوری که داشته باشیم:

$$ab = \circ.$$

[۱۴] Subring

۲. a را یک **مقسوم‌علیه صفر راست** می‌نامیم اگر عنصر $c \neq 0$ در R وجود داشته باشد به طوری که داشته باشیم:

$$ca = 0.$$

۳. a را یک **مقسوم‌علیه صفر**[۱۵] می‌نامیم اگر a یک مقسوم‌علیه صفر چپ یا یک مقسوم‌علیه صفر راست باشد.

تعریف ۶.۲.۱. یک **دامنه‌ی صحیح** یک حلقه‌ی جابه‌جایی با یکه است که مقسوم علیه صفر غیربدیهی نداشته باشد.

حلقه‌های $(\mathbb{Z}, +, \cdot)$ ، $(\mathbb{Q}, +, \cdot)$ ، $(\mathbb{R}, +, \cdot)$ ، $(\mathbb{C}, +, \cdot)$ ، و به ازای هر عدد اول P ، $(\overline{\mathbb{Z}}_P, +, \cdot)$ دامنه‌ی صحیح هستند.

تعریف ۷.۲.۱. زیرمجموعه‌ی I از حلقه‌ی R یک **ایده‌آل**[۱۶] است اگر:

۱. I یک زیرگروه جمعی R باشد،

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

$$ai, ia \in I.$$

آ. I را یک **ایده‌آل چپ**[۱۷] R گویند اگر به ازای هر $a \in R$ و هر $i \in I$، داشته باشیم: $ai \in I$.

ب. I را یک **ایده‌آل راست**[۱۸] R گویند اگر به ازای هر $a \in R$ و هر $i \in I$، داشته باشیم: $ai \in I$.

پ. I را یک ایده‌آل[۱۹] (دوطرفه‌ی) R می‌گویند، اگر هم یک ایده‌آل چپ و هم یک ایده‌آل راست R باشد.

تعریف ۸.۲.۱. فرض کنیم X زیرمجموعه‌ای 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 متناهی و $X = \{x_1, x_2, \ldots, x_n\}$ باشد، آن‌گاه ایده‌آل $\langle X \rangle$ را با $\langle x_1, x_2, \ldots, x_n \rangle$ نشان داده و آن را **متناهی‌المولد** می‌گویند. اگر $X = \{x\}$، ایده‌آل $\langle X \rangle$ تولید شده توسط X را **ایده‌آل اصلی**[۲۰] تولید شده توسط x می‌نامند. **یک حلقه‌ی ایده‌آل اصلی** حلقه‌ای است که در آن هر ایده‌آل اصلی باشد. یک حلقه ایده‌آل اصلی که یک دامنه‌ی صحیح باشد، یک **دامنه‌ی ایده‌آل اصلی** نام دارد.

---

[۱۵] Zero divisor
[۱۶] Ideal
[۱۷] Left ideal
[۱۸] Right ideal
[۱۹] Ideal
[۲۰] Principal ideal

تعریف ۹.۲.۱. اگر I یک ایده‌آل از حلقه‌ی R باشند، R/I را **حلقه خارج‌قسمتی**[۲۱] R بر I می‌نامیم و داریم:

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

تعریف ۱۰.۲.۱. ایده‌آل P از حلقه‌ی جابه‌جایی R یک **ایده‌آل اول** است اگر برای هر $a, b \in R$ داشته باشیم:

$$a \cdot b \in P \Longrightarrow a \in P \vee b \in P.$$

تعریف ۱۱.۲.۱. 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 ۱۲.۲.۱. فرض کنید $(R, +, \cdot)$ و $(R', \oplus, \circ)$ دو حلقه باشند و $f : R \to R'$ یک تابع باشد. در این صورت f را یک **همریختی**[۲۲]**(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 ۱۳.۲.۱. فرض کنید f یک همریختی از یک حلقه‌ی R به یک حلقه‌ی R' باشد. در این صورت **هسته‌ی** f عبارت است از: $\ker(f) = \{a \in R | f(a) = \circ\}$.

تعریف ۱۴.۲.۱. فرض کنیم $f : R \to R'$ یک همریختی از یک حلقه‌ی R به یک حلقه‌ی باشد. در این صورت:

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

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

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

تعریف ۱۵.۲.۱. فرض کنید R یک حلقه باشد.

۱.هر همریختی $f : R \to R$ را یک **درونریختی** از R نامند.

۲.هر یکریختی $f : R \to R$ را یک **خودریختی**[۲۳] از R می‌نامند.

تعریف ۱۶.۲.۱. 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 Char(R) نشان می‌دهیم.

---

[۲۱] Quotient ring

[۲۲] Homomorphism

[۲۳] Automorphism

تعریف ۱.۲.۱۷. 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**[۲۴] روی R می‌نامند. مجموعه‌ی تمام چندجمله‌ای‌های روی R را با $R[X]$ نشان می‌دهند.

تعریف ۱.۲.۱۸. 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 $\beta = (b_0, b_1, \dots, b_n, \dots)$،

$$\alpha + \beta = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$$

و

$$\alpha \cdot \beta = (c_0, c_1, \dots, c_n, \dots),$$

که در آن به ازای هر $k \in \mathbb{N}_0$ ($\mathbb{N}_0$ مجموعه اعداد صحیح نامنفی است)، $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. متذکر می‌شویم که

$$\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j$$

می‌باشد، که اغلب آن را به صورت $\sum_{i+j=k} a_i b_j$ می‌نویسیم.

تعریف ۱.۲.۱۹. اگر $\alpha(x) \in R[X]$ ، **درجه‌ی** α که آن را با $\deg(\alpha)$ نشان می‌دهیم چنین تعریف می‌شود:

فرض کنیم $\alpha(x) \neq 0$. در این صورت $\deg(\alpha) = \mathbb{N}$ ($\mathbb{N}$ مجموعه اعداد طبیعی است) می‌باشد اگر $a_{\mathbb{N}} \neq 0$، ولی به ازای هر $k > n$، $a_k = 0$ باشد که در آن a_i ضریب x^i در $\alpha(x)$ می‌باشد. اگر $\alpha(x) = 0$ باشد آنگاه تعریف می‌کنیم: $\deg(\alpha) = -\infty$.

در صورتی که $\deg(\alpha) = -\infty$ و یا $\deg(\alpha) = 0$ باشد، می‌گوییم که $\alpha(x)$ یک **چندجمله‌ای ثابت** است.

تعریف ۱.۲.۲۰. فرض کنیم R یک حلقه‌ی جابه‌جایی 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 ۱.۲.۲۱. فرض کنیم R یک حلقه‌ی جابه‌جایی یکدار باشد.

۱.یک عنصر $c \in R$ را **تحویل‌ناپذیر** گویند اگر دو شرط زیر برقرار باشد:

آ. c یک عنصر غیرصفر غیریکه باشد.

ب. $c = ab$، $a, b \in R$ نتیجه دهد a یا b یک یکه است.

۲.یک عنصر $P \in R$ را **اول** گویند اگر دو شرط زیر برقرار باشد:

آ. P یک عنصر غیرصفر غیریکه باشد.

ب. $P|ab$ و $a, b \in R$ نتیجه دهد $P|a$ یا $P|b$.

[۲۴] Polynomial

تعریف ۲۲.۲.۱. فرض کنید $\mathbb{N}_\circ$ مجموعه‌ی اعداد صحیح نامنفی باشد. فرض کنید R یک حلقه‌ی جابه‌جایی باشد.

۱. R را یک **حلقه‌ی اقلیدسی** می‌نامند، اگر یک تابع $\varphi: R \to \mathbb{N}_\circ$ وجود داشته باشد به قسمی که شرایط زیر برقرار باشد:

آ. $\varphi(a) = \circ$ اگر و فقط اگر $a = \circ$.

ب. به ازای هر $a, b \in R$، $\varphi(a, b) = \varphi(a)\varphi(b)$.

پ. به ازای هر $a, b \in R$، به قسمی که $b \neq \circ$، عناصر $q, r \in R$ وجود داشته باشد به طوری که: $a = bq + r, \varphi(r) < \varphi(b)$.

۲. یک حلقه‌ی اقلیدسی که یک دامنه‌ی صحیح باشد را یک **دامنه‌ی اقلیدسی** می‌نامند.

تعریف ۲۳.۲.۱. مجموعه ناتهی $\mathbb{F}$ را به همراه دو عمل دوتایی جمع $(+)$ و ضرب $(\cdot)$ **میدان** نامیم هرگاه در شرایط زیر صدق کند:

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

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

۳. عمل ضرب نسبت به عمل جمع توزیع‌پذیر باشد. یعنی:

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

برقرار باشد.

تعریف ۲۴.۲.۱. تعداد عناصر میدان را **مرتبه**[۲۵] میدان گوییم. یک میدان با تعداد عناصر متناهی را یک **میدان متناهی** می‌نامیم.

تعریف ۲۵.۲.۱. ۱. فرض کنید $\mathbb{F}$ یک میدان باشد، زیرمجموعه K از $\mathbb{F}$ که تحت اعمال $\mathbb{F}$ خود یک میدان باشد را یک **زیرمیدان** $\mathbb{F}$ می‌نامند. همچنین $\mathbb{F}$ را **توسیع میدان** K گویند.

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

تعریف ۲۶.۲.۱. فرض کنید $\mathbb{F}$ یک میدان باشد. مجموعه

$$\mathbb{F}[X] = \{a_\circ + a_1 X + \cdots + a_n X^n \quad , \quad a_i \in \mathbb{F}, n \geq \circ\}$$

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

تعریف ۲۷.۲.۱. فرض کنیم $\mathbb{F}$ یک میدان باشد و $f(X) \in \mathbb{F}[X]$. یک عنصر $s \in \mathbb{F}$ را یک **ریشه** از چندجمله‌ای $f(X)$ یا از f گویند، اگر $f(s) = \circ$. در این صورت می‌گویند s در معادله‌ی چندجمله‌ای $f(X)$ صدق می‌کند.

[۲۵] Order

تعریف ۲۸.۲.۱. فرض کنید $\alpha: R \to R$ همریختی حلقه‌ای باشد. در این صورت **حلقه‌ی چندجمله‌ای‌های اریب** $R[x;\alpha]$ به صورت زیر تعریف می‌شود:

$$R[x;\alpha] = \{\sum_{i=0}^{n} a_i x^i | a_i \in R, n \in \mathbb{F}, xr = \alpha(r)x, \forall r \in R\}$$

در حلقه‌ی $R[x;\alpha]$ هر چندجمله‌ای به صورت $f(x) = \sum_{i=0}^{n} a_i x^i$ را یک **چندجمله‌ای چپ** و هر چندجمله‌ای به صورت $g(x) = \sum_{i=0}^{n} x^i a_i$ را **چندجمله‌ای راست** می‌نامیم. توجه شود که اگر $\alpha \neq I_R$ باشد آنگاه $R[x;\alpha]$ جابه‌جایی نیست، حتی اگر R جابه‌جایی باشد را به ازای هر a ای در R، $\alpha(a) \neq a$ و از این رو $xa = \alpha(a)X \neq a(x)$ خواهد بود.

تعریف ۲۹.۲.۱. فرض کنیم $\mathbb{F}$ یک میدان باشد و $\alpha(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{F}[X]$ که در آن $a_n \neq 0$. در این صورت a_n را **ضریب پیشرو** $\alpha(X)$ و a_0 را **جمله‌ی ثابت** آن می‌نامند. اگر $a_n = 1$ باشد در این صورت $\alpha(X)$ را یک چندجمله‌ای **تکین یا مونیک** می‌نامند.

تعریف ۳۰.۲.۱. چندجمله‌ای $f(x)$ از درجه n (بالاترین توان موجود در چندجمله‌ای را درجه آن می‌نامیم) را **تحویل‌پذیر** نامیم، هرگاه دو چندجمله‌ای $h(X)$ و $g(X)$ هر دو از درجه کمتر از n موجود باشند به گونه‌ای که داشته باشیم:

$$f(x) = h(x)g(x)$$

در غیر این صورت (یعنی اگر چنین $g(x)$ و $h(x)$ یافت نشود) چندجمله‌ای $f(x)$ را **تحویل‌ناپذیر** نامیم.

تعریف ۳۱.۲.۱. فرض کنید $f(x) \in \mathbb{F}[x]$، چندجمله‌ای از درجه $n \geq 1$ باشد. در این صورت، برای هر چندجمله‌ای $q(x) \in \mathbb{F}[x]$، چندجمله‌ای‌های $r(x)$ و $s(x)$ با شرط $\deg r(x) \leq \deg f(x)$ یا $r(x) = 0$ وجود دارند به‌طوری که داشته باشیم: $q(x) = s(x)f(x) + r(x)$. چندجمله‌ای $r(x)$، باقیمانده‌ی $q(x)$ در تقسیم بر $f(x)$ نامیده می‌شود.

تعریف ۳۲.۲.۱. فرض کنید $f(x), g(x) \in \mathbb{F}[x]$ دو چندجمله‌ای غیرصفر باشند. **بزرگترین مقسوم‌علیه مشترک** $f(x)$ و $g(x)$ را با $\gcd(f(x), g(x))$ نشان می‌دهند که برابر است با چندجمله‌ای منحصر به فرد 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 $\gcd(f(x), g(x)) = 1$ خواهد بود. همچنین **کوچکترین مضرب مشترک** $f(x)$ و $g(x)$ را با $lcm(f(x), g(x))$ نشان می‌دهیم و برابر است با چندجمله‌ای منحصر به فرد با کمترین درجه به طوری که $f(x)$ و $g(x)$ هردو آن را عاد می‌کنند.

تعریف ۳۳.۲.۱. 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 $(.)$ از $\mathbb{F} \times V$ به V تعریف شده باشد. مجموعه V را یک **فضای برداری**[۲۶] روی $\mathbb{F}$ نامند اگر در شرایط زیر صدق کند:

[۲۶] Vector space

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

آ. $a(u+v) = au + av$.

ب. $(a+b)v = av + bv$.

۲. قانون شرکت پذیری بین $\mathbb{F}$ و V برقرار باشد. یعنی برای هر $a,b \in \mathbb{F}$ و $u \in V$ 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 $1 \cdot u = u$ برقرار باشد.

تعریف ۳۴.۲.۱. یک دنباله مرتب شده با n مؤلفه $a_0, a_1, \ldots, a_{n-1}$ 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، nـتایی متفاوت موجود است. مجموعه $(\mathbb{F}_q)^n$ همه nـتایی‌های 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 ۳۵.۲.۱. دو عمل روی $\mathbb{F}_q^n$ تعریف می‌کنیم:

۱. جمع دو بردار: برای هر $V = (v_0, v_1, \ldots, v_{n-1})$ و $U = (u_0, u_1, \ldots, u_{n-1})$ در $\mathbb{F}_q^n$ بردار $U+V$ به فرم زیر می‌باشد:

$$U + V = (u_0 + v_0, u_1 + v_1, \ldots, u_{n-1} + v_{n-1}) \in \mathbb{F}_q^n.$$

۲. حاصلضرب یک بردار در یک اسکالر: اگر $V = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ و $a \in \mathbb{F}_q$ موجود باشد، آنگاه داریم:

$$a(v_0, v_1, \ldots, v_{n-1}) = (av_0, av_1, \ldots, av_{n-1}) \in \mathbb{F}_q^n.$$

جمع برداری و ضرب اسکالر تعریف شده در (۱) و (۲) به ترتیب در قوانین توزیع‌پذیری و شرکت‌پذیری صدق می‌کنند. بنابراین مجموعه $\mathbb{F}_q^n$ یک فضای برداری روی $\mathbb{F}_q$ است.

تعریف ۳۶.۲.۱. یک زیر مجموعه از $\mathbb{F}_q^n$ یک **زیرفضای**[۲۷] $\mathbb{F}_q^n$ است هرگاه تحت عمل جمع و ضرب تعریف شده روی $\mathbb{F}_q^n$ یک فضای برداری باشد.

تعریف ۳۷.۲.۱. فرض کنید V یک فضای برداری روی $\mathbb{F}_q$ باشد و فرض کنید $S = \{v_1, v_2, \ldots, v_k\}$ زیر مجموعه‌ای ناتهی از V باشد. **زیرفضای (خطی تولید شده توسط)** S به شکل زیر تعریف می‌شود:

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

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

[۲۷] Subspace

تعریف ۳۸.۲.۱. فرض کنید V یک فضای برداری روی میدان $\mathbb{F}_q$ باشد. آنگاه زیر مجموعه غیرتهی مانند $B = \{v_1, v_2, \ldots, v_k\}$ از V را یک **پایه** برای V می‌نامیم هرگاه $V = \langle B \rangle$ و B یک مجموعه مستقل خطی باشد.

تعریف ۳۹.۲.۱. 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 **بعد** V روی $\mathbb{F}_q$ می‌نامیم و با $\dim_{\mathbb{F}_q}(V)$ نشان می‌دهیم.

تعریف ۴۰.۲.۱. فرض کنید $W = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ و $V = (v_1, \ldots, v_n)$ موجود باشند.

۱. دو بردار V و W برهم عمودند اگر داشته باشیم $V \cdot W = 0$.

۲. فرض کنید S یک زیر مجموعه‌ی غیر تهی از $\mathbb{F}_q^n$ باشد، دوگان S به صورت زیر تعریف می‌شود:

$$S^{\perp} = \{v \in \mathbb{F}_q^n \colon v \cdot s = 0, \forall s \in S\}.$$

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

تعریف ۴۱.۲.۱. فرض کنید R یک حلقه بوده و $(M, +)$ یک گروه آبلی و $f \colon R \times M \to M$ 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 $m_1, m_2 \in M$ داشته باشیم:

$$r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2.$$

۲. به ازای هر $r_1, r_2 \in R$ و $m \in M$ داشته باشیم:

$$(r_1 + r_2)m = r_1 \cdot m + r_2 \cdot m.$$

۳. به ازای هر $r_1, r_2 \in R$ و $m \in M$ داشته باشیم:

$$r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m.$$

در این صورت M رایک Rـ**مدول چپ** گویند. به طریق مشابه Rـ**مدول راست** نیز تعریف می‌شود.

۳.۱ مفاهیم کدگذاری

تعریف ۱.۳.۱. 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 $W = w_1 w_2 \dots w_n$ است که در آن، به ازای هر $1 \leq i \leq n$، $w_i \in A$ می‌باشد. به طور معادل، می‌توان W را به صورت بردار $(w_1, w_2, \dots, w_n)$ در نظر گرفت.

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

۳. A^n را **فضای کد** و اعضای کد C را **کد واژه**[۲۸] 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.

معمولا 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 ۲.۳.۱. فرض کنید x و y دو واژه به طول n روی الفبای A باشند. در این صورت **فاصله (همینگ)**[۲۹] 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 اگر $x = x_1, x_2, \dots, x_n$ و $y = y_1, y_2, \dots, y_n$ آنگاه داریم:

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

تعریف ۳.۳.۱. 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:

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

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

تعریف ۴.۳.۱. 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 مولفه‌های ناصفر x تعریف می‌شود .

تعریف ۵.۳.۱. فرض کنید C یک کد باشد. **مینیمم وزن همینگ** کد C که با $wt(C)$ نمایش داده می‌شود، کمترین وزن کدواژه‌های ناصفر C است.

۱.۳.۱ کدهای خطی

تعریف ۶.۳.۱. کد خطی C از طول n روی $\mathbb{F}_q$ یک زیرفضا از $\mathbb{F}_q^n$ می‌باشد.

