
بسم الله
الرحمن الرحیم

دانشکده علوم ریاضی

رشته ریاضی کاربردی، گرایش رمز و کد

پایان‌نامه کارشناسی ارشد

برخی خواص کدهای ماکسیمم فاصله مجزای کوانتومی

نگارنده: امیر کریمی

استاد راهنما

دکتر عبدالله آل‌هوز

استاد مشاور

دکتر ابراهیم هاشمی

مهر ماه ۱۳۹۸

فرم شماره ۶: صورتجلسه دفاع از پایان نامه تحصیلی دوره کارشناسی ارشد

با تأییدات خداوند متعال و با استعانت از حضرت ولی عصر (عج) ارزیابی جلسه دفاع از پایان نامه کارشناسی ارشد [redacted] به شماره دانشجویی [redacted] رشته ریاضی کاربردی گرایش آنالیز عددی تحت عنوان [redacted] که در تاریخ ۱۳۹۴/۱۰/۲۷ با حضور هیأت محترم داوران در دانشگاه صنعتی شاهرود برگزار گردید به شرح ذیل اعلام می‌گردد:

قبول (با درجه : عالی امتیاز ۱۸/۱) ☐ دفاع مجدد ☐ مردود ☐

۱ـ عالی (۲۰ ـ ۱۹)
۲ـ بسیار خوب (۱۸/۹۹ ـ ۱۸)
۳ـ خوب (۱۷/۹۹ ـ ۱۶)
۴ـ قابل قبول (۱۵/۹۹ ـ ۱۴)
۵- نمره کمتر از ۱۴ غیر قابل قبول

عضو هیات داوران	نام ونام خانوادگی	مرتبهٔ علمی	امضاء
۱ـ استادراهنمای اول	دکتر علی مس فروش	استادیار	
۲- استادراهنمای دوم			
۳- استاد مشاور	دکتر مهدی قوتمند	استادیار	
۴- نماینده شورای تحصیلات تکمیلی	دکتر ابراهیم هاشمی	استاد	
۵- استاد ممتحن اول	دکتر حجت احسنی طهرانی	استادیار	
۶ـ استاد ممتحن دوم	دکتر علیرضا ناظمی	دانشیار	

رئیس دانشکده:

تقدیم به

پدر و مادر عزیز و همسر مهربانم

سپاس گزاری

اینک که به فضل خداوند این پروژه به سرانجام رسیده، وظیفه خود می‌دانم از زحمات بی دریغ استاد گرامی جناب آقای دکتر عبدالله آل‌هوز و جناب آقای دکتر ابراهیم هاشمی که دراجراي این پروژه مرا یاري فرموده‌اند، کمال تشکر و قدردانی را داشته باشم. همچنین از داوران گرامی آقایان دکتر علیشاهی و دکتر پورعیدی که زحمت مطالعه و داوری این پایان نامه را متقبل شده‌اند، کمال تشکر و قدردانی را دارم.

همواره از خداوند متعال سلامتی و توفیق روز افزون شما را خواهانم .

امیر کریمی
مهر ماه ۱۳۹۸

تعهد نامه

اینجانب **امیر کریمی** دانشجوی کارشناسی ارشد رشته **ریاضی کاربردی** دانشکده **علوم ریاضی** دانشگاه صنعتی شاهرود، نویسنده پایان‌نامه با عنوان **برخی خواص کدهای ماکسیمم فاصله مجزای کوانتومی** ، تحت راهنمایی دکتر **عبدالله آل‌هوز** متعهد می‌شوم:

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

امیر کریمی
مهر ماه ۱۳۹۸

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

در این پایان‌نامه سیستم‌های جبری خواهیم ساخت که بتوان براساس آن‌ها رده‌ای از کدهای ماکسیمم فاصله مجزا (MDS) را به‌دست آورد. روش کار عمدتاً براساس استفاده از خودتوان‌ها و عناصر یکه حلقه می‌باشد. کدهای MDS کوانتومی یک کلاس مهم و با اهمیت از کدهای کوانتومی می‌باشد. ساختن کدهای MDS کوانتومی که فاصله‌ی آن‌ها عدد بزرگی باشد، کار دشواری می‌باشد. در این پایان‌نامه ما با استفاده از کدهای دوری_ثابت کلاسیک دو کلاس از کدهای MDS کوانتومی با پارامترهای $[[\lambda(q-1),\lambda(q-1)-2d+2,d]]_q$ جایی‌که $2 \leq d \leq \frac{(q-1)}{2}+\lambda-1$ و $q+1=\lambda r$ با r زوج و $[[\lambda(q-1),\lambda(q-1)-2d+2,d]]_q$ جایی‌که $2 \leq d \leq \frac{(q-1)}{2}+\frac{\lambda}{2}-1$ و $q+1=\lambda r$ با r فرد را معرفی می‌کنیم. این دو کلاس از کدهای MDS کوانتومی، پارامترهایی بهتر از آنچه که کدهای شناخته شده‌ی قبلی داشته‌اند، دارا می‌باشند.

کدواژه‌ها: کدهای_دوری_ثابت، کدهای کوانتومی، کدهای MDS، یکه‌ها، خودتوان.

فهرست مطالب

فهرست جداول **س**

۱ تعاریف و مفاهیم مقدماتی **۱**

۱.۱ مقدمه ۱

۲.۱ تاریخچه ۱

۳.۱ مفاهیم و تعاریف لازم از نظریه‌ی کدگذاری ۳

۱.۳.۱ کدگذاری منبع پیام ۳

۲.۳.۱ کدگذاری کانال ارتباطی ۴

۳.۳.۱ قواعد کدگشایی ۷

۴.۱ مفاهیم و تعاریف لازم از نظریه‌ی جبر ۹

۱.۴.۱ کدهای BCH و RS ۱۷

۲.۴.۱ طراحی کدهای BCH ۱۷

۳.۴.۱ کران BCH ۱۷

۴.۴.۱ کدهای RS ۱۸

۲ مجموعه‌ای از کدهای MDS حاصل از خودتوان‌ها و یکه‌ها **۱۹**

۱.۲ مقدمه ۱۹

۲.۲ کدهای حاصل از یکه‌ها ۲۰

۳.۲ میدان‌های متناهی ۲۴

۴.۲ ماتریس فوریه روی میدان‌های متناهی ۲۵

۱.۴.۲ $GF(۲^r)$ ۲۸

۲.۴.۲ $GF(۳^r)$ ۳۰

۳.۴.۲ $GF(۵^r)$ ۳۰

۴.۴.۲ $GF(۷^r)$ ۳۱

۵.۴.۲ $GF(۱۱^r)$ ۳۱

۵.۲ کدهای حاصل از مجموعه‌های خودتوان متعامد کامل ۳۳

۱.۵.۲ رتبه ۳۳
۲.۵.۲ کدها ۳۴
۳.۵.۲ به‌دست آوردن فاصله ۳۵
۴.۵.۲ کدهای MDS از نوع دوری ۳۶
۵.۵.۲ کدهای MDS روی میدان‌های متناهی ۳۷
۶.۵.۲ تساوی ۴۰
۶.۲ کدگشایی ۴۰

۳ کدهای MDS کوانتومی جدید حاصل از کدهای دوری ـ ثابت ۴۵
۱.۳ مقدمه ۴۵
۲.۳ خلاصه‌ای از کدهای دوری ـ ثابت ۴۷
۳.۳ ساختن کدها ۴۸

مراجع ۵۵

واژه‌نامه فارسی به انگلیسی ۵۷

واژه‌نامه انگلیسی به فارسی ۵۹

فهرست جداول

۱.۱ . . . . . ۴
۲.۱ . . . . . ۵
۱.۳ کدهای MDS کوانتومی جدید ۵۱
۲.۳ کدهای MDS کوانتومی جدید ۵۳
۳.۳ کدهای MDS کوانتومی جدید ۵۴

فصل ۱

تعاریف و مفاهیم مقدماتی

۱.۱ مقدمه

در این فصل تعاریف و مفاهیم لازم از نظریه‌ی کد و همچنین مفاهیم لازم از جبر را برای فصل‌های آتی بیان کنیم. تعاریف این فصل همگی برگرفته از مراجع [۱۳] و [۱۵] می‌باشد.

۲.۱ تاریخچه

عصر جدید، عصر فناوری‌های نوین اطلاعاتی و ارتباطی است. سرعت نوآوری در این حوزه نیازمندی‌های علمی و عملی خاصی را طلب می‌کند، حجم داده‌های فراوان در این حوزه که نیازمند امنیت و محرمانگی هستند و نیاز به پردازش و ارسال سریع اطلاعات حجیم که نیازمند فناوری‌های نوین ارتباطی هستند، تربیت متخصصین و کارشناسان خبره و مسلط بر دانش کد و رمز را طلب می‌کند. شاخه‌ی کد و رمز یک رشته‌ی بین رشته‌ای، بین رشته‌های مهندسی برق، کامپیوتر، فیزیک و ریاضی است که بخش اعظم آن بر بنیاد دانش ریاضی بنا شده است. نظریه‌ی کدگذاری، شاخه‌ای از ریاضیات است که روش‌های کنترل خطاهای به‌وجود آمده در انتقال اطلاعات را بررسی می‌کند.
این نظریه با طراحی کدهای تشخیص‌دهنده و تصحیح‌کننده‌ی خطا، برای ارسال قابل اعتماد پیام‌ها و اطلاعات در بین کانال‌های پارازیت‌دار سروکار دارد و ارتباطات مدرن بدون آن انجام

نمی‌گیرد و تحقیق روی این کدها همچنان ادامه دارد.
ابداع این نظریه به قضیه‌ی معروفی از شانون[۱] برمی‌گردد که وجود کدهایی را تضمین می‌کند که می‌توانند اطلاعات را به میزانی نزدیک به حداکثر ظرفیت کانال ارتباطی و با احتمال خطایی به‌اندازه‌ی کوچک انتقال دهند. نظریه‌ی کدگذاری توسط تحقیقات شانون و همینگ[۲] پایه‌گذاری شده است. شانون چهارچوب نظری این نظریه را بنا نهاد. او نخستین بار مفهوم نظریه‌ی ارتباطات را تعریف کرد. وی با تحقیقاتی که در زمینه‌ی به‌کارگیری ریاضیات در نظریه‌ی ارتباطات انجام داده بود در پی جواب این سوال بود که چگونه یک فرستنده می‌تواند به طور بهینه اطلاعات را از طریق یک کانال ارتباطی به گیرنده ارسال کند.
در سال ۱۹۴۸ چند مقاله تحت نظریه ریاضی ارتباطات منتشر شد. همینگ نیز که همکار شانون بود به مطالعه در مورد دستگاه‌هایی پرداخته بود که می‌توانستند اطلاعات را در خود ذخیره کرده یا به جای دیگر مخابره کنند. برخی از این دستگاه‌ها اگر با خطایی مواجه می‌شدند عملیات اجرایی آنها متوقف شده و دیگر قادر به ادامه‌ی کار نبودند. در آن زمان همینگ به این موضوع پی‌برد که اگر دستگاه‌هایی که قادر به تشخیص خطا هستند وجود داشته باشد، می‌توان دستگاه‌هایی را یافت که قادر به تصحیح خطا نیز باشند.
تحقیقات همینگ منجر به تعریف مفهوم فاصله‌ای شد که هم‌اکنون در نظریه‌ی کدگذاری به نام فاصله‌ی همینگ مشهور است. مقاله‌ی مشهور همینگ تحت عنوان کدهای تشخیص‌دهنده و تصحیح‌کننده‌ی خطا در سال ۱۹۵۰ منتشر شد. پس از شانون و همینگ، اسلپین[۳] اولین کسی بود که جبرخطی را وارد این نظریه کرده و کدهای خطی تصحیح‌کننده‌ی خطا را ابداع نمود. کدهایی که در این پایان‌نامه مورد بررسی قرار گرفته است کدهای ماکسیمم فاصله‌ی مجزا[۴] (MDS) نامیده می‌شوند. کدهای MDS کدهای خطی می‌باشند که برای آن‌ها حالت مرزی کران سینگلتون رخ می‌دهد. کدهای MDS یک از مهمترین انواع کد می‌باشند، زیرا از نظر طول و بعد بهینه بوده و دارای ساختار ترکیبیاتی جالبی نیز می‌باشند. در این پایان‌نامه در ابتدا روش‌هایی برای ساختن کدهای MDS از مجموعه‌های متعامد کامل و خودتوان‌ها بررسی شده و در ادامه دو کلاس از کدهای MDS کوانتومی معرفی و ساخته می‌شوند.

[1] Shannon
[2] Hamming
[3] Slepian
[4] Maximum distance separable codes

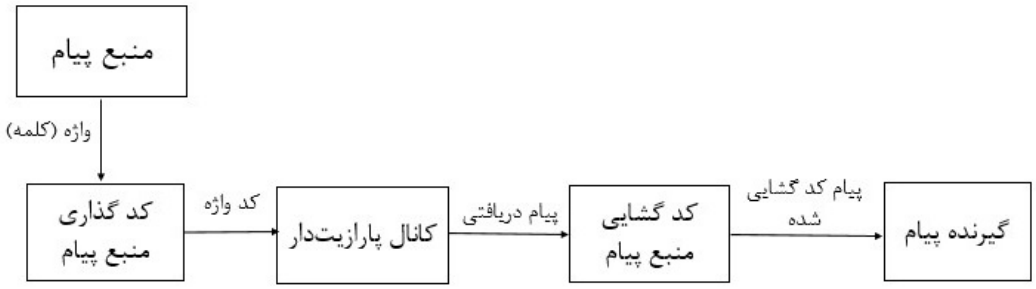
۳.۱ مفاهیم و تعاریف لازم از نظریه‌ی کدگذاری

کدگذاری تصحیح خطا ابزاری جهت تصحیح خطاهایی است که در اثر عبور از کانال مخابراتی بر روی داده‌های دیجیتال ایجاد می‌شود. در این روش تصحیح خطا صرفاً بر مبنای داده دریافتی صورت می‌گیرد. کدگذاری تشخیص خطا نیز ابزاری جهت تشخیص خطاهای ایجاد شده است. در حقیقت کدگذاری تشخیص خطا و کدگذاری تصحیح خطا در کنار یکدیگر ابزاری جهت کنترل خطا می‌باشند که به همین دلیل به نام کدگذاری کنترل خطا نیز شناخته می‌شوند. در حقیقت کدگذاری کنترل خطا را می‌توانیم تفاوت اصلی یک سامانه مخابراتی کارآمد و یک سامانه مخابراتی ناکارآمد تلقی نمائیم. این ابزار یک روش توانمندساز بسیار مهم در انقلاب مخابرات راه دور، اینترنت، ضبط دیجیتال و اکتشاف‌های فضایی بوده است. کدگذاری کنترل خطا تقریباً در تمامی جامعه مدرن مبتنی بر اطلاعات، حضور دارد. هر دیسک فشرده‌ای اعم از CD-ROM و DVD ،از چنین کدهایی برای محافظت از داده ذخیره شده روی دیسک پلاستیکی استفاده می‌کند. تمامی دیسک‌های سخت از کدگذاری تصحیح خطا استفاده می‌کنند. هر تماس تلفنی که در یک شبکه سلولی برقرار می‌شود از آن استفاده می‌کند. هر بسته‌ای که در اینترنت منتقل می‌شود دارای یک بسته‌بندی محافظتی جهت تشخیص دریافت سالم بسته است. حتی تجارت روزانه و معمولی که با آن سروکار داریم ، از کدگذاری کنترل خطا بهره می‌برد.

منبع داده‌ای است که باید مخابره شود. به‌عنوان مثال این داده می‌تواند یک فایل رایانه‌ای، یک ویدئو و یا یک مکالمه‌ی تلفنی باشد.

۱.۳.۱ کدگذاری منبع پیام

این نوع کدگذاری در واقع به این صورت انجام می‌پذیرد که تغییراتی در منبع پیام داده تا کدهای مناسب جهت انتقال پیام فراهم شود. در واقع فرآیند زیر را داریم:



مثال ۱.۳.۱. مثال ساده از کدگذاری منبع اطلاعاتی: فرض کنیم چند میوه‌ی مختلف مانند موز، سیب، انگور و گیلاس داشته باشیم و برای آنها کدگذاری منبع را به‌صورت جدول ۱.۱ انجام دهیم.

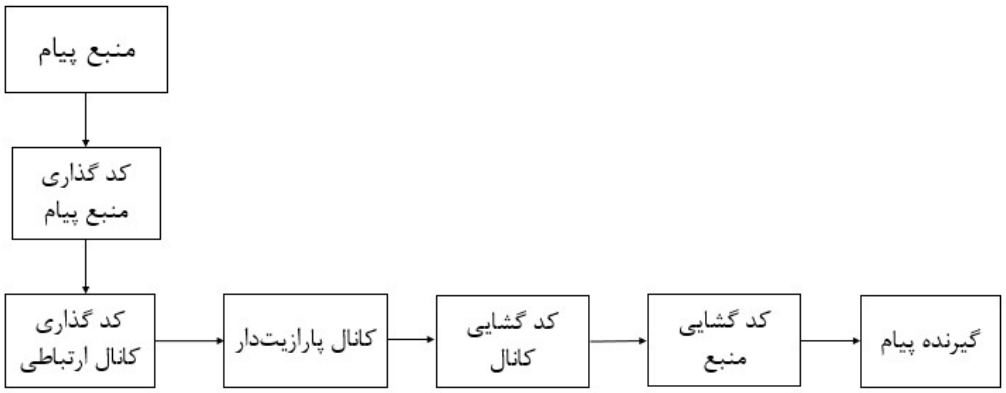
حال فرض کنیم کلمه‌ی انگور (۱۱) ارسال شود و در کانال پارازیت‌دار با تحریف اعمال شده، پیام دریافتی به‌صورت (۱۰) دریافت شود، لذا گیرنده در واقع به خطا پیام گیلاس دریافت می‌کند و لذا یک ارتباط ناموفق رخ می‌دهد.

جدول ۱.۱

سیب	۰۰
موز	۰۱
انگور	۱۱
گیلاس	۱۰

۲.۳.۱ کدگذاری کانال ارتباطی

در واقع کد کردن مجدد کلمات کد شده در فرآیند کدگذاری منبع قبل از ورود به کانال پارازیت‌دار می‌باشد. این کار به جهت بالا بردن قابلیت تشخیص و تصحیح خطای اعمال شده در کانال پارازیت‌دار صورت می‌پذیرد و در واقع فرآیند زیر را داریم:



با فرضیات مثال قبلی پس از کدگذاری منبع یک بار دیگر کدگذاری کانال را به‌صورت جدول ۲.۱ انجام می‌دهیم.

جدول ۲.۱

سیب	۰۰	۰۰۰
موز	۰۱	۰۱۱
انگور	۱۱	۱۱۰
گیلاس	۱۰	۱۰۱

حال فرض کنیم کلمه انگور از منبع اطلاعاتی ارسال شود. در مرحله‌ی کدگذاری منبع به ۱۱ تبدیل شده و سپس در مرحله‌ی کدگذاری کانال به ۱۱۰ تبدیل می‌شود. حال اگر این کدواژه در یک کانال پارازیت‌دار ارسال شود و بدانیم که یک خطا روی آن اعمال می‌شود، دراین‌صورت پس از خروج بایستی یکی از حالات ۰۱۰، ۱۰۰ یا ۱۱۱ دریافت شود. حال چون هیچ‌کدام از سه حالت فوق جزء کدواژه‌های ما نمی‌باشند لذا گیرنده‌ی پیام به محض دریافت هر کدام از سه حالت فوق سریعاً قادر به تشخیص خطای کانال می‌باشد.
در فرآیند کدگذاری مثال فوق برای ارسال ۲ بیت اطلاعات مجبور به ارسال ۳ بیت شدیم. در واقع با افزایش هزینه، قابلیت تشخیص خطا را برای گیرنده فراهم کردیم که این فرآیند با کاهش سرعت انتقال داده نیز همراه بود. لذا درصدد طراحی کدهایی هستیم که ضمن ایجاد قابلیت تشخیص و تصحیح خطای بالاتر از لحاظ هزینه نیز مقرون به صرفه باشد و از سرعت انتقال مناسبی نیز برخوردار باشد.

تعریف ۱.۳.۱. فرض کنیم A یک مجموعه‌ی qـ عنصری بصورت $A = \{a_1, a_2, \ldots, a_q\}$ باشد. دراین‌صورت مجموعه‌ی A را الفبای کد نامیم و هر یک از عناصر A را، سمبل کد می‌نامیم. کلمه‌ی qـ تایی با طول n روی الفبای A،در واقع دنباله‌ای به‌صورت $w = w_1 w_2 ... w_n$ می‌باشد، جایی‌که $w_i \in A$ برای هر $1 \leq i \leq n$ ، همچنین می‌توان هر کلمه را به‌صورت برداری $w = (w_1, w_2, \ldots, w_n)$ نیز در نظر گرفت.

تعریف ۲.۳.۱. کد بلوکی qـ تایی با طول n روی مجموعه‌ی A، مجموعه‌ای ناتهی مانند C، متشکل از کلمات qـ تایی می‌باشد که تمام کلمات آن از طول یکسان n می‌باشند.

تعریف ۳.۳.۱. تعداد کدواژه‌های کد را اندازه‌ی کد C نامیده و با نماد $|C|$ نمایش می‌دهیم.

هر کد بلوکی از طول n و اندازه‌ی m یک $[n, m]$ ـ کد نامیده می‌شود. مثلاً اگر گوییم یک کد به‌صورت $[۲,۳]$ ـ کد می‌باشد آنگاه با یک کد با تعداد ۳ کدواژه سروکار داریم که هر کدام

از کدواژه‌ها از طول ۲ می‌باشند.

$$C = \{w_۱ = a_۱a_۲, w_۲ = a_۳a_۴, w_۳ = a_۵a_۶ \mid \ a_i \in A \ , \ ۱ \leq i \leq ۶\} \qquad (۱.۱)$$

تعریف ۴.۳.۱. نرخ ارسال اطلاعات کد C به‌صورت $r = \frac{k}{n}$ می‌باشد. جایی‌که k تعداد بیت‌های اطلاعات مفید می‌باشد و n تعداد بیت‌هایی است که کد کننده صرف کدکردن اطلاعات و داده‌ها می‌کند. یعنی $n > k$ و به تعداد $n - k$ تا بیت اضافی در فرآیند کدگذاری اعمال شده است. در واقع نرخ هر کد C به‌صورت نسبت تعداد بیت‌های پیام ارسالی به تعداد بیت‌های پیام کد شده می‌باشد.
در واقع نرخ کد C ،کمیتی برای اندازه‌گیری کارایی کد C می‌باشد و کدهای با نرخ بالا از اهمیت ویژه‌ای در نظریه‌ی کدگذاری برخوردار می‌باشند. هر چند در عمل به غیر از فاکتور نرخ کد، قابلیت تشخیص و تصحیح خطای کد نیز از اهمیت ویژه‌ای برخوردار می‌باشد.

تعریف ۵.۳.۱. در اکثر اوقات الفبای کد را یک میدان متناهی در نظر می‌گیرند و اگر $A = F_۲$ دراین‌صورت کد را یک کد دودویی و اگر $A = F_۳$ کد را یک کد سه‌تایی و اگر $A = F_۴$ کد را یک کد چهارتایی نامیم.
مثلاً اگر $A = F_۲$ دراین‌صورت کد $c = \{۰۰۰, ۰۱۰, ۱۰۰, ۱۱۰, ۱۰۱\}$ یک $[۳,۵]$ ـ کد دودویی می‌باشد.

تعریف ۶.۳.۱. فاصله‌ی همینگ: فاصله‌ی همینگ بین دو کدواژه‌ی $a = (a_۱, a_۲, \ldots, a_n)$ و $b = (b_۱, b_۲, \ldots, b_n)$ در یک کد بلوکی، به‌صورت تعداد جایگاه‌های (بیت‌های) متمایز a و b تعریف می‌شود. یعنی تعداد بیت‌هایی که a و b با هم تفاوت دارند. لذا داریم:

$$d_H(a,b) = |\{i | a_i \neq b_i \ , \ i = ۱, ۲, ..., n\}|$$

و یا به طور معادل:

$$d_H(a,b) = \sum_{i=۱}^{n} d_H(a_i, b_i)$$

جایی‌که

$$d_H(a_i, b_i) = \begin{cases} ۱ & a_i \neq b_i \\ ۰ & a_i = b_i. \end{cases}$$

تعریف ۷.۳.۱. فاصله‌ی کد: فرض کنید C یک کد بلوکی باشد و حداقل دو کدواژه داشته باشد. دراین‌صورت فاصله‌ی همینگ کد C به‌صورت مینیمم فاصله‌ی همینگ بین تمام کدواژه‌های C تعریف می‌شود، یعنی داریم:

$$d(C) = min\left\{d_H(a,b) | \ a, b \in c \ , \ a \neq b\right\}.$$

هر کد بلوکی که طول آن n، اندازه‌ی آن m و فاصله‌ی همینگ آن d باشد را یک $[n, m, d]$ ـ کد می‌نامیم. در این حالت اعداد n و m و d را پارامترهای کد C می‌نامیم.

مثال ۲.۳.۱. فرض کنید $A = F_۳ = \{۰,۱,۲\}$ و $C = \{۰۱۲۰۱,۱۲۲۰۰,۲۱۰۱۱\}$ یک کد روی الفبای A باشد دراین‌صورت اگر $a = ۱۲۰۱$ و $b = ۱۲۲۰۰$ و $c = ۲۱۰۱۱$ داریم:

$$d_H(a,b) = ۳ \quad , \quad d_H(a,c) = ۳ \quad , \quad d_H(b,c) = ۵$$

لذا $d(C) = min\{۳,۳,۵\} = ۳$ و کد C یک $[۵,۳,۳]$ ـ کد سه تایی می‌باشد.

۳.۳.۱ قواعد کدگشایی

در طی فرآیند کدگذاری داده‌ها، یعنی پس از انجام کدگذاری منبع و کدگذاری کانال بر روی پیام مدنظر ما کدواژه‌های ما از طریق کانال ارتباطی ارسال می‌شود و در این حالت می‌توانیم دو حالت مختلف برای گیرنده‌ی پیام متصور باشیم: اول اینکه که واژه‌های دریافتی معتبر باشند که در این حالت ممکن است گیرنده‌ی پیام، حتی اگر خطایی رخ داده باشد قادر به تشخیص خطا نباشد. دوم اینکه کلمه‌ی دریافتی معتبر نباشد (در بین کدواژه‌های کد ما موجود نباشد)، دراین‌صورت گیرنده قادر به تشخیص خطای اعمال شده و حتی تعداد خطا می‌باشد. حال گیرنده دنبال محتمل‌ترین کدواژه‌ی ارسالی برای کدگشایی کردن کلمه‌ی دریافت شده، به آن کدواژه می‌باشد که برای این امر دو روش عام کدگشایی داریم:

(۱). قاعده‌ی کدگشایی مینیمم فاصله MDD

(۲). قاعده‌ی کدگشایی ماکزیمم احتمال MLD

(۱). قاعده‌ی کدگشایی مینیمم فاصله MDD:

فرض کنید کدواژه‌های کد C در یک کانال ارتباطی پارازیت‌دار ارسال شود و ما کلمه‌ی x را دریافت کرده باشیم. دراین‌صورت قاعده‌ی کدگشایی مینیمم فاصله، کلمه‌ی x را به کدواژه‌ی c_x کدگشایی می‌کند هرگاه فاصله‌ی (همینگ) بین x و c_x در بین تمام کدواژه‌های کد C، مینیمم مقدار ممکن باشد، یعنی داشته باشیم:

$$d_H(x,c_x) = min\{d_H(x,c) \mid \ c \in C\}.$$

دو نوع قاعده‌ی کدگشایی مینیمم فاصله داریم:

آ. قاعده‌ی کدگشایی مینیمم فاصله‌ی کامل $(CMDD)$: در این روش اگر کلمه‌ی xدریافت شود و تعداد کدواژه‌هایی که با کلمه‌ی x دارای مینیمم فاصله باشند بیش از یک مورد باشند، آنگاه یکی از کدواژه‌ها را به دلخواه انتخاب کرده و کلمه‌ی x را به آن کدواژه، کدگشایی می‌کند.

ب. قاعده‌ی کدگشایی مینیمم فاصله‌ی غیرکامل $(IMDD)$: در این روش اگر کلمه‌ی x دریافت شود و تعداد کدواژه‌هایی که با کلمه‌ی x دارای فاصله‌ی مینیمم می‌باشند بیش از یک مورد باشد، آنگاه بدون هیچ تصمیم‌گیری صرفاً درخواست ارسال مجدد کد را انجام می‌دهد.

(۲). قاعده‌ی کدگشایی ماکزیمم احتمال $(IMLD)$:
فرض کنیم کدواژه‌های کد C از طریق یک کانال پارازیت‌دار ارسال شده باشد و ما کلمه‌ی x را دریافت کرده باشیم. دراین‌صورت قاعده‌ی کدگشایی ماکزیمم احتمال، کلمه‌ی x را به کدواژه‌ی c_x کدگشایی می‌کند هرگاه احتمال کانال ارسال برای c_x ماکزیمم باشد یعنی:

$$p\left(x\text{دریافت}|c_x\text{ارسال}\right) = max\left\{p\left(x\text{دریافت}|c\text{ارسال}\right) \mid c \in C\right\}.$$

دو نوع قاعده‌ی کدگشایی ماکزیمم احتمال داریم:

آ. قاعده‌ی کدگشایی ماکزیمم احتمال کامل $(CMLD)$: در این روش اگر کلمه‌ی x دریافت شود و تعداد کدواژه‌هایی که با کلمه‌ی x دارای ماکزیمم احتمال کانال ارسال هستند، بیش از یک مورد باشند، آنگاه یکی از کدواژه‌ها را به دلخواه انتخاب کرده و کلمه‌ی x را به آن کدواژه، کدگشایی می‌کند.

ب. قاعده‌ی کدگشایی ماکزیمم احتمال غیرکامل $(IMLD)$: در این روش اگر کلمه‌ی x دریافت شود و تعداد کدواژه‌هایی که با کلمه‌ی x دارای ماکزیمم احتمال کانال ارسال می‌باشند بیش از یک مورد باشد، آنگاه بدون هیچ تصمیم‌گیری صرفاً درخواست ارسال مجدد کد را انجام می‌دهد.

تعریف ۸.۳.۱. برای هر عدد صحیح مثبت u، گوییم کد C یک کد uـ تشخیص‌گر خطا می‌باشد هرگاه اگر در کدواژه‌های کد C، حداقل یک خطا و حداکثر uـ خطا رخ دهد، دراین‌صورت کلمه‌ی حاصل کدواژه‌ای از کد C نباشد.
همچنین کد C را یک کد دقیقاً uـ تشخیص‌گر خطا نامیم هرگاه این کد، uـ تشخیص‌گر خطا باشد ولی $(u+۱)$ ـ تشخیص‌گر خطا نباشد.

تعریف ۹.۳.۱. برای عدد صحیح مثبت u، گوییم کد C یک کد uـ تصحیح‌کننده‌ی خطا می‌باشد هرگاه روش کدگشایی مینیمم فاصله‌ی غیرکامل $IMDD$ قادر به تصحیح حداکثر u خطا باشد. همچنین گوییم کد C یک کد دقیقاً uـ تصحیح‌کننده‌ی خطا می‌باشد، هرگاه uـ تصحیح‌کننده‌ی خطا باشد ولی $(u+۱)$ ـ تصحیح‌کننده‌ی خطا نباشد.

مثال ۳.۳.۱. کد دودویی $C = \{۰۰۰۰۰, ۰۱۱۱۰, ۱۰۰۱۱\}$ را در نظر بگیرید. دراین‌صورت، یک $[۵,۳,۳]$ ـ کد دودویی می‌باشد. $(d(C) = ۳)$ می‌توان دید که روش کدگشایی مینیمم فاصله غیرکامل $IMDD$ قابلیت تشخیص و تصحیح یک خطا را دارد. (یک خطا را تشخیص داده و تصحیح می‌کند. دو خطا را تشخیص داده، ولی نمی‌تواند تصحیح کند).
به‌عنوان مثال فرض کنید ۰۰۰۰۰ ارسال شده باشد و با یک خطا کلمه ۱۰۰۰۰ را دریافت کرده باشیم، دراین‌صورت چون کلمه‌ی دریافتی در بین کدواژه‌ها نمی‌باشد خطا تشخیص داده می‌شود و چون $d_H(۱۰۰۰۰, ۰۰۰۰۰) = ۱$.
در حالی‌که $d_H(۱۰۰۰۰, ۰۱۱۱۰) = ۴$ و $d_H(۱۰۰۰۰, ۱۰۰۱۱) = ۲$ بنابراین $IMDD$ ، ۱۰۰۰۰ را

به ۰۰۰۰۰ کدگشایی می‌کند. لذا این کد ۱ـ تصحیح کننده‌ی خطا می‌باشد. این کد ۲ـ تصحیح کننده‌ی خطا نمی‌باشد. زیرا اگر ۰۰۰۰۰ را ارسال کنیم و کلمه‌ی x دریافتی با دو خطا به‌صورت $x = ۰۰۰۱۱$ باشد دراین صورت چون $d_H(x, ۰۰۰۰۰) = ۲$ و $d_H(x, ۰۱۱۱۰) = ۳$ و $d_H(x, ۱۰۰۱۱) = ۱$ لذا $IMDD$ کدواژه‌ی x، را به اشتباه به کدواژه‌ی ۱۰۰۱۱ کدگشایی می‌کند. بنابراین این کد دقیقاً ۱ـ تصحیح کننده‌ی خطا می‌باشد.

قضیه ۱.۳.۱. کد C یک کد uـ تشخیص‌گر خطا می‌باشد اگر و تنها اگر $d(C) \geq u + ۱$.

قضیه ۲.۳.۱. کد C یک کد uـ تصحیح کننده‌ی خطا می‌باشد اگر و تنها اگر $d(C) \geq ۲u + ۱$.

۴.۱ مفاهیم و تعاریف لازم از نظریه‌ی جبر

از آنجایی که هر کد خطی از طول n، یک زیرفضای برداری از فضای برداری F_q^n می‌باشد، لذا بایستی ابتدا فضای برداری روی یک میدان را مورد مطالعه قرار دهیم:

تعریف ۱.۴.۱. فضای برداری: فرض کنیم V یک مجموعه ناتهی باشد دراین‌صورت مجموعه V به همراه عمل جمع + و عمل ضرب اسکالر را یک فضای برداری روی میدان F_q نامیم هرگاه خواص زیر را داشته باشد:

آ. $(V, +)$ یک گروه آبلی باشد، یعنی داشته باشیم:

۱. $(V, +)$ بسته باشد $\quad \forall\, v_۱, v_۲ \in V : \quad v_۱ + v_۲ \in V$

۲. $(V, +)$ شرکت‌پذیر باشد

$$\forall\, v_۱, v_۲, v_۳ \in V : \quad v_۱ + (v_۲ + v_۳) = (v_۱ + v_۲) + v_۳$$

۳. وجود عنصر خنثی نسبت به عمل جمع

$$\forall\, v \in V : \quad \exists\ \circ \in V \quad s.t \quad v + \circ = \circ + v = v$$

۴. وجود عنصر وارون نسبت به عمل جمع

$$\forall\, v \in V : \quad \exists\ w = -v \quad s.t \quad v + w = \circ$$

۵. $(V, +)$ خاصیت جابجایی داشته باشد

$$\forall\, v, w \in V \quad v + w = w + v$$

ب. برای هر $v \in V$ و $\lambda \in F_q$ داشته باشیم: $\lambda.v \in V$

پ. برای هر $\lambda \in F_q$ و $v, w \in V$ داشته باشیم: $\lambda.(v + w) = \lambda v + \lambda w$

ت. برای هر $\lambda, \mu \in F_q$ و $v \in V$ داشته باشیم: $(\lambda\mu).v = \lambda.(\mu v)$

ث. اگر عنصر ۱_F همانی ضربی را داشته باشیم آنگاه: $\forall\, v \in V : \quad ۱_F.v = v$

مثال ۱.۴.۱. مجموعه تمام nـ تایی‌های روی میدان متناهی F_q به‌صورت زیر تعریف می‌شود:

$$F_q^n = \{(a_۱, a_۲, \ldots, a_n) \mid a_i \in F_q \quad ۱ \leq i \leq n\}.$$

عمل جمع روی F_q^n را به‌صورت مؤلفه‌ای زیر تعریف می‌کنیم:

$$\forall \quad v = (a_۱, a_۲, \ldots, a_n) \in F_q^n \quad , \quad w = (b_۱, b_۲, \ldots, b_n) \in F_q^n$$
$$v + w = (a_۱ + b_۱, a_۲ + b_۲, \ldots, a_n + b_n) \in F_q^n$$

و همچنین عمل ضرب اسکالر را به‌صورت زیر تعریف می‌کنیم:

$$\cdot : F_q \times v \longrightarrow V$$
$$\forall \ \lambda \in F_q \qquad \forall \ v = (v_۱, \ldots, v_n) \in V$$
$$\lambda \cdot v = (\lambda v_۱, \lambda v_۲, ..., \lambda v_n)$$

حال مجموعه‌ی F_q^n به همراه عمل جمع و عمل ضرب اسکالر فوق یک فضای برداری روی میدان F_q می‌باشد.

مثال ۲.۴.۱. مجموعه تمام ماتریس‌های $m \times n$ روی میدان متناهی F_q با عمل جمع معمولی ماتریس‌ها و ضرب اسکالر یک فضای برداری روی میدان F_q می‌باشد.

$$V = \{M_{m\times n}(F_q) \ \mid \ m, n \in \mathbb{N}\}$$
$$\forall \ \lambda \in F_q \ , \ \forall M_{m\times n} \in V \ : \ M_{m\times n}(a_{ij})_{m\times n} \Longrightarrow \lambda \cdot M_{m\times n} = (\lambda a_{ij})_{m\times n}$$

تعریف ۲.۴.۱. فرض کنیم V یک فضای برداری روی میدان متناهی F_q باشد و $\emptyset \neq W \subseteq V$. دراین‌صورت گوییم W یک زیرفضای برداری از V می‌باشد هرگاه خود W به همراه عمل جمع و ضرب اسکالر تعریف شده بر روی V، یک فضای برداری باشد.

تعریف ۳.۴.۱. محک زیر فضا بودن: زیر مجموعه‌ی ناتهی W از فضای برداری V یک زیرفضا از V می‌باشد اگر و تنها اگر داشته باشیم:

$$\forall \ w_۱, w_۲ \in W \quad , \quad \forall \ \lambda, \mu \in F_q \quad \Longrightarrow \lambda w_۱ + \mu w_۲ \in W$$

اگر W یک زیرفضای، فضای برداری V باشد آنگاه می‌نویسیم $W \leq V$.

یک فضای برداری روی میدان F_q می‌تواند چندین پایه‌ی مختلف داشته باشد، ولی بایستی تمام پایه‌های آن هم‌عدد (کاردینال) باشند. این عدد بعد فضای برداری نامیده می‌شود و با نماد $dim_F(v)$ نمایش داده می‌شود.

تعریف ۱.۴.۱. فرض کنیم V یک فضای برداری روی میدان F_q باشد و $\emptyset \neq S \subseteq V$ دراین‌صورت گوییم S یک مجموعه‌ی مستقل خطی می‌باشد هرگاه داشته باشیم:

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0 \Longrightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$$
$$v_1, \ldots, v_n \in V \quad , \quad \lambda_1, \ldots, \lambda_n \in F_q$$

در غیر این‌صورت بردارهای $v_1, v_2, \ldots, v_n$ را وابسته‌ی خطی نامیم.

تعریف ۱.۴.۱. فرض کنیم V یک فضای برداری روی میدان F_q باشد دراین‌صورت $S = \{v_1, \ldots, v_n\}$ را یک پایه برای V نامیم هرگاه:

۱. S مستقل خطی باشد.

۲. S مولد V باشد.

تعریف ۱.۴.۱. فرض کنیم S یک زیرمجموعه‌ی ناتهی از فضای برداری F_q^n باشد، مکمل متعامد مجموعه‌ی S را که با نماد $S^\perp$ نمایش داده می‌شود به‌صورت زیر تعریف می‌کنیم:

$$S^\perp = \{v \in F_q^n \mid v.s = 0 \quad \forall\, s \in S\}.$$

اگر $S = \emptyset$، آنگاه داریم: $S^\perp = F_q^n$.