---

[۲۸] Code words

[۲۹] Hamming distance

تعریف ۷.۳.۱. فرض کنید C یک کد خطی در $\mathbb{F}_q^n$ باشد. در این صورت:

۱. **دوگان**[۳۰] 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:

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

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

۲.۳.۱ ماتریس مولد و ماتریس کنترل توازن

فرض می‌کنیم 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 می‌کنیم G یک ماتریس $k \times n$ است که شامل تمام سطرهای غیر صفر بدست آمده در ماتریس سطری پلکانی تحویل شده A باشد. یعنی

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

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

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

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

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

که 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.

تعریف ۸.۳.۱. ۱. **ماتریس مولد** کد خطی C ماتریس G است که سطرهای آن یک پایه برای کد C تشکیل می‌دهند.

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

تعریف ۹.۳.۱. ۱. ماتریس مولدی به شکل $(I_k|X)$، ماتریس مولد به شکل استاندارد گفته می‌شود.

۲. ماتریس کنترل توازن به شکل $(Y|I_{n-k})$، ماتریس کنترل توازن به شکل استاندارد گفته می‌شود.

[۳۰] Dual

۳.۳.۱ کدگذاری کدهای خطی

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

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

یک کدواژه در C است. برعکس، هر کدواژه در C می‌تواند به صورت یکتای uG بیان شود که در آن G ماتریس مولد کد C و $u \in \mathbb{F}_q^k$ است. فرآیند نمایش اعضای $u \in \mathbb{F}_q^k$ به صورت کدواژه‌های $v = uG$ در C، **کدگذاری** کد خطی نامیده می‌شود.

۴.۳.۱ کدهای دوری

تعریف ۱۰.۳.۱. کد خطی C به طول n روی $\mathbb{F}_q$ را یک **کد دوری** گوییم هرگاه هر انتقال دوری (یک مکان به راست) از یک کدواژه در C حاصل شود. به عبارت دیگر، هرگاه $(c_0, c_1, \ldots, c_{n-1})$ کدواژه‌ای در C باشد، آنگاه $(c_{n-1}, c_0, \ldots, c_{n-2})$ نیز به کد C تعلق داشته باشد. فرض کنید C یک کد دوری به طول n روی $\mathbb{F}_q$ باشد، به هر کدواژه $(c_0, c_1, \ldots, c_{n-1}) \in C$، چندجمله‌ای $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ را نظیر می‌کنیم. طبق این تناظر به سادگی ثابت می‌شود که هر کد دوری به طول n نظیر یک ایده‌آل از حلقه $R = \mathbb{F}_q[x]/(x^n - 1)$ است.

۵.۳.۱ کدهای خوددوگان اقلیدسی و هرمیتی

در این قسمت به معرفی کد خوددوگان اقلیدسی و هرمیتی برای یک کد می‌پردازیم. برای این منظور ابتدا باید تعریف ضرب داخلی اقلیدسی و هرمیتی و کد دوگان اقلیدسی و هرمیتی را بیان کنیم.

تعریف ۱۱.۳.۱. اگر R یک حلقه‌ی جابه‌جایی باشد و $n \in \mathbb{N}$، آنگاه **ضرب داخلی اقلیدسی** [۳۱] به صورت زیر تعریف می‌شود:

$$\forall a = (a_1, \ldots, a_n) \in R^n, \forall b = (b_1, \ldots, b_n) \in R^n, \qquad \langle a, b \rangle_e = \sum_{i=1}^{n} a_i b_i$$

حال می‌توانیم کد دوگان اقلیدسی یک کد را به صورت زیر تعریف نماییم:

[۳۱] Euclidean inner product

تعریف ۱.۳.۱۲. فرض کنیم R یک حلقه‌ی جابه‌جایی باشد و $n \in \mathbb{N}$. به علاوه فرض کنیم C یک کد به طول n روی R باشد. در این صورت، مجموعه‌ی زیر را **کد دوگان اقلیدسی**[۳۲] کد C می‌نامند:

$$\{d \in R^n : \forall c \in C, \langle c, d\rangle_e = 0\}.$$

کد دوگان اقلیدسی کد C را با $C^{\perp_e}$ نمایش می‌دهند.

تعریف ۱.۳.۱۳. فرض کنیم R یک حلقه‌ی جابه‌جایی، $n \in \mathbb{N}$ و θ یک خودریختی R از مرتبه‌ی ۲ باشد. در این صورت، **ضرب داخلی هرمیتی**[۳۳] در R^n به صورت زیر تعریف می‌شود:

$$\forall a = (a_1, \ldots, a_n) \in R^n, \forall b = (b_1, \ldots, b_n) \in R^n, \qquad \langle a, b\rangle_h = \sum_{i=1}^{n} a_i \theta(b_i).$$

حال به تعریف کد دوگان هرمیتی می‌پردازیم:

تعریف ۱.۳.۱۴. اگر R یک حلقه‌ی جابه‌جایی، $n \in \mathbb{N}$ و C کدی به طول n روی R باشد، آنگاه مجموعه‌ی زیر را **کد دوگان هرمیتی**[۳۴] می‌نامند:

$$\{d \in R^n : \forall c \in C, \langle c, d\rangle_h = 0\}.$$

کد دوگان هرمیتی کد C را با $C^{\perp_h}$ نمایش می‌دهند.

تعریف ۱.۳.۱۵. برای کد C داریم:

۱. C را **کد خوددوگان اقلیدسی** نامیم هرگاه $C = C^{\perp_e}$،

۲. C **کد خوددوگان هرمیتی** می‌باشد هرگاه $C = C^{\perp_h}$.

تعریف ۱.۳.۱۶. برای یک (n, M, d)ـ کد qـ مؤلفه‌ای C فرض کنیم A_i دلالت بر تعداد کدواژه‌هایی با وزن همینگ i داشته باشد، جایی که $0 \leq i < n$. به وضوح $A_0 = 1$ و $M = \sum_{i=0}^{n} A_i$. مجموعه‌های مرتب A_i را **توزیع وزنی**[۳۵] کد C می‌گویند.

۴.۱ قضایا

قضیه ۱.۴.۱. [۲۷، قضیه ۲.۱۲] فرض کنید K یک میدان متناهی باشد. اگر چندجمله‌ای f یک ایده‌آل دوطرفه در حلقه‌ی چندجمله‌ای‌های اریب $K[X, \theta]$ تولید کند، آنگاه چندجمله‌ای f به فرم زیر نوشته می‌شود:

$$(a_0, a_1 X^m + \cdots + a_n X^{mn}) X^t$$

که در آن m مرتبه‌ی خودریختی θ می‌باشد ($m = |<\theta>|$).

[۳۲] Euclidean dual code

[۳۳] Hermitian inner product

[۳۴] Hermitian dual code

[۳۵] Weight distribution

قضیه ۱.۴.۲. [۲۳، قضیه ۱۵، فصل سوم] فرض کنید ϕ یک حلقه تقسیم یکریخت با حلقه‌ی درون‌ریختی‌های یک فضای برداری و S یک خودریختی از ϕ باشد. اگر ϕ دارای بعد متناهی روی مرکز خود باشد، و برای هر $\circ < r < \infty$، S^r داخلی باشد، آنگاه هر ایده‌آل روی حلقه $\phi[t, S]$ (حلقه‌ی چندجمله‌ای‌های اریب با یک متغیر t) کراندار می‌باشد.

قضیه ۱.۴.۳. [۲۳، قضیه۱۲، فصل سوم] اگر $a_\circ = bcd_\circ$ کراندار باشد و کران آن $a^*_\circ$ باشد، آنگاه $c_\circ$ نیز کراندار بوده و کرانی برابر با $c^*_\circ$ دارد که حاوی $a^*_\circ$ می‌باشد.

قضیه ۱.۴.۴. [۶، قضیه۳.۲.۱۶] فرض کنیم D یک حلقه تقسیم باشد. ایده‌آل‌های دوطرفه حلقه چندجمله‌ای‌های اریب $D[T, \alpha]$، دقیقا ایده‌آل‌های راست اصلی هستند که مولدهای آن به فرم $T^t g$ می‌باشد، جایی که داریم: $g \in Z(D[T, \alpha])$ و $t \geq \circ$.

قضیه ۱.۴.۵. [۱۰، قضیه ۱] فرض کنید $\mathbb{F}_q$ یک میدان متناهی از مرتبه q، θ یک خودریختی از $\mathbb{F}_q$ و C یک کد خطی روی $\mathbb{F}_q$ با طول n باشد. اگر $(|< \theta >|)$، مرتبه‌ی خودریختی θ باشد و n را عاد کند، آنگاه کد C یک θـ کد دوری است، اگر و تنها اگر نمایش چندجمله‌ای اریب $C(X)$ از کد C یک ایده‌آل چپ $\frac{\mathbb{F}_q[X,\theta]}{(X^n - 1)} \supset (G)$ باشد.

تعریف ۱.۴.۱. فرض کنیم

$$K[Y^q; \circ] = \{a_\circ Y + a_1 Y^q + \cdots + a_n Y^{q^n} | n = \circ, 1, \ldots, a_i; a_i \in K\}$$

باشد. برای هر دو عضو $f = a_\circ Y + a_1 Y^q + \cdots + a_n Y^{q^n}$ و $g = b_\circ Y + b_1 Y^q + \cdots + b_t Y^{q^n}$، عمل جمع به صورت جمع معمولی چندجمله‌ای‌ها و عمل ضرب به صورت زیر تعریف می‌شود:

$$f \circ g = f(g) = a_\circ g + a_1 g^q + \cdots + a_n g^{q^n}.$$

$K[Y^q; \circ]$ همراه با دو عمل فوق تشکیل یک حلقه‌ی ناجابه‌جایی می‌دهد که به آن **حلقه چندجمله‌ای‌های اور** گفته می‌شود.

قضیه ۱.۴.۶. [۲۷، قضیه ۲.۱۳] نگاشت $\Phi : K[X; \theta] \to K[Y^q; \circ]$ یک خودریختی حلقه‌ای بین حلقه چندجمله‌ای اریب $K[X; \theta]$ و حلقه چندجمله‌ای‌های اور $K[Y^q; \circ]$ را تعیین می‌کند.

فصل ۲

کلیات θـ کدها

فرض کنیم $\mathbb{F}_q$ یک میدان متناهی از مرتبه q باشد. یک $[n,k]$ـ کد خطی روی میدان $\mathbb{F}_q$، یک زیر فضای برداری kـ بعدی C، از فضای برداری V است که در آن $V=\mathbb{F}_q^n$ بوده و به صورت زیر نوشته می‌شود:

$$V=\mathbb{F}_q^n=\{(a_0,\dots,a_{n-1})|a_i\in\mathbb{F}_q\}.$$

در ادامه ما از نمایش کد C به فرم چندجمله‌ای استفاده می‌کنیم، که در آن کدواژه‌های $(a_0,a_1,\dots,a_{n-1})$، از کد C را با چندجمله‌ای‌هایی که ضرایب آن $a_{n-1},\dots,a_0$ می‌باشد مشخص می‌کنیم، به این ترتیب چندجمله‌ای زیر را داریم:

$$a_{n-1}X^{n-1}+\cdots+a_1X+a_0\in\mathbb{F}_q[X].$$

در حالت کلاسیک این چندجمله‌ای‌ها را می‌توانیم به‌عنوان عناصری از حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X]}{(f)}$ ببینیم، جایی که f یک چندجمله‌ای از درجه n می‌باشد.

به منظور تعمیم دادن مفهوم کدهایی که وابسته به ایده‌آل‌ها هستند، حالت کلی‌تر حلقه چندجمله‌ای‌های اریب که از نوع خودریختی هستند را در نظر می‌گیریم که اکنون به تعریف این حلقه‌ها می‌پردازیم:

فرض کنید $\mathbb{F}_q$ یک میدان متناهی و θ یک خودریختی روی این میدان باشد. در این صورت یک ساختار حلقه‌ای روی مجموعه $\mathbb{F}_q[X,\theta]$ را می‌توان به صورت زیر تعریف کرد:

$$\mathbb{F}_q[X,\theta]=\{a_{n-1}X^{n-1}+\cdots+a_1X+a_0|a_i\in\mathbb{F}_q,n\in\mathbb{N}\}.$$

این مجموعه، مجموعه‌ای متشکل از چندجمله‌ای‌های سوری است که ضرایب در سمت چپ متغیر X نوشته می‌شوند. عمل جمع در حلقه $\mathbb{F}_q[X,\theta]$، به صورت جمع معمولی چندجمله‌ای‌ها و عمل ضرب برای هر عنصر $a \in \mathbb{F}_q$ طبق قاعده $Xa = \theta(a)X$، تعریف می‌شود، که بنا به قوانین شرکت‌پذیری و توزیع پذیری در عناصر، به تمام عناصر $\mathbb{F}_q[X,\theta]$، توسیع می‌یابد. این حلقه‌ها خوب شناخته شده‌اند. (مراجع [۲۸] و [۲۹] را ببینید.)

ضرایب حلقه‌های چندجمله‌ای روی یک میدان متناهی، یک میدان جابه‌جایی است، که در آن درجه حاصلضرب دو عنصر با مجموع درجات عناصر برابر است.

حلقه $\mathbb{F}_q[X,\theta]$، هم یک حلقه اقلیدسی راست و هم یک حلقه اقلیدسی چپ می‌باشد که ایده‌آل‌های راست و چپ آن همگی ایده‌آل‌های اصلی هستند. (مرجع [۲۹] را ببینید.)

بزرگترین مقسوم علیه مشترک و کوچکترین مضرب مشترک چپ و راست در حلقه $\mathbb{F}_q[X,\theta]$ موجود است و می‌توانند با استفاده از الگوریتم اقلیدسی راست و چپ محاسبه شوند.(به مرجع [۱۴] مراجعه کنید.)

بنابر قضیه ۱.۴.۱ و یا قضیه ۴.۴.۱، ایده‌آل‌های دوطرفه‌ی حلقه $\mathbb{F}_q[X,\theta]$، توسط عناصری از $X^t\mathbb{F}_q^{\theta}[X^m]$ تولید می‌شود، که در آن t یک عدد صحیح، m مرتبه خودریختی θ و $\mathbb{F}_q^{\theta}$ میدان ثابتی از θ می‌باشد.

مرکز حلقه $\mathbb{F}_q[X,\theta]$ که آن را با نماد $Z(\mathbb{F}_q[X,\theta])$ نمایش می‌دهیم، برابر با $\mathbb{F}_q^{\theta}[X^m]$ می‌باشد. همچنین ایده‌آل های چپ یا راست در حلقه $\mathbb{F}_q[X,\theta]$ که توسط یک عنصر مرکزی تولید می‌شود یک ایده‌آل دوطرفه می‌باشند. اگر I یک ایده‌آل دوطرفه در حلقه $\mathbb{F}_q[X,\theta]$ باشد، آنگاه I توسط یک چند جمله‌ای f، از درجه n، در حلقه $X^t\mathbb{F}_q^{\theta}[X^m]$ تولید می‌شود.

بنا به تناظر ایده‌آل‌ها می‌توان دید که ایده‌آل‌های چپ حلقه‌ی خارج قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(f)}$، همگی ایده‌آل‌های اصلی بوده، که هر کدام از آن‌ها توسط مقسوم علیه راست g، از f تولید می‌شوند.

عنصر $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ را به عنصر $a(X) = a_{n-1}X^{n-1} + \cdots + a_1X + a_0$، در حلقه $\frac{\mathbb{F}_q[X,\theta]}{(f)}$ نظیر می‌کنیم. عناصر $a(X) \in \frac{\mathbb{F}_q[X,\theta]}{(f)}$، که به یک ایده‌آل چپ در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(f)}$، دلالت دارند، توسط یک مقسوم علیه راست g از f تولید می‌شوند تشکیل یک $[n,k]$ـ کد خطی در $\mathbb{F}_q^n$ می‌دهند، که در آن، $k = n - \deg(g)$ می‌باشد. به طور دقیق‌تر داریم:

تعریف ۱.۰.۲. فرض کنید $f \in \mathbb{F}_q[X,\theta]$، یک چندجمله‌ای از درجه n باشد. اگر $I = (f)$ یک ایده‌آل دوطرفه از حلقه چندجمله‌ای‌های اریب $\mathbb{F}_q[X,\theta]$ باشد، آنگاه یک θـ کد C شامل کدواژه‌هایی به فرم $a = (a_0, a_1, \ldots, a_{n-1})$ می‌باشد، که ضرایب عناصر

$$a(X) = a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

هستند و از ایده‌آل چپ حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{I}$ می‌باشند. در این حالت عناصر $a(X)$ مضارب چپ مقسوم علیه راست g، از f هستند.

اکنون به دو حالت خاص می‌پردازیم:

۱. اگر $f \in Z(\mathbb{F}_q[X,\theta])$ باشد، آنگاه θــ کد متناظر با ایده‌آل چپ $\frac{(g)}{(f)}$ را یک θــ کد مرکزی گوییم.

۲. فرض کنید m مرتبه‌ی خودریختی θ باشد. اگر m ، n را عاد کند و $f = X^n - ۱$ باشد، آنگاه θــ کد متناظر با ایده‌آل چپ $\frac{(g)}{X^{n-۱}}$ را θــ کد دوری می‌گوییم.

اگر چندجمله‌ای $g = g_r X^r + \cdots + g_۱ X + g_۰$، یک چند جمله‌ای $f \in \mathbb{F}_q[X,\theta]$ از درجه n را عاد کند، به طوری که ایده‌آل (f)، یک ایده‌آل دوطرفه باشد، آنگاه ماتریس مولد θــ کد تولید شده توسط g از نوع $[n, n-r]$، به صورت زیر می‌باشد:

$$G = \begin{pmatrix} g_۰ & \dots & g_{r-۱} & g_r & ۰ & \dots & ۰ \\ ۰ & \theta(g_۰) & \dots & \theta(g_{r-۱}) & \theta(g_r) & \dots & ۰ \\ ۰ & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ ۰ & & & & & & \\ ۰ & \dots & ۰ & \theta^{n-r-۱}(g_۰) & \dots & \theta^{n-r-۱}(g_{r-۱}) & \theta^{n-r-۱}(g_r) \end{pmatrix}$$

جایی که می‌توان چندجمله‌ای

$$X^i g(X) = \sum_{j=۰}^{r} \theta^i(g_i) X^j$$

که در آن $i \in \{۰, \dots, n-r-۱\}$ می‌باشد را روی $(i+۱)$ امین سطر مشاهده کرد. در واقع یک کدواژه توسط یک چند جمله‌ای به صورت $m(X)g(X) = \sum_{i=۰}^{n-r-۱} m_i X^i g(X)$، نمایش داده می‌شود که در آن $m(X) = \sum_{i=۰}^{n-r-۱} m_i X^i$، می‌باشد.

توجه کنید که فقط چندجمله‌ای مولد برای تعریف یک θــ کد استفاده می‌شود. در بخش بعد خواهیم دید که هر چندجمله‌ای اریب g می‌تواند به عنوان چندجمله‌ای مولد یک θــ کد نقش ایفا کند، اما نه برای هرطول دلخواهی. لذا نشان می‌دهیم مینیمم طولی که برای g تعیین می‌شود، توسط درجه چندجمله‌ای مولد ایده‌آل دوطرفه ماکزیمالی که مشمول باشد در ایده‌آل چپ $(g) \subset \mathbb{F}_q[X,\theta]$ به دست می‌آید.

ساختار ایده‌آلی یک ابزار ارزشمند است و می‌تواند خواص یک θــ کد را به خوبی توصیف کند. از این رو ابزاری مفید برای کدگشایی و کدگذاری می‌باشد.