تعریف ۱.۴.۱. کد خطی: یک کد خطی از طول n روی میدان F_q، یک زیرفضایی از فضای برداری F_q^n می‌باشد.

مثال ۱.۴.۱. اگر $C = \{\underbrace{(\lambda, \lambda, \ldots, \lambda)}_{\text{n تا}} \mid \lambda \in F_q\}$، دراین‌صورت طبق تعریف فوق، C یک کد از طول n روی F_q می‌باشد. زیرا طبق محک زیرفضا بودن مجموعه‌ی C زیرفضایی از F_q^n می‌باشد. این کد یک کد تکراری نامیده می‌شود.

تعریف ۱.۴.۱. فرض کنیم C یک کد خطی در F_q^n باشد:

آ. کد دوگان کد C که با نماد $C^\perp$ نمایش داده می‌شود، برابر با مکمل متعامد C در F_q^n می‌باشد:

$$C^\perp = \{v \in F_q^n \mid v.c = 0 \quad \forall\, c \in C\}.$$

ب. بعد یک کد خطی C برابر با بعد C به‌عنوان یک فضای برداری می‌باشد. (به‌عنوان یک زیرفضای برداری از F_q^n) لذا بعد یک کد خطی همواره کوچکتر یا مساوی n می‌باشد.

تعریف ۱.۴.۱. فرض کنیم C یک کد خطی باشد، دراین‌صورت:

آ. کد C را یک کد خودمتعامد گوییم هرگاه داشته باشیم $C \subseteq C^\perp$. دراین‌صورت به‌وضوح داریم $dim(C) \leq dim(C^\perp)$.

ب. کد C را یک کد خوددوگان نامیم هرگاه داشته باشیم $C = C^{\perp}$. دراین‌صورت به‌وضوح داریم $dim(C) = dim(C^{\perp}) = \frac{n}{۲}$.

تعریف ۱.۴.۱۰. آ. ماتریس مولد کد خطی Cماتریسی است که سطرهای آن پایه‌ای برای کد خطی C می‌باشد.

ب. ماتریس زوج‌آزمایی کد خطی C ماتریسی است که سطرهای آن پایه‌ای برای دوگان کد C، یعنی $C^{\perp}$ می‌سازند.

اگر کد خطی C یک $[n,k]$ ـ کد باشد (n طول کدواژه‌ها و kبعد کد C) دراین‌صورت ماتریس مولد کد C ماتریسی $k\times n$ می‌باشد و ماتریس زوج‌آزمایی کد C یک ماتریس $(n-k)\times n$ می‌باشد.

همان‌طور که تعداد پایه‌های یک فضای برداری لزوماً منحصربه‌فرد نمی‌باشد، تعداد ماتریس‌های مولد یک کد خطی نیز می‌تواند بیش از یکی باشد. سطرهای ماتریس مولد و سطرهای ماتریس زوج‌آزمایی هر دو باید مستقل خطی باشند.
برای این‌که نشان دهیم که یک ماتریس $k \times n$ داده شده G، ماتریس مولد کد خطی C از بعد k می‌باشد کافی است نشان دهیم سطرهای ماتریس G، کدواژه‌هایی از کد C می‌باشند و همچنین سطرهای G مستقل خطی می‌باشند. به بیان معادل کافی است نشان دهیم کد C مشمول در فضای سطری ماتریس G می‌باشد.

تعریف ۱.۴.۱۱. کد C را یک کد دوری نامیم هرگاه:

آ. خطی باشد.

ب. هر انتقال دوری از یک کدواژه‌ی C، باز هم کدواژه‌ای در خود C باشد به عبارت دیگر اگر $C = (a_۱, a_۲, \ldots, a_n) \in C$ آنگاه $C' = (a_n, a_۱, a_۲, \ldots, a_{n-۱}) \in C$.

مثال ۱.۴.۴. کد $\{۰۰۰, ۱۰۱, ۰۱۱, ۱۱۰\}$ یک کد دودویی دوری می‌باشد.

تعریف ۱.۴.۱۲. فرض کنیم مجموعه‌ی الفبای A مفروض باشد که $|A| = q > ۱$ و مقادیر n و d مشخص باشد. دراین صورت عدد $A_q(n,d)$ را بصورت ماکسیمم اندازه‌ی ممکن برای m به‌گونه‌ای که یک $[n,m,d]$ ـ کد موجود باشد تعریف می‌کنیم و داریم:

$$A_q(n,d) = max\{m \mid \text{یک } [n,m,d] \text{ ـ کد موجود باشد}\}.$$

تعریف ۱.۴.۱۳. کدی مانند C که اندازه‌ی آن برابر با $A_q(n,d)$ باشد، را کد بهینه می‌نامیم.

از آنجایی که محاسبه‌ی مقدار $A_q(n,d)$ کار راحتی نبوده، ولی مسئله‌ی جالب و تأثیرگذاری در نظریه کد می‌باشد از آن به‌عنوان مهمترین مسئله‌ی نظریه‌ی کدگذاری یاد می‌شود. چون محاسبه‌ی مقدار دقیق $A_q(n,d)$ کار ساده‌ای نمی‌باشد، ولی می‌توان برای آن کران‌های بالا و پایین مشخص کرد که در عمل کار ما را راحت می‌کند.

تعریف ۱.۴.۱. کران سینگلتون[۵]: برای هر عدد صحیح $q > ۱$ و هر عدد صحیح مثبت n و همچنین عدد صحیح d به‌گونه‌ای که $۱ \leq d \leq n$ همواره داریم:

$$A_q(n,d) \leq q^{n-d+۱}$$

در حالت خاص که q توانی از عدد اول باشد، پارامترهای $[n,k,d]$ هر کد خطی روی میدان F_q در نامساوی $k+d \leq n+۱$ صدق می‌کند.

تعریف ۱.۴.۱۵. هر $[n,k,d]$ ـ کد خطی C به‌گونه‌ای که برای آن حالت مرزی کران سینگلتون رخ دهد، یعنی داشته باشیم $k+d=n+۱$ یک کد MDS (کد تفکیک‌پذیر ماکسیمم فاصله) نامیده می‌شود.

تعریف ۱.۴.۱۶. حلقه: مجموعه‌ی R به همراه دو عمل جمع و ضرب را یک حلقه نامیم و با نماد $(R,+,.)$ نمایش می‌دهیم، هرگاه دارای خواص زیر باشد:

آ. R نسبت به عمل جمع یک گروه آبلی باشد:

۱. بسته بودن نسبت به عمل جمع

۲. شرکت‌پذیری نسبت به عمل جمع

۳. وجود عنصر خنثی نسبت به عمل جمع

۴. وجود عنصر وارون نسبت به عمل جمع

۵. نسبت به عمل جمع دارای خاصیت جابجایی باشد.

ب. R نسبت به عمل ضرب یک نیم گروه باشد:

۱. R نسبت به عمل ضرب بسته باشد.

۲. R نسبت به عمل ضرب شرکت‌پذیر باشد.

پ. خاصیت پخشی (توزیع‌پذیری) ضرب نسبت به جمع

$$\forall \quad a,b,c \in R \qquad a.(b+c) = a.b + a.c$$

تعریف ۱.۴.۱۷. حلقه‌ی جابجایی: اگر حلقه‌ی R نسبت به عمل ضرب دارای خاصیت جابجایی باشد آنگاه R را یک حلقه‌ی جابجایی می‌نامیم و در غیراین‌صورت حلقه‌ی R را حلقه‌ی ناجابجایی گوییم.

تعریف ۱.۴.۱۸. حلقه‌ای که دارای عنصر همانی ۱ باشد را یک حلقه‌ی یکدار نامیم و در غیراین‌صورت حلقه‌ی غیر یکدار نامیده می‌شود.

[۵] Singelton bound

تعریف ۱.۴.۱۹. میدان: یک حلقه‌ی جابجایی و یکدار که هر عنصر ناصفر آن دارای وارون ضربی باشد را یک میدان نامیم:

$$\forall\, a \neq 0 \in F \quad \exists\ a^{-1} \in F \qquad s.t \qquad a.a^{-1} = 1_F$$

مثال ۱.۴.۵. مجموعه‌ی اعداد حقیقی $\mathbb{R}$ مجموعه‌ی اعداد گویا $\mathbb{Q}$ و مجموعه‌ی اعداد مختلط $\mathbb{C}$ همگی میدان‌های نامتناهی می‌باشند.

تعریف ۱.۴.۲۰. فرض کنیم R یک حلقه‌ی جابجایی باشد دراین‌صورت زیر مجموعه‌ی I از R را یک ایده‌آل از R نامیم هرگاه دارای شرایط زیر باشد:

آ. برای هر دو عنصر دلخواه، a و b از I داشته باشیم $a-b \in I$ و $a+b \in I$.

ب. برای هر عنصر $r \in R$ و هر $a \in I$ داشته باشیم $ra \in I$ و $ar \in I$ (R جابجایی است) در این حالت می‌نویسیم $I \trianglelefteq R$.

تعریف ۱.۴.۲۱. فرض کنیم F یک میدان باشد. دراین‌صورت حلقه‌ی چندجمله‌ای‌ها روی میدان F، که با نماد $F[x]$ نمایش داده می‌شود، حلقه‌ای است که هر عنصر آن به فرم چندجمله‌ای

$$f(x) = a_0 + a_1 x^1 + \cdots + a_n x^n$$

می‌باشد، جایی‌که برای هر $0 \leq i \leq n$ داریم $a_i \in F$ و n را درجه‌ی چندجمله‌ای $f(x)$ نامیم. (a_n که ضریب پیشرو نامیده می‌شود ناصفر است) در حالت خاص که $a_n = 1$ باشد، چندجمله‌ای $f(x)$ را تکین[6] نامیم.

تعریف ۱.۴.۲۲. فرض کنیم $f(x)$ یک چندجمله‌ای از $F[x]$ باشد. دراین‌صورت ایده‌آل تولید شده توسط $f(x)$ را با نماد $I = \langle f(x) \rangle$ نمایش داده و به‌صورت زیر تعریف می‌کنیم:

$$I = \langle f(x) \rangle = \{ f(x)g(x) \mid g(x) \in F[x] \}.$$

ایده‌آل فوق را ایده‌آل اصلی تولید شده توسط $f(x)$ می‌نامند.

قضیه ۱.۴.۱. فرض کنیم

$$\Pi : F_q^n \longrightarrow \frac{F_q[x]}{\langle x^n - 1 \rangle}$$
$$(a_0, a_1, \ldots, a_{n-1}) \longrightarrow a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

تناظر دوسویی بین F_q^n و $\frac{F_q[x]}{\langle x^n-1 \rangle}$ باشد. دراین‌صورت زیر مجموعه‌ی ناتهی C از F_q^n یک کد دوری است اگر و تنها اگر $\Pi(C)$ ایده‌آلی از حلقه‌ی $\frac{F_q[x]}{\langle x^n-1 \rangle}$ باشد.

[6] Monic

قضیه ۲.۴.۱. فرض کنیم I ایده‌آلی ناصفر از حلقه‌ی خارج‌قسمتی $\frac{F_q[x]}{\langle x^n-1\rangle}$ باشد. همچنین فرض کنیم $g(x)$ چندجمله‌ای تکین ناصفر از درجه‌ی مینیمم در I باشد. دراین‌صورت $g(x)$ مولد ایده‌آل I بوده و $g(x)|x^n-1$.

تعریف ۲۳.۴.۱. الگوریتم تقسیم: فرض کنیم $a(x)$ و $b(x) \neq 0$ دو چندجمله‌ای در $F[x]$ باشند. دراین‌صورت چندجمله‌ای‌های یکتای $q(x)$ و $r(x)$ موجودند به‌گونه‌ای که داریم:

$$a(x) := b(x)q(x) + r(x)$$

که $deg(r(x)) < deg(b(x))$.

تعریف ۲۴.۴.۱. هم‌نهشتی: اگر یک عدد صحیح m تفاضل $a-b$ را عاد کند، می‌گوییم که a و b به‌پیمانه‌ی m هم‌نهشت هستند و می‌نویسیم $a \equiv b(mod\ m)$. اگر یک چندجمله‌ای $m(x)$ تفاضل $a(x)-b(x)$ را عاد کند، می‌گوییم که $a(x)$ و $b(x)$ به‌پیمانه‌ی $m(x)$ هم‌نهشت هستند و می‌نویسیم $a(x) \equiv b(x)(mod\ m(x))$.

تعریف ۲۵.۴.۱. تابع φ: تابع فی‌اویلر $\varphi(n)$ برابر تعداد اعداد صحیح مثبت کمتر از n است که نسبت به n اول است.

مثال ۶.۴.۱. $\varphi(۵) = ۴$ (اعداد ۱ و ۲ و ۳ و ۴ نسبت به ۵ اول هستند)
$\varphi(۴) = ۲$ (اعداد ۱ و ۳ نسبت به ۴ اول هستند)
می‌توان نشان داد که برای هر $n \geq ۲$،

$$\varphi(n) = n\prod_{p|n}(۱ - \frac{۱}{p}) = n\prod_{p|n}\frac{p-۱}{p}$$

که در آن ضرب روی تمام اعداد اول شمارنده‌ی n انجام می‌شود.
اگر p اول باشد $\varphi(p) = p-۱$ و همچنین برای اعداد صحیح مثبت m و n و با شرایط $(m,n) = ۱$ داریم:

$$\varphi(mn) = \varphi(m)\varphi(n)$$

قضیه ۳.۴.۱. در هر ایده‌آل ناصفر I از حلقه‌ی خارج‌قسمتی $\frac{F_q[x]}{\langle x^n-1\rangle}$، یک چندجمله‌ای (منحصربه‌فرد) تکین از درجه مینیمم وجود دارد که این چندجمله‌ای مولد ایده‌آل I می‌باشد.

قضیه ۴.۴.۱. هر مقسوم‌علیه تکین از $x^n-۱$ چندجمله‌ای مولدی برای یک کد دوری در F_q^n می‌باشد.

قضیه ۵.۴.۱. فرض کنیم $g(x)$ چندجمله‌ای مولد یک ایده‌آل از حلقه‌ی خارج‌قسمتی $\frac{F_q[x]}{\langle x^n-1\rangle}$ باشد. دراین‌صورت کد دوری متناظر با ایده‌آل فوق دارای بعد k می‌باشد هرگاه درجه‌ی $g(x)$ برابر با $n-k$ باشد.

تعریف ۱.۴.۲۶. عنصر α در میدان متناهی F_q را عنصر اولیه (مولد) نامیم هرگاه بتوان F_q را به فرم زیر نوشت:

$$F_q = \left\{ ۰, \alpha, \alpha^۲, \dots, \alpha^{q-۱} \right\}.$$

تعریف ۱.۴.۲۷. مرتبه‌ی یک عنصر ناصفر $\alpha \in F_q$ با نماد $ord(\alpha)$ نمایش داده می‌شود و برابر با کوچکترین عدد صحیح مثبت k می‌باشد به‌گونه‌ای که $\alpha^k = ۱$.

قضیه ۱.۴.۶. عنصر ناصفر α در میدان متناهی F_q اولیه است اگر و تنها اگر مرتبه‌ی α برابر $q-۱$ باشد $(ord(\alpha) = q-۱)$.

تعریف ۱.۴.۲۸. فرض کنیم n عددی باشد که نسبت به q اول باشد $((n,q) = ۱)$. هم‌دسته‌ی دایره‌بر[۷] qـ پیمانه‌ی n که شامل i می‌باشد به‌صورت زیر تعریف می‌شود:

$$C_i = \{ i.q^j (mod\ n) \ \mid \ j = ۰, ۱, ۲, ... \}.$$

دو هم‌دسته‌ی دایره‌بر یا مساوی می‌باشند و یا مجزا می‌باشند، لذا هم‌دسته‌های دایره‌بر $\mathbb{Z}_n$ را افراز می‌کنند.

مثال ۱.۴.۷. هم‌دسته‌های دایره بر ۲ به پیمانه‌ی ۱۵ را مشخص کنید.

$$C_i = \{ i.q^j (mod\ n) \ \mid \ j = ۰, ۱, ۲, ... \} \qquad q = ۲ \quad n = ۱۵$$

$$C_۰ = \{ ۰ \}$$

$$C_۱ = \{ ۱ \cdot ۲^j (mod\ ۱۵) \ \mid \ j = ۰, ۱, ۲, ... \} = \{ ۱, ۲, ۴, ۸ \} \Longrightarrow C_۱ = C_۲ = C_۴ = C_۸$$

$$C_۳ = \{ ۳ \cdot ۲^j (mod\ ۱۵) \ \mid \ j = ۰, ۱, ۲, ... \} = \{ ۳, ۶, ۹, ۱۲ \} \Longrightarrow C_۳ = C_۶ = C_۹ = C_{۱۲}$$

$$C_۵ = \{ ۵ \cdot ۲^j (mod\ ۱۵) \ \mid \ j = ۰, ۱, ۲, ... \} = \{ ۵, ۱۰ \} \Longrightarrow C_۵ = C_{۱۰}$$

$$C_۷ = \{ ۷ \cdot ۲^j (mod\ ۱۵) \ \mid \ j = ۰, ۱, ۲, ... \} = \{ ۷, ۱۴, ۱۱, ۱۳ \} \Longrightarrow C_۷ = C_{۱۱} = C_{۱۳} = C_{۱۴}$$

$$\bigcup_{i=۰}^{۱۴} C_i = \mathbb{Z}_{۱۵}.$$

قضیه ۱.۴.۷. فرض کنیم α یک عنصر اولیه از میدان متناهی F_q^m باشد. دراین‌صورت چندجمله‌ای مینیمال α^i نسبت به میدان F_q به‌صورت

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

می‌باشد. جایی‌که C_i هم‌دسته‌ی دایره‌بر منحصربه‌فرد q شامل i به پیمانه‌ی $q^n - ۱$ می‌باشد.

[۷] Cyclotomic

۱.۴.۱ کدهای BCH و RS

متداول‌ترین کدهای دوری تصحیح خطایی که امروزه مورد استفاده قرار می‌گیرند کدهای BCH و RS هستند.
کد BCH نام خود را از حرف اول نام سه نفری[۸] که در سال‌های ۱۹۵۹ و ۱۹۶۰ آن را معرفی کردند، گرفته شده است. معرفی این کدها در حقیقت معرفی کدهایی روی $GF(۲)$ بود که امکان طراحی با فاصله‌ی کمینه مشخص را فراهم می‌کنند. کد RS[۹] نیز که نام آن از حرف اول نام مخترعان آن گرفته شده است، در سال ۱۹۶۰ منتشر شد.

۲.۴.۱ طراحی کدهای BCH

کدهای BCH کدهای دوری هستند و لذا می‌توان آنها را با استفاده از چندجمله‌ای سازنده، مشخص کرد. یک کد BCH به طول n بر روی $GF(q)$ و با قابلیت تصحیح دست‌کم t خطا به‌صورت زیر ساخته می‌شود:

۱ـ کوچکترین مقدار n را انتخاب می‌کنیم که به ازای آن میدان $GF(q^m)$ دارای ریشه‌ی nام و اولیه‌ی یکه باشد. این ریشه را α می‌نامیم.

۲ـ یک عدد صحیح غیرمنفی b را انتخاب می‌کنیم. معمولاً $b = ۱$ را انتخاب می‌کنیم.

۳ـ فهرست $۲t$ توان متوالی α را می‌نویسیم:

$$\alpha^b, \alpha^{b+۱}, \ldots, \alpha^{b+۲t-۱}$$

چندجمله‌ای کمین هر یک از این توان‌های α را بر روی $GF(q)$ می‌یابیم. به دلیل مزدوج بودن برخی عناصر، معمولاً همه‌ی این چندجمله‌ای‌ها متمایز نیستند.

۴ـ چند جمله‌ای سازنده‌ی $g(x)$ برابر کوچکترین مضرب مشترک این چندجمله‌ای‌های کمین است. کد حاصل، یک کد دوری $(n, n - deg(g(x)))$ است.

تعریف ۲۹.۴.۱. اگر در فرآیند ساخت کد BCH داشته باشیم $b = ۱$، این کد، کد تشخیص محدود[۱۰] نامیده می‌شود. اگر رابطه‌ی $n = q^m - ۱$ برقرار باشد به کد BCH اولیه گفته می‌شود.

۳.۴.۱ کران BCH

فرض کنید C یک $[n, k]$ ـ کد دوری با الفبای q ـ تایی و دارای چندجمله‌ای مولد $g(x)$ باشد. همچنین فرض کنید که $GF(q^m)$ کوچکترین میدان توسعه‌یافته از میدان $GF(q)$ باشد که

[8] Base, Ray- Chaudhari, and Hocquenghem
[9] Reed- Soloman
[10] Narrow sense

شامل یک ریشه‌ی nام و اولیه یکه به نام α است. فرض کنید $g(x)$ یک چندجمله‌ای با درجه‌ی کمینه در $GF(q)[x]$ است که تا ۲ توان متوالی α را به‌عنوان ریشه دارد یعنی:

$$g(\alpha^q) = g(\alpha^{b+1}) = g(\alpha^{b+2}) = \cdots = g(\alpha^{b+2t-1}).$$

دراین‌صورت فاصله‌ی کمینه‌ی کد در رابطه‌ی $d_{min} > \delta = 2t + 1$ صدق می‌کند. به عبارت دیگر چنین کدی قابلیت تصحیح دست‌کم t خطا را دارد.

۴.۴.۱ کدهای RS

یک کد q^m RS ـ تایی، کد q^m BCH ـ تایی از طول $q^m - 1$ و تولید شده توسط

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \dots (x - \alpha^{b+\delta-2})$$

می‌باشد، جایی‌که $b \geq 0$ و $2 \leq \delta \leq q - 1$ و α عنصری اولیه از F_q است. در $g(x)$ هیچ ریشه‌ی اضافه‌ای نداریم و لذا درجه‌ی آن برابر $2t$ است. بنابراین برای یک کد RS داریم $n - k = 2t$. فاصله‌ی کد برابر $\delta = n-k+1$ می‌باشد. معمولاً کد RS را در حالت دودویی در نظر نمی‌گیریم، زیرا در این حالت $q - 1 = 1$، یعنی طول ۱ را داریم.

لم ۱.۴.۱. فاصله‌ی کمینه‌ی یک $[n, k]$ ـ کد RS برابر $d_{min} = n - k + 1$ است.

مثال ۸.۴.۱. کد RS، ۷ـ تایی از طول ۶ با چند جمله‌ای مولد

$$g(x) = (x - 3)(x - 3)^2 = 6 + x + 3x^2 + x^3$$

را در نظر بگیرید. این کد یک $[6, 3]$ ـ کد دوری ۷ آرایه‌ای می‌باشد. ماتریس مولد این کد به فرم

$$G = \begin{pmatrix} 6 & 1 & 3 & 1 & 0 & 0 \\ 0 & 6 & 1 & 3 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{pmatrix}_{3\times 6}$$

می‌باشد و ماتریس کنترل توازن آن به فرم

$$H = \begin{pmatrix} 1 & 4 & 1 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 1 & 0 \\ 0 & 0 & 1 & 4 & 1 & 1 \end{pmatrix}$$

می‌باشد که از معادله زیر بدست آمده است.

$$h(x) = \frac{x^6 - 1}{g(x)} \quad , \quad h(x) = 1 + x + 4x^2 + x^3$$

فاصله‌ی کد برابر ۴ می‌باشد، زیرا (کد C دارای فاصله‌ی بزرگتر یا مساوی d است اگر و تنها اگر هر $d - 1$ ستون از H مستقل خطی باشد). لذا کد فوق یک $[6, 3, 4]$ ـ کد دوری ۷ـ تایی می‌باشد که بوضوح یک کد MDS می‌باشد.

فصل ۲

مجموعه‌ای از کدهای MDS حاصل از خودتوان‌ها و یکه‌ها

۱.۲ مقدمه

یک $[n,r,d]$ ـ کد خطی، یک کد از طول n، بعد r و فاصله‌ی d می‌باشد. با استفاده از کران سینگلتون، ماکسیمم مقدار d برابر $(n-r+1)$ می‌باشد. همچنین یک کد MDS به‌صورت یک $[n,r,n-r+1]$ ـ کد تعریف می‌شود که معادل کدی به فرم $[n,n-r,r+1]$ می‌باشد. در این فصل مجموعه‌ای از کدهای MDS بررسی می‌شوند. با استفاده از نتایج چبوتارو و روش کدگذاری یکتا ما قادریم که یک مجموعه از کدهای MDS را روی $\mathbb{C}$ با استفاده از ماتریس فوریه بسازیم.

مجموعه بردارهای $S=\{e_1,\ldots,e_{n-1}\}$ در K^n روی میدان‌های گوناگون k و n اول به‌دست می‌آیند به‌طوری‌که هر r عضو از S یک $[n,r,n-r+1]$ ـ کد تولید می‌کند. برای r داده شده $\binom{n}{r}$ انتخاب وجود دارد که طبق تعریف کد S، هر کدام متفاوت می‌باشند.

مجموعه‌هایی از ماتریس‌های خودمتعامد $T=\{E_0,E_1,\ldots,E_{s-1}\}$ در $K_{n\times n}$ روی میدان K تعریف شده‌اند به‌طوری‌که $\{E_j \mid j\in J\}$ مولدهای یک $[n,r]$ ـ کد می‌باشند جایی‌که $J\subseteq I=\{0,1,\ldots,s-1\}$ و $r=\sum_{j\in J} rankE_j$.

در موارد خاص زمانی‌که $s = n$ و n نیز اول باشند، نشان داده می‌شود که کد، MDS می‌باشد. کدهای MDS با استفاده از خودمتعامد بودن روی حلقه‌ی گروه‌های دوری به‌دست آمده است که ممکن است با تبدیل فوریه مقایسه شوند. صفرهایی در K موقعیت مشخص که لزومی ندارد پشت سرهم باشند.
یکی از ویژگی‌های کدهای MDS این است که این کدها روی میدان‌های متناهی F_p که p یک عدد اول است به‌دست می‌آیند و در محاسبات پیمانه‌ای مورد استفاده قرار می‌گیرند.
بعد و فاصله‌ی فضای اصلی به‌وسیله‌ی یک زیرمجموعه‌ی S راحت‌تر مشخص می‌شود و پیدا کردن زوج‌های tـ تصحیح‌کننده‌ی خطا در بسیاری از $[n, r, n-r+1]$ ـ کدها برای t ماکزیمم $(t = \frac{n-r}{2})$ ممکن می‌شود.

۲.۲ کدهای حاصل از یکه‌ها

فرض کنید R یک حلقه و $R_{n\times n}$ حلقه‌ی تمام ماتریس‌های $n \times n$ روی R و $UV = I$ در $R_{n\times n}$ باشد. U را به دو ماتریس بلوکی A و B به‌صورت $U = \begin{pmatrix} A \\ B \end{pmatrix}$ تقسیم کنید به‌طوریکه A یک ماتریس $r \times n$ و B یک ماتریس $(n-r) \times n$ باشند. به‌صورت مشابه V را به دو قسمت C و D که $V = \begin{pmatrix} C & D \end{pmatrix}$ تقسیم کنید جایی‌که C یک ماتریس $n \times r$ و D یک ماتریس $(n, n-r)$ می‌باشد.
حال چون $UV = I$ لذا داریم $AD = 0$. به‌آسانی نشان داده می‌شود که A مولد یک $[n, r]$ ـ کد می‌باشد و D^T یک ماتریس کنترل توازن برای این کد می‌باشد.
فرض کنید که $\{u_1, \ldots, u_n\}$ سطرهای U و $\{v_1, \ldots, v_n\}$ ستون‌های V باشد. سطر $\{u_{i1}, \ldots, u_{ir}\}$ از U را طوری انتخاب می‌کنیم که مولد ماتریس A باشد که از اندازه‌ی $r \times n$ می‌باشد و رتبه‌ی آن r است. فرض کنید $K = \{1, 2, \ldots, n\}$ و $L = \{i_1, i_2, \ldots, i_r\}$ و $J = (K - L)$.
ماتریس D را ستون‌های $S = \{v_j \mid j \in J\}$ انتخاب می‌کنیم. بنابراین رتبه‌ی D، برابر $n-r$ می‌باشد و اندازه‌ی آن $n \times (n-r)$ می‌باشد و D^T یک ماتریس کنترل توازن برای $[n, r]$ ـ کد اصلی A می‌باشد. (r ردیفی از U که برای ساختن A استفاده می‌شود معمولاً به ترتیب گرفته می‌شود اما این ضروری نیست. ماتریس D از ستون‌های بردارهای S با هر ترتیبی ساخته می‌شود اما معمولاً یک ترتیب نرمال از عضوهای S استفاده می‌شود) این کدها خطی می‌باشند ولی در حقیقت ایده‌آل نمی‌باشند.
بنابراین هر ردیفی از U برای ساختن ماتریس مولد یک کد ممکن است مورد استفاده قرار گیرد و سپس با ستون‌هایی از V برای به‌دست آوردن ماتریس کنترل توازن مورد مطابقت قرار می‌گیرند. در نتیجه چون اندازه $n \times n$ می‌باشد $\binom{n}{r}$ انتخاب برای یک $[n, r]$ ـ کد وجود دارد که هر کد نیز متفاوت می‌باشد. در حقیقت این کدها نسبت به آنچه در لم ۱.۲.۲ نشان

داده شده است متفاوت می‌باشند. (یک فضای برداری X زیرفضایی از فضای مولد است که به‌وسیله‌ی X تعریف می‌شود).

لم ۱.۲.۲. فرض کنید T یک مجموعه از بردارهای مستقل خطی باشد و $S \subseteq T$ و $W \subseteq T$. دراین‌صورت

$$\langle S \rangle \cap \langle W \rangle = \langle S \cap W \rangle.$$

اثبات. مستقیماً از مستقل خطی بودن S و W به‌دست می‌آید. □

فرض کنید $UV = ۱$ در $R_{n\times n}$ هر r ردیف از U را در نظر بگیرید و ماتریس مولد U_r را بسازید. سپس طبق تعریف $(n-r)$ ستون از V را در نظر بگیرید و ماتریس کنترل توازن V_{n-r} را بسازید و یک $[n,r]$ ـ کد تعریف کنید. این کد را با نماد C_r مشخص کنید.
اگر ماتریس V دارای این خاصیت باشد که دترمینان هر زیر ماتریس مربعی از V غیرصفر باشد، دراین‌صورت چنین کدی یک $[n,r,n-r+۱]$ ـ کد MDS می‌باشد.

قضیه ۱.۲.۲. کد C شامل یک کد واژه‌ی غیرصفر با وزن همینگ W یا کمتر است اگر و تنها اگر یک مجموعه متشکل از Wتا ستون از ماتریس H وابسته‌ی خطی باشد.

نتیجه ۱.۲.۲. اگر H یک ماتریس کنترل توازن برای کد خطی C باشد، دراین‌صورت مینیمم فاصله‌ی کد C برابر است با کمترین تعداد از ستون‌های H که وابسته‌ی خطی باشد.

قضیه ۲.۲.۲. فرض کنید دترمینان هر زیرماتریس مربعی از V غیرصفر باشد دراین‌صورت هر کد C_r فاصله‌ی $(n-r+۱)$ را دارد و بنابراین یک $[n,r,n-r+۱]$ ـ کد MDS می‌باشد.

اثبات. به‌وسیله‌ی قضیه‌ی ۱.۲.۲ و نتیجه‌ی ۱.۲.۲ اثبات می‌شود که هر زیرماتریس $(n-r)\times(n-r)$ از V دترمینان غیرصفر دارد. □

انتخاب هر r ردیف از U به ما اجازه می‌دهد که $[n,r]$ ـ کدهای متفاوت زیادی بسازیم که در سیستم واحد $UV = I_{(n\times n)}$ و زمانی که V در شرایط قضیه ۲.۲.۲ صدق کند هر کد MDS نیز می‌باشد.

تعریف ۱.۲.۲. ماتریس فوریه[1]: فرض کنید α یک ریشه‌ی nـام اولیه روی میدان K باشد به‌طوری‌که معکوس آن روی n وجود داشته باشد. ماتریس فوریه $n\times n$ روی K به‌صورت زیر تعریف می‌شود:

$$F_n = \begin{bmatrix} ۱ & ۱ & ۱ & \cdots & ۱ \\ ۱ & \alpha & \alpha^{۲} & \cdots & \alpha^{(n-۱)} \\ ۱ & \alpha^{۲} & \alpha^{۴} & \cdots & \alpha^{۲(n-۱)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ ۱ & \alpha^{(n-۱)} & \alpha^{۲(n-۱)} & \cdots & \alpha^{(n-۱)(n-۱)} \end{bmatrix}$$

[1] Fourier

و معکوس F_n نیز به این صورت است:

$$F_n^* = \frac{1}{n}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{-(n-1)} & \alpha^{-2(n-1)} & \cdots & \alpha^{-(n-1)(n-1)} \end{bmatrix}$$

(α^{-1} یک ریشه‌ی nـام اولیه‌ی واحد می‌باشد و ماتریس nF_n^* با یک ماتریس فوریه روی K مطابقت دارد).

قضیه ۳.۲.۲. قضیه‌ی چبوتارو[2]: فرض کنید $w \in \mathbb{C}$ یک ریشه ی pـام اولیه‌ی واحد باشد جایی‌که p عددی اول است و فرض کنید V ماتریس فوریه‌ای باشد که درایه‌ی (i,j) ـام آن برابر با w^{ij} باشد که $0 \leq i,j \leq p-1$. و دراین‌صورت همه‌ی زیرماتریس‌های مربعی از V دترمینان غیرصفر دارند.

فرض کنید که F_n ماتریس $n \times n$ فوریه روی $\mathbb{C}$ باشد و $F_nF_n^* = I_n$. در این‌جا nF_n^* ترانهاده‌ی توأم مختلط از F_n می‌باشد. ما می‌توانیم کدهای یکتایی با استفاده از F_n یکتا تعریف نماییم. (با nF_n^* یکتا)

فرض کنید C_r یک $[n,r]$ ـ کد به‌دست آمده یکتا باشد جایی‌که C_r با استفاده از هر r ردیف از F_n تعریف شده باشد و ماتریس توازن مستقیماً از F_n^* به‌دست آمده باشد که در مورد آن توضیح دادیم. ماتریس توازن ممکن است مستقیماً از nF_n^* به‌دست آمده باشد که این غالباً راحت‌تر می‌باشد.

قضیه ۴.۲.۲. فرض کنید n اول باشد، و C_r کدی باشد که با r ردیف از ماتریس فوریه ساخته شود.

دراین‌صورت فاصله‌ی کد C_r، برابر $(n-r+1)$ می‌باشد.

اثبات. با استفاده از قضیه‌ی ۲.۲.۲ دترمینان هر زیرماتریس مربعی از V غیرصفر می‌باشد و با استفاده از قضیه‌ی چبوتارو حکم ثابت می‌شود. □

بنابراین متناظر با هر C_r یک $[n,r,n-r+1]$ ـ کد MDS موجود می‌باشد زمانی‌که n اول باشد هر مجموعه از r ردیف F_n ممکن است مورد استفاده قرار گیرد. برای ساختن یک $[n,r,n-r+1]$ ـ کد MDS، $\binom{n}{r}$ تا $[n,r,n-r+1]$ ـ کد MDS متفاوت وجود دارد که از F_n یکتا به‌دست می‌آیند.

کدهای دوری با استفاده از مجموعه‌های متعامد کامل و مستقل به ماتریس فوریه به‌دست

[2] Chebotarev

آمده در بخش ۳ـ۳ مربوط می‌شوند و این باعث می‌شود که ساختن مجموعه کدهای MDS روی $\mathbb{R}$ آسانتر شود. در بخش ۳ـ۲ به ساخت مجموعه‌ای از کدهای MDS روی میدان‌های متناهی می‌پردازیم و در بخش ۳ـ۳ مجموعه‌ای از کدهای دوری ساخته شده‌اند.

مثال ۱.۲.۲. فرض کنید w یک ریشه ی ۷ـام اولیه‌ی واحد در C باشد.

$$F_۷ = \begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & w & w^۲ & w^۳ & w^۴ & w^۵ & w^۶ \\ ۱ & w^۲ & w^۴ & w^۶ & w & w^۳ & w^۵ \\ ۱ & w^۳ & w^۶ & w^۲ & w^۵ & w & w^۴ \\ ۱ & w^۴ & w & w^۵ & w^۲ & w^۶ & w^۳ \\ ۱ & w^۵ & w^۳ & w & w^۶ & w^۴ & w^۲ \\ ۱ & w^۶ & w^۵ & w^۴ & w^۳ & w^۲ & w \end{pmatrix}$$

فرض کنید $C_۴$ کد مولدی باشد که به‌وسیله‌ی ماتریس A به‌دست آمده باشد:

$$A = \begin{pmatrix} ۱ & w & w^۲ & w^۳ & w^۴ & w^۵ & w^۶ \\ ۱ & w^۲ & w^۴ & w^۶ & w & w^۳ & w^۵ \\ ۱ & w^۵ & w^۳ & w & w^۶ & w^۴ & w^۲ \\ ۱ & w^۶ & w^۵ & w^۴ & w^۳ & w^۲ & w \end{pmatrix}$$

A دارای رتبه‌ی ۴ می‌باشد. ماتریس توازن برای $C_۴$ به‌صورت زیر است که دارای رتبه‌ی ۳ می‌باشد.

$$\begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & w^۴ & w & w^۵ & w^۲ & w^۶ & w^۳ \\ ۱ & w^۳ & w^۶ & w^۲ & w^۵ & w & w^۴ \end{pmatrix}$$

کد $C_۴$ یک $[۷, ۴, ۴]$ ـ کد می‌باشد. در واقع $\binom{۷}{۴} = ۳۵$ کد متفاوت ممکن است از $F_۷$ استخراج شود.

۳.۲ میدان‌های متناهی

در مورد میدان‌های متناهی این صدق نمی‌کند که در تمام مواردی‌که n اول باشد ماتریس فوریه F_n وجود داشته باشد و هر زیرماتریس مربعی آن دترمینان غیرصفر داشته باشد. هدف آن است تا در میدان‌های متناهی K و p اولی را پیدا کنیم که ماتریس فوریه F_p و هر زیرماتریس مربعی آن دترمینان غیرصفر داشته باشد.

برای اینکه ماتریس فوریه $p \times p$ روی K وجود داشته باشد لازم‌است که $K \nmid p$ و $p|(q-1)$ جایی‌که q مرتبه‌ای از میدان K است.

گوییم ماتریس مربعی M روی میدان K دارای ویژگی چبوتارو است اگر دترمینان هر زیرماتریس مربعی از آن غیرصفر باشد.

اگر مشخصه K صفر باشد، ماتریس فوریه‌ی F_n روی K برای یک n اول دارای ویژگی چبوتارو می‌باشد.

$F[G]$ نشان‌دهنده‌ی حلقه‌ی گروهی، گروه G روی میدان F می‌باشد. فرض کنید z یک مولد برای گروه دوری G از مرتبه‌ی اول p باشد. هر بردار $v \in F[G]$ یک فرم منحصربه‌فرد $f(z)$ دارد. جایی‌که $f \in F[X]$ و $degf < p$. مقدار $t = t(v)$ برابر $|supp(v)|$ می‌باشد که دقیقاً ضرایب غیرصفر چندجمله‌ای f می‌باشند و این عدد به‌صورت $t(f)$ نوشته می‌شود.

دراین‌صورت $d(v)$ بعد فضای ایجاد شده توسط V را نشان می‌دهد.

اگر K یک میدان حاوی یک ریشه‌ی pـام اولیه واحد باشد، دراین‌صورت نتیجه‌ی قضیه‌ی چبوتارو روی K معادل با این است که $t(v) + d(v) > p$ برای همه‌ی بردارهای غیرصفر $v \in K[G]$.

قضیه ۱.۳.۲. فرض کنید $G = \langle Z \rangle$ یک گروه از مرتبه‌ی اول p باشد و فرض کنید $v \in K[G]$ غیرصفر باشد جایی‌که K یک میدان دلخواه است. $v = f(z)$ جایی‌که $f \in K[X]$ و $degf < p$.