با استفاده از ساختار حلقه اقلیدسی $\mathbb{F}_q[X,\theta]$، می‌توان تصمیم‌گیری کرد که چه‌وقت یک چندجمله‌ای می‌تواند با استفاده از تقسیم توسط یک چندجمله‌ای مولد از کد، بیانگر یک کدواژه باشد و همچنین خواهیم دید که با استفاده از تقسیم در حلقه $\mathbb{F}_q[X,\theta]$، می‌توان ماتریس کنترل توازن یک θــ کد دوری را به دست آورد.

مثال ۲.۱.۰. چندجمله‌ای مولد g برای θ ــ کد دوری یک فاکتور راست از $X^n - ۱$ می‌باشد، لذا بنابر قضیه ۵.۴.۱ این کدها دارای خاصیت زیر می‌باشند:

$$(a_۰, a_۱, \dots, a_{n-۱}) \in C_\theta \Rightarrow (\theta(a_{n-۱}), \theta(a_۰), \theta(a_۱), \dots, \theta(a_{n-۲})) \in C_\theta.$$

رده‌ی خاصی از θـ کدهای دوری در مرجع [۲۲]، با استفاده از حلقه چندجمله‌ای‌های خطی شده و در مرجع [۱۰]، با استفاده از حلقه چندجمله‌ای‌های اریب، معرفی شده‌اند.

فرض کنید $\mathbb{F}_{q_\circ} \subset \mathbb{F}_q$ باشد، که در آن θ یک خودریختی فروبنیوس از حلقه‌ی خارج‌قسمتی $\frac{\mathbb{F}_q}{\mathbb{F}_{q_\circ}}$ می‌باشد که توسط $\theta(a) = a^{q_\circ}$، تعریف شده است. بنابر قضیه ۶.۴.۱، یک یکریختی حلقه‌ای بین حلقه چندجمله‌ای‌های اریب $k[X,\theta]$ و حلقه چند جمله‌ای‌های خطی شده‌ی $K[Y^q,\circ]$، وجود دارد که این یکریختی به صورت $X \longmapsto Y^q$ تعریف می‌شود. به عبارت دیگر داریم:

$$f : k[X,\theta] \to k[Y^{q_\circ},\circ]$$
$$X \longmapsto Y^{q_\circ}.$$

مثال ۲.۰.۲. فرض کنید $\mathbb{F}_۴[X,\theta]$ یک حلقه اریب باشد که در آن θ یک خودریختی فروبنیوس و α مولد گروه ضربی میدان $\mathbb{F}_۴$ باشد. چند جمله‌ای $X^۲ + \alpha X + ۱$، یک ایده آل چپ در حلقه خارج قسمتی $\frac{\mathbb{F}_۴[X,\theta]}{(x^۴+x^۲+۱)}$، تولید می‌کند که متناظر با یک کد خطی غیر دوری C، با مینیمم فاصله همینگ ۲ می‌باشد. لذا منجر به تولید یک $[۴,۲,۲]$ـ کدی می‌شود که یک θ کد مرکزی می‌باشد، در حالی که یک θ کد دوری نیست.

توجه کنید که $a(X) = a_\circ + a_۱X + a_۲X^۲ + a_۳X^۳ \in C$ می‌باشد، که در آن $X \cdot a(X) \in C$ است. لذا داریم:

$$\begin{aligned} Xa(X) &= \theta(a_\circ)X + \theta(a_۱)X^۲ + \theta(a_۲)X^۳ + \theta(a_۳)X^۴ \\ &= \theta(a_۳) + \theta(a_\circ)X + (\theta(a_۱) + \theta(a_۳))X^۲ + \theta(a_۲)X^۳ + \theta(a_۳)(X^۴ + X^۲ + ۱). \end{aligned}$$

بنابراین در حلقه خارج‌قسمتی $\frac{\mathbb{F}_۴[X,\theta]}{(X^۴+X^۲+۱)}$ داریم:

$$Xa(X) = \theta(a_۳) + \theta(a_\circ)X + (\theta(a_۱) + \theta(a_۳))X^۲ + \theta(a_۲)X^۳$$

که نتیجه می‌دهد:

$$(\theta(a_۳), \theta(a_\circ), \theta(a_۱) + \theta(a_۳), \theta(a_۲)) \in C.$$

۱.۲ برخی از خواص θ کدها

لم زیر نشان می‌دهد که کلاس θـ کدها خیلی بزرگ‌تر از کلاس θـ کد های دوری بوده و کلاس این کدها، کدهای گابیدولین را تعمیم می‌دهد.

لم ۱.۱.۲. فرض کنید $f = X^n - ۱ \in \mathbb{F}_q[X,\theta]$ یک ایده آل دو طرفه را تولید کند. یک θـ کد دوری تولید شده توسط یک مقسوم علیه راست تکین g از f از درجه کوچکتر اکید از $n-۱$، یک کد دوری تولید می‌کند، اگر و تنها اگر تمام ضرایب g، در میدان $\mathbb{F}_q^\theta$ باشند. جایی که $\mathbb{F}_q^\theta$ میدان ثوابت θ در میدان $\mathbb{F}_q$ می‌باشد.

برهان. فرض کنید $g = X^r + \sum_{i=0}^{r-1} g_i X^i$، یک چندجمله‌ای باشد. توجه کنید که اگر تمام ضرایب g در $\mathbb{F}_q^\theta$ باشند، آنگاه ماتریس مولد G متناظر با ماتریس یک کد دوری می‌باشد. اگر θـ کد C، تولید شده توسط ایده‌آل چپ $(g) \subseteq \frac{\mathbb{F}_q[X,\theta]}{(f)}$ دوری باشد، آنگاه $g \cdot X \in C$ خواهد بود. چون این کد کدی خطی می‌باشد، لذا داریم $X \cdot g - g \cdot X \in C$. بنابراین

$$(\theta(g_0) - g_0)X + (\theta(g_1) - g_1)X^2 + \cdots + (\theta(g_{r-1}) - g_{r-1})X^r$$

مضرب چپ (ثابتی) λg از g می‌باشد. چون g، f را عاد می‌کند، جمله ثابت آن غیر صفر می‌باشد و بنابراین λ باید برابر با صفر باشد. لذا $X \cdot g - g \cdot X$ نیز باید برابر با صفر باشد. بنابراین تمام ضرایب g_i از چندجمله‌ای g تحت θ پایا هستند و لذا باید در میدان ثوابت $\mathbb{F}_q^\theta$ باشند. □

مثال بعد نشان می‌دهد که کلاس θـ کدهای مرکزی، بزرگتر از θـ کدهای دوری می‌باشد.

مثال ۱.۱.۲. حلقه چندجمله‌ای‌های اریب $\mathbb{F}_4[X,\theta]$ را در نظر بگیرید، که در آن θ یک خودریختی فروبنیوس و α بیانگر مولد گروه ضربی از $\mathbb{F}_4$ می‌باشد. با در نظر گرفتن تمام فاکتورهای راست از درجه ۳، از چندجمله‌ای $X^{12} - 1 \in \mathbb{F}_4[X,\theta]$، می‌توانیم تمام $[12,9]$ـθـ کدهای دوری را بسازیم و ببینیم که بهترین فاصله همینگ این کدها ۲ می‌باشد. همچنین می‌توانیم یک $[12,9,3]$ـ θـ کد مرکزی نیز بسازیم. برای این منظور چندجمله‌ای مرکزی

$$f = X^{12} + X^{10} + X^8 + X^6 + X^4 + X^2 + 1 \in \mathbb{F}_4[X,\theta]$$

را در نظر می‌گیریم، که از سمت راست توسط عامل $g = X^3 + X^2 + X + \alpha$ قابل تقسیم است. θـ کد دوری متناظر یک $[12,9,3]$ـ کد است، که وزن همینگ آن چندجمله‌ای شمارنده به صورت زیر به دست می‌آید:

$$1 + 102Y^3 + 651Y^4 + 3000Y^5 + 10416Y^6 + 27156Y^7 + 50943Y^8$$
$$+ 67224Y^9 + 61248Y^{10} + 33078Y^{11} + 8325Y^{12}.$$

لذا تعداد θـ کدهای مرکزی وابسته به تعداد فاکتورهای راست چندجمله‌ای‌های مرکزی می‌باشد.

مثال ۲.۱.۲. حلقه چندجمله‌ای‌های اریب $\mathbb{F}_4[X,\theta]$ را در نظر بگیرید، که در آن θ یک خودریختی فروبنیوس و α یک مولد از $\mathbb{F}_4^*$ می‌باشد. در حلقه چندجمله‌ای‌های اریب $\mathbb{F}_4[X,\theta]$، چند جمله ای $X^4 + X^2 + 1$ دارای ۵ تجزیه‌ی متمایز به حاصلضرب چندجمله‌ای‌های تکین تحویل‌ناپذیر،

به صورت زیر می‌باشد:

$$\begin{aligned} X^۴ + X^۲ + ۱ &= (X^۲ + X + ۱)(X^۲ + X + ۱) \\ &= (X^۲ + \alpha^۲)(x^۲ + \alpha) \\ &= (X^۲ + \alpha)(X^۲ + \alpha^۲) \\ &= (X^۲ + \alpha^۲ X + ۱)(X^۲ + \alpha^۲ X + ۱) \\ &= (X^۲ + \alpha X + ۱)(X^۲ + \alpha X + ۱). \end{aligned}$$

حلقه‌ی $\mathbb{F}_۲[X]$، زیر حلقه‌ای جابه‌جایی از حلقه چندجمله‌ای‌های اریب $\mathbb{F}_۴[X, \theta]$ را تولید می‌کند. این موضوع بیان می‌کند که چرا لیست تمام تجزیه‌های ممکن برای

$$f \in Z(\mathbb{F}_۴[X, \theta]) = \mathbb{F}_۲[X^۲],$$

به حاصلضرب دو چندجمله‌ای هستند، همیشه شامل تجزیه‌های در $\mathbb{F}_۲[X]$ نیز می‌باشند. تجزیه‌ای که در حلقه $\mathbb{F}_۲[X]$ در نظر بگیریم دارای دو عامل در $\mathbb{F}_۲[X]$ می‌باشد و یا هیچ کدام از عوامل را ندارد.

لم زیر بیان می‌کند که چرا در مثال ۲.۱.۲، دو فاکتور در تجزیه‌ی مولد ایده‌آل دوطرفه جابه‌جا می‌شوند.

لم ۲.۱.۲. اگر $h \cdot g \in Z(\mathbb{F}_q[X, \theta])$ باشد، آنگاه در حلقه $\mathbb{F}_q[X, \theta]$، $h \cdot g = g \cdot h$ می‌باشد.

برهان. چون $h \cdot g \in Z(\mathbb{F}_q[X, \theta])$ می‌باشد، لذا داریم $h \cdot (g \cdot h) = (h \cdot g) \cdot h = h \cdot (h \cdot g)$. از طرفی چون $\mathbb{F}_q[X, \theta]$، دارای هیچ مقسوم علیه صفر غیربدیهی نمی‌باشد، می‌توانیم در هر دو طرف، h را از سمت چپ حذف کنیم. بنابراین در حلقه $\mathbb{F}_q[X, \theta]$، $h \cdot g = g \cdot h$ خواهد بود. □

بر اساس لم ۲.۱.۲ که جابه‌جایی را برای فاکتورهای تجزیه ارائه می‌کرد، می‌توانیم مشابه آنچه در حالت دوری داشته‌ایم، برای محاسبه چندجمله‌ای کنترل توازن عمل کنیم.

لم ۳.۱.۲. فرض کنید $h \cdot g \in Z(\mathbb{F}_q[X, \theta])$ باشد و C بیانگر θـ کد مرکزی متناظر با ایده‌آل چپ تولید شده توسط g، در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(h \cdot g)}$ باشد آنگاه $a \in C$ است اگر و تنها اگر در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(h \cdot g)}$، $a(X) \cdot h = ۰$ باشد.

برهان. اگر $a \in C$ باشد، آنگاه $a(X) = m \cdot g$ می‌باشد. بنابر مطالب بالا، در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(h \cdot g)}$ داریم:

$$a(X) \cdot h = (m \cdot g) \cdot h = m \cdot (h \cdot g) = ۰.$$

برای اثبات عکس مطلب، اگر در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(h\cdot g)}$، $a(X)\cdot h=\circ$ باشد آنگاه در حلقه چندجمله‌ای‌های اریب $\mathbb{F}_q[X,\theta]$،

$$a(X)\cdot h=f\cdot(h\cdot g)=(f\cdot g)\cdot h$$

خواهد بود. چون حلقه چندجمله‌ای‌های اریب $\mathbb{F}_q[X,\theta]$ حلقه‌ای است که از سمت راست خاصیت حذفی را دارد، لذا داریم $a(X)=f\cdot g$ و این نشان می‌دهد که a متعلق به C می‌باشد.

حال می‌توانیم ماتریس کنترل توازن در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(hg)}$ را از شرط:

$$a\in C\Longleftrightarrow a(X)\cdot h=\circ$$

به دست آوریم. □

در بخش بعد نشان می‌دهیم که هر چندجمله‌ای $g\in\mathbb{F}_q[X,\theta]$، که چندجمله‌ای f در حلقه $\mathbb{F}_q[X,\theta]$ را عاد می‌کند، یک ایده‌آل دوطرفه تولید می‌کند، بنابراین می‌تواند چندجمله‌ای مولد یک θـ کد باشد.

۲.۲ طول θـ کدها

تعریف ۱.۲.۲. یک عنصر $P\in\mathbb{F}_q[X,\theta]$ را محدود یا کراندار گوییم، هرگاه ایده‌آل چپ (P) (تولید شده توسط P)، شامل ایده‌آل دوطرفه (P^*) (تولید شده توسط P^*) باشد. چند جمله‌ای تکین P^*، از درجه مینیمم را کران P می‌گوییم. چون P^* یک ایده‌آل دوطرفه را تولید می‌کند، لذا باید به فرم زیر باشد:

$$(b_\circ+b_1X^m+b_2X^{2m}+\cdots+b_sX^{s\cdot m})X^t,$$

که در آن، t یک عدد صحیح، m مرتبه‌ی خودریختی θ و $b_i\in\mathbb{F}_q^\theta$ می‌باشند، که $\mathbb{F}_q^\theta$ میدان ثابت‌های خودریختی θ می‌باشد.

بنا به قضیه‌ی ۲.۴.۱، تمام عناصر حلقه چندجمله‌ای‌های اریب $\mathbb{F}_q[X,\theta]$، محدود یا کراندار می‌باشند. همچنین بنا به مطالب قبل از قضیه ۱۵ در مرجع [۲۴]، لم زیر را داریم:

لم ۱.۲.۲. فرض کنید m مرتبه‌ی خودریختی θ و $l=[\mathbb{F}_q:\mathbb{F}_q^\theta]$ باشد. اگر $P\in\mathbb{F}_q[X,\theta]$، چند جمله‌ای از درجه n باشد، آنگاه کران P^* از درجه کوچکتر مساوی $m\cdot l\cdot n$ خواهد بود.

برهان. عناصر حلقه چندجمله‌ای‌های اریب $\mathbb{F}_q[X,\theta]$، که از درجه کوچکتر از n هستند، یک فضای برداری از بعد n، تشکیل می‌دهند و لذا تشکیل یک فضای برداری از بعد $l\cdot n$، روی میدان $\mathbb{F}_q^\theta$، خواهند داد. با در نظر گرفتن باقی‌مانده‌های تقسیم $X^{m\cdot i}=P\cdot Q_i+R_i$، برای

$i = ۰, ۱, \ldots, l \cdot n$، که در آن $\deg(R_i) < n$ می‌باشد، یک ترکیب خطی غیر بدیهی به صورت $\sum_{i=۰}^{l \cdot n} \delta_i R_i = ۰$ وجود دارد که $\delta_i \in \mathbb{F}_q^\theta$ می‌باشد. لذا داریم:

$$\sum_{i=۰}^{l \cdot n} \delta_i X^{m \cdot i} = P \cdot (\sum_{i=۰}^{l \cdot n} \delta_i Q_i).$$

چند جمله‌ای بالا به فرم $\sum_{i=۰}^{l \cdot n} \delta_i X^{m \cdot i}$، یک کران برای P می‌باشد. بنابر قضیه ۳.۴.۱، کران P^* یک مقسوم علیه‌ای از این چندجمله‌ای می‌باشد. □

براساس لم فوق ثابت می‌شود که یک عنصر $g \in \mathbb{F}_۴[X, \theta]$، از درجه r، دارای کرانی از درجه حداکثر $۴r$ می‌باشد. نتیجه بعد که نتیجه‌ای قوی تر می‌باشد، توسط سوله[۱] برای حلقه‌ی $\mathbb{F}_۴[X, \theta]$ ثابت شده است.

لم ۲.۲.۲. فرض کنید $\mathbb{F}_۴[X, \theta]$، حلقه‌ی اریب باشد که در آن θ، یک خودریختی فروبنیوس می‌باشد. کران چندجمله‌ای از درجه‌ی r در حلقه‌ی $\mathbb{F}_۴[X, \theta]$، از درجه‌ی حداکثر $۲r$ می‌باشد.

برهان. فرض کنید که $g = \sum_{i=۰}^{r} g_i X^i$ و $\tilde{g} = \sum_{i=۰}^{r} \theta^{i+۱}(g_i) X^i$ باشند. در این صورت داریم:

$$g\tilde{g} = \sum_{k=۰}^{۲r} a_k X^k,$$

که در آن

$$a_{۲k+۱} = \sum_{i+j=۲k+۱} g_i g_j = ۰$$

و

$$a_{۲k} = \sum_{i+j=۲k} g_i \theta(g_i) \in \mathbb{F}_۲$$

می‌باشند. لذا $g\tilde{g} \in \mathbb{F}_۲[X^۲]$ خواهد بود و کران g، چندجمله‌ای $g\tilde{g} \in \mathbb{F}_۲[X^۲]$ که درجه آن $۲r$ می‌باشد، را عاد می‌کند. □

نکته ۱.۲.۲. علت وجود θـ کدها از نوع $[n, k]$، به ازای $r = n - k < \frac{n}{۲}$، این است که درجه کران g می‌تواند کمتر از $۲r$ باشد.

مثال ۱.۲.۲. حلقه چندجمله‌ای‌های اریب $\mathbb{F}_۴[X, \theta]$ را در نظر بگیرید، که θ یک خودریختی فروبنیوس و α به عنوان مولد $\mathbb{F}_۴^*$ می‌باشد. در حلقه چند جمله‌ای‌های اریب $\mathbb{F}_۴[X, \theta]$، چندجمله‌ای

$$g = X^{۱۲} + X^{۱۱} + \alpha X^{۱۰} + X^۹ + \alpha^۲ X^۸ + X^۶ + X^۵ + \alpha^۲ X^۴ + X^۲ + X + \alpha^۲$$

[۱] Sole

یک مقسوم علیه راست از چندجمله‌ای $f = X^{۱۴} + X^{۱۲} + X^{۱۰} + ۱ \in \mathbb{F}_۴[X,\theta]$ می‌باشد. لذا کران g از درجه کوچکتر مساوی ۱۴ بوده و حلقه خارج‌قسمتی $\frac{(g)}{(f)} \subset \frac{\mathbb{F}_۴[X,\theta]}{(f)}$، θـ کدی می‌باشد که یک $[۱۴,۲,۱۱]$ـ کد، با بهترین فاصله ممکن یعنی ۱۱ است.