دراین‌صورت $t(v) + d(v) \leq p$ اگر و تنها اگر $t(f) \leq degh$ ، جایی‌که

$$h(x) = gcd(x^p - 1, f(x)).$$

قابل ذکر است که نمونه‌های داده شده در مقاله [۷] صفحات (۴۰۳۴ـ۴۰۳۵) با استفاده از قضیه‌ی چبوتارو با مقدار p و q اول که q به پیمانه‌ی p کمتر از $\phi(p) = p - 1$ باشد با شکست مواجه می‌شود. این باید با لم ۱.۴.۲ مقایسه شود. ما به میدان‌های متناهی K و pهای اولی علاقه‌مندیم که ماتریس فوریه روی K وجود داشته باشد و در شرایط چبوتارو صدق نماید. در مقاله‌ی [۸] بحث زیادی شده است تا نشان داده شود که برای هر p اول، کاراکترهای متناهی زیادی وجود دارد که چبوتارو می‌تواند شکست بخورد.

در قضیه‌ی ۳.۲.۲ دترمینان همه‌ی زیرماتریس‌های مربعی از ماتریس جامع $[\delta_{ij}]$ بررسی شده‌اند. این عددها صحیح می‌باشند و با استفاده از قضیه‌ی چبوتارو غیرصفر می‌باشند و همچنین اصل

بر غیرصفر بودن آن‌ها است.
باید به‌وضوح مشخص شود که کاراکترهایی که نتیجه‌ی چبوتارو را با شکست مواجه می‌کند دقیقاً همان اول‌هایی هستند که حداقل یکی از این اعداد صحیح را تقسیم کرده و واضح است که فقط مقدار کمی از این اول‌ها وجود دارد.

۴.۲ ماتریس فوریه روی میدان‌های متناهی

برای ساختن ماتریس فوریه F_n روی $GF(q)$ لازم است که $n|(q-1)$.
برای مقادیر p و t اول و غیرمساوی، به‌وسیله‌ی قضیه‌ی فرمتس[3] $p|(t^{\phi(p)}-1)$.
چون p اول می‌باشد بنابراین $\phi(p)=p-1$. ما به دنبال $p-1$ هایی با کمترین توان r هستیم که $p|(t^r-1)$.
برای داده‌های t و p اول و نامساوی داده شده، یک میدان $GF(t^r)$ وجود دارد که $p|(t^r-1)$ و روی این میدان ماتریس فوریه F_p وجود دارد.
فرض کنید که p و q اول و نامساوی $(p\neq q)$ باشند و $K=GF(q^{\phi(p)})$ دراین‌صورت

$$p|(q^{\phi(p)}-1)$$

و ماتریس فوریه F_p روی K وجود دارد.

لم ۱.۴.۲. فرض کنید که p و q اول و نامساوی باشند. همچنین فرض کنید که رتبه‌ی q به پیمانه‌ی p برابر $\phi(p)=p-1$ می‌باشد. دراین‌صورت چندجمله‌ای $(x^{p-1}+x^{p-2}+\cdots+x+1)$ روی $GF(q)$ تفکیک‌پذیر می‌باشد.

اثبات. واضح است که فاکتورهای چندجمله‌ای $\phi_n(x)$ روی میدان متناهی $GF(q)$ یک چندجمله‌ای تفکیک‌ناپذیر از درجه‌ی r می‌باشد. جایی‌که مرتبه‌ی r از q به پیمانه‌ی n است. در این‌جا

$$\phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

و $r=\phi(p)=p-1=deg(\phi_p(x))$. بنابراین $\phi_p(x)$ تفکیک‌ناپذیر است. □

قضیه ۱.۴.۲. فرض کنید که p و q اول و نامساوی باشند و $K=GF(q^{\phi(p)})$. فرض کنید که مرتبه‌ی q به پیمانه‌ی p، برابر $\phi(p)$ باشد. در این‌جا چندجمله‌ای

$$f(x)=(x^{p-1}+x^{p-2}+\cdots+x+1)$$

روی $GF(q)=Z_q$ تفکیک‌ناپذیر است. دراین‌صورت ماتریس فوریه‌ی F_p روی K وجود دارد و در شرایط چبوتارو صدق می‌کند.

[3] Fermat's litlle

اثبات. توجه کنید که قبلاً اشاره شد که F_p وجود دارد. حال

$$GF(q^{\phi(p)}) \cong GF(q)[\alpha] \cong Z_q[\alpha] \cong \frac{Z_q[x]}{(f(x))}$$

جایی‌که α، $cofactor\ x+(f(x))$ است. برای w که یک ریشه‌ی pـام اولیه‌ی واحد درون C است داریم:

$$z[w] \cong \frac{z[y]}{(f(y))}$$

با این روش بدیهی است که

$$z[w] \cong \frac{z[y]}{(f(y))} \longrightarrow \frac{z_q[x]}{(f(x))} = GF_{(q)}[\alpha]$$

در این روش هسته‌ی چندجمله‌ای‌ها از درجه‌ای پایین‌تر از p در y می‌باشد و همه‌ی ضرایب بر q بخش‌پذیرند. (هر ضریب مشترک به‌وسیله q قابل تقسیم است) این روش ممکن است به‌صورت زیر بیان شود:

$$\frac{z[y]}{(f(y))}[z] \longrightarrow \frac{z_q[x]}{(f(x))}[z]$$

حال فرض کنید $g(z) \in \frac{z_q[x]}{(f(x))} \neq ۰$ که در آن $deg\ g < p$. فرض کنید $h(z) = gcd(g(z), z^p - ۱)$ ، ما نشان می‌دهیم که $t(g(z)) > deg\ h$ و دراین‌صورت قضیه ۱.۳.۲ به کار برده می‌شود.
اگر $h(z) = ۱$ دراین‌صورت این بدیهی است. به یاد داشته باشید که $t(g(z))$ پایه‌ای از $g(z)$ می‌باشد. ملاحظه می‌فرمایید که:

$$\widehat{g}(z) \in \frac{z[y]}{(f(y))}[z] \subset \frac{Q[y]}{(f(y))}[z]$$

با پیش فرض ضرایب $g(z)$ ضرایب $\widehat{g}(z)$ است. حال فرض کنید

$$\widehat{h} = gcd(\widehat{g}(z), z^p - ۱).$$

در $\frac{z[y]}{(f(y))}[z]$. دراین‌صورت به‌وسیله‌ی قضیه‌ی ۱.۳.۲ داریم: $t(\widehat{g}) > deg\widehat{h}$.
حال $\frac{z[y]}{(f(y))} = z[w]$ جایی‌که w یک ریشه‌ی pـام اولیه‌ی واحد درون C می‌باشد و $\frac{z_q[x]}{(f(x))} = z_q[\alpha]$ ، جایی‌که α یک ریشه‌ی pـام اولیه‌ی واحد در z_q می‌باشد. لذا داریم:

$$z^p - ۱ = \prod_{i=۰}^{p-۱}(z - w^i) \ \ in\ z[w] \quad , \quad z^p - ۱ = \prod_{i=۰}^{p-۱}(z - \alpha^i) \ \ in\ GF(q^{p-۱}) = z_q[\alpha]$$

بنابراین در $z_q[\alpha]$

$$gcd(g(z), z^p - ۱) = \prod_{j \in J}(z - \alpha_j) = h(z)$$

جایی‌که J زیرمجموعه‌هایی مناسب از $I = \{۰, ۱, \ldots, p-۱\}$ می‌باشد. در $z[w]$ داریم:

$$gcd(\widehat{g}(z), z^p - ۱) = \prod_{j \in J}(z - w_j) = \widehat{h}(z)$$

در این‌جا $deg\widehat{h}(z) = deg\ h(z)$ و دراین‌صورت داریم:

$$t(\widehat{g}(z)) = t(g(z)) \quad , \quad deg\ \widehat{h}(z) = deg\ h(z)$$

و $t(\widehat{g}) > deg\ \widehat{h}$ که دراین‌صورت $t(g(z)) > deg\ h(z)$.
حال به‌وسیله‌ی قضیه‌ی ۱.۳.۲ ماتریس فوریه F_p روی $GF(q^{\phi(p)})$ در شرایط چبوتارو صدق می‌کند. □

بنابراین میدان‌های $GF(q^{\phi(p)})$ با p و q اول و غیرمساوی $p \neq q$ جایی‌که مرتبه‌ی q به پیمانه‌ی p، $\phi(p) = p - ۱$ می‌باشد و جایی‌که $x^{p-۱} + x^{p-۲} + \cdots + ۱$ روی $GF(q)$ تفکیک‌ناپذیر باشد، همان ماتریس فوریه F_p روی $GF(q^{\phi(p)})$ می‌باشد که شرایط (خاصیت) چبوتارو را تصدیق می‌نماید.

تعریف ۱.۴.۲. فرض کنیم p یک عدد اول باشد. در این‌صورت اگر $۲p + ۱$ نیز عددی اول باشد، آنگاه عدد p را اول ژرمین[۴] نامیده و عدد اول $۲p + ۱$ متناظر با آن را عدد اول ایمن می‌نامیم.

گزاره ۱.۴.۲. فرض کنید p و $q = ۲p + ۱$ اول باشد. دراین‌صورت ماتریس فوریه F_p روی $GF(q)$ وجود دارد و در شرایط چبوتارو صدق می‌نماید.

اثبات. $p|q-۱$ و مرتبه‌ی q به پیمانه‌ی ۱، p می‌باشد. فرض کنید α عضوی از مرتبه‌ی $۲p = q-۱$ در $GF(q)$ باشد. بنابراین $\alpha^۲$ مرتبه (رتبه) p دارد و ماتریس فوریه F_p روی $GF(q)$ وجود دارد و می‌تواند به‌وسیله‌ی توانی از $\alpha^۲$ ساخته شود. فرض کنید که $f(x)$ یک چندجمله‌ای از درجه‌ی کمتر از p باشد. واضح است که

$$gcd((x^p - ۱), f(x)) = h(x)$$

در $GF(q)$ می‌باشد. حال در $GF(q)$ داریم:

$$x^p - ۱ = \prod_{i=۰}^{p-۱}(x - \alpha^{۲i})$$

که هر $\alpha^{۲i}$، $۰ \leqslant i \leqslant (p-۱)$ یک ریشه از $x^p - ۱$ می‌باشد. بنابراین:

$$h(x) = gcd((x^p - ۱), f(x)) = \prod_{j \in J}(x - \alpha^{۲j})$$

جایی‌که $J \subseteq \{۰, ۱, \ldots, p-۱\}$. حال فرض کنید که w یک ریشه‌ی pـام اولیه‌ی واحد باشد. $(x^p - ۱)$ و $f(x)$ چندجمله‌ای در $Z[x]$ می‌باشند. هم‌اکنون $t(f)$ در $GF(q)$ را در نظر بگیرید. ضرایب $t(f)$ در $Z[x]$ می‌باشد. بنابراین

$$gcd((x^p - ۱), f(x)) = h(x)$$

[4] Germaine Prime

و این یعنی $t(f) > deg\ h(x)$ برای هر عضو درون $Z[x]$. حال $h(x) = \prod_{j\in J}(x - w^j)$ برای $\widehat{J} \subseteq \{۰, ۱, \ldots, (p-۱)\}$. دراین‌صورت $\widehat{J} = J$ و بنابراین $deg(h(x))$ در $C[x]$ باید همانند درجه $deg\ h(x)$ در $GF(q)[x]$ باشد. بنابراین ماتریس فوریه F_p روی $GF(q)$ در شرایط چبوتارو صدق می‌نماید. □

ماتریس‌های فوریه موارد زیر نسبتاً خوب می‌باشند و آنها شامل اعداد صحیح به پیمانه‌ی یک q اول می‌باشند.

مثال ۱.۴.۲. یک نرم‌افزار جبری کامپیوتر نظیر GAP[۷]، $MAPLE$ یا $MATLAB$ برای محاسبات مناسب می‌باشد. یک ماتریس دوری به فرم

$$\begin{bmatrix} a_۰ & a_۱ & \cdots & a_{n-۱} \\ a_{n-۱} & a_۰ & \cdots & a_{n-۲} \\ \vdots & \vdots & \vdots & \vdots \\ a_۱ & a_۲ & \cdots & a_۰ \end{bmatrix}$$

می‌باشد. بنابراین با مشخص بودن اولین ردیف $(a_۰, a_۱, \ldots, a_{n-۱})$ ماتریس دوری با شیفت $(a_۰, a_۱, \ldots, a_{n-۱})$ مشخص می‌شود.

۱.۴.۲ $GF(۲^r)$

۱ـ $GF(۲^۲)$:

رتبه‌ی ۲ به پیمانه‌ی ۳ برابر ۲ می باشد و چندجمله‌ای $(x^۲ + x + ۱)$ روی $Gf(۲)$ تفکیک‌ناپذیر می‌باشد. بنابراین

$$F_۳ = \begin{pmatrix} ۱ & ۱ & ۱ \\ ۱ & w & w^۲ \\ ۱ & w^۲ & w \end{pmatrix}$$

خاصیت چبوتارو را دارد جایی‌که w یک ریشه‌ی سوم اولیه‌ی واحد در $Gf(۴)$ می‌باشد. چون $\binom{۳}{۲} = ۳$ پس ۳ کد از نوع $[۳,۲,۲]$ داریم.

۲ـ $GF(۲^۴)$:

رتبه‌ی ۲ به پیمانه‌ی ۵ برابر ۴ می‌باشد و چندجمله‌ای $(x^۴ + x^۳ + x^۲ + x + ۱)$ روی $Gf(۲)$ تفکیک‌ناپذیر می‌باشد. بنابراین به‌وسیله‌ی قضیه‌ی ۱.۴.۲ ماتریس فوریه $F_۵$ روی $Gf(۲^۴)$ وجود دارد و شرایط چبوتارو را برآورده می‌سازد که هر زیرماتریس، دترمینان غیرصفر دارد. $F_۵$ را در نظر بگیرید. فرض کنید α یک عنصر اولیه باشد و $w = \alpha^۳$

بگیرید. ازاین‌رو

$$F_۵ = \begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & w & w^۲ & w^۳ & w^۴ \\ ۱ & w^۲ & w^۴ & w & w^۳ \\ ۱ & w^۳ & w & w^۴ & w^۲ \\ ۱ & w^۴ & w^۳ & w^۲ & w \end{pmatrix}$$

هر زیرماتریس $F_۵$ دترمینان غیرصفر دارد. ما می‌توانیم از $F_۵$ برای تعریف کدهایی با بیشترین فاصله‌ی جداکننده MDS روی $GF(۱۶)$ استفاده نماییم. برای مثال ما ۳ ردیف از ماتریس مولد (اصلی) را انتخاب می‌کنیم و سپس با استفاده از ۲ ردیف دیگر F^* ماتریس توازن را که $[۵,۳,۳]$ ـ کد است، به‌دست می‌آوریم. در مجموع $\binom{۵}{۳} = ۱۰$، $[۵,۳,۳]$ ـ کد متفاوت به‌دست می‌آوریم.

۳ـ $GF(۲^۶)$:

حال $۲^۶ - ۱ | ۷$ و بنابراین ماتریس فوریه $F_۷$ روی $GF(۲^۶)$ وجود دارد اما $(x^۳ + x + ۱)$ یکی از فاکتورهای تجزیه‌ی $(x^۷ - ۱)$ می‌باشد و بنابراین $F_۷$ در شرایط چبوتارو صدق نمی‌نماید. در این‌جا رتبه ۲ به پیمانه‌ی ۷ برابر ۳ می‌باشد و چندجمله‌ای $(x^۳ + x + ۱)$ روی $GF(۲)$ تفکیک‌ناپذیر است.

۴ـ $GF(۲^{۱۰})$:

رتبه‌ی ۲ به پیمانه‌ی ۱۱ برابر $\phi(۱۱) = ۱۰$ می‌باشد و $(x^{۱۰} + x^۹ + \cdots + x + ۱)$ روی $GF(۲)$ تفکیک‌ناپذیر است. بنابراین به‌وسیله‌ی قضیه‌ی ۱.۴.۲ ماتریس فوریه $F_{۱۱}$ روی $GF(۲^{۱۰})$ دارای خاصیت چبوتارو می‌باشد و کدهای MDS از آن ساخته می‌شوند. برای مثال $\binom{۱۱}{۷} = ۳۳۰$، $[۱۱,۷,۵]$ ـ کد MDS (از ریشه‌ی $\frac{۷}{۱۱}$) روی $GF(۲^{۱۰})$ می‌تواند ساخته شود و همه‌ی آنها ۲ـ تصحیح‌کننده‌ی خطا می‌باشند.

۵ـ $GF(۲^{۱۲})$:

رتبه‌ی ۲ به پیمانه‌ی ۱۳ برابر $\phi(۱۳) = ۱۲$ می‌باشد. بنابراین به‌وسیله‌ی قضیه ۳.۲.۲،

$$(x^{۱۲} + x^{۱۱} + \cdots + x + ۱)$$

روی $GF(۲)$ تفکیک‌ناپذیر می‌باشد. بنابراین به‌وسیله‌ی قضیه‌ی ۱.۴.۲، $F_{۱۳}$ روی $GF(۲^{۱۲})$ وجود دارد و شرایط چبوتارو را برآورده می‌سازد. بنابراین به‌عنوان مثال ما قادریم $\binom{۱۳}{۷} = ۱۷۱۶$ کد متفاوت $[۱۳,۷,۷]$ در $GF(۲^{۱۲})$ بسازیم که هر کدام از آنها ۳ـ تصحیح‌کننده‌ی خطا می‌باشند.

۲.۴.۲ $GF(۳^r)$

۱ـ $GF(۳^۴)$:
رتبه‌ی ۳ به پیمانه‌ی ۵ برابر ۴ $= \phi(۵)$ می‌باشد و بنابراین چندجمله‌ای

$$(x^۴ + x^۳ + x^۲ + x + ۱)$$

روی $GF(۳)$ تفکیک‌ناپذیر است. ماتریس فوریه $F_۵$ روی $GF(۳^۴)$ وجود دارد و خاصیت چبوتارو را دارا می‌باشد. به‌وسیله‌ی قضیه‌ی ۱.۴.۲ کدهای MDS می‌توانند ساخته شوند.

۲ـ $GF(۳^۶)$:
رتبه‌ی ۳ به پیمانه‌ی ۷ برابر ۶ می‌باشد و چندجمله‌ای $(x^۶ + x^۵ + \cdots + x + ۱)$ روی $Gf(۳)$ تفکیک‌ناپذیر می‌باشد. در این‌جا به‌وسیله‌ی قضیه‌ی ۱.۴.۲، $F_۷$ وجود داشته و شرایط چبوتارو را برآورده می‌سازد. یعنی ما قادریم کدهای MDS به فرم $F_۷$ بسازیم.
برای مثال $\binom{۷}{۳} = ۳۵$ تا $[۷,۳,۵]$ ـ کد MDS در $GF(۳^۶)$ می‌توانیم بسازیم.

۳ـ $GF(۳^{۱۶})$:
رتبه‌ی ۳ به پیمانه‌ی ۱۷ برابر ۱۶ می‌باشد و چندجمله‌ای $(x^{۱۶} + x^{۱۵} + \cdots + x + ۱)$ روی $Gf(۳)$ تفکیک‌ناپذیر می‌باشد. پس با استفاده از قضیه‌ی ۱.۴.۲، $F_{۱۷}$ شرایط چبوتارو را برآورده می‌سازد و ما قادریم کدهای MDS به فرم $F_{۱۷}$ را بسازیم.
برای مثال $\binom{۱۷}{۹} = ۲۴۳۱۰$ تا $[۱۷,۹,۹]$ ـ کد MDS و $\binom{۱۷}{۱۳} = ۲۳۸۰$ تا $(۱۷,۱۳,۵)$ ـ کد MDS به فرم $F_{۱۷}$ در $GF(۳^{۱۶})$ می‌توانیم بسازیم.

۳.۴.۲ $GF(۵^r)$

۱ـ $GF(۵^۲)$:
رتبه‌ی ۵ به پیمانه‌ی ۳ برابر ۲ می‌باشد و چندجمله‌ای $(x^۲+x+۱)$ در $GF(۵)$ تفکیک‌ناپذیر می‌باشد. بنابراین ماتریس فوریه $F_۳$ وجود دارد و دارای خاصیت چبوتارو می‌باشد.

۲ـ $GF(۵^۶)$:
رتبه‌ی ۵ به پیمانه‌ی ۷ برابر ۶ می‌باشد و چندجمله‌ای $(x^۶ + x^۵ + \cdots + x + ۱)$ در $GF(۵)$ تفکیک‌ناپذیر می‌باشد. بنابراین ماتریس فوریه $F_۷$ روی $GF(۵^۶)$ وجود دارد و در شرایط چبوتارو صدق می‌نماید. در این‌جا برای مثال می‌توانیم $\binom{۷}{۴} = ۳۵$ تا $[۷,۴,۴]$

ـ کد MDS متفاوت روی $GF(۵^۶)$ و همچنین $\binom{۷}{۵} = ۲۱$، $[۷,۵,۳]$ ـ کد متفاوت روی $GF(۵^۶)$ می‌توانیم بسازیم.

۴.۴.۲ $GF(۷^r)$

۱ـ $GF(۷^۴)$:
رتبه‌ی ۷ به پیمانه‌ی ۵ برابر ۴ می‌باشد و چندجمله‌ای $(x^۴+x^۳+x^۲+x+۱)$ روی $GF(۷)$ تفکیک‌ناپذیر می‌باشد. بنابراین طبق قضیه‌ی ۱.۴.۲، $F_۵$ روی $GF(۷^۴)$ وجود داشته و شرایط چبوتارو را برآورده می‌سازد. بنابراین کدهای MDS برای $F_۵$ ساخته می‌شوند.

۲ـ $GF(۷^{۱۰})$:
رتبه‌ی ۷ به پیمانه‌ی ۱۱ برابر ۱۰ می‌باشد و چندجمله‌ای $(x^{۱۰}+x^۹+\cdots+x+۱)$ روی $GF(۷)$ تفکیک‌ناپذیر می‌باشد. بنابراین طبق قضیه‌ی ۱.۴.۲ ماتریس فوریه $F_{۱۱}$ روی $GF(۷^{۱۰})$ وجود داشته و شرایط چبوتارو را تصدیق می‌نماید.

۵.۴.۲ $GF(۱۱^r)$

۱ـ $GF(۱۱)$:
در اینجا ۵ عدد اول ژرمین است و بنابراین ماتریس فوریه $F_۵$ روی $GF(۱۱)$ وجود دارد. قضیه ۱.۴.۲ نمی‌تواند به‌کاربرده شود زیرا فاکتورهای تفکیک‌ناپذیر $x^۵-۱$ در $GF(۱۱)$، به‌صورت

$$\left\{x-۱, x-\alpha^۲, x-\alpha^۴, x-\alpha^۶, x-\alpha^۸\right\}$$

می‌باشند جایی‌که α یک عنصر اولیه در $GF(۱۱)$ می‌باشد (این α می‌تواند ۲ انتخاب شود که رتبه‌ی ۲ به پیمانه‌ی ۱۱ برابر ۱۰ می‌باشد). در اینجا ۵ عدد اول ژرمین می‌باشد ($۱+۲\times ۵ = ۱۱$ اول می‌باشد). بنابراین گزاره‌ی ۱.۴.۲ را می‌توان به‌کار برد.
بنابراین ماتریس فوریه $F_۵$ روی $GF(۱۱)$ دارای خاصیت چبوتارو می‌باشد و کدهای MDS از این فرم ساخته می‌شوند. در این‌جا ۲ یک ریشه‌ی اولیه می‌باشد و $۴ = ۲^۲$ رتبه‌ی ۵ دارد. بنابراین:

$$F_۵ = \begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۴ & ۴^۲ & ۴^۳ & ۴^۴ \\ ۱ & ۴^۲ & ۴^۴ & ۴ & ۴^۳ \\ ۱ & ۴^۳ & ۴ & ۴^۴ & ۴^۲ \\ ۱ & ۴^۴ & ۴^۳ & ۴^۲ & ۴ \end{pmatrix} = \begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۴ & ۵ & ۹ & ۳ \\ ۱ & ۵ & ۳ & ۴ & ۹ \\ ۱ & ۹ & ۴ & ۳ & ۵ \\ ۱ & ۳ & ۹ & ۵ & ۴ \end{pmatrix}$$

یک ماتریس فوریه روی $GF(۱۱)$ می‌باشد که خاصیت چبوتارو را دارد. برای مثال $\binom{۵}{۳} = ۱۰$، $[۵,۳,۳]$ ـ کد MDS روی $\mathbb{Z}_{۱۱}$ به‌دست می‌آوریم که ۱ـ تصحیح‌کننده‌ی خطا می‌باشد.

۲ـ $GF(۲۳)$:

در این‌جا $p = ۱۱$ یک عدد اول ژرمین می باشد زیرا داریم $q = ۲p + ۱ = ۲۳$. ماتریس فوریه $F_{۱۱}$ روی $GF(۲۳)$ وجود داشته و به‌وسیله‌ی گزاره ۱.۴.۲ شرایط چبوتارو را تصدیق می‌نماید در $GF(۲۳)$ یک عنصر اول ۵ می‌باشد و $۵^۲ = ۲۵$ یک عنصر از مرتبه‌ی ۱۱ می‌باشد. بنابراین ماتریس فوریه $F_{۱۱}$ روی $GF(۲۳)$ می‌تواند ساخته شود، لذا داریم:

$$F_{۱۱} = \begin{pmatrix} ۱ & ۱ & ۱ & \cdots & ۱ \\ ۱ & ۲ & ۲^۲ & \cdots & ۲^{۱۰} \\ ۱ & ۲^۲ & ۲^۴ & \cdots & ۲^{۲۰} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ۱ & ۲^{۱۰} & ۲^{۲۰} & \cdots & ۲^{۱۰۰} \end{pmatrix} = \begin{pmatrix} ۱ & ۱ & ۱ & \cdots & ۱ \\ ۱ & ۲ & ۲ & \cdots & ۱۲ \\ ۱ & ۴ & ۱۴ & \cdots & ۶ \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ۱ & ۱۲ & ۶ & \cdots & ۲ \end{pmatrix}$$

۳ـ $GF(۱۱^۳)$:

$۱۱^۳ - ۱ | ۷$ و $(x^۷ - ۱)$ فاکتورهای تجزیه‌ناپذیر $(x - ۱)$ و $(x^۳ + \alpha^۴x^۲ + \alpha^۲x - ۱)$ و $(x^۳ + \alpha^۷x^۲ + \alpha^۹x - ۱)$ روی $GF(۱۱)$ را دارد جایی‌که α اولیه می‌باشد. $F_۷$ روی $GF(۱۱^۳)$ نمی‌تواند دارای خاصیت چبوتارو باشد.

۴ـ یک مثال گسترده:

$GF(۲۲۷)$ را در نظر بگیرید. ماتریس فوریه $F_{۱۱۳}$ روی $GF(۲۲۷)$ وجود دارد و با استفاده از گزاره‌ی ۱.۴.۲ خاصیت چبوتارو را تصدیق می‌نماید. چون که ۱۱۳ یک عدد اول ژرمین است که با ۲۲۷ که اول می‌باشد مطابقت دارد. برای این مثال ما قادریم $\binom{۱۱۳}{۵۷}$ تا $[۱۱۳,۵۷,۵۷]$ ـ کد MDS متفاوت روی $\mathbb{Z}_{۲۲۷}$ بسازیم. عدد $\binom{۱۱۳}{۵۷}$ هم تراز $۱۰^{۳۲}$ با $۲^{۱۰۹}$ می‌باشد. همچنین برای مثال $\binom{۱۱۳}{۹۹}$، $[۱۱۳,۹۹,۱۵]$ ـ کد MDS نسبتاً بزرگ می‌تواند روی $\mathbb{Z}_{۲۲۷}$ ساخته شود که ۷ـ تصحیح‌کننده‌ی خطا می‌باشند. عدد $\binom{۱۱۳}{۹۹}$ به بزرگی $۱۰^{۱۷}$ یا $۲^{۵۷}$ می باشد.

۵.۲ کدهای حاصل از مجموعه‌های خودتوان متعامد کامل

نکته ۱.۵.۲. فرض کنید R یک حلقه با عنصر همانی ۱ باشد ($1_R = 1$). در حالت کلی از نماد ۱ برای نمایش عنصر همانی سیستم مورد مطالعه‌ی خود استفاده می‌کنیم. یک خانواده از خودتوان‌های متعامد کامل مجموعه‌ی $\{e_1, e_2, \ldots, e_k\}$ در R می‌باشد که:

i) $e_i^2 = e_i$ و $e_i \neq 0 \quad 1 \leq i \leq k$

ii) اگر $i \neq j$ باشد دراین‌صورت $e_i e_j = 0$

iii) $e_1 + e_2 + \cdots + e_k = 1$.

خودتوان e_i را اولیه می‌نامیم اگر نتوان آن را به‌صورت $e_i = e_i' + e_i''$ نوشت جایی‌که e_i' و e_i'' خودتوان هستند و $e_i', e_i'' \neq 0$ و $e_i' e_i'' = 0$. یک مجموعه از عناصر خودتوان را اولیه نامیم هرگاه هر خودتوان در این مجموعه یک عنصر اولیه باشد. روش‌هایی برای ساختن کامل مجموعه‌های متعامد از خودتوان‌ها در [۱۱] بررسی شده‌اند. چنین مجموعه‌های خودتوان همیشه در FG وجود دارند.حلقه‌ی گروهی روی یک میدان F، زمانیکه $char\ F \nmid |G|$. مجموعه‌های خودتوان متعامد کامل با نظریه‌ی نمایش حلقه‌های گروهی FG در ارتباط می‌باشند.

۱.۵.۲ رتبه

لم ۱.۵.۲. فرض کنید A یک ماتریس خودتوان باشد. دراین‌صورت رتبه‌ی ماتریس A برابر با اثر ماتریس A می‌باشد یعنی $rank\ A = trA$.

اثبات. فرض کنیم $A_{n\times n}$ یک ماتریس خودتوان باشد. دراین‌صورت بنابر قاعده‌ی تجزیه رتبه[۵]، داریم $A_{n\times n} = B_{n\times r} C_{r\times n}$ ، جایی‌که B ماتریسی با رتبه‌ی ستونی کامل[۶] و C ماتریسی با رتبه‌ی سطری کامل[۷] می‌باشد. دراین‌صورت B دارای وارون چپ و C دارای وارون راست می‌باشد. و چون $A^2 = A$، دراین‌صورت داریم $BCBC = BC$. چون B دارای وارون چپ می‌باشد لذا $CBC = C$. حال چون C دارای وارون راست می‌باشد لذا $CB = I_{r\times r}$، بنابراین داریم:

$$trace(A) = trace(BC) = trace(CB) = trace(I_{r\times r}) = r = rank(A).$$

لذا حکم ثابت می‌شود. □

لم ۲.۵.۲. فرض کنید $\{E_1, E_2, \ldots, E_s\}$ یک مجموعه از ماتریس‌های خودتوان متعامد روی میدان اعداد مختلط $\mathbb{C}$ باشد. دراین‌صورت

$$rank(E_1 + E_2 + \cdots + E_s) = tr(E_1 + E_2 + \cdots + E_s) = trE_1 + trE_2 + \cdots + trE_s$$

[5] Rank factorization
[6] Full column rank matrix
[7] Full row rank matrix

$$= rank\ E_۱ + rank\ E_۲ + \cdots + rank\ E_s.$$

اثبات. بنابر لم ۱.۵.۲ می‌دانیم برای یک ماتریس خودتوان $rank\ A = trA$. بنابراین برای هر i،

$$rank\ E_i = trE_i.$$

اگر $\{E, F, G\}$ یک مجموعه از ماتریس‌های متعامد خودتوان باشد، دراین‌صورت $\{E + F, G\}$ نیز متعامد خودتوان است. لذا با استفاده از استقراء به‌دست می‌آوریم:

$$rank(E_۱ + E_۲ + \cdots + E_s) = tr(E_۱ + E_۲ + \cdots + E_s) = trE_۱ + trE_۲ + \cdots + trE_s$$

$$= rank\ E_۱ + rank\ E_۲ + \cdots + rank\ E_s.$$

□

نتیجه ۱.۵.۲. فرض کنیم $E_{i_۱}+E_{i_۲}+\cdots+E_{ik}$ ماتریس‌های متعامد خودتوان باشند. دراین‌صورت داریم:

$$rank(E_{i_۱} + E_{i_۲} + \cdots + E_{ik}) = rank\ E_{i_۱} + rank\ E_{i_۲} + \cdots + rank\ E_{ik}$$

برای $i_j \neq i_l$, $i, j \in \{۱, ۲, \ldots, s\}$.

۲.۵.۲ کدها

فرض کنید $\{E_۱, E_۲, \ldots, E_k\}$ یک مجموعه متعامد کامل از خودتوان‌ها در $F_{n\times n}$ باشد جایی‌که $rank\ E_i = r_i$ و $\sum_{i=۱}^{k} r_i = n$. فرض کنید $I = \{۱, ۲, \ldots, k\}$ و $J \subseteq I$، دراین‌صورت بنابر لم ۲.۵.۲،

$$rank\left(\sum_{j\in J} E_j\right) = \sum_{j\in J} rank(E_j).$$

حال فرض کنید $G = (E_۱ + E_۲ + \cdots + E_s)$ که $s < k$ و

$$H = (E_{s+۱} + \cdots + E_k), r = rank\ G = (r_۱ + r_۲ + \cdots + r_s)$$

و سپس

$$(n - r) = rank\ H = (r_{s+۱} + r_{s+۲} + \cdots + r_k).$$

توجه کنید که $GH = ۰$، دراین‌صورت C_s کدی با ماتریس مولد G و ماتریس کنترل توازن H^T مشخص می‌کند و C_s یک $[n, r]$ ـ کد می‌باشد.

لم ۳.۵.۲. فرض کنید $A \in F_{n\times n}$، دراین‌صورت $AH = ۰$ اگر و تنها اگر $AE_i = ۰$ برای $i = s+۱, s+۲, \ldots, k$.

اثبات. فرض می‌کنیم $AH = ۰$. از سمت راست E_i را در آن ضرب می‌کنیم برای $s+۱ \leq i \leq k$، دراین‌صورت $AE_i = ۰$ و $E_iE_i = E_i$ و $E_iE_j = ۰$ برای $i \neq j$. برعکس اگر $AE_i = ۰$ برای $i = s+۱, s+۲, \ldots, k$، دراین‌صورت واضح است که $AH = ۰$. □

هر s عنصر از $\{E_۱, E_۲, \ldots, E_k\}$ می‌تواند برای ماتریس مولد استفاده شود و سپس $(k-s)$ عنصر دیگر ماتریس توازن را به ما می‌دهد. مسلماً رتبه به‌وسیله‌ی رتبه‌ی عنصرهای انتخاب شده مشخص می‌شوند. هر مجموعه‌ی متعامد کامل از خودتوان‌ها ممکن است مورد استفاده قرار گیرد. هم‌اکنون به بررسی مواردی در ارتباط با خودتوان‌ها در حلقه‌ی گروه‌های دوری می‌پردازیم.
فرض کنید $S = \{E_۱, E_۲, \ldots, E_n\}$ یک مجموعه متعامد کامل از خودتوان‌ها در $K_{n\times n}$ باشد جایی‌که هر E_i رتبه‌ی ۱ دارد. دراین‌صورت می‌توانید ببینید که انتخاب r عنصر یک $[n, r]$ ـ کد به ما می‌دهد با ماتریس مولدی که از جمع این r عنصر به‌دست می‌آید و ماتریس توازن که به‌وسیله‌ی ترانهاده جمع $(n-r)$ عنصر دیگر به‌دست می‌آید. هر انتخاب از r عنصر به ما یک $[n, r]$ ـ کد متفاوت می‌دهد. بنابراین $\binom{n}{r}$ تا $[n, r]$ ـ کد متفاوت داریم.

۳.۵.۲ به‌دست آوردن فاصله

فرض کنید که $S = \{E_۱, E_۲, \ldots, E_n\}$ یک مجموعه از خودتوان‌های متعامد کامل در $F_{n\times n}$ روی میدان F باشد. فرض کنید F_n یک ماتریس $n\times n$ که شامل اولین ستون از هر $\{E_۱, E_۲, \ldots, E_n\}$ باشد. فرض کنید G ماتریس به‌دست آمده از جمع r عنصر از s باشد و H نیز ماتریس به‌دست آمده از جمع $(n-r)$ عنصر دیگر s باشد، دراین‌صورت با استفاده از توضیحات ارائه شده در بخش ۴.۳، C_r یک $[n, r]$ ـ کد با ماتریس مولد G و ماتریس توازن H^T تعریف می‌شود.

قضیه ۱.۵.۲. فرض کنید که دترمینان هر زیرماتریس مربعی از F_n غیرصفر باشد، دراین‌صورت هر کد C_r فاصله‌ی $(n-r+۱)$ را دارد و بنابراین یک $[n, r, n-r+۱]$ ـ کد MDS می‌باشد.

اثبات. فرض کنید $u = (u_۱, u_۲, \ldots, u_n) \in C_r$. بنابراین u در r مکان، مقدار ۰ دارد. فرض کنید u در مکان‌های $\{u_{k_۱}, u_{k_۲}, \ldots, u_{k_{n-r}}\}$ مقدار صفر دارد. تعریف کنید $\widehat{u} = (u_{k_۱}, u_{k_۲}, \ldots, u_{k_{n-r}})$.
فرض کنید $H = E_{j_۱} + E_{j_۲} + \cdots + E_{j_{n-r}}$. حال $uH = ۰$ و بنابراین به‌وسیله‌ی لم ۳.۵.۲ داریم:

$$uE_{ij} = ۰ \qquad \forall\ i = ۱, ۲, \ldots, (n-r).$$

فرض کنید k_l^{th} ورودی ستونی از E_{jt} باشد که توسط E_{jt_l} مشخص می‌شود. بنابراین

$$\sum_{i=۱}^{n-r} u_{kl}E_{ji_l} = ۰ \qquad \forall\ i = ۱, ۲, \ldots, (n-r).$$

حال فرض کنید که T_i ستون $(E_{ji_1}, E_{ji_2}, \ldots, E_{ji_{n-r}})^T$ باشد، دراین‌صورت داریم $\widehat{u}T_i = 0$ برای $i = 1, 2, \ldots, (n-r)$ در این‌جا $\widehat{u}(T_1, T_2, \ldots, T_{n-r}) = 0$. فرض کنید A یک ماتریس $(n-r) \times (n-r)$ باشد $(T_1, T_2, \ldots, T_{n-r})$ یک زیرماتریس مربعی از F_n می‌باشد و بنابراین دترمینان آن غیرصفر است. در این‌جا $\widehat{u} = 0$ و بنابراین $u = 0$. □

۴.۵.۲ کدهای MDS از نوع دوری

فرض کنید $N = \{E_0, E_1, \ldots, E_{n-1}\}$ مجموعه‌ای از خودتوان‌های اولیه‌ی متعامد کامل، حاصل از گروه دوری C_n از مرتبه‌ی n در $\mathbb{C}$ باشد. $E_i = circ(w^i, w^{2i}, \ldots, w^{(n-r)i})$ را در نظر بگیرید جایی‌که w یک ریشه‌ی nـام اولیه‌ی واحد می‌باشد.
فرض کنید C_r یک کد با ماتریس مولد $G = (E_0 + E_1 + \cdots + E_{r-1})$ و ماتریس کنترل توازن $H = (E_r + E_{r+1} + \cdots + E_{r-1})$ باشد، دراین‌صورت بنا بر لم ۲.۵.۲ رتبه‌ی ماتریس G، برابر r و رتبه‌ی ماتریس H، برابر $(n-r)$ می‌باشد و لذا C_r یک $[n, r]$ ـ کد می‌باشد. r ردیف اول G مستقل خطی هستند و $(n-r)$ ردیف اول از H نیز مستقل خطی می‌باشند. از این‌رو r ردیف اول G را می‌توان به‌عنوان ماتریس مولد در نظر گرفت و به‌طور مشابه، $(n-r)$ ردیف اول از H^T می‌توان به‌عنوان ماتریس کنترل توازن کد C_r در نظر گرفت.
در حالت کلی مجموع هر r عنصر دلخواه از مجموعه‌ی $S = \{E_0, E_1, \ldots, E_{n-1}\}$ می‌تواند برای ساختن ماتریس مولد G_r برای یک $[n, r]$ ـ کد C_r استفاده شده، و همچنین به‌صورت مشابه $(n-r)$ عنصر باقیمانده‌ی دیگر برای ساختن ماتریس H_{n-r} به‌کار گرفته می‌شود، جایی‌که H_{n-r}^T یک ماتریس کنترل توازن کد C_r می‌باشد. همان‌طور که توضیح دادیم، r ردیف اول از G_r مستقل خطی هستند و می‌تواند به‌عنوان ماتریس مولد کد دوری در نظر گرفته شود و $(n-r)$ ردیف اول از H_{n-r}^T می‌تواند به‌عنوان ماتریس کنترل توازن در نظر گرفته شود.