دو چندجمله‌ای اریب $P_۱$ و $P_۲$ را مشابه گویند و با نماد $P_۱ \sim P_۲$ نمایش می‌دهند، هرگاه $\mathbb{F}_۴[X,\theta]$ـ مدول‌های چپ (یا راست) $\frac{\mathbb{F}_q[X,\theta]}{(P_۱)}$ و $\frac{\mathbb{F}_q[X,\theta]}{(P_۲)}$ خودریخت باشند.
بنابر مرجع [۲۴]، کران‌های چپ و راست بر هم منطبق بوده و چندجمله‌ای‌های مشابه دارای کران‌های یکسانی می‌باشند.

گزاره ۱.۲.۲. فرض کنید m مرتبه‌ی خودریختی θ باشد. اگر مولد g، از یک θـ کد، در حلقه $\frac{\mathbb{F}_q[X,\theta]}{(f)}$، دارای عواملی مشابه با X باشد، آنگاه g به فرم

$$g = \tilde{g} \cdot X^t$$

خواهد بود، که در آن $\tilde{g}$ دارای هیچ عاملی مشابه X نمی‌باشد. در این حالت داریم:

$$f = X^{l-t} \cdot \tilde{f} \cdot X^t,$$

که در آن $l \geq t$ بوده و داریم:

$$\tilde{f} = b_۰ + b_۱X^m + b_۲X^{۲m} + \cdots + b_sX^{s\cdot m} \in \mathbb{F}_q^\theta[X^m] \qquad b_۰ \neq ۰.$$

چندجمله‌ای $\tilde{f}$، کران برای $\tilde{g}$، می‌باشد و θـ کد $\frac{(g)}{(f)}$، با اضافه کردن t تا صفر به سمت چپ هر کدواژه، از θـ کد $\frac{(\tilde{g})}{(\tilde{f})}$، به دست می‌آید.

برهان. به وضوح در حلقه $\mathbb{F}_q[X,\theta]$، چندجمله‌ای‌هایی که درجه آن‌ها یک باشد، تحویل ناپذیر هستند. از مراجع [۲۴] و [۳۱] نتیجه می‌شود که چندجمله‌ای‌های اریب تحویل ناپذیر $P_۱$ و $P_۲$، مشابه می‌باشند اگر و تنها اگر از درجات یکسانی باشند و چندجمله‌ای مانند $U \in \mathbb{F}_q[X,\theta]$، از درجه کوچکتر از $\deg(P_i)$ موجود باشد، به طوری که $P_۱U$ کوچکترین مضرب مشترک چپ $P_۲$ و U باشد.
چندجمله‌ای X تنها مشابه مضارب خود می‌باشد. از آنجایی که بنا به مطالب بالا

$$(\alpha X + \beta) \sim X$$

لذا u و γ، در میدان F_q وجود دارند به طوری که $(\alpha X + \beta)u = \gamma X$ خواهد بود. بنابراین تعداد عوامل تحویل‌ناپذیر مشابه با X، با تعداد عوامل X در این تجزیه متناظر می‌باشد.
با توجه به اینکه $X_a = \theta(a)X$ می‌باشد، نتیجه می‌گیریم که یک عامل از X می‌توانند جابه‌جا شود، به گونه‌ای که یک عامل چپ یا راست باشند. لذا داریم:

$$g = \tilde{g}X^t, \quad f = X^{l-t}\tilde{f}X^t,$$

که در آن $l \geq t$ بوده و داریم:

$$\tilde{f} = b_0 + b_1 X + b_2 X^{2m} + \cdots + b_s X^{sm} \in \mathbb{F}_q^*[X^m] \quad b_0 \neq 0.$$

چون چندجمله‌ای اریب $\mathbb{F}_q[X,\theta]$، یک دامنه‌ی چپ و راست می‌باشد، لذا $\tilde{g}$ عاملی راست از چندجمله‌ای $X^{l-t}\tilde{f}$ است.

تنها تفاوت ماتریس مولد $\frac{(g)}{(X^{l-t}fX^t)}$ و $\frac{\tilde{g}}{(X^{l-t}\tilde{f})}$، در t تا ستون صفر در سمت راست می‌باشد. کدواژه‌ها در حالت اول به صورت $(\sum_{j=0}^{k} c_j X^j)\tilde{g}X^t$ و در حالت دوم به صورت $(\sum_{j=0}^{k} c_j X^j)\tilde{g}$، نوشته می‌شوند. □

بنابراین θـ کدهای تولید شده توسط چندجمله‌ای‌هایی که عناصر ثابت آن‌ها صفر است، با استفاده از θـ کدهایی از طول‌های بلوکی کوچکتر که در آن‌ها مولفه‌های صفر به سمت راست اضافه شده‌اند، به دست می‌آیند. در حلقه‌ی ناجابه‌جایی $\mathbb{F}_q[X,\theta]$، تجزیه‌های مختلفی در حد یکریختی وجود دارد.

قضیه ۱.۲.۲. ([۱۳] قضیه ۱۴) اگر چندجمله‌ای $P \in \mathbb{F}_q[X,\theta]$، دارای دو تجزیه به عوامل تحویل‌ناپذیر به صورت $P = P_1 P_2 \dots P_n = \tilde{P}_1 \tilde{P}_2 \dots \tilde{P}_m$ باشد، آنگاه $n = m$ خواهد بود و یک جایگشت $\sigma \in S_n$ وجود دارد، به طوری که P_i و $\tilde{p}_{\sigma(i)}$، مشابه هستند.

لم ۱.۲.۲ روشی را برای محاسبه‌ی کران یک چندجمله‌ای ارائه می‌دهد. نگرش دیگر این است که کران حاصلضرب، برابر با مقسوم‌علیه حاصلضرب کران عوامل آن می‌باشد. (قضیه ۳.۴.۱ را ببینید.)

مثال ۲.۲.۲. در مثال ۱.۲.۲، چندجمله‌ای

$$g = X^{12} + X^{11} + \alpha X^{10} + X^9 + \alpha^2 X^8 + X^6 + X^5 + \alpha^2 X^4 + X^2 + X + \alpha^2$$

را می‌توان به فرم

$$g = (X^4 + X + 1)^2 (X + \alpha)(X + \alpha)(X + 1)^2,$$

تجزیه کرد. به علاوه کران چندجمله‌ای $X + \alpha$، برابر با $X^2 + 1$ می‌باشد، که $(X^4 + X + 1)^2$ و $(X + 1)^2$، چندجمله‌ای‌هایی از $\mathbb{F}_2[X^2]$ می‌باشند. لذا می‌توان کران g را به فرم حاصلضرب، به صورت

$$(X^4 + X + 1)^2 (X^2 + 1)(X^2 + 1)(X + 1)^2 = X^{14} + X^{12} + X^{10} + 1$$

نوشت، که همان چندجمله‌ای f در مثال ۱.۲.۲ می‌باشد.

جدول ۱.۲، بهترین فاصله همینگ ممکن را برای $[n,k]$ـ θـ کدها روی حلقه $\mathbb{F}_4[X,\theta]$ ارائه می‌دهد، که در آن $r = n - k \leq \min(n, 10)$ و n یک عدد زوج کوچکتر مساوی ۴۴ می باشد.

جدول ۱.۲: کدهای دوری و مرکزی از طول داده شده‌ی n

n \ r	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
۴	$C^{\theta}_{۳s}$	$C_{۴}$							
۶	$C_{۲}$	$C_{۴}$	$C^{\theta}_{۴}$	$C_{۶}$					
۸	$C_{۲}$	$C^{\theta}_{۳}$	$C^{\theta}_{۴s}$	$C^{\theta}_{۵}$	$C^{\theta}_{۶}$	$C_{۸}$			
۱۰	$C_{۲}$	$\theta_{۳}$	$C^{\theta}_{۴}$	$C^{\theta}_{۵}$	$C^{\theta}_{۶}$	$\theta_{۶}$	$\theta_{۸}$	$C_{۱۰}$	
۱۲	$C_{۲}$	$\theta_{۳}$	$\theta_{۴}$	$C_{۴}$	$C^{\theta}_{۶s}$	$C^{\theta}_{۶}$	$C^{\theta}_{۷}$	$C^{\theta}_{۸}$	$C^{\theta}_{۹}$
۱۴	$C_{۲}$	$C^{\theta}_{۳}$	$C^{\theta}_{۴}$	$C_{۴}$	$C^{\theta}_{۵}$	$C^{\theta}_{۶s}$	$C^{\theta}_{۷}$	-۱	-۱
۱۶	$C_{۲}$	-۱	-۱	$C^{\theta}_{۴}$	-۱	-۱	-۱	-۱	$C^{\theta}_{۸}$
۱۸	$C_{۲}$	-۱	$\theta_{۳}$	$\theta_{۴}$	-۱	-۱	$C^{\theta}_{۶}$	-۱	$C^{\theta}_{۸}$
۲۰	$C_{۲}$	-۱	$\theta_{۳}$	$\theta_{۴}$	-۱	-۱	$\theta_{۶}$	$C^{\theta}_{۷}$	$C^{\theta}_{۸}$
۲۲	$\theta_{۲}$	$\theta_{۲}$	$\theta_{۳}$	$\theta_{۴}$	$\theta_{۴}$	$\theta_{۵}$	-۱	$C^{\theta}_{۶}$	$C^{\theta}_{۷}$
۲۴	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	$\theta_{۳}$	$C^{\theta}_{۴}$	$C^{\theta}_{۴}$	-۱	-۱	$C^{\theta}_{۶}$	$C^{\theta}_{۷}$
۲۶	$\theta_{۲}$	$\theta_{۲}$	$\theta_{۳}$	$\theta_{۴}$	$\theta_{۴}$	-۱	-۱	$C^{\theta}_{۶}$	-۱
۲۸	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	$\theta_{۳}$	$C^{\theta}_{۴}$	$C^{\theta}_{۴}$	-۱	$\theta_{۵}$	$C^{\theta}_{۶}$	$C^{\theta}_{۶}$
۳۰	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	$C^{\theta}_{۳}$	$C^{\theta}_{۴}$	$C^{\theta}_{۴}$	-۱	$C^{\theta}_{۵}$	$C^{\theta}_{۶}$	$C^{\theta}_{۶}$
۳۲	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	-۱	-۱	$\theta_{۴}$	-۱	$\theta_{۵}$	$C^{\theta}_{۶}$	$\theta_{۶}$
۳۴	$\theta_{۲}$	$\theta_{۲}$	-۱	-۱	$\theta_{۴}$	-۱	$C^{\theta}_{۵}$	$C^{\theta}_{۶}$	$C^{\theta}_{۶}$
۳۶	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	-۱	-۱	$\theta_{۴}$	-۱	-۱	-۱	$\theta_{۶}$
۳۸	$\theta_{۲}$	$\theta_{۲}$	-۱	-۱	$\theta_{۴}$	-۱	-۱	-۱	$\theta_{۶}$
۴۰	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	-۱	-۱	$\theta_{۴}$	-۱	-۱	-۱	$\theta_{۶}$
۴۲	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	-۱	$C^{\theta}_{۳}$	$C^{\theta}_{۴}$	-۱	-۱	-۱	$C^{\theta}_{۶}$
۴۴	$C^{\theta}_{۲}$	$C^{\theta}_{۲}$	-۱	$\theta_{۳}$	$\theta_{۴}$	$\theta_{۴}$	-۱	-۱	-۱

از آنجایی که کران چندجمله‌ای g از درجه‌ی r، حداکثر از درجه $۲r$ می‌باشد (بنا به لم ۲.۲.۲)، لذا هر چندجمله‌ای از درجه r، یک θـ کد از طول $n \geq ۲r$، تولید می‌کند. در واقع کران چندجمله‌ای g لزوما θـ کد مورد نظر را تولید نمی‌کند (تنها وجود آن کفایت می‌کند) و ما را قادر به محاسبه کران با مقادیر n به اندازه کافی بزرگ می‌سازد، تا زمانی که $r \leq \frac{n}{۴}$ باشد.

نمادگذاری: فرض کنید C_d نماد کد دوری با فاصله همینگ d، C_d^θ نماد θـ کد دوری با فاصله همینگ d و θ_d نماد θـ کد مرکزی با فاصله همینگ d باشد. همچنین $C_{۴s}^\theta$ نماد θـ کد دوری خوددوگان با فاصله همینگ ۳ باشد.

اگر نتوانیم کدی که فاصله همینگ آن سازگار با کد شناخته شده با بهترین فاصله همینگ در نرم افزار ماگما باشد، به دست آوریم (مرجع [۹])، آنگاه اختلاف فاصله همینگ را با یک عدد منفی نشان می‌دهیم. جدول ۱.۲ نشان می‌دهد که با افزایش طول، بهترین θـ کدها لزوما همه‌ی کدهای دوری یا کدهای θـ دوری نمی‌باشد.

توجه کنید که بهترین کدهای داده شده در نرم افزار ماگما، اغلب توزیع وزنی ضعیف دارند، و با استفاده از θـ کدها می‌توان کدهایی که توزیع وزنی بهتری دارند را به دست آورد.

مثال ۳.۲.۲. بهترین $[۶,۲,۴]$ـ کد شناخته شده روی میدان $\mathbb{F}_۴$ که توسط نرم‌افزار ماگما به دست آمده، دارای توزیع وزنی برابر با $۱ + ۱۵Y^۴$ است، در حالی که چند جمله‌ای مولد $X^۴+X^۳+\alpha^۲X^۲+X+\alpha$، با کران $X^۶+X^۴+X^۲+۱$، دارای توزیع وزنی برابر با $۱+۳Y^۴+۱۲Y^۵$ است.

$[۱۲,۷]$ـ θـ کد دوری تولید شده توسط $X^۵ + \alpha X^۴ + \alpha X^۲ + \alpha X + \alpha$ دارای توزیع وزنی

$$۱ + ۱۸Y^۴ + ۲۵۲Y^۵ + ۶۷۲Y^۶ + ۱۵۴۸Y^۷ + ۳۲۸۵Y^۸ + ۴۲۱۲Y^۹ + ۳۸۱۶Y^{۱۰} + ۲۰۵۲Y^{۱۱} + ۵۲۸Y^{۱۲}$$

است. توزیع بهترین $[۱۲,۷,۴]$ـ کد ماگما برابر با

$$۱ + ۱۴۱Y^۴ + ۴۵۹Y^۵ + ۱۲۱۵Y^۶ + ۲۸۹۵Y^۷ + ۴۲۳۰Y^۸ + ۴۲۰۹Y^۹ + ۲۵۴۱Y^{۱۰} + ۶۹۳Y^{۱۱}$$

می‌باشد.

فصل ۳

دوگان θـ کدها

۱.۳ مقدمه

θـ کدهای دوری در مرجع [۲۲] مورد مطالعه گسترده‌ای قرار گرفته‌اند، که در آن ماتریس کنترل توازن چنین کدهایی داده شده است. در این فصل ماتریس کنترل توازن را از تجزیه‌های چندجمله‌ای $X^n - ۱$، در حلقه $\mathbb{F}_q[X, \theta]$، به دست می‌آوریم و ثابت می‌کنیم که، دوگان یک θـ کد دوری، (برای حاصلضرب اقلیدسی) θـ کد دوری می‌باشد.

۲.۳ دوگان θـ کدهای دوری

در لم زیر ماتریس کنترل توازن برای θـ کدهای دوری در مرجع [۲۲] داده شده است.

لم ۱.۲.۳. فرض کنید که مرتبه‌ی θ، n را عاد کند. همچنین فرض کنید: $X^n - ۱ = h \cdot g \in Z(\mathbb{F}_q[X, \theta])$. و کد C یک θـ کد دوری متناظر با ایده‌آل چپ تولید شده توسط g در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(X^n-۱)}$، باشد. اگر داشته باشیم:

$$g = g_۰ + g_۱X + \cdots + g_rX^r, \quad h = h_۰ + h_۱X + \cdots + h_{n-r}X^{n-r},$$

آنگاه ماتریس زیر، ماتریس کنترل توازن برای کد C، می‌باشد.

$$H=\begin{pmatrix} h_{n-r} & \dots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \dots & 0 \\ 0 & \theta(h_{n-r}) & \dots & \dots & \theta^{n-r+1}(h_0) & \dots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & 0 & \theta^{r-1}(h_{n-r}) & \dots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}$$

برهان. همانطور که در لم ۳.۱.۲ بیان کردیم، اگر $a(X)\in C$ باشد، آنگاه در حلقه خارج قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(X^n-1)}$، حاصلضرب $a(X)\cdot h=0$ خواهد بود. با توجه به اینکه درجه $(a(X)\cdot h)$، کوچکتر از $n+k$ می‌باشد، که در آن $k=n-r$، بعد کد C و درجه‌ی h است. مرتبه‌ی کد C است، می‌توان نتیجه گرفت که ضرایب $X^k, X^{k+1},\dots,X^{n-1}$، در این حاصلضرب باید صفر باشد. همچنین برای $l\in\{0,\dots,r-1\}$، ضرایب X^{l+k} در حاصلضرب $a(X)\cdot h$، برابر با $\sum_{i=1}^{l+k} a_i\theta^i(h_{l+k}-i)$ می‌باشد. لذا از اینکه $a(X)\in C$ است، نتیجه می‌گیریم $H\cdot a^t=0$. بنابراین کد تولید شده توسط ماتریس H، مشمول در دوگان کد C $(C^\perp)$، می‌باشد. از آنجا که بعد کد $C^\perp$ برابر با $n-\dim(C)=r$، تعداد سطرهای H است نتیجه می‌گیریم که H یک ماتریس مولد برای دوگان کد C می‌باشد. □

در مرجع [۲۲]، ماتریس کنترل توازن یک θـ کد دوری داده شده است، اما این که دوگان θـ کدهای دوری، θـ کد دوری خواهد بود نشان داده نشده است.

نتیجه ۱.۲.۳. فرض کنید که مرتبه‌ی خودریختی θ، n را عاد کند. و همچنین فرض کنید که $g=\sum_{i=0}^{r} g_iX^i$ و $h=\sum_{i=0}^{n-r} h_iX^i$، عناصری از حلقه $\mathbb{F}_q[X,\theta]$، باشند، به طوری که

$$h\cdot g=X^n-1\in Z(\mathbb{F}_q[X,\theta])$$

باشد. دوگان θـ کد دوری تولید شده توسط g، در حلقه خارج‌قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(X^n-1)}$، θـ کد دوری تولید شده توسط $g^\perp=h_{n-r}+\theta(h_{n-r-1})X+\dots+\theta^{n-r}(h_0)X^{n-r}$ می‌باشد.

برهان. همانطور که می‌دانیم، ماتریس کنترل توازن H، در یک کد، یک ماتریس مولد برای کد دوگان می‌باشد. اکنون باید نشان دهیم که H، ماتریسی از یک θـ کد دوری می‌باشد. بر اساس نتیجه قبل، $\theta^{n-r}(h_0)X^{n-r}+\dots+\theta(h_{n-r-1})X+h_{n-r}$ ، یک مقسوم علیه از X^n-1 می‌باشد.

اما از آنجا که حلقه‌ی $\mathbb{F}_q[X,\theta]$ یک دامنه‌ی اور راست است، دارای یک میدان کسر اریب راست است. (مرجع [۱۹] را ببینید.) فرض کنید که $\mathbb{F}_q(X,\theta)$ نمایش دهنده‌ی میدان کسر راست از حلقه $\mathbb{F}_q[X,\theta]$ باشد و همچنین فرض کنید که X^{-1}، معکوس X باشد. در این صورت داریم $aX^{-1}=X^{-1}\theta(a)$. حال فرض کنید که حلقه‌ی $R\subset\mathbb{F}_q(X,\theta)$، شامل عناصر $\sum_{i=0}^{n} X^{-i}a_i$ باشد، که در آن ضرایب در سمت راست قرار گرفته و قانون ضرب به صورت

$aX^{-1} = X^{-1}\theta(a)$، می‌باشد. لذا حلقه‌ی R یکریخت است با حلقه‌ی چندجمله‌ای‌های اریب $\mathbb{F}_q[X^{-1}, \theta^{-1}]$. نگاشت:

$$\phi : \mathbb{F}_q[X, \theta] \to R \subset \mathbb{F}_q(X, \theta)$$
$$\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} X^{-i} a_i$$

یک یکریختی حلقه‌ای نمی‌باشد. لذا برای $P_1 = \sum_{i=0}^{s} a_i X^i$ و $P_2 = \sum_{i=0}^{t} b_i X^i$، داریم:

$$\begin{aligned}
\varphi(P_1 + P_2) &= \varphi(P_1 + P_2) \\
\varphi(P_1 P_2) &= \varphi(\sum_{k=0}^{s+t} \sum_{i+j=k} a_i X^i b_j X^j) \\
&= \varphi(\sum_{k=0}^{s+t} \sum_{i+j=k} a_i \cdot \theta^i(b_j) X^{i+j}) \\
&= \sum_{k=0}^{s+t} X^{-k} \sum_{i+j=k} \theta^i(b_j) \cdot a_i \\
&= \sum_{k=0}^{s+t} \sum_{i+j=k} X^{-j}(X^{-i}\theta^i(b_j)) a_i \\
&= (\sum_{k=0}^{s+t} \sum_{i+j=k} X^{-j} b_j X^{-i} a_i) \\
&= \varphi(P_2) \cdot \varphi(P_1).
\end{aligned}$$

اگر $x^n - 1 = h \cdot g$ باشد، آنگاه داریم:

$$\varphi(X^n - 1) = X^{-n} - 1 = \varphi(h \cdot g) = \varphi(g \cdot h) = (\sum_{j=0}^{n-r} X^{-j} h_j)(\sum_{k=i=0}^{r} X^{-i} g_j).$$

به این ترتیب در میدان $\mathbb{F}_q(X, \theta)$ داریم:

$$\begin{aligned}
X^{n-r}(X^{-n} - 1)X^r &= -(X^n - 1) \\
&= (h_{n-r} + \theta(h_{n-r-1})X + \cdots + \theta^{n-r}(h_0)X^{n-r}) \cdot \tilde{g}
\end{aligned}$$

که در آن، $\tilde{g} \in \mathbb{F}_q[X, \theta]$ می‌باشد. بنابراین چندجمله‌ای $h_{n-r} + \theta(h_{n-r-1})X + \cdot + \theta^{n-r}(h_0)$، چندجمله‌ای $X^n - 1$، در حلقه‌ی $\mathbb{F}_q[X, \theta]$ را عاد می‌کند. □

مثال ۱.۲.۳. حلقه‌ی چندجمله‌ای‌های اریب $\mathbb{F}_4[X, \theta]$ را در نظر بگیرید، که در آن θ یک خودریختی فروبنیوس و α به عنوان مولد $\mathbb{F}_4^*$ باشد. با استفاده از چندجمله‌ای‌های

$$g = X^2 + \alpha X + \alpha^2$$

و

$$h = X^۲ + \alpha X + \alpha$$

در حلقه‌ی $\mathbb{F}_۴[X, \theta]$، نتیجه می‌گیریم:

$$g \cdot h = X^۴ - ۱,$$

و چندجمله‌ای

$$g^\perp = \theta^۲(\alpha)X^۲ + \theta(\alpha)X + ۱ = \alpha X^۲ + \alpha^۲ X + ۱$$

خواهد بود. همچنین با استفاده از $\alpha^۲ g^\perp = g$ نتیجه می‌گیریم که کد تولید شده توسط g، در حلقه خارج‌قسمتی $\frac{\mathbb{F}_۴[X]}{(X^۴-۱)}$، یک کد خوددوگان اقلیدسی می‌باشد.

اکنون نشان می‌دهیم که دوگان θـ کد مرکزی، لزوماً θـ کد دوری نمی‌باشد.

مثال ۳.۲.۳. مثالی از $[۱۲, ۹, ۳]_\theta$ـ کد مرکزی که در فصل ۲ بیان شده، را در نظر بگیرید. با استفاده از نرم‌افزار ماگما می‌توان ماتریس مولدی برای کد دوگان، به صورت زیر محاسبه کرد:

$$G^\perp = \begin{pmatrix} ۱ & ۰ & ۰ & \alpha & \alpha & ۰ & \alpha^۲ & ۰ & \alpha^۲ & \alpha & ۱ & \alpha \\ ۰ & ۱ & ۰ & ۱ & \alpha & \alpha^۲ & \alpha & \alpha & \alpha & \alpha^۲ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۱ & ۰ & \alpha^۲ & ۰ & \alpha^۲ & ۱ & \alpha & ۱ & ۱ \end{pmatrix}$$

کدواژه $a = (۰, \ldots, ۰, ۱)G^\perp$ توسط چندجمله‌ای زیر ارائه می‌شود:

$$\begin{aligned} a(X) &= X^۲ + X^۳ + \alpha^۲ X^۵ + \alpha^۲ X^۷ + X^۸ + \alpha X^۹ + X^{۱۰} + X^{۱۱} \\ &= (۱ + x + \alpha^۲ X^۳ + \alpha^۲ X^۵ + X^۶ + \alpha X^۷ + X^۸ + X^۹)X^۲. \end{aligned}$$

از آنجا که $\theta^۲ = Id$، چندجمله‌ای $a(X)$ را به صورت $a(X) = X^۲ g^\perp(X)$ هم می‌توان نوشت، که در آن

$$g^\perp(X) = ۱ + x + \alpha^۲ X^۳ + \alpha^۲ X^۵ + X^۶ + \alpha X^۷ + X^۸ + X^۹$$

می‌باشد. کد $C^\perp$ یک $[۱۲, ۳]$ـ کد می‌باشد، اما چندجمله‌ای $g^\perp$، که تکین و از درجه ۹ است، مقسوم‌علیه راست هیچ چندجمله‌ای مرکزی از درجه ۱۲ نیست و بنابراین نمی‌تواند یک θـ کد مرکزی باشد.

برای کامل کردن این مثال می‌توانیم کران چندجمله‌ای $g^\perp$ را از تجزیه‌های زیر محاسبه کنیم:

$$g^\perp = (X + \alpha^۲)(X + \alpha^۲)(X + ۱)(X + \alpha)(X + \alpha)(\alpha + ۱)(X^۳ X^۲ + \alpha X + ۱).$$

در واقع چندجمله‌ای $g^\perp$، سمت راست چندجمله‌ای

$$\tilde{g} = (X^2+1)^6(X^3+X+1)^2 = X^{18}+X^{12}+X^8+X^4+X^2+1,$$

را عاد می‌کند. که در آن درجه چندجمله‌ای ۱۸ بوده و چندجمله‌ای $g^\perp$، هیچ عاملی از درجه کوچکتر از ۱۸ از $\tilde{g}$ را عاد نمی‌کند. لذا $\tilde{g}$، کران برای $g^\perp$ می‌باشد.

۳.۳ محاسبه‌ی θـ کدهای دوری خوددوگان اقلیدسی روی میدان $\mathbb{F}_4$

در این بخش کدهای θـ دوری خوددوگان اقلیدسی روی میدان $\mathbb{F}_4$ را بررسی می‌نماییم. تعمیم نتایجی که در این بخش برای میدان $\mathbb{F}_4$ بیان می‌شود به حالت کلی $\mathbb{F}_q$ ساده می‌باشد.

هدف ما، محاسبه‌ی همه‌ی θـ کدهای دوری خوددوگان اقلیدسی، با طول $n \leq 40$، روی حلقه‌چندجمله‌ای‌های اریب $\mathbb{F}_4[X,\theta]$ می‌باشد، که در آن θ یک خودریختی فروبنیوس می‌باشد. لذا باید تمام چندجمله‌ای‌های اریب g را که $X^n-1 = h\cdot g$ محاسبه کنیم، به طوری که θـ کد دوری C، که $C = \frac{(g)}{(X^n-1)}$، یک کد خوددوگان باشد.

نتیجه ۱.۲.۳ به ما این اجازه را می‌دهد که، ضرایب چندجمله‌ای مولد $g^\perp$، از کد $C^\perp$، را برحسب ضرایب چندجمله‌ای h بیان کنیم. برای اینکه کد C یک کد خوددوگان باشد، چندجمله‌ای‌های $\tilde{g}$ و g، باید در حد یک ضریب ثابت تفاوت داشته باشند.

تمام مولدهای ممکن چندجمله‌ای g، برای کدهای θـ دوری خوددوگان اقلیدسی، از طول داده شده را می‌توان با محاسبه‌ی پایه گروبنر[1] این چندجمله‌ای در نرم‌افزار ماگما به دست آورد. برای محاسبه‌ی این دستگاه چندجمله‌ای، فرض کنید که چندجمله‌ای $g = \sum_{i=0}^{r-1} g_iX_i + X^r$، که در آن g_0 مخالف صفر است، چندجمله‌ای مولد یک θـ کد دوری خوددوگان با طول $n = 2r$ باشد. همچنین فرض کنید که چندجمله‌ای $h = X^r + \sum_{i=0}^{r-1} h_iX_i$ باشد، به طوری که $gh = X^n - 1$ باشد.

بر اساس نتیجه ۱.۲.۳ ، کد $C^\perp$ توسط $g^\perp = 1 + \sum_{i=1}^{r} \theta^i(h_{r-i})X^i$ تولید می‌شود. از آنجا که $C = C^\perp$، چندجمله‌ای $g^\perp$ یک مضربی از چندجمله‌ای g است، یعنی داریم $g^\perp = \theta^r(h_0)g$. با مقایسه‌ی ضرایب دو چندجمله‌ای، داریم:

$$\begin{cases} 1 = \theta^r(h_0)\cdot g_0 \\ \theta^i(h_{r-i}) = \theta^r(h_0)\cdot g_i, \quad i = 0,\ldots,r-1 \end{cases}$$

چون خودریختی فروبنیوس θ، از $\mathbb{F}_q$، از مرتبه ۲ می‌باشد، لذا داریم $\theta = \theta^{-1}$. همچنین با

[1] Groebner

استفاده از اینکه $g_\circ \neq \circ$ و $g_\circ \in \mathbb{F}_۴$ داریم $g_\circ^{-۱} = g_\circ^۲$ و لذا داریم:

$$\begin{cases} h_\circ = \theta^r(g_\circ)^۲ \\ h_{r-i} = \theta^i(g_\circ^۲ \cdot g_i), \quad i = \circ, \ldots, r-۱. \end{cases}$$

در نتیجه $h = \theta^r(g_\circ^۲) + \sum_{i=۱}^{r} \theta^{r-i}(g_\circ^۲)\theta^{r-i}(g_{r-i})X^i$. باتوجه به اینکه $\theta^i(a) = a^{۲^i mod ۳}$ می‌توانیم عبارت شامل θ^i را با توانی از g_i، از درجه کوچکتر مساوی ۴، به صورت زیر جایگذاری کنیم:

$$h = g_\circ^{(۲^{r+۱} mod ۳)} + \sum_{i=۱}^{r} g_\circ^{(۲^{r-i+۱} mod ۳)} g_{r-i}^{(۲^{r-i} mod ۳)} X^i.$$

با گسترش حاصلضرب اریب $(X^n - ۱) - (h \cdot g) = \circ$ و با استفاده از قاعده $X^i a = a^{۲^i mod ۳} X^i$، $۲r+۱$ معادله چندجمله‌ای را به دست می‌آوریم، که درآن ضریب g_i در هر متغیر، کمتر از ۴ می‌باشد. از آنجا که به دنبال حل g_i، در میدان $\mathbb{F}_۴$ می‌باشیم، r معادله‌ی $g_i^۴ - g_i = \circ$ را به این معادلات می‌افزاییم و لذا به یک دستگاه با $۳r+۱$ معادله‌ی چندجمله‌ای و r متغیر می‌رسیم، که درجه هر متغیر کوچکتر مساوی ۴، می‌باشد که از پایه‌های گروبنر در نرم‌افزار ماگما از حل این دستگاه استفاده می‌کنیم.

به وضوح مجموعه جواب باید متناهی باشد. برای هر چندجمله‌ای g متناظر با یک جواب، کد خطی که چندجمله‌ای تولید می‌کند و مینیمم فاصله همینگ آن کد را محاسبه می‌کنیم.

جدول ۱.۳، بهترین فاصله همینگ θـ کدهای دوری خوددوگان با طول n، که n کوچکتر مساوی ۴۰ می‌باشد را ارائه می‌دهد. در ستون چهارم که با D مشخص شده است، بهترین فاصله همینگ شناخته شده، از کدهای خطی، با طول n و بعد $\frac{n}{۲}$ داده شده است. در ستون پنجم، که با D_s مشخص شده است، بهترین فاصله همینگ، برای کدهای خوددوگان، از طول n داده شده است. (مرجع [۲۳] را ببینید.)

دو ستون آخر با n_d و E_d مشخص شده‌اند، که ستون n_d، شامل θـ کدهای دوری با مینیمم فاصله همینگ d و ستون E_d، شامل کلاس کدهایی می‌باشد که با هم معادل‌اند. (با جایگشت دادن)

توجه شود که همیشه به بهترین فاصله همینگ شناخته شده از کدهای خوددوگان روی میدان $\mathbb{F}_۴$ می‌رسیم، به جز زمانی که $n \in \{۱۶, ۲۴, ۳۲\}$ باشد. همچنین بهترین فاصله همینگ کدهای خوددوگان با طول ۳۶ که برابر با ۱۰ می‌باشد را بهبود می‌بخشیم. در واقع، بهترین $[۳۶, ۱۸]$ـθـ کدهای دوری، دارای فاصله همینگ ۱۱ می‌باشند و ۳۶ گونه از چنین کدهایی موجودند که در ۳ کلاس مشابه کدها، طبقه‌بندی شده‌اند. در ادامه، چندجمله‌ای‌های مولد سه تا از $[۳۶, ۱۸, ۱۱]$ـθـ کدهای دوری خوددوگان که معادل نیستند، داده شده است:

$$X^{۱۸} + X^{۱۶} + \alpha^۲ X^{۱۵} + \alpha X^{۱۴} + \alpha^۲ X^{۱۳} + X^{۱۲} + \alpha X^{۱۰} + \alpha X^۹ + \alpha X^۸ + \alpha^۲ X^۶ + X^۵ + \alpha X^۴ + X^۳ + \alpha^۲ X^۲ + \alpha^۲,$$

$$X^{۱۸}+\alpha X^{۱۷}+\alpha^۲X^{۱۶}+\alpha^۲X^{۱۵}+X^{۱۴}+X^{۱۳}+\alpha^۲X^{۱۲}+X^{۱۰}$$
$$+\alpha X^۹+\alpha^۲X^۸+X^۶+\alpha^۲X^۵+\alpha^۲X^۴+X^۳+X^۲+\alpha X+\alpha^۲,$$

$$X^{۱۸}+\alpha^۲X^{۱۷}+\alpha X^{۱۶}+\alpha^۲X^{۱۵}+\alpha^۲X^{۱۴}+X^{۱۳}+\alpha^۲X^{۱۲}+\alpha^۲X^{۱۱}$$
$$+\alpha^۲X^{۱۰}+X^۸+X^۷+X^۶+\alpha^۲X^۵+X^۴+X^۳+\alpha X^۲+X+\alpha^۲.$$

محاسبه‌ی همه‌ی $[۳۶,۱۸]$ـθـ کدهای دوری خوددوگان، مستلزم حل دستگاه ۵۵ معادله‌ی چندجمله‌ای، روی میدان $\mathbb{F}_۴$ می‌باشد، که در آن درجه‌ی هر ۱۸ متغیر کوچکتر مساوی ۴ بوده و برای هر چنین چندجمله‌ای باید از دستور IsSelfDual در نرم‌افزار ماگما، به منظور بررسی این نکته که آیا کد متناظر خوددوگان است یا نه استفاده نمود. اگر کد متناظر خوددوگان باشد، روش استفاده از پایه‌های گروبنر، روش موثرتری را برای به دست آوردن همه‌ی کدهای خوددوگان از یک طول داده شده، ارائه می‌دهد. محاسبه‌ی تمام کدهای خوددوگان، با طول کوچکتر مساوی ۴۰، روی میدان $\mathbb{F}_۴$، با استفاده از نرم‌افزار ماگما در کل $۱۰۵۸۰۴/۲۷۹s$ $(۳۰h)$ زمان می‌برد و $۱۵۱۱/۳۸MB$ حافظه استفاده می‌شود.

۴.۳ محاسبه‌ی θـ کدهای دوری خوددوگان هرمیتی روی میدان $\mathbb{F}_۴$

کدهای خوددوگان هرمیتی روی میدان $\mathbb{F}_۴$ را، با استفاده از روشی مشابه کدهای خوددوگان اقلیدسی محاسبه می‌کنیم. فرض کنید q توان زوجی از عدد اول بوده و θ یک خودریختی از مرتبه ۲، روی $\mathbb{F}_q : a \mapsto a^{\sqrt{q}}$ باشد. ضرب اسکالر هرمیتی روی میدان $\mathbb{F}_q^n$، به صورت زیر تعریف می‌شود:

$$\forall x,y \in \mathbb{F}_q^n, \langle x,y\rangle_H = \sum_{i=۱}^{n} x_i \cdot \theta(y_i).$$

دوگان هرمیتی یک کد دوری روی $\mathbb{F}_q^n$، مجموعه‌ای از کلمات می‌باشد که تحت این ضرب اسکالر هرمیتی به کدواژه‌های کد متعامد می‌شود.