قضیه ۲.۵.۲. فرض کنید n عددی اول باشد، دراین‌صورت فاصله‌ی کد G_r برابر $(n-r+1)$ می‌باشد.

اثبات. با استفاده از قضیه‌ی ۱.۵.۲ دترمینان هر زیرماتریس مربعی از F_n غیرصفر می‌باشد و با استفاده از قضیه‌ی چبوتارو حکم ثابت می‌شود. □

کدهای ساخته شده در این بخش کدهای دوری می‌باشند و لذا ایده‌آل‌هایی از حلقه‌ی گروهی یک گروه دوری می‌باشند. توجه کنید که کاربرد مجموعه‌های متعامد از خودتوان‌ها در ساختن کدهای MDS روی $\mathbb{R}$ با استفاده از ترکیب توأم خودتوان‌ها برای به‌دست آوردن ماتریس مولد می‌باشد. این موضوع در مثال‌های زیر مشهود است. با استفاده از مجموعه‌های متعامد کامل از خودتوان‌ها در $\mathbb{Q}_{n\times n}$ کدهایی روی $\mathbb{Q}$ به‌دست می‌آیند.

چند مثال از کدهای خودتوان

مجموعه متعامد کامل خودتوان $\mathbb{C}_۵$ را در نظر بگیرید. $\mathbb{C}_۵ = \{E_۰, E_۱, E_۲, E_۳, E_۴\}$

$$E_۰ = \frac{۱}{۵} circ(۱,۱,۱,۱,۱)$$
$$E_۱ = \frac{۱}{۵} circ(۱, w, w^۲, w^۳, w^۴)$$
$$E_۲ = \frac{۱}{۵} circ(۱, w^۲, w^۴, w, w^۳)$$
$$E_۳ = \frac{۱}{۵} circ(۱, w^۳, w, w^۴, w^۲)$$
$$E_۴ = \frac{۱}{۵} circ(۱, w^۴, w^۳, w^۲, w)$$

اگر ما $u = (E_۰ + E_۱ + E_۲)$ را به‌عنوان ماتریس مولد کد C انتخاب کنیم، دراین‌صورت $V = (E_۳ + E_۴)$ ماتریس کنترل توازن V^T از C می‌باشد. با استفاده از قضیه‌ی ۲.۵.۲ این یک $[۵,۳,۳]$ ـ کد می‌باشد. سه ردیف اول از u مستقل خطی هستند و ماتریس مولد ما را می‌سازند. دو ستون اول از V نیز مستقل خطی هستند و هر زیرماتریس ۲×۲ آن $(det \neq ۰)$ دترمینان مخالف صفر دارد که فاصله‌ی ۳ را به‌دست می‌آوریم.
ماتریس مولد u به‌صورت زیر می‌باشد:

$$u = (E_۰ + E_۱ + E_۲) = \frac{۱}{۵} circ(۳, ۱ + w, w^۲, ۱ + w^۲ + w^۴, ۱ + w^۳ + w, ۱ + w^۲ + w^۳)$$

فرض کنید قصد داریم تا یک $[۵,۳,۳]$ ـ کد حقیقی از $\{E_۰, E_۱, E_۲, E_۳, E_۴\}$ به‌دست آوریم. توجه کنید که $\{E_۱, E_۴\}$ و $\{E_۲, E_۳\}$ جفت‌هایی هستند که جمع آن‌ها حقیقی می‌باشد و $E_۰$ نیز حقیقی می‌باشد. $G = (E_۰, E_۱, E_۴)$ را ماتریس مولد و $H = (E_۲, E_۳)$ را به‌عنوان ماتریس کنترل توازن در نظر بگیرید. هر دو ماتریس G و H حقیقی هستند و بنابراین یک $[۵,۳,۳]$ ـ کد حقیقی داریم.

۵.۵.۲ کدهای MDS روی میدان‌های متناهی

ما هم‌اکنون با استفاده از کاربرد قضیه‌ی ۱.۵.۲ و تحلیل قضیه‌ی ۱.۳.۲ و گزاره‌ی ۳.۲.۲ مجموعه‌ای از کدهای MDS دوری روی میدان‌های متناهی را معرفی می‌کنیم. دقت کنید که اگر $\{F_۱, F_۲, \ldots, F_k\}$ ماتریس‌های خودتوان متعامد دوری باشند و

$$rank\ F_۱ + rank\ F_۲ + \cdots + rank\ F_k = r$$

دراین‌صورت $G = (F_۱ + F_۲ + \cdots + F_k)$ نیز دوری می‌باشد و r ردیف اول از G مستقل خطی می‌باشند. مثال [۹] این‌گونه می‌باشد. بنابراین از ماتریس‌های توازن و مولد $[n, r]$ ـ کد ما می‌توانیم ماتریس‌های $n \times n$ را با استفاده از r ردیف اول ماتریس مولد و $(n - r)$ ردیف اول

ماتریس توازن به‌دست آوریم.
حال بخش ۴.۲ را که دو عدد اول غیرمساوی p و q و $GF(q^{\phi(p)})$ را در نظر بگیرید، جایی‌که رتبه‌ی q به پیمانه‌ی p برابر $\phi(p)$ می‌باشد و چندجمله‌ای $x^{p-1}+x^{p-2}+...+x+1$ روی $GF(q)$ تفکیک‌ناپذیر باشد، دراین‌صورت با استفاده از قضیه‌ی ۳.۵.۲ ماتریس فوریه F_p روی $GF(q^{\phi(p)})$ وجود دارد و شرایط چبوتارو را تصدیق می‌کند.

قضیه ۳.۵.۲. فرض کنید p و q دو عدد اول غیرمساوی و $K=GF(q^{\phi(p)})$ باشد و فرض کنید رتبه‌ی q به پیمانه‌ی p برابر $\phi(p)$ باشد و چندجمله‌ای $(x^{p-1}+x^{p-2}+...+x+1)$ روی $GF(q)$ تفکیک‌ناپذیر باشد. فرض کنید w یک ریشه‌ی pـام اولیه‌ی واحد در K باشد. تعریف کنید ($K_{p\times p}$ در)

$$E_i=\frac{1}{p}circ(1,w^i,w^{2i},\dots,w^{(p-1)i}) \qquad \forall\, i=0,1,\dots,(p-1)$$

در این‌صورت $S=\{E_0,E_1,\dots,E_{p-1}\}$ یک مجموعه از خودتوان‌های متعامد کامل می‌باشد. (هر E_i رتبه ۱ دارد) و کدهای تولید شده با استفاده از هر زیرمجموعه S کدهای MDS دوری می‌باشند.

اثبات. به‌وضوح مشخص است که S یک مجموعه از خودتوان‌های متعامد کامل در $GF(q^{\phi(p)})$ می‌باشد. بنابراین عنصرهای ردیف‌های اول از S یک ردیف از ردیف‌های ماتریس فوریه F_p را تشکیل می‌دهند. در نتیجه با استفاده از قضیه ۱.۵.۲ حکم ثابت می‌شود. □

گزاره ۱.۵.۲. فرض کنید p و $q=2p+1$ اول باشند و w یک ریشه‌ی pـام اولیه‌ی واحد در $K=GF(q)$ باشد. تعریف کنید در K

$$E_i=\frac{1}{p}circ(1,w^i,w^{2i},\dots,w^{(p-1)i}) \qquad \forall\, i=0,1,\dots,(p-1)$$

در این‌صورت $S=\{E_0,E_1,\dots,E_{p-1}\}$ یک مجموعه از خودتوان‌های متعامد کامل می‌باشد. بنابراین کدهای تولید شده به‌وسیله‌ی زیر مجموعه‌های S، کدهای MDS دوری می‌باشند.

ساختارها نسبتاً عمومی هستند و مثال‌ها راحت ساخته می‌شوند. مثال‌هایی مشابه آنچه در بخش ۳ـ۵ در مورد مجموعه‌های متعامد از خودتوان‌ها دیدیم مرور می‌شوند. یک انتخاب از مثال‌های متشابه در بخش ۳ـ۵ با حذف جزییات در زیر آمده است.

مثال‌هایی در میدان‌های متناهی

۱ـ $GF(2^2)$:

فرض کنید w یک ریشه‌ی سوم اولیه‌ی واحد در $GF(2^2)$ باشد. S مجموعه‌ای از خودتوان‌های متعامد کامل می‌باشد.

$$S=\Big\{E_0=circ(1,1,1),E_1=circ(1,w,w^2),E_2=circ(1,w^2,w)\Big\}$$

از ردیف‌های اول این مجموعه یک ماتریس فوریه $F_۳$ غیرصفر مضاعف به‌دست می‌آید که شرایط چبوتارو را دارد. بنابراین انتخاب هر زیر مجموعه از S یک ماتریس مولد برای کد MDS تعیین می‌کند و هر کدام از کدها دوری می‌باشند. برای مثال $\binom{۳}{۲} = ۳$ ، بنابراین ۳ کد دوری از نوع $[۳,۲,۲]$ به‌دست می‌آوریم.

۲ـ $GF(۲^۴)$:

فرض کنید w یک ریشه‌ی ۵ـام اولیه‌ی واحد در $GF(۲^۴)$ باشد. مجموعه‌ی خودتوان‌های متعامد کامل را در نظر بگیرید.

$$S = \{E_۰ = circ(۱,۱,۱,۱,۱), E_۱ = circ(۱,w,w^۲,w^۳,w^۴), E_۲ = circ(۱,w^۲,w^۴,w,w^۳)$$
$$E_۳ = circ(۱,w^۳,w,w^۴,w^۲), E_۴ = circ(۱,w^۴,w^۳,w^۲,w)\}.$$

ردیف‌های اول $\{E_۰, E_۱, E_۲, E_۳, E_۴\}$ یک ماتریس فوریه $F_۵$ غیرصفر (مضاعف) روی $GF(۲^۴)$ تعیین می‌کنند. برای مثال با انتخاب مجموع ۳ عضو از S یک $[۵,۳,۳]$ ـ کد به‌دست می‌آوریم و $\binom{۵}{۳} = ۱۰$ ، $[۵,۳,۳]$ ـ کد دوری متفاوت داریم.

۳ـ $GF(۲^{۱۰})$:

فرض کنید $E_i = circ(۱, w^i, w^{۲i}, \ldots, w^{(۱۰)i})$ جایی‌که w یک ریشه‌ی ۱۱ـام اولیه واحد در $GF(۲^{۱۰})$ می‌باشد و $S = \{E_۰, E_۱, \ldots, E_{۱۰}\}$. با استفاده از ردیف‌های اول $E_۰, E_۱, \ldots, E_{۱۰}$ ماتریس فوریه $F_{۱۱}$ روی $GF(۲^{۱۰})$ را تشکیل دهید. حال با استفاده از بخش ۴.۲ ماتریس $F_{۱۱}$ فوق ویژگی چبوتارو را دارد و کدهایی که با استفاده از مجموع عناصر S ساخته می‌شود کدهای MDS و همچنین دوری می‌باشند.

۴ـ $GF(۲^{۱۲})$:

فرض کنید $E_i = circ(۱, w^i, w^{۲i}, \ldots, w^{(۱۲)i})$ جایی‌که w یک ریشه‌ی ۱۳ـام اولیه واحد در $GF(۲^{۱۲})$ می‌باشد و $S = \{E_۰, E_۱, ..., E_{۱۲}\}$ با استفاده از ردیف‌های اول $E_۰, E_۱, ..., E_{۱۲}$ یک ماتریس فوریه $F_{۱۳}$ (مضاعفـ چندگانه) روی $GF(۲^{۱۲})$ را تشکیل دهید. حال با استفاده از بخش ۴.۲ ماتریس فوریه $F_{۱۳}$ فوق ویژگی چبوتارو را دارد و کدهایی که با استفاده از مجموع عناصر S ساخته می‌شوند، کدهای MDS و همچنین دوری می‌باشند.

۵ـ $GF(۳^۴)$:

فرض کنید $E_i = circ(۱, w^i, w^{۲i}, ..., w^{(۴)i})$ جایی‌که w یک ریشه‌ی ۵ـام اولیه واحد در $GF(۳^۴)$ باشد و فرض کنید $S = \{E_۰, E_۱, E_۲, E_۳, E_۴\}$. دراین‌صورت ردیف‌های اول یک ماتریس فوریه $F_۵$ (مضاعفـ چندگانه) روی $GF(۳^۴)$ تشکیل می‌دهد که با توجه

به بخش ۴.۲ ویژگی چبوتارو را دارا می‌باشد. بنابراین کدهای ساخته شده با استفاده از زیر مجموعه‌های S، کدهای MDS دوری می‌باشند.

۶ـ $GF(۳^۶)$:
E_i ها را به‌صورت زیر بسازید:

$$E_i = circ(۱, w^i, w^{۲i}, \ldots, w^{(۶)i})$$

جایی‌که w یک ریشه‌ی ۷ـام اولیه واحد در $GF(۳^۶)$ باشد و فرض کنید $S = \{E_۰, E_۱, E_۲, \ldots, E_۶\}$.
سطرهای اول $\{E_۰, E_۱, E_۲, \ldots, E_۶\}$ یک ماتریس فوریه $F_۷$ (مضاعفـ چندگانه) روی $GF(۳^۶)$ تشکیل می‌دهد که با توجه به بخش ۴.۲ شرایط چبوتارو را دارد. بنابراین کدهای ساخته شده به‌وسیله‌ی زیر مجموعه‌های S، کدهای MDS می‌باشند.

۷ـ $GF(۳^{۱۶})$:
از $\{E_۰, E_۱, \ldots, E_{۱۶}\}$ کدهای MDS دوری به‌دست آورده می‌شوند که جزییات را بیان نکردیم. برای مثال ما $\binom{۱۷}{۹} = ۲۴۳۱۰$ ، $[۱۷, ۹, ۹]$ ـ کد MDS دوری داریم.

مثال‌های دوری بیشتری با استفاده از بخش ۳ـ۵ و به‌کاربردن $GF(۵^r)$ و $GF(۷^r)$ و $GF(۱۱^r)$ می‌توانیم به‌دست آوریم.

۶.۵.۲ تساوی

در این‌جا یک سؤال مطرح می‌شود که آیا کدهای به‌دست آمده از خودتوان‌ها در حلقه‌ی گروهی از گروه دوری، مشابه کدهای متناظر حاصل از عناصر یکه در بخش ۲ با استفاده از ردیف‌های ماتریس فوریه می‌باشند یا نه؟
ثابت شده است که ماتریس زوج‌آزمایی یکسانی دارند، بنابراین مساوی هستند. اما این مطلب از نحوه‌ی ساختن آن‌ها واضح نیست و رسیدن از ماتریس مولد یکی به ماتریس مولد دیگری کار راحتی نیست. هر نمایشی مزیت خاص خود را دارد.

۶.۲ کدگشایی

برای بردارهای $U = (u_۰, u_۱, \ldots, u_{n-۱})$ و $V = (v_۰, v_۱, \ldots, v_{n-۱})$ تعریف می‌کنیم:

$$U * V = (u_۰v_۰, u_۱v_۱, \ldots, u_{n-۱}v_{n-۱}).$$

حال برای زیرفضاهای U و V تعریف می‌کنیم:

$$U * V = \{u * v \mid u \in U \ , \ v \in V\}.$$

فرض کنید $C^{\perp}$ مکمل متعامد C باشد. $k(C)$ بعد C و $d(C)$ مینیمم فاصله‌ی C را مشخص می‌کنند. فرض کنید U و V و C کدهای خطی روی میدان K باشند، دراین‌صورت (U,V) یک زوج tـ تصحیح‌کننده‌ی خطا برای C می‌باشد اگر:

(i $U * V \subseteq C^{\perp}$

(ii $k(U) > t$

(iii $d(V^{\perp}) > t$

(iv $d(C) + d(U) > n$

جایی‌که n طول کد را مشخص می‌کند و (U,V) یک زوج tـ تصحیح‌کننده‌ی خطا برای C می‌باشد.
حال نشان می‌دهیم که چطور تصحیح tـ خطا از $[n, r, n-r+1]$ ـ کدها صورت می‌گیرد و با روش یکتای به‌دست آمده در بخش ۲ با $2t = n - r$ به شرح موضوع می‌پردازیم.
فرض کنید K یک میدان شامل ریشه‌ی nـ ام اولیه یکه w باشد به‌طوری‌که معکوس n در K وجود داشته باشد. تعریف می‌کنیم:

$$e_0 = (1, 1, \ldots, 1), e_1 = (1, w, w^2, \ldots, w^{(n-1)}), \ldots,$$

$$e_{n-1} = (1, w^{n-1}, w^{2(n-1)}, \ldots, w^{(n-1)(n-1)})$$

مجموعه‌ی $S = \{e_0, e_1, \ldots, e_{n-1}\}$ یک پایه برای K^n می‌باشد و متشکل از ردیف‌های ماتریس فوریه می‌باشد و S یک مجموعه از n بردار مستقل خطی در K^n می‌باشد.
ضرب اسکالر بردارهای U و V که $(U, V \in K^n)$ به‌صورت $U.V$ نمایش داده می‌شود.

لم ۱.۶.۲. $e_i * e_j = e_{i+j}$ جایی‌که $i + j$ به پیمانه‌ی n محاسبه می‌شود.

اثبات.

$$e_i * e_j = (1, w^i, w^{2i}, \ldots, w^{(n-1)i}) * (1, w^j, w^{2j}, \ldots, w^{(n-1)j})$$

$$= (1, w^{i+j}, w^{2(i+j)}, \ldots, w^{(n-1)(i+j)}) = e_{i+j}$$

□

لم ۲.۶.۲. فرض کنید $U = \langle u_1, u_2, \ldots, u_k \rangle$ و $V = \langle v_1, v_2, \ldots, v_s \rangle$ برای بردارهای v_j و u_i داریم:

$$U * V \subseteq \langle u_i * v_j \mid 1 \leq i \leq k \ , \ 1 \leq j \leq s \rangle.$$

لم ۳.۶.۲. فرض کنید $I = \{0, 1, 2, \ldots, n-1\}$ و $J \subseteq I$، $C = \langle e_j \mid j \in J \rangle$. تعریف کنید $\widehat{J} = \{n - j \ mod \ n | j \in J\}$ و $K = (I - \widehat{J})$، دراین‌صورت $C^{\perp} = \langle e_k \mid k \in K \rangle$.