لم ۱.۴.۳. فرض کنید $g, h = \sum_{i=۰}^{r} h_i X^i$، عناصر حلقه چندجمله‌ای‌های اریب $\mathbb{F}_q[X,\theta]$ باشند، به طوری که، $h \cdot g = X^{۲r}-۱$ باشد. دوگان هرمیتی از θـ کد دوری تولید شده توسط g، در حلقه خارج قسمتی $\frac{\mathbb{F}_q[X,\theta]}{(X^{۲r}-۱)}$، نیز یک کد دوری می‌باشد و توسط چندجمله‌ای زیر تولید شده است:

$$g^H = \theta(h_r) + \theta^۲(h_{r-۱})X + \cdots + \theta^{۱+r}(h_۰)X^r.$$

جدول ۱.۳: بهترین فاصله همینگ θـ کدهای دوری خوددوگان با طول $n \leq ۴۰$

n	g	d	D	D_s	n_d	E_d
۴	$X^۲ + \alpha^۲X + \alpha$	۳	۳	۳	۲	۱
۶	$X^۳ + \alpha X^۲ + \alpha X + ۱$	۳	۴	۳	۲	۱
۸	$X^۴ + \alpha^۲X^۳ + \alpha^۲X^۲ + \alpha^۲X + \alpha$	۴	۴	۴	۲	۱
۱۰	$X^۵ + X^۴ + \alpha X^۳ + \alpha X^۲ + X + ۱$	۴	۵	۴	۴	۱
۱۲	$X^۶ + X^۵ + \alpha^۲X^۴ + X^۳ + \alpha X^۲ + X + ۱$	۶	۶	۶	۴	۱
۱۴	$X^۷ + X^۵ + \alpha X^۴ + \alpha X^۳ + X^۲ + ۱$	۶	۷	۶	۲	۱
۱۶	...	۴	۷	۶	۲	۱
۱۸	$X^۹ + \alpha X^۶ + X^۵ + X^۴ + \alpha X^۳ + ۱$	۶	۸	۶	۱۲	۲
۲۰	$X^{۱۰} + \alpha^۲X^۹ + \alpha X^۸ + X^۷ + X^۶ + X^۴ + X^۳ + \alpha^۲X^۲ + \alpha X + ۱$	۸	۸	۸	۸	۱
۲۲	$X^{۱۱} + X^۸ + X^۷ + \alpha X^۶ + \alpha X^۵ + X^۴ + X^۳ + ۱$	۸	۸	۸	۱۰	۱
۲۴	...	۷	۹	۸	۱۶	۲
۲۶	$X^{۱۳} + X^{۱۰} + \alpha^۲X^۸ + \alpha X^۷ + \alpha X^۶ + \alpha^۲X^۵ + X^۳ + ۱$	۸	۱۰	۸	۳۶	۳
۲۸	$X^{۱۴} + X^{۱۱} + X^{۱۰} + X^۹ + \alpha^۲X^۸ + X^۷ + \alpha X^۶ + X^۵ + X^۴ + X^۳ + ۱$	۹	۱۱	۹	۳۲	۴
۳۰	$X^{۱۵} + \alpha X^{۱۲} + X^{۱۱} + \alpha^۲X^{۱۰} + \alpha^۲X^۹ + X^۸ + X^۷ + \alpha^۲X^۶ + \alpha^۲X^۵ + X^۴ + \alpha X^۳ + ۱$	۱۰	۱۲	۱۰	۸	۱
۳۲	...	۴	۱۰	۱۰	۲	۱
۳۴	$X^{۱۷} + X^{۱۳} + X^{۱۱} + X^{۱۰} + \alpha X^۹ + \alpha X^۸ + X^۷ + X^۶ + X^۴ + ۱$	۱۰	۱۱	۱۰	۹۶	۶
۳۶	(cf.three polynomials above)	۱۱	۱۲	۱۰	۳۶	۳
۳۸	$X^{۱۹} + X^{۱۸} + \alpha X^{۱۷} + \alpha X^{۱۵} + X^{۱۴} + \alpha^۲X^{۱۱} + X^۲X^۸ + X^۵ + \alpha X^۴ + \alpha X^۲ + X + ۱$	۱۱	۱۲	۱۱	۳۶	۲
۴۰	$X^{۲۰} + X^{۱۷} + \alpha^۲X^{۱۵} + \alpha X^{۱۴} + \alpha^۲X^{۱۳} + \alpha^۲X^{۱۲} + X^{۱۱} + X^۹ + \alpha X^۸ + \alpha X^۷ + \alpha^۲X^۶ + \alpha X^۵ + X^۳ + ۱$	۱۲	۱۲	۱۲	۱۶	۱

برهان. فرض کنید c یک کدواژه باشد، آنگاه از لم ۱.۲.۳ ، نتیجه می‌گیریم که برای مولد $g^\perp$، از کد $C^\perp$، به ازای هر $k = \{0, \dots, r-1\}$ داریم:

$$\begin{aligned} 0 &= \langle c(X), X^k g^\perp \rangle \\ &= \sum c_{i+k} \cdot \theta^{i+k}(h_{r-i}) \\ &= \sum c_{i+k} \cdot \theta(\theta^{i+m-1+k}(hr-i)) \\ &= \langle c(X), X^k g^H \rangle_H. \end{aligned}$$

لذا برای اینکه ثابت کنیم دوگان هرمیتی نیز یک θـ کد دوری می‌باشد، باید نشان دهیم که چندجمله‌ای g^H، یک فاکتور راست از $X^{2r}-1$ می‌باشد. فرض می‌کنیم

$$\phi : \mathbb{F}_4[X,\theta] \to \mathbb{F}_4[X,\theta]$$

توسط $\phi(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \theta(a_i)X^i$ تعریف شده باشد. از آنجایی که

$$\phi(Xa) = \phi(\theta(a)X) = \theta^2(a)X = X\theta(a) = \phi(X)\phi(a),$$

ϕ یک مورفیسم است. با توجه به اینکه $g^\perp$، یک مقسوم علیه راست از $X^{2r}-1$ می‌باشد، (نتیجه ۱.۲.۳ رابببینید) داریم:

$$X^{2r}-1 = \phi(X^{2r}-1) = \phi(\tilde{h} \cdot g^\perp) = \phi(\tilde{h}) \cdot \phi(g^\perp)$$

و نتیجه می‌گیریم که، $\phi(g^\perp) = g^H$ می‌باشد. □

روش دیگر بر اساس محاسبات پایه‌های گروبنر می‌باشد. باتوجه به اینکه چندجمله‌ای h از کد خوددوگان هرمیتی روی حلقه $\mathbb{F}_4[X,\theta]$ برابر با

$$h = X^r + \sum_{i=1}^{r-1} (\theta^{r-i+1}(g_0^2)\theta^{r-i+1}(g_{r-i})X^i) + \theta^{r+1}(g_0^2)$$

می‌باشد. رابطه $X^{2r}-1 = g \cdot h$ نیز یک دستگاه چندجمله‌ای از معادلات را تولید می‌کند، که آن را با استفاده از پایه‌های گروبنر حل می‌کنیم.

جدول ۲.۳، بهترین فاصله همینگ از θـ کدهای دوری خوددوگان هرمیتی با طول $n \leq 40$، را ارائه می‌دهد. برای هر n، بهترین فاصله همینگ d را داریم. D_s، بهترین فاصله همینگ شناخته شده برای کدهای خوددوگان هرمیتی با طول n (مرجع [۲۳] را ببینید) و ستون E_d، کلاس کدهای خوددوگان هرمیتی را ارائه می‌دهند که معادل (با جایگشت)، با بهترین فاصله d می‌باشد. هنگامی که $d = D_s$ باشد، مثالی از چندجمله‌ای مولد g، از کدی با چنین فاصله همینگ ارائه می‌شود.

جدول ۲.۳: بهترین فاصله همینگ از θـ کدهای دوری خوددوگان هرمیتی با طول $n \leq ۴۰$

n	g	d	D_s	E_d
۴	$X^۲ + ۱$	۲	۲	۱
۶	$X^۳ + \alpha^۲X^۲ + \alpha X + ۱$	۴	۴	۱
۸	...	۲	۴	۱
۱۰	$X^۵ + X^۴ + \alpha^۲X^۳ + \alpha X^۲ + X + ۱$	۴	۴	۲
۱۲	$X^۶ + X^۵ + \alpha X^۴ + \alpha X^۲ + X + ۱$	۴	۴	۱
۱۴	...	۶	۸	۱
۱۶	...	۲	۸	۱
۱۸	...	۶	۸	۳
۲۰	...	۶	۸	۱
۲۲	$X^{۱۱} + X^۸ + X^۷ + \alpha^۲X^۶ + \alpha X^۵ + X^۴ + X^۳ + ۱$	۸	۸	۲
۲۴	...	۶	۸	۲
۲۶	$X^{۱۳} + X^{۱۰} + X^۸ + \alpha^۲X^۷ + \alpha X^۶ + X^۵ + X^۳ + ۱$	۸	۸-۱۰	۵
۲۸	$X^{۱۴} + X^{۱۱} + X^{۱۰} + X^۹ + \alpha X^۸ + \alpha X^۶ + X^۵ + X^۴ + X^۳ + ۱$	۱۰	۱۰	۲
۳۰	$X^{۱۵} + X^{۱۳} + \alpha^۲X^{۱۲} + \alpha X^{۱۱} + \alpha^۲X^{۱۰} + \alpha X^۸ + \alpha^۲X^۷ + \alpha X^۵ + \alpha^۲X^۴ + \alpha X^۳ + X^۲ + ۱$	۱۲	۱۲	۱
۳۲	...	۲	۱۰-۱۲	۱
۳۴	$X^{۱۷} + X^{۱۳} + X^{۱۱} + X^{۱۰} + \alpha^۲X^۹ + \alpha X^۸ + X^۷ + X^۶ + X^۴ + ۱$	۱۰	۱۰-۱۲	۱۴
۳۶	...	۱۰	۱۲-۱۴	۶
۳۸	$X^{۱۹} + X^{۱۵} + \alpha^۲X^{۱۴} + X^{۱۳} + \alpha X^{۱۱} + \alpha X^{۱۰} + \alpha^۲X^۹ + \alpha^۲X^۸ + X^۶ + \alpha X^۵ + X^۴ + ۱$	۱۲	۱۲-۱۴	۴
۴۰	...	۱۰	۱۲-۱۴	۳

فصل ۴

کدهای دوری اریب روی حلقه‌ی $\mathbb{F}_p + u\mathbb{F}_p$

۱.۴ مقدمات

فرض کنید p یک عدد اول فرد باشد. میدان گالوا[۱] $\mathbb{F}_p$ از مرتبه p و حلقه‌ی

$$R = \mathbb{F}_p + u\mathbb{F}_p = \{a + ub | a, b \in \mathbb{F}_p, u^۲ = ۰\} = \frac{\mathbb{F}_p[u]}{\langle u^۲ \rangle}$$

را در نظر می‌گیریم، و مجموعه یکه‌های $\mathbb{F}_p$ را با $\mathbb{F}_p^* = \mathbb{F}_p - \{۰\}$ نمایش می‌دهیم. فرض کنید θ یک خودریختی از حلقه R با مرتبه $o(\theta) = |\langle\theta\rangle| = e > ۱$ باشد. آنگاه هر عنصر در میدان متناهی $\mathbb{F}_p$ ، تحت θ ثابت است و لذا به ازای هر $a \in \mathbb{F}_p$، $\theta(a) = a$ خواهد بود.

لم بعد عناصر گروه $Aut(R)$ را مشخص می‌کند.

لم ۱.۱.۴. فرض کنید $\theta \in Aut(R)$ و $a + ub \in R$ باشد. آنگاه عنصر $s \in \mathbb{F}_p^*$ وجود دارد به طوری که $\theta(a + ub) = a + usb$ می‌باشد.

برهان. عنصر دلخواه $\theta \in Aut(R)$ را در نظر بگیرید و فرض کنید که $\theta(u) = r + us$ باشد که

[۱] Galois

در آن $r, s \in \mathbb{F}_p$ می‌باشد. در این صورت $u^۲ = ۰$ می‌باشد و در نتیجه داریم:

$$\begin{aligned} ۰ &= \theta(u^۲) = \theta(u)\theta(u) \\ ۰ &= (r+us)(r+us) = r^۲ + ۲urs \\ ۰ &= r^۲. \end{aligned}$$

از این رو $r = ۰$ خواهد بود و وجود دارد $s \in \mathbb{F}_p^*$ به طوری که $\theta(u) = us$ می‌باشد. اگر $a+ub \in R$ باشد، آنگاه

$$\begin{aligned} \theta(a+ub) &= \theta(a) + \theta(u)\theta(b) \\ &= a + usb, \end{aligned}$$

خواهد بود. □

همچنین می‌توانیم با استقراء نشان دهیم که اگر $\theta(a+ub) = a+usb$ باشد، آنگاه برای هر عدد صحیح i داریم:

$$\theta^i(a+ub) = a + us^i b.$$

تعریف ۱.۱.۴. خودریختی θ را روی R در نظر بگیرید. مجموعه‌ی چندجمله‌ای‌های اریب $R[x;\theta]$ را به صورت زیر تعریف می‌کنیم:

$$R[x;\theta] = \{f(x) = a_۰ + a_۱x + \cdots + a_n x^n | a_i \in R, \forall i = ۰, ۱, \ldots, n\}.$$

جمع این چندجمله‌ایی‌ها به صورت معمول و ضرب آن به صورت زیر تعریف می‌شود:

$$(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}.$$

مجموعه تمام چندجمله‌ای‌های فوق با عمل جمع معمولی و ضربی که از این قاعده تبعیت می‌کند، یک حلقه از نوع ناجابه‌جایی تشکیل می‌دهد که حلقه چندجمله‌ای‌های اریب نامیده می‌شود. توجه کنید که اگر $a, b \in \mathbb{F}_p[x]$ باشد، آنگاه $(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}$ خواهد بود. زیرا برای هر $b \in \mathbb{F}_p$ ، $\theta(b) = b$ می‌باشد. بنابراین حلقه‌ی $\mathbb{F}_p[x]$ زیرحلقه‌ای از $R[x;\theta]$ است.

قضیه ۱.۱.۴. (مرجع [۲۸]) (الگوریتم تقسیم) فرض کنید f و g دو چندجمله‌ای در مجموعه‌ی $R[x;\theta]$ باشند و ضریب پیشرو f یکه باشد. آنگاه چندجمله‌ای منحصر به فرد v و q وجود دارند به طوری که: $g = g * f + r$ می‌باشد، که در آن $r = ۰$ یا $\deg(r) < \deg(f)$ است.

قضیه ۲.۱.۴. (مرجع [۲۵]) مرکز حلقه‌ی $R[x;\theta]$، مجموعه‌ی

$$Z(R[x;\theta]) = \mathbb{F}_p[x^e]$$

می‌باشد، که در آن $\theta \in Aut(R)$ از درجه e می‌باشد.

نتیجه زیر به عنوان نتیجه‌ای از قضیه ۲.۱.۴ واضح می‌باشد.

نتیجه ۱.۱.۴. x^n-1 در مرکز حلقه‌ی $R[x;\theta]$ می‌باشد ($x^n-1 \in Z(R[x;\theta])$)، اگر و تنها اگر $e|n$.

نتیجه بالا نشان می‌دهد که چندجمله‌ای (x^n-1) در مرکز $Z(R[x;\theta])$، از حلقه‌ی $R[x;\theta]$ می‌باشد. بنابراین یک ایده‌آل دوطرفه تولید می‌کند اگر و تنها اگر $e|n$. در نتیجه فضای خارج‌قسمتی $R_n = \frac{R[x;\theta]}{\langle x^n-1\rangle}$ یک حلقه است، اگر و تنها اگر $e|n$. در این حالت کدهای دوری اریب می‌توانند به عنوان ایده‌آل‌های (چپ) در R_n در نظر گرفته شوند.

در این فصل از پایان‌نامه به کدهای دوری اریب برای هر طول n، بدون در نظر گرفتن اینکه $e \mid n$ یا $e \nmid n$ علاقه‌مندیم. نشان می‌دهیم که در نظر گرفتن آنها به عنوان مدول‌ها نسبت به ایده‌آل‌ها، برای کار کردن کدهای دوری اریب، از همه‌ی طول‌ها در روشی مشابه، به ما قابلیت انعطاف بیشتری می‌دهد.

فرض کنید $r(x) \in R[x;\theta]$ و $(f(x)+\langle x^n-1\rangle) \in R_n$ باشد. تعریف می‌کنیم:

$$r(x) * (f(x)+\langle x^n-1\rangle) = r(x)f(x)+\langle x^n-1\rangle,$$

که این ضرب با جمع معمولی لم زیر را نتیجه می‌دهد:

لم ۲.۱.۴. فضای خارج قسمتی R_n یک $R[x;\theta]$ـ مدول چپ است.

تعریف ۲.۱.۴. فرض کنید R حلقه‌ی $\mathbb{F}_p + u\mathbb{F}_p$ و θ یک درونریختی از حلقه‌ی R باشد، که در آن $e = |\langle\theta\rangle|$ است. یک زیرمجموعه‌ی C از R^n کد دوری اریب از طول n نامیده می‌شود اگر C در شرایط زیر صدق کند:

۱. C یک زیرمدول از R^n باشد.

۲. اگر $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ باشد، آنگاه شیفت‌های دوری اریب آن نیز چنین است، یا به عبارتی داشته باشیم:

$$(\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

نمایش معمولی از بردارهای $(c_0, c_1, \ldots, c_{n-1}) \in R^n$، توسط چندجمله‌ای‌های $c(x) = c_0 + c_1x + \ldots, c_{n-1}x^{n-1}$ را داریم. با این نمایش، شیفت‌های دوری اریب از یک کدواژه $c(x) = c_0 + c_1x + c_2x^2 + \ldots, c_{n-1}x^{n-1} \in C$ نظیر می‌شود به $x * c(x) \bmod (x^n-1)$ که برابر با

$$\theta(c_{n-1}) + \theta(c_0)x + \cdots + \theta(c_{n-2})x^{n-1}$$

می‌باشد.

همانطور که در بحث کدهای دوری متداول است، برای کدهای دوری اریب نیز می‌توانیم کدواژه‌ها را به عنوان بردارهایی (یا چندجمله‌ای‌هایی) قابل تبدیل به یکدیگر بیان نماییم. این قرارداد را در تعریف بعد و در ادامه پایان‌نامه در نظر می‌گیریم.

تعریف ۳.۱.۴. (تعریف چندجمله‌ای‌هایی از کدهای دوری اریب) یک زیرمجموعه‌ی $C \subseteq R_x$، یک کد دوری اریب نامیده می‌شود، اگر C در شرایط زیر صدق کند:

۱. C یک Rـ زیرمدول از R_n باشد.

۲. اگر $c(x) = (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) \in C$ است، آنگاه

$$x * c(x) = (\theta(a_{n-1}) + \theta(a_0)x + \cdots + \theta(a_{n-2})x^{r-1}) \in C$$

باشد.

به عنوان نتیجه‌ای از تعریف بالا، لم زیر را به دست می‌آوریم:

لم ۳.۱.۴. C یک کد دوری اریب از طول n روی R است، اگر و تنها اگر C یک $R[x;\theta]$ـ زیر مدول از $R_n = \frac{R[x;\theta]}{\langle x^n - 1\rangle}$ باشد.

۲.۴ چندجمله‌ای‌های مولد از کدهای دوری اریب روی R

در این بخش علاقه‌مندیم ساختار جبری کدهای دوری اریب، روی R را مطالعه کنیم. هدف ما پیدا کردن چندجمله‌ای مولد از این کدها به عنوان $R[x;\theta]$ـ زیر مدول چپ از $R_n = \frac{R[x;\theta]}{\langle x^n - 1\rangle}$ می‌باشد. (با استفاده از لم ۳.۱.۴)

لم ۱.۲.۴. برای هر $g(x) \in R[x;\theta]$، یک $g'(x) \in \mathbb{F}_p[x]$ وجود دارد که منحصر به فرد و از درجه‌ی $g(x)$ می‌باشد به طوری که داریم:

$$g(x) * u = ug(x)'.$$

برهان. $g(x) = \sum_{i=0}^{n} g_i x^i \in R[x;\theta]$ را در نظر بگیرید. از آنجا که به ازای هر i، $g_i \in R$ می‌باشد، $g', g'' \in \mathbb{F}_p$ وجود دارند به طوری که $g_i = g_i' + ug_i''$ است. بنابراین $g(x) = \sum(g_i' + ug_i'')x^i$ می‌باشد. از لم ۱.۱.۴، نتیجه می‌گیریم $us^i = \theta^i(u)$. از این رو داریم:

$$\begin{aligned} g(x) * u &= (\sum(g_i' + ug_i'')x^i) * u = (\sum g_i' x^i) * u + (\sum ug_i'' x^i) * u \\ &= \sum g_i' \theta^i(u)x^i + \sum ug_i'' \theta^i(u)x^i = \sum g_i' us^i x^i + \sum ug_i'' us^i x^i. \end{aligned}$$

به وضوح جمع دوم صفر است (شامل فاکتور از u^2 است)، بنابراین داریم:

$$g(x) * u = \sum g_i' us^i x^i = u \sum g_i' s^i x^i = ug'(x).$$

در این اثبات، یکتایی g' در $\mathbb{F}_p[x]$ واضح است. □

نمادگذاری: برای عنصر $g \in \mathbb{F}_p[x]$، عنصر $g' \in \mathbb{F}_p[x]$ (در لم ۱.۲.۴) منحصر به فرد است. بنابراین آن را شریک g می‌نامیم. توجه کنید که اگر $g = g_1 + ug_2 \in R[x;\theta]$ باشد، آنگاه $ug = u(g_1 + ug_2) = ug_1 = g'u$ خواهد بود.

مثال ۱.۲.۴. اگر $g(x) = 1 + x + x^2 \in (\mathbb{F}_p + u\mathbb{F}_p)[x;\theta]$ باشد، که در آن برای $s \in \mathbb{F}_p$، داریم:

$$\theta(a + ub) = a + sub,$$

آنگاه

$$\begin{aligned} g(x) * u &= (1 + x + x^2) * u = u + x * u + x^2 * u \\ &= u + \theta(u)x + \theta^2(u)x^2 = u + sux + s^2ux^2 \end{aligned}$$

خواهد بود. بنابراین $g(x)u = u(1 + sx + s^2x^2)$ است. لذا $g' = s^2x^2 + sx + 1$ می‌باشد.

توجه کنید که تعداد نامتناهی عنصر $h \in R$ وجود دارد، به طوری که $gu = uh$ می‌باشد و این برای تعریف $h = g' + ul$ به ازای هر $l \in \mathbb{F}_p[x]$ کافی است.

لم ۲.۲.۴. چندجمله‌ای $x^n - 1$، فاکتورهایی در حلقه‌ی $\mathbb{F}_p[x]$، به فرم $x^n - 1 = f_1(x)g_1(x)$ دارد، اگر و تنها اگر در حلقه‌ی $R[x;\theta]$، داشته باشیم

$$x^n - 1 = f(x) * g(x),$$

که در آن $f_2(x), g_2(x) \in \mathbb{F}_p[x]$ وجود دارند، به طوری که

$$f(x) = f_1(x) + uf_2(x)$$

و

$$g(x) = g_1(x) + ug_2(x)$$

می‌باشد.

برهان. فرض کنید در حلقه‌ی $\mathbb{F}_p[x]$، $x^n - 1 = f_1(x)g_1(x)$ باشد. از آنجا که $\mathbb{F}_p[x]$ یک زیرحلقه از $R[x;\theta]$ می‌باشد، بنابراین در حلقه‌ی $R[x;\theta]$، $x^n - 1 = f_1(x)g_1(x)$ خواهد بود. از این رو خواهیم داشت

$$f_2(x) = g_2(x) = 0.$$

برعکس فرض کنید در حلقه‌ی $R[x;\theta]$، $x^n - 1 = f(x) * g(x)$ باشد و $f(x), g(x) \in \mathbb{F}_p[x]$ وجود داشته باشند، به طوری که

$$f(x) = f_1(x) + uf_2(x), g(x) = g_1(x) + ug_2(x),$$

برقرار باشد. در این صورت خواهیم داشت:

$$\begin{aligned} x^n - ۱ &= f(x) * g(x) \\ &= (f_۱(x) + uf_۲(x)) * (g_۱(x) + ug_۲(x)) \\ &= f_۱(x)g_۱(x) + f_۱(x) * ug_۲(x) + uf_۲(x)g_۱(x). \end{aligned}$$

با توجه به لم ؟؟، $k(x) \in \mathbb{F}_p[x]$ وجود دارد، به طوری که $f_۱(x)u = uk(x)$ می‌باشد. بنابراین داریم:

$$\begin{aligned} x^n - ۱ &= f(x) * g(x) \\ &= f_۱(x)g_۱(x) + f_۱(x) * ug_۲(x) + uf_۲(x)g_۱(x) \\ &= f_۱(x)g_۱(x) + uk(x)g_۲(x) + uf_۲(x)g_۱(x) \\ &= f_۱(x)g_۱(x) + u(k(x)g_۲(x) + f_۲(x)g_۱(x)). \end{aligned}$$

فرض کنید در حلقه‌ی $\mathbb{F}_p[x]$، $x^n - ۱ = f_۱(x)g_۱(x) + r_۱(x)$ باشد. چون $\mathbb{F}_p[x]$ یک زیرحلقه از $R[x;\theta]$ است، بنابراین در این حلقه $x^n - ۱ = f_۱(x)g_۱(x) + r_۱(x)$ خواهد بود. از این رو داریم:

$$\begin{aligned} x^n - ۱ &= f_۱(x)g_۱(x) + u(k(x)g_۲(x) + f_۲(x)g_۱(x)) \\ &= x^n - ۱ - r_۱(x) + u(k(x)g_۲(x) + f_۲(x)g_۱(x)), \end{aligned}$$

و

$$r_۱(x) = u(k(x)g_۲(x) + f_۲(x)g_۱(x)).$$

اما $r_۱(x) \in \mathbb{F}_p[x]$ می‌باشد که این یک تناقض است، مگر اینکه در حلقه‌ی $\mathbb{F}_p[x]$، $r_۱(x) = ۰$ و $x^n - ۱ = f_۱(x)g_۱(x)$ باشد. □

توجه کنید که در لم ۲.۲.۴، $f_۱(x)$ و $g_۱(x)$ چندجمله‌ای‌های منحصربه‌فرد هستند، زیرا حلقه $\mathbb{F}_p[x]$ یک حلقه‌ی خارج‌قسمتی منحصربه‌فرد است. بنابراین $f_۲(x)$ و $g_۲(x)$ منحصربه‌فرد نیستند، زیرا حلقه‌ی $R[x;\theta]$ یک حلقه‌ی تقسیم منحصربه‌فرد نیست. می‌دانیم:

$$U(R) = \mathbb{F}_p^* + u\mathbb{F}_p,$$

لذا $U(R[x;\theta])$ را به دست می‌آوریم.

لم ۳.۲.۴. $U(R[x;\theta]) = \{a + uh(x) | a \in \mathbb{F}_p^*, h(x) \in \mathbb{F}_p[x]\}$ می‌باشد.

برهان. فرض کنید $a + uh(x) \in R[x;\theta]$ باشد، که در آن $a \in \mathbb{F}_p^*$ و $h(x) \in \mathbb{F}_p[x]$ می‌باشد. در این صورت داریم:

$$\begin{aligned} (a + uh) * (a^{-۱} - a^{-۱}uha^{-۱}) &= ۱ - uha^{-۱} + uha^{-۱} - uh * a^{-۱}uha^{-۱} \\ &= ۱ - uh * a^{-۱}uha^{-۱} = ۱ - u^۲h_۱a^{-۱}ha^{-۱} \\ &= ۱. \end{aligned}$$

از این رو $a+uh(x)\in U(R[x;\theta])$ خواهد بود.

برعکس، فرض کنید $f\in U(R[x;\theta])$ باشد. آنگاه $g\in U(R[x;\theta])$ وجود دارد، به طوری که $f*g=g*f=1$ است. همچنین فرض کنید که برای $f_i,g_i\in\mathbb{F}_p[x]$، $f=f_1+uf_2$ و $g=g_1+ug_2$ باشد. در این صورت، $f*g=(f_1+uf_2)*(g_1+ug_2)=1$ بوده و این دلالت دارد بر این که: $f_1g_1=1$ و $uf_2g_1+f_1ug_2=0$ است. از این رو $f_1\in\mathbb{F}_p^*$ یک چندجمله‌ای ثابت مخالف صفر می‌باشد. بدین ترتیب $f=f_1+uf_2$ بوده، که در آن $f_1\in\mathbb{F}_p^*$ و $f_2\in\mathbb{F}_p[x]$ می‌باشد. □

فرض کنید C یک کد دوری اریب مخالف صفر روی R و

$$c(x)=(a_0+a_1x+\cdots+a_{n-1}x^{n-1})\in C$$

باشد. اگر a_{n-1} یک عنصر یکه (وارون‌پذیر) در R با وارون w باشد، آنگاه $wc(x)$ یک چندجمله‌ای تکین در C می‌باشد. از این رو برای هر کد دوری اریب موارد زیر را در نظر می‌گیریم:

۱. C چندجمله‌ای تکین نداشته باشد.

۲. C حداقل یک چندجمله‌ای تکین داشته باشد.

لم بعد همه‌ی کدهای دوری اریب که از حالت ۱ پیروی می‌کنند را طبقه‌بندی می‌کند.

لم ۴.۲.۴. فرض کنید C یک کد دوری اریب غیر صفر باشد که چندجمله‌ای‌های تکین ندارد. آنگاه $C=\langle u\overline{a(x)}\rangle$ خواهد بود، که در آن $\overline{a(x)}$ یک چندجمله‌ای از مینیمم درجه در C است و $x^n-1=\overline{b(x)}\,\overline{a(x)}\in\mathbb{F}_p[x]$ می‌باشد.

برهان. فرض کنید که

$$\theta(a+ub)=a+usb,$$

که در آن $s\in\mathbb{F}_p^*$ است. فرض کنید $a(x)=a_0+a_1x+\cdots+u\overline{a_r}x^r$ یک چندجمله‌ای از درجه مینیمم در کد C است، که در آن به ازای هر $i=0,1,\ldots,r-1$ داریم: $a_i\in R$ و $\overline{a_r}\in\mathbb{F}_p^*$. توجه داریم که

$$ua(x)=ua_0+ua_1x+\cdots+ua_{r-1}x^{r-1}\in C.$$

چون $a(x)$ در C از درجه مینیمم است، لذا $ua(x)=0$ و $a(x)=u\overline{a(x)}$ می‌باشد، که در آن $\overline{a(x)}\in\mathbb{F}_p[x]$، به طوری که: $a_i=u\overline{a_i}$ برای هر $i=0,1,\ldots,r$.

اگر $c(x)$ را یک کدواژه در کد C در نظر بگیرید، آنگاه $c(x)$ تکین نمی‌باشد، بنابراین

$$c(x)=c_0+c_1x+\cdots+u\overline{c_t}x^t,$$

که در آن به ازای $i=0,1,\ldots,t-1$ داریم: $t\leq n-1$، $\overline{c_t}\in\mathbb{F}_p^*$ و $c_i\in R$. ثابت کنیم: $c(x)=u\overline{c(x)}$. قرار می‌دهیم:

$$c(x)=c_1(x)+c_2(x),$$

جایی که تمام عبارت‌های موجود در $c_1(x)$، توانی کمتر از r دارند و تمام عبارت‌های در $c_2(x)$، دارای توانی بیشتر یا مساوی با r هستند.(r منحصربه‌فرد است.)

به برهان خلف فرض کنید c_{t-1} یک واحد است. توجه کنید که $\theta^i(u) = us^i$ می باشد. چندجمله‌ای $Z(x) = z_1(x) - z_2(x) \in C$ را در نظر بگیرید، که در آن داریم:

$$\begin{aligned} z_1(x) &= (s^t - r)^{-1}(\overline{a_r})^{-1}x^{t-r}a(x) \\ &= (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_0}\theta^{t-r}(u)x^{t-r} + (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_1}\theta^{t-r}(u)x^{t-r+1} + \\ &\cdots + (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_{r-1}}\theta^{t-r}(u)x^{t-r} + (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_r}\theta^{t-r}(u)x^t \\ &= (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_0}\theta^{t-r}(u)x^{t-r} + (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_1}\theta^{t-r}(u)x^{t-r+1} + \\ &\cdots + (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_{r-1}}\theta^{t-r}(u)x^{t-1} + ux^t, \end{aligned}$$

و همچنین

$$z_2(x) = (c_t)^{-1}c(x) = (c_t)^{-1}c_0 + (c_t)^{-1}c_1x + \cdots + (c_t)^{-1}c_{t-1}x^{t-1} + ux^t$$

می‌باشد. از این رو $Z(x) = z_1(x) - z_2(x)$ یک چندجمله‌ای از درجه $t-1$ در کد C بوده، که در آن ضریب x^{t-1} برابر با:

$$z_{t-1} = (s^t - r)^{-1}(\overline{a_r})^{-1}\overline{a_{r-1}}\theta^{t-r}(u) - (c_t)^{-1}c_{t-1} = \eta u - (c_t)^{-1}c_{t-1}$$

می‌باشد، که در آن $(c_t)^{-1}c_{t-1}$، یک عنصر یکه (وارون‌پذیر) است. با توجه به لم ۳.۲.۴، z_{t-1} یک واحد می‌باشد. بنابراین کد C یک چندجمله‌ای تکین دارد و این تناقض است، زیرا C چندجمله‌ای‌های تکین ندارد.

با روشی مشابه می‌توانیم نشان دهیم که به ازای هر $c_i \in c_2(x)$، c_i یک واحد نیست. فرض کنید که $i \in c_1(x)$ وجود داشته باشد که c_i یک عنصر یکه باشد، آنگاه $uc(x) = uc_1(x) \in C$ و $uc_1(x)$ چندجمله‌ای مخالف صفر با درجه کوچکتر از درجه $a(x)$ می‌باشد که تناقض است. از این رو $c(x) = u\overline{c(x)}$ بوده، که در آن $\overline{c(x)} \in \mathbb{F}_p[x]$ و برای هر $i = 0, 1, \ldots, t$، $c_i = u\overline{c_i}$ می‌باشد. بنابراین $\overline{a(x)}$ و $\overline{c(x)}$، دوچندجمله‌ای در $\mathbb{F}_p[x]$ هستند. با استفاده از الگوریتم تقسیم، چندجمله‌ای‌های $q(x)$ و $r(x)$ وجود دارند، به طوری که:

$$\overline{c(x)} = q(x)\overline{a(x)} + r(x)$$

می‌باشد، که در آن $r(x) = 0$ و یا $\deg r(x) < \deg \overline{a(x)} = \deg a(x)$ است. لذا با استفاده از لم ۱.۲.۴، داریم:

$$\begin{aligned} u\overline{c(x)} &= uq(x)\overline{a(x)} + ur(x) \\ &= q'(x)u\overline{a(x)} + ur(x). \end{aligned}$$

رابطه بالا دلالت دارد بر اینکه

$$ur(x) = u\overline{c(x)} - q'(x)u\overline{a(x)} \in C$$

می‌باشد. این تناقض می‌باشد، زیرا $\deg ur(x) < \deg \overline{a(x)} = \deg a(x)$ است. بنابراین $ur(x) = ۰$ می‌باشد. چون $r(x) \in \mathbb{F}_p[x]$ است، لذا داریم:

$$r(x) = ۰$$

و

$$u\overline{c(x)} = q'(x)u\overline{a(x)}.$$

از این رو $C = \langle u\overline{a(x)} \rangle$ است. همچنین چون $\overline{a(x)}$ و $x^n - ۱$ چندجمله‌ای‌هایی در $\mathbb{F}_p[x]$ می‌باشند، با استفاده از الگوریتم تقسیم، چندجمله‌ای‌های $\overline{b(x)}$ و $r_۱(x)$ در $\mathbb{F}_p[x]$ وجود دارند، به طوری که داریم:

$$x^n - ۱ = \overline{b(x)}\,\overline{a(x)} + r_۱(x),$$

که در آن $r_۱(x) = ۰$ یا $\deg r_۱(x) < \deg \overline{a(x)} = \deg a(x)$ است. از این رو داریم:

$$\begin{aligned} u(x^n - ۱) &= u\overline{b(x)}\,\overline{a(x)} + ur_۱(x) \\ &= q'_۱(x)u\overline{a(x)} + ur_۱(x). \end{aligned}$$

در حلقه‌ی $R_n = \frac{R[x;\theta]}{\langle x^n - ۱ \rangle}$، داریم:

$$۰ = q'_۱(x)u\overline{a(x)} + ur_۱(x)$$

و یا

$$ur_۱(x) = -q'_۱(x)u\overline{a(x)} \in C,$$

که یک تناقض می‌باشد. بنابراین $ur_۱(x) = ۰$ می‌باشد، زیرا $r_۱(x) \in \mathbb{F}_p[x]$ و $r_۱(x) = ۰$ و $x^n - ۱ = \overline{b(x)}\,\overline{a(x)}$ است. □

لم ۵.۲.۴. فرض کنید C یک کد دوری اریب باشد که حداقل یک چندجمله‌ای تکین دارد و $g(x)$ را یک چندجمله‌ای در کد C، با مینیمم درجه در نظر بگیرید. همچنین فرض کنید که $g(x)$ تکین باشد، آنگاه $C = \langle g(x) \rangle$ خواهد بود، که در آن $x^n - ۱ = k(x)g(x)R_n$ می‌باشد.

برهان. با استفاده از قضیه ۱.۱.۴ به سادگی می‌توان لم را ثابت کرد. □

لم ۶.۲.۴. فرض کنید C یک کد دوری اریب مخالف صفر باشد که حداقل یک چندجمله‌ای تکین دارد. همچنین فرض کنید که همه‌ی چندجمله‌ای‌ها با مینیمم درجه، مونیک نباشند. اگر $a(x)$ را یک چندجمله‌ای با مینیمم درجه در C و $g(x)$ را یک چندجمله‌ای تکین با مینیمم درجه در میان تمام چندجمله‌ای‌های تکین در C در نظر بگیریم، آنگاه خواهیم داشت:

$$C = \langle g(x) + up(x), a(x)\rangle = \langle g(x) + up(x), u\overline{a(x)}\rangle$$

که در آن $x^n - ۱ = k(x) * g(x) \in R[x;\theta]$ و $x^n - ۱ = \overline{b(x)}\,\overline{a(x)} \in \mathbb{F}_p[x]$ می‌باشند و همچنین درجه $a(x)$ کوچکتر از درجه $g(x)$ خواهد بود.

برهان. فرض کنید C یک کد دوری اریب باشد. که حداقل یک چندجمله‌ای تکین دارد و $a(x)$ را یک چندجمله‌ای در کد C، با مینیمم درجه در نظر بگیرید. چون $a(x)$ تکین نیست و دارای مینیمم درجه در C است، طبق اثبات لم ۱۰، $a(x) = u\overline{a(x)}$ است که در آن $\overline{a(x)} \in \mathbb{F}_p[x]$ می‌باشد.

حال فرض کنیم که $c(x)$ یک کدواژه در کد C، و $f(x)$ یک چندجمله‌ای تکین با مینیمم درجه در کد C باشد، آنگاه با توجه به قضیه ۲ دو چندجمله‌ای $q_۲(x)$ و $r_۲(x)$ در R_n وجود دارند به طوری که داریم:

$$c(x) = q_۲(x) * f(x) + r_۲(x)$$

که در آن $r_۲(x) = ۰$ و یا درجه $r_۲(x)$ کوچکتر از درجه $f(x)$ می‌باشد. لذا

$$r_۲(x) = c(x) - q_۲(x) * f(x) \in C$$

خواهد بود. چون $f(x)$ یک چندجمله‌ای تکین در کد C، از حداقل درجه می‌باشد، لذا $r_۲(x)$ تکین نیست. در حقیقت طبق اثبات لم ۱۰، به راحتی می‌توان نشان داد که $r_۳(x)$ در $\mathbb{F}_p[x]$ موجود است به طوری که $r_۲(x) = ur_۳(x)$ می‌باشد. اکنون الگوریتم تقسیم را بر روی $a(x)$ و $r_۳(x)$، برای به دست آوردن

$$r_۳(x) = q_۳(x)\overline{a(x)} + r_۴(x)$$

اعمال می‌کنیم. که در آن $r_۴(x) = ۰$ و یا درجه $r_۴(x)$ کوچکتر از درجه $\overline{a(x)}$ می‌باشد. از این رو داریم:

$$\begin{aligned} r_۲(x) = ur_۳(x) &= uq_۳(x)\overline{a(x)} + ur_۴(x) \\ &= q_۴u\overline{a(x)} + ur_۴(x). \end{aligned}$$

بدین ترتیب $ur_۴(x) \in C$ است. چون $\deg r_۴(x) < \deg \bar{a(x)} = \deg a(x)$ می‌باشد، لذا $ur_۴(x) = ۰$ است. از آنجا که $r_۴(x) \in \mathbb{F}_p[x]$ است، داریم:

$$r_۴(x) = ۰$$

و

$$r_۲(x) = ur_۳(x) = uq_۳(x)\bar{a(x)} = q_۴u\bar{a(x)}.$$

بنابراین

$$\begin{aligned} c(x) &= q_۲(x)f(x) + r_۲(x) \\ &= q_۲(x)f(x) + q_۴\overline{ua(x)} \end{aligned}$$

می‌باشد. بدین ترتیب $C = \langle f, a(x)\rangle = \langle f, \overline{ua(x)}\rangle$ می‌باشد. توجه کنید که $x^n - ۱$ و $\overline{a(x)}$ چندجمله‌ای‌هایی در $\mathbb{F}_p[x]$ می‌باشند. لذا با استفاده از الگوریتم تقسیم می‌توانیم قرار دهیم:

$$x^n - ۱ = q_۵\overline{a(x)} + r_۵.$$

که در آن $r_۵(x) = ۰$ و یا $r_۵(x)$ یک چندجمله‌ای در $\mathbb{F}_p[x]$ با درجه کوچکتر از درجه $\overline{a(x)}$ است. از این رو خواهیم داشت:

$$\begin{aligned} u(x^n - ۱) &= uq_۵\overline{a(x)} + ur_۵ \\ &= q'_۵\overline{ua(x)} + ur_۵. \end{aligned}$$

در R_n به دست می‌آوریم:

$$ur_۵(x) = -q'_۵\overline{ua(x)} \in C$$

که $\deg ur_۵(x) = \deg r_۵(x) < \deg \overline{a(x)}$ است، و این تناقض می‌باشد مگر اینکه $ur_۵(x) = ۰$ باشد. چون $r_۵(x) \in \mathbb{F}_p[x]$ است، پس داریم: $r_۵(x) = ۰$ و $x^n - ۱ = q_۵\overline{a(x)}$. به علاوه فرض کنید $f(x) = f_۱(x) + uf_۲(x)$ باشد که در آن $f_۱(x), f_۲(x) \in \mathbb{F}_p[x]$ هستند، آنگاه با استفاده از قضیه ۱.۱.۴، خواهیم داشت:

$$x^n - ۱ = q_۳(x)(f_۱(x) + uf_۲(x)) + R(x),$$

که در آن $R(x) = ۰$ یا $\deg R(x) < \deg f(x) = \deg f_۱(x)$ می‌باشد که دلالت دارد بر اینکه $R(x) \in C$. با توجه به اینکه $f(x)$ یک چندجمله‌ای تکین با مینیمم درجه در کد C است، نتیجه می‌گیریم که $R(x)$ تکین نیست. باتوجه به لم ۱.۲.۴ داریم: $R(x) = w(x)\overline{ua(x)} = uw_۱(x)\overline{a(x)}$. بدین ترتیب داریم:

$$\begin{aligned} x^n - ۱ &= q_۳(x)(f_۱(x) + uf_۲(x)) + uw_۱(x)\overline{a(x)} \\ &= q_۳(x)f_۱(x) + q_۳(x)uf_۲(x) + uw_۱(x)\overline{a(x)} \\ &= q_۳(x)f_۱(x) + uq_۴(x)f_۲(x) + uw_۱(x)\overline{a(x)}. \end{aligned}$$

بنابراین در حلقه‌ی $\mathbb{F}_p[x]$، داریم:

$$x^n - ۱ = q_۳(x)f_۱(x).$$

با توجه به لم ۲.۲.۴، باید یک چندجمله‌ای $g(x)$ در $R[x;\theta]$ از درجه $f_۱(x)$ وجود داشته باشد، به طوری که $g(x)$ یک مقسوم‌علیه راست از $x^n - ۱$ در $R[x;\theta]$ باشد. پس

$$g(x) = f_۱(x) + ul_۱(x)$$

خواهد بود که در آن $l_۱(x)$ یک چندجمله‌ای در $\mathbb{F}_p[x]$ از درجه کمتر از درجه‌ی $f_۱(x)$ می‌باشد. بدین ترتیب خواهیم داشت:

$$\begin{aligned} f(x) &= f_۱(x) + uf_۲(x) \\ &= g(x) - ul_۱(x) + uf_۲(x) \\ &= g(x) + u(f_۲(x) - l_۱(x)). \end{aligned}$$

بنابراین

$$C = \langle f, a(x)\rangle = \langle f, u\overline{a(x)}\rangle = \langle g(x) + u(f_۲(x) - l_۱(x)), u\overline{a(x)}\rangle$$

بوده، همچنین $x^n - ۱ = k(x)g(x) \in R[x;\theta]$، $x^n - ۱ = \overline{b(x)}\,\overline{a(x)} \in \mathbb{F}_p[x]$ و $\deg \overline{a(x)} < \deg g(x)$ می‌باشند. □

لم ۷.۲.۴. فرض کنید $C = \langle g(x) + up(x), a(x)\rangle = \langle g(x) + up(x), u\overline{a(x)}\rangle$ باشد، آنگاه داریم: $\overline{a(x)} | g(x) \mod u$ و $\frac{x^n-۱}{g} up \in \langle ua\rangle$.

برهان. فرض کنید $C = \langle g(x) + up(x), a(x)\rangle = \langle g(x) + up(x), u\overline{a(x)}\rangle$ باشد. همچنین فرض کنید که $uc(x) \in C$ بوده که در آن $c(x) \in \mathbb{F}_p[x]$ می‌باشد. با توجه به الگوریتم تقسیم می‌توانیم بنویسیم:

$$c(x) = q(x)\overline{a(x)} + r(x),$$

جایی که $r(x) = ۰$ و یا درجه $r(x)$ کوچکتر از درجه $\overline{a(x)}$ است. از این رو خواهیم داشت:

$$\begin{aligned} uc(x) &= uq(x)\overline{a(x)} + ur(x) \\ &= q'(x)u\overline{a(x)} + ur(x). \end{aligned}$$

عبارت بالا دلالت دارد بر این که $ur(x) \in C$ است. این یک تناقض می‌باشد، زیرا

$$\deg ur(x) = \deg r(x) < \deg a(x) = \ deg\overline{a(x)}.$$

بنابراین $ur(x) = 0$ و $r(x) = 0$ است، چون $r(x) \in \mathbb{F}_p[x]$ می‌باشد. لذا

$$uc(x) = uq(x)\overline{a(x)} = q'(x)u\overline{a(x)} \in \langle ua \rangle$$

است. از این رو برای هر چندجمله‌ای به فرم $uc(x) \in C$، داریم: $c(x) = q(x\overline{a(x)})$ و $uc(x) \in \langle ua \rangle$. چون $u(g(x) + up(x)) = ug(x) \in C$ می‌باشد، خواهیم داشت:

$$\overline{a(x)}|g(x) \mod u.$$

همچنین داریم:

$$\frac{x^n - 1}{g}(g(x) + up(x)) = \frac{x^n - 1}{g}up(x) = u(\frac{x^n - 1}{g})p(x) \in C,$$

از این رو $\frac{x^n-1}{g}up \in \langle ua \rangle$ می‌باشد. □

قضیه ۱.۲.۴. اگر فرض کنیم C یک کد دوری اریب مخالف صفر روی حلقه‌ی R باشد، آنگاه C از یکی از حالت‌های زیر پیروی می‌کند:

۱. C چندجمله‌ای‌های تکین ندارد. پس $C = \langle u\overline{a(x)} \rangle$ است، جایی که $\overline{a(x)}$ یک چندجمله‌ای در C با مینیمم درجه و $x^n - 1 = \overline{b(x)}\,\overline{a(x)} \in \mathbb{F}_p[x]$ می‌باشد.

۲. C یک چندجمله‌ای تکین $g(x)$ از مینیمم درجه در C دارد. پس $C = \langle g(x) \rangle$ است، که در آن $g(x)$ یک چندجمله‌ای با مینیمم درجه در C بوده و $x^n - 1 = k(x) * g(x) \in R_n$ می‌باشد.

۳. همه‌ی چندجمله‌ای‌های تکین در کد C دارای مینیمم درجه نمی‌باشند، پس خواهیم داشت:

$$C = \langle g(x) + up(x), a(x) \rangle = \langle g(x) + up(x), u\overline{a(x)} \rangle,$$

که در آن $a(x)$ یک چندجمله‌ای با مینیمم درجه در C است که تکین نمی‌باشد و $g(x)$ یک چندجمله‌ای تکین با مینیمم درجه در میان همه‌ی چندجمله‌ای‌های تکین در C می‌باشد. همچنین داریم:

$$x^n - 1 = k(x) * g(x) in R[x; \theta],$$

$$x^n - 1 = \overline{b(x)}\,\overline{a(x)} \in \mathbb{F}_p[x],$$

$$\overline{a(x)}|g(x) \mod u,$$

و

$$\frac{x^n - 1}{g}up \in \langle ua \rangle.$$

برهان. اثبات از لم‌های ۴.۲.۴، ۵.۲.۴، ۶.۲.۴ و ۷.۲.۴ حاصل می‌شود. □

مراجع

[۱] ع محمدی حسن‌آبادی، (۱۳۸۴)، *"جبر"* جلد اول، چاپ پنجم، انتشارات دانشگاه اصفهان، ۵۸۶ صفحه.

[۲] سان لینگ و چائو بینگ شینگ (مترجمان: حسام‌الدین شریفی و کبری علی محمدی)، (۱۳۹۳)، *"درآمدی بر نظریه کدگذاری"* جلد اول، چاپ اول، انتشارات دانشگاه شاهد تهران، ۲۸۷ صفحه.

[3] T. Abualrub, A. Ghrayeb, N. Aydin and I. Siap, On the construction of skew quasi-cyclic codes, *IEEE Trans. Inform. Theory*, 56(5) (2010), 2081–2090.

[4] T. Abualrub and I. Siap, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.*, 42(3) (2007), 273–287.

[5] T. Abualrub, I. Siap and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, *IEEE Trans. Inform. Theory*, 60(3) (2014), 1508–1514.

[6] A. Berrick and M. Keating, *An Introduction to Rings and Modules*, 65, Cambridge University Press, (2000).

[7] M. Bhaintwal, Skew quasi-cyclic codes over Galois rings, *Des. Codes Cryptogr.*, 62(1) (2012), 85–101.

[8] A. Bonnecaze and U. Parampalli, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, 45(4) (1999), 1250–1255.

[9] W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language, *J. Symbol. Comput.*, 24 (1997), 235-265.

[10] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes, *Appl. Algebra Eng. Commun. Comput.*, 18(4) (2007), 379-389.

[11] D. Boucher, P. Sole and F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, 2 (2008), 273–292.

[12] D. Boucher and F. Ulmer, A note on the dual codes of module skew codes, *Cryptogr. and coding, Springer Berlin Heidelberg*, (2011), 230–243.

[13] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.*, 44(12) (2009), 1644-1656.

[14] M. Bronstein and M. Petkovsek, On Ore Rings, Linear operators and factorisation, *Program. Comput. Soft.*, 20 (1994), 14-18.

[15] R. Dastbasteh, H. Mousavi, T. Abualrub, N. Aydin and J. Haghighat, skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *Int. J. of Information, and Coding Theory*, In Press.

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

[17] A. Casavola, D. Famularo and G. Franze, A feedback min-max MPC algorithm for LPV systems subject to bounded rates of change of parameters, *IEEE Trans. Aut. Control*, 47(7) (2002), 1147–1153.

[18] E. Chen, [online] Online Database of Quasi-Twisted Codes (Accessed 12 December 2017) http://www.tec.hkr.se/∼ chen/research/codes/searchqc2.htm

[19] P. Cohn, *Free Rings and their Relations*, Academic Press Inc, 1 (1971).

[20] Code Tables: Bounds on the parameters of various types of codes. [online] http : //www.codetables.de (Accessed 12 December 2017).

[21] B. Delphine, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *Appl. Alg. Eng. Commun. Comput.*, 18(4) (2007), 379–389.

[22] E. Gabidulin, Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii*, 21 (1985), 1-12.

[23] P. Gaborit and A. Otmani, Tables of Euclidian and Hermitian self-dual codes over GF(4), (2002). http://www.unilim.fr/pages-perso/ philippe.gaborit/SD/.

[24] N. Jacobson, *The Theory of Rings*, Publication of the AMS, 1 (1943), 155.

[25] G. Jian, Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *J. Appl. Math. Inform.*, 31(3-4) (2013), 337–342.

[26] P. Kanwar and S. R. Lopez-Permouth, Cyclic codes over the integers modulo pm, *Finite Fields Appl.*, 3(4) (1997), 334–352.

[27] D. Mandelbaum, An application of cyclic coding to message identification, *IEEE Trans. Commun. Tech.*, 17(1) (1969), 42–48.

[28] B. McDonald, *Finite Rings with Identity*, Marcel Dekker Inc, 1 (1974).

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

[30] V. S. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, 42(7) (1996), 1594–1600.

[31] M. Singer, Testing reducibility of linear differential operators: A group theoretic perspective, *Appl. Alg. Eng. Commun. Comput.*, 7 (1996), 77-104.

[32] K. Tokiwa, M. Kasahara and T. Namekawa, Burst-error-correction capability of cyclic codes, *Electronics Commun. in Japan (Part I: Commun.6s)*, 66(11) (1983), 60–66.

[33] J. Wolfmann, Binary images of cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, 4(5) (2001), 1773–1779.

واژه‌نامه فارسی به انگلیسی

الگوریتم اقلیدسی . . . . . Euclidean algorithm
الگوریتم تقسیم . . . . . Division algorithm
ایده‌آل . . . . . Ideal
ایده‌آل اصلی . . . . . Principal ideal
ایده‌آل چپ . . . . . Left ideal
ایده‌آل دوطرفه . . . . . Two-sided ideal
بزرگترین مقسوم‌علیه مشترک . . . . . Greatest common divisor
پایه گروبنر . . . . . Groebner basis
تجزیه . . . . . Factorization
تحویل‌ناپذیر . . . . . Irreducible
چندجمله‌ای . . . . . Polynomial
چندجمله‌ای تکین . . . . . Monic polynomial
چندجمله‌ای مولد . . . . . Generating polynomial
حاصلضرب اقلیدسی . . . . . Euclidean product
حلقه . . . . . Ring
حلقه اقلیدسی . . . . . Euclidean ring
حلقه تقسیم . . . . . Factorization ring
حلقه چندجمله‌ای‌های اریب . . . . . Skew polynomial ring
حلقه خارج‌قسمتی . . . . . Quotient ring
حلقه ناجابه‌جایی . . . . . Non-commutative ring
خودریختی . . . . . Automorphism
خودریختی فروبنیوس . . . . . Frobenius automorphism
درجه . . . . . Degree
زیرفضای برداری . . . . . Vector subspace
زیرمدول . . . . . Submodule
ضریب پیشرو . . . . . Leading coefficient

فاصله همینگ . . . . . Hamming distance
فضای برداری . . . . . Vector space
کد . . . . . Code
کد خطی . . . . . Linear code
کد خوددوگان اقلیدسی . . . . . Euclidean self dual code
کدخوددوگان هرمیتی . . . . . Hermitian self dual code
کد دوری . . . . . Cyclic code
کد دوگان . . . . . Dual code
کدواژه . . . . . Code word
کران . . . . . Bound
کوچکترین مضرب مشترک . . . . . Lowest common multiple
ماتریس کنترل توازن . . . . . Parity check matrix
ماتریس مولد . . . . . Generator matrix
مدول . . . . . Module
مرتبه . . . . . Order
مرکز حلقه . . . . . Center of ring
مقسوم‌علیه راست . . . . . Right divisor
مقسوم‌علیه صفر . . . . . Zero divisor
مولد . . . . . Generator
میدان . . . . . Field
میدان متناهی . . . . . Finite field
مینیمم درجه . . . . . Minimal degree
یکریختی . . . . . Isomorphism

واژه‌نامه انگلیسی به فارسی

خودریختی ..... Automorphism
کران ..... Bound
مرکز حلقه ..... Center of ring
کد ..... Code
کد واژه ..... Code word
کد دوری ..... Cyclic code
درجه ..... Degree
الگوریتم تقسیم ..... Division algorithm
کد دوگان ..... Dual code
الگوریتم اقلیدسی ..... Euclidean algorithm
حاصلضرب اقلیدسی ..... Euclidean product
حلقه اقلیدسی ..... Euclidean ring
کد خوددوگان اقلیدسی ..... Euclidean self dual code
تجزیه ..... Factorization
حلقه تقسیم ..... Factorization ring
میدان ..... Field
میدان متناهی ..... Finite field
خودریختی فروبنیوس ..... Frobenius automorphism
چندجمله‌ای مولد ..... Generating polynomial
مولد ..... Generator
ماتریس مولد ..... Generator matrix
بزرگترین مقسوم‌علیه مشترک ..... Greatest common divisor
پایه گروبنر ..... Groebner basis
فاصله همینگ ..... Hamming distance
کد خوددوگان هرمیتی ..... Hermitian self dual code
ایده‌آل ..... Ideal

تحویل‌ناپذیر ..... Irreducible
یکریختی ..... Isomorphism
ضریب پیشرو ..... Leading coefficient
ایده‌آل چپ ..... Left ideal
کد خطی ..... Linear code
کوچکترین مضرب مشترک ..... Lowest common multiple
مینیمم درجه ..... Minimal degree
مدول ..... Module
حلقه ناجابه‌جایی ..... Non-commutative ring
چندجمله‌ای تکین ..... Monic polynomial
مرتبه ..... Order
ماتریس کنترل توازن ..... Parity check matrix
چندجمله‌ای ..... Polynomial
ایده‌آل اصلی ..... Principal ideal
حلقه خارج‌قسمتی ..... Quotient ring
مقسوم‌علیه راست ..... Right divisor
حلقه ..... Ring
حلقه چندجمله‌ای‌های اریب ..... Skew polynomial ring
زیرمدول ..... Submodule
ایده‌آل دوطرفه ..... Two-sided ideal
فضای برداری ..... Vector space
زیرفضای برداری ..... Vector subspace
مقسوم‌علیه صفر ..... Zero divisor

Abstract

In analogy to cyclic codes, we study linear codes over finite fields obtained from left ideals in a quotient ring of a (non-commutative) skew polynomial ring. The results in this thesis show how existence and properties of such codes are linked to arithmetic properties of skew polynomials. This class of codes is a generalization of the θ-cyclic codes discussed earlier in the literature. However, θ-cyclic codes are powerful representatives of this family and we show that the dual of a θ-cyclic code is still θ-syclic. Using Groebner bases, we compute all Euclidean and Hermitian self-dual θ-cyclic codes over F_4 of length less than 40, including a $[36, 18, 11]$-Euclidean self-dual θ-cyclic code which improves the previously best known self-dual code of length 36 over F_4.

Keywords: Automorphism, Cyclic code, Euclidean self dual code, Finite field, Generator matrix, Hamming distance, Hermitian self dual code, Left ideal, Monic polynomial, Parity check matrix, Quotient ring, Skew polynomials ring, Two-sided ideal.

Shahrood University of Technology

Faculty Of Mathematical Sciences

MSc Thesis in: Graphs and Combinatorics

Cyclic codes over non-commutative skew polynomial rings

By: Nahid Bagheri Hashemabad

Supervisors

Dr. Sadegh Rahimi Sherbaf
Dr. Abdollah Alhevaz

Advisor

Dr. Ebrahim Hashemi

October 2018