اثبات. چون $e_ie_j = ۰$ اگر و تنها اگر $j = n - i$ به پیمانه‌ی n. □

حال فرض کنید ماتریس فوریه با ردیف‌های $S = \{e_i \mid ۰ \leq i \leq (n-۱)\}$ خاصیت چبوتارو را داشته باشد یعنی دترمینان هر زیرماتریس از آن غیرصفر باشد، دراین‌صورت مولد کد، به‌وسیله‌ی هر r بردار S که یک $[n, r, n-r+۱]$ ـ کد می‌باشد، به‌دست می‌آید.
هم‌اکنون ما ماکزیمم t، برای تصحیح tـخطا برای تعداد زیادی از این کدها را به‌دست می‌آوریم.
فرض کنید r بردار $\{e_i, e_{i+۱}, \ldots, e_{i+r-۱}\}$ از S به‌صورت متوالی انتخاب شوند تا کد مورد نظر را تشکیل دهند جایی‌که پیشوندها به پیمانه‌ی n محاسبه می‌شوند. ما باید نشان دهیم که چطور زوج تصحیح tـخطا را می‌سازیم جایی‌که $۲t = n - r$. ما می‌دانیم که در این مورد کد C به‌وسیله $\{e_۰, e_۱, \ldots, e_{r-۱}\}$ تولید می‌شود. در موارد دیگر هم بنابر لم ۳.۶.۲ $\langle e_۱, e_۲, \ldots, e_{n-r}\rangle \subseteq C^{\perp}$ می‌باشد $K(U) = t + ۱ > t$ برابر U بعد $U = \langle e_۰, \ldots, e_t\rangle$ و مجموعه $(\{e_۰, e_۱, \ldots, e_t\})$ که یک مجموعه‌ی مستقل خطی می‌باشد. مجموعه $V = \langle e_۱, \ldots, e_t\rangle$ دراین‌صورت $V^{\perp} = \langle e_۰, e_۱, \ldots, e_{n-t-۱}\rangle$.
حال $V^{\perp}$ یک $[n, n-t, t+۱]$ ـ کد می‌باشد و همچنین $d(V^{\perp}) > t$. حال با استفاده از لم ۱.۶.۲ و لم ۲.۶.۲ داریم:

$$U * V \subseteq \langle e_۱, e_۲, \ldots, e_{۲t}\rangle = \langle e_۱, e_۲, \ldots, e_{n-r}\rangle \subseteq C^{\perp}$$

بنابراین (U, V) در شرایط $(i) - (iii)$ صدق می‌کنند. حال U یک $[n, t+۱, n-t]$ ـ کد می‌باشد و بنابراین $d(U) = n - t$. در این‌جا داریم:

$$d(C) + d(U) = (n - r + ۱) + (n - t) = ۲n - r - t + ۱ = n + (n - r) - t + ۱$$

$$= n + ۲t - t + ۱ = n + t + ۱ > n$$

بنابراین زوج (U, V) در شرط iv نیز صدق می‌کند و بنابراین (U, V) یک زوج tـ تصحیح‌کننده‌ی خطا می‌باشند.
به‌طور مشابه ما قادریم تا هر زوج tـ تصحیح‌کننده‌ی خطا را بسازیم زمانی‌که $\{e_{i_۱}, e_{i_۲}, \ldots, e_{i_r}\}$.
برای مثال ماتریس فوریه $F_{۱۱}$ روی $K = GF(۲۳)$ ساخته شده در بخش ۵.۴.۲ را بررسی می‌کنیم.
$w = ۵^۲ = ۲۵$ که یک ریشه‌ی ۱۱ـام اولیه‌ی واحد در K می‌باشد. فرض کنید سطرهای $F_{۱۱}$ به‌وسیله $\langle e_۰, e_۱, \ldots, e_{۱۰}\rangle$ مشخص شود و فرض کنید که $C_۷$ یک $[۱۱, ۷, ۵]$ ـ کد ساخته شده توسط ۷ سطر اول از $F_{۱۱}$ باشد. حال یک زوج ۲ـ تصحیح‌کننده‌ی خطا را به‌صورت زیر تعریف می‌کنیم.
$U = \langle e_۰, e_۱, e_۲\rangle$ و $V = \langle e_۱, e_۲\rangle$ در این‌صورت:

(i $U * V \subseteq \langle e_۱, e_۲, e_۳, e_۴\rangle \subseteq C_۷^{\perp}$

ii) بعد U ، برابر ۳ می‌باشد.

iii) فاصله‌ی $V^{\perp}$ برابر ۳ می‌باشد.

iv) $d(C_{۷}) + d(U) = ۵ + ۹ > ۱۱$

بنابراین (U,V) یک زوج ۲ـ تصحیح‌کننده‌ی خطا می‌باشد. ماتریس‌های $M(U)$ و $M(V)$ از U و V به‌صورت زیر می‌باشند.

$$M(U) = \begin{pmatrix} ۱ & ۱ & ۱ & \cdots & ۱ \\ ۱ & w & w^{۲} & \cdots & w^{۱۰} \\ ۱ & w^{۲} & w^{۴} & \cdots & w^{۲۰} \end{pmatrix} = \begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۲ & ۴ & ۸ & ۱۶ & ۹ & ۱۸ & ۱۳ & ۳ & ۶ & ۱۲ \\ ۱ & ۴ & ۱۶ & ۱۸ & ۳ & ۱۲ & ۲ & ۸ & ۹ & ۱۳ & ۶ \end{pmatrix}$$

$$M(V) = \begin{pmatrix} ۱ & w & w^{۲} & \cdots & w^{۱۰} \\ ۱ & w^{۲} & w^{۴} & \cdots & w^{۲۰} \end{pmatrix} = \begin{pmatrix} ۱ & ۲ & ۴ & ۸ & ۱۶ & ۹ & ۱۸ & ۱۳ & ۳ & ۶ & ۱۲ \\ ۱ & ۴ & ۱۶ & ۱۸ & ۳ & ۱۲ & ۲ & ۸ & ۹ & ۱۳ & ۶ \end{pmatrix}$$

به طور مشابه می‌توانیم زوج ۲ـ تصحیح‌کننده‌ی خطا را برای هر کد تولید شده توسط

$$\{e_i, e_{i+۱}, e_{i+۲}, \ldots, e_{i+۶}\}$$

را به‌دست آوریم. (پیشوندها باید به پیمانه‌ی ۱۱ باشند)
برای کد تولید شده توسط $\{e_{۰}, e_{۲}, e_{۴}, e_{۶}, e_{۱۰}, e_{۱}\}$ (که دارای فاصله ۲ در پیشوندهای متوالی است) زوج (U,V) با $U = \langle e_{۰}, e_{۲}, e_{۴}\rangle$ و $V = \langle e_{۲}, e_{۴}\rangle$ یک زوج ۲ـ تصحیح‌کننده‌ی خطا می‌باشد. با روش مشابهی زوج ۳ـ تصحیح‌کننده‌ی خطا برای [۱۱,۵,۷] ـ کد تولید شده به‌وسیله‌ی هر

$$\{e_i, e_{i+۱}, e_{i+۲}, e_{i+۳}, e_{i+۴}\}$$

و به طور کلی تولید شده به‌وسیله‌ی هر $\{e_i, e_{i+j}, e_{i+۲j}, e_{i+۳j}, e_{i+۴j}\}$ با $۱ \le j \le ۱۰$ به‌دست می‌آید.
برای مثال اگر $C = \langle e_{۰}, e_{۲}, e_{۴}, e_{۶}, e_{۸}\rangle$ در این‌صورت $U = \langle e_{۰}, e_{۲}, e_{۴}, e_{۶}\rangle$ و $V = \langle e_{۲}, e_{۴}, e_{۶}\rangle$ زوج (U,V) یک ۳ـ تصحیح‌کننده‌ی خطا تشکیل می‌دهد.

فصل ۳

کدهای MDS کوانتومی جدید حاصل از کدهای دوری_ ثابت

۱.۳ مقدمه

کدهای کوانتومی با ماکسیمم فاصله‌ی جدا کننده (MDS) یک کلاس پراهمیت از کدهای کوانتومی می‌باشد. ساختن کدهای MDS کوانتومی که فاصله‌ی آن عددی بزرگ باشد، کار دشواری می‌باشد. در این فصل ما دو کلاس از کدهای MDS کوانتومی با پارامترهای زیر را معرفی می‌کنیم:

۱_ $[[\lambda(q-۱),\lambda(q-۱)-۲d+۲,d]]_q$ جایی‌که $۲\leq d\leq \frac{(q-۱)}{۲}+\lambda-۱$ و $q+۱=\lambda r$ با r زوج

۲_ $[[\lambda(q-۱),\lambda(q-۱)-۲d+۲,d]]_q$ جایی‌که $۲\leq d\leq \frac{(q-۱)}{۲}+\frac{\lambda}{۲}-۱$ و $q+۱=\lambda r$ با r فرد

این دو کلاس از کدهای MDS کوانتومی، پارامترهایی بهتر از آنچه که کدهای شناخته شده‌ی قبلی داشته‌اند، دارا می‌باشند.
کدهای تصحیح‌کننده‌ی خطای کوانتومی نقش مهمی در ارتباطات و محاسبات کوانتومی ایفا می‌کنند. ارتباط بین کدهای کوانتومی و کدهای کلاسیک پیشرفت بسیار خوبی داشته و

نشان داده شده است که ساختن کدهای کوانتومی به ساختن کدهای تصحیح‌کننده‌ی خطای خطی کلاسیک، با خاصیت خودمتعامدبودن، قابل کاهش است.
فرض کنید q توانی از یک عدد اول باشد. یک کد کوانتومی qـ تایی Q از طول n و اندازه‌ی k یک زیرمجموعه‌ی kـ بعدی از زیرفضای q^n بعدی هیلبرت[1] می‌باشد:

$$H = C^{q^n} = C^q \otimes \cdots \otimes C^q.$$

در یک کد تصحیح‌کننده‌ی کوانتومی قابلیت تشخیص و تصحیح خطا مهم می‌باشد. اگر کد کوانتومی دارای مینیمم فاصله‌ی d باشد، می‌تواند هر $d-1$ خطا را شناسایی و هر $\lfloor \frac{d-1}{2} \rfloor$ خطا را تصحیح کند. فرض کنید $k = log_q K$. ما از $[[n,k,d]]_q$ برای نشان دادن یک کد کوانتومی qـ تایی از طول n و اندازه‌ی q^k و فاصله‌ی d استفاده می‌کنیم.

کدهای کوانتومی با پارامترهای $[[n,k,d]]_q$ باید در شرایط کران سینگلتون کوانتومی صدق نمایند، یعنی $k \leq n - 2d + 2$. کد کوانتومی که حالت مرزی این کران را به‌دست می‌آورد یک کد کوانتومی با ماکسیمم فاصله‌ی جدا کننده (MDS) نامیده می‌شود. همان‌گونه که در [۱۷] ذکر شده است تقریباً تمام کدهای MDS کوانتومی qـ تایی فاصله‌ای کمتر یا مساوی $\frac{q}{4} + 1$ دارند. اخیراً کای[2] و ژو[3] دو کلاس جدید از کدهای MDS کوانتومی ساخته‌اند که بر اساس کدهای غیردوری کلاسیک طراحی شده‌اند. همچنین ۶ کلاس جدید از کدهای MDS کوانتومی ساخته‌اند که بر اساس کدهای دوری‌ـ ثابت طراحی شده‌اند. به‌طور کلی این کدها فاصله‌ای بزرگتر از $\frac{q}{4} + 1$ دارند. دو کلاس از کدهای MDS ساخته شده در [۱۸] به‌صورت زیر می‌باشند:

۱ـ $[[\lambda(q-1), \lambda(q-1) - 2d + 2, d]]$ جایی‌که $\lambda = \frac{(q+1)}{2}$ و $2 \leq d \leq q$.

۲ـ $[[\lambda(q-1), \lambda(q-1) - 2d + 2, d]]$ جایی‌که $2 \leq d \leq \frac{(q+1)}{2}$ و $\lambda = \frac{(q+1)}{r}$ با r زوج و $r \neq 2$.

ما این دو کلاس از کدهای کوانتومی را گسترش داده و اولین کلاس از کدهای MDS کوانتومی با پارامترهای

$$\left[[\lambda(q-1), \lambda(q-1) - 2d + 2, d]\right]_q$$

را به‌دست می‌آوریم، جایی‌که $2 \leq d \leq \frac{(q+1)}{2} + \lambda - 1$ و $q + 1 = \lambda r$ با r زوج.
به‌طور کلی کدهای کوانتومی به‌دست آمده فاصله‌ای بزرگتر از $\frac{q}{4} + 1$ دارند. علاوه بر این ما بررسی می‌کنیم وقتی r یک مقسوم‌علیه فرد از $q+1$ باشد، دومین کلاس از کدهای MDS کوانتومی با پارامترهای زیر را به‌دست می‌آوریم:
$\left[[\lambda(q-1), \lambda(q-1) - 2d + 2, d]\right]_q$ جایی‌که $2 \leq d \leq \frac{(q+1)}{2} + \frac{\lambda}{4} - 1$ و $q + 1 = \lambda r$.

[1] Hilbert
[2] Kai
[3] Zhu

۲.۳ خلاصه‌ای از کدهای دوری_ثابت

فرض کنید $F_{q^۲}$ یک میدان گالوا[۴] با $q^۲$ عضو باشد، جایی‌که q یک عدد اول می‌باشد. C یک کد خطی $q^۲$ ـ تایی از طول n و زیرفضایی غیرتهی از $F_{q^۲}^n$ می‌باشد.
یک کد خطی $q^۲$ ـ تایی C از طول n، یک کد η ـ دوری_ثابت نامیده می‌شود اگر با انتقال دوری روی $F_{q^۲}^n$ به‌صورت زیر تعریف شود:

$$(c_۰, c_۱, \ldots, c_{n-۱}) \longrightarrow (\eta c_{n-۱}, c_۰, \ldots, c_{n-r}),$$

جایی که η یک عنصر غیرصفر از $F_{q^۲}$ می‌باشد.
هر کدواژه‌ی $c = (c_۰, c_۱, \ldots, c_{n-۱})$ معمولاً با یک چندجمله‌ای

$$c(x) = c_۰ + c_۱x + \cdots + c_{n-۱}x^{n-۱}$$

معرفی می‌شود و کد C یک ارتباط دوری با مجموعه همه‌ی چندجمله‌ای‌های حاضر از کدواژه‌ها دارد. بنابراین در حلقه‌ی $\frac{F_{q^۲}[x]}{(x^n-\eta)}$، $xc(x)$ یک انتقال η ـ دوری_ثابت از $c(x)$ می‌باشد. می‌دانیم که یک کد خطی C از طول n روی $F_{q^۲}$ یک η ـ دوری_ثابت می‌باشد اگر و تنها اگر C یک ایده‌آل از حلقه‌ی خارج قسمتی $\frac{F_{q^۲}[x]}{x^n-\eta}$ باشد. علاوه بر این، $\frac{F_{q^۲}[x]}{x^n-\eta}$ یک ایده‌آل اصلی می‌باشد که ایده‌آل‌ها به‌وسیله‌ی فاکتورهایی از $x^n - \eta$ تولید می‌شوند و $C = \langle f(x)\rangle$ و $f(x)|(x^n - \eta)$.
دو بردار $x = (x_۰, x_۱, \ldots, x_{n-۱})$ و $y = (y_۰, y_۱, \ldots, y_{n-۱})$ متعلق به $F_{q^۲}^n$ را در نظر بگیرید. ضرب داخلی هرمیتی[۵] به‌صورت زیر تعریف می‌شود:

$$\langle x.y\rangle = x_۰\overline{y_۰} + x_۱\overline{y_۱} + \cdots + x_{n-۱}\overline{y_{n-۱}} \in F_{q^۲}$$

جایی‌که $\overline{y_i} = y_i^q$.
بردارهای x و y متعامدند اگر ضرب داخلی هرمیتی آنها صفر باشد یعنی $\langle x.y\rangle = ۰$.
برای یک کد خطی $q^۲$ ـ تایی C از طول n، کد دوگان هرمیتی از C به‌صورت زیر تعریف می‌شود:

$$C^{\perp H} = \left\{x \in F_{q^۲}^n \mid \langle x.y\rangle = ۰ \quad y \in C \text{ برای همه}\right\}.$$

یک کد خطی C از طول n روی $F_{q^۲}$ خودمتعامد هرمیتی نامیده می‌شود اگر $C \subseteq C^{\perp H}$ و خوددوگان هرمیتی نامیده می‌شود اگر $C = C^{\perp H}$.
فرض کنیم $gcd(q, n) = ۱$. فرض کنیم δ یک ریشه‌ی rnـام اولیه از یکه‌ها باشد و گسترش میدان $F_{q^۲}$ را وقتی که $\delta^n = \eta$ در نظر بگیرید. فرض کنیم $\varepsilon = \delta^r$. بنابراین ε یک ریشه‌ی nـام اولیه از یکه‌ها می‌باشد، بنابراین داریم:

$$x^n - \eta = \prod_{i=۰}^{n-۱}(x - \delta\varepsilon^i) = \prod_{i=۰}^{n-۱}(x - \delta^{۱+ir}).$$

[4] Galois
[5] Hermitian

فرض کنید $\Omega = \{1 + ir \mid 0 \leq i \leq n-1\}$ باشد. برای هر $j \in \Omega$، c_j یک چرخه‌ی q^2 ـعضوی شامل j به پیمانه‌ی rn باشد. حال فرض کنید C یک کد η ـدوری_ثابت از طول n روی F_{q^2} با چندجمله‌ای مشخصه‌ی $g(x)$ باشد. بنابراین مجموعه‌ی $Z = \{j \in \Omega \mid g(\delta^j) = 0\}$ تعریف دیگری از C می‌باشد. به‌راحتی می‌توان دید که مجموعه‌ی C اجتماع تعدادی از هم‌دسته‌های q^2 ـدایره‌بر به پیمانه‌ی rn و بعد $dim(C) = n - |Z|$ می‌باشد و به‌سادگی می‌توانید ببینید که $C^{\perp}$ به‌صورت زیر تعریف می‌شود:

$$Z^{\perp H} = \{z \in \Omega \mid -qz \ mod \ rn \notin z\}.$$

مشابه کدهای دوری، برای کدهای دوری_ثابت نیز یک کران BCH وجود دارد.

قضیه ۱.۲.۳ (کران BCH برای کدهای دوری_ثابت). فرض کنید $gcd(q, n) = 1$ و $C = \langle g(x) \rangle$ یک کد η ـدوری_ثابت از طول n روی F_{q^2} با ریشه‌های

$$\left\{\delta^{1+ir} | 0 \leq i \leq d-2\right\}$$

باشد، جایی‌که δ یک ریشه‌ی rnـام اولیه از یکه‌ها باشد. دراین‌صورت مینیمم فاصله‌ی کد C، حداقل d می‌باشد.

نتیجه‌ی زیر محکی برای تعیین این‌که کد q^2 ـتایی η ـدوری_ثابت داده شده شامل کد دوگان خود می‌باشد یا نه ارایه می‌دهد.

لم ۱.۲.۳. فرض کنید r یک مقسوم علیه مثبت از $q+1$ باشد و $\eta \in F_{q^2}$ دارای رتبه‌ی r باشد. فرض کنید C یک کد η ـدوری_ثابت از طول n روی F_{q^2} باشد، طبق تعریف $Z \subseteq \Omega$ و C شامل کد دوگان هرمیتی است اگر و تنها اگر $Z \cap Z^{-q} = \emptyset$ جایی‌که $Z^{-q} = \{-qz \ mod \ rn | n \in z\}$.

۳.۳ ساختن کدها

فرض کنید $r = \frac{(q+1)}{gcd(v,q+1)}$ و q یک توان اول فرد باشد. در ادامه با توجه به‌این‌که r فرد یا زوج باشد ما با استفاده از ساختار هرمیتی کدهای MDS کوانتومی را می‌سازیم. در ابتدا ساختن کدهای کوانتومی هرمیتی را یادآوری می‌نماییم.

لم ۱.۳.۳. اگر C یک کد خطی q^2 ـتایی با پارامترهای $[n, k, d]$ باشد به‌طوری‌که $C^{\perp H} \subseteq C$. دراین‌صورت یک کد کوانتومی $[[n, 2k-n, \geq d]]_q$ وجود دارد.

حالت اول: $n = \lambda(q-1)$ و λ یک مقسوم‌علیه از $q+1$ است و r زوج می‌باشد.

فرض کنید $r = \frac{(q+1)}{gcd(v,q+1)}$ زوج باشد. برای هر $r \in \{1,2,\ldots,q\}$ و فرض کنید $\varepsilon = w^{v(q-1)}$ و $\lambda = \frac{(q+1)}{r}$.
با استفاده از کدهای ε ـ دوری ـ ثابت، کدهای MDS کوانتومی q ـ تایی از طول $\lambda(q-1)$ را می‌سازیم. واضح است که مجموعه‌ی q^2 ـ دایره‌بر شامل $1 + jr + \frac{r-2}{2}(q+1)$ به پیمانه‌ی rn تنها یک عضو $1 + jr + \frac{r-2}{2}(q+1)$ را دارد جایی‌که

$$C_{1+jr+\frac{r-2}{2}(q+1)} = \left\{1 + jr + \frac{r-2}{2}(q+1)\right\},$$

$$0 \leq j \leq \frac{r-2}{2}(q+1)$$

لم ۲.۳.۳. فرض کنید $r = \frac{(q+1)}{gcd(v,q+1)}$ زوج باشد و $r \neq q+1$ برای هر $v \in \{1,2,\ldots,q\}$ باشد. فرض کنید $n = \lambda(q-1)$ و $\lambda = \frac{(q+1)}{r}$.
فرض کنید که C یک کد ε ـ دوری ـ ثابت از طول n روی F_{q^2} باشد که به‌صورت زیر تعریف می‌شود:

$$Z = \bigcup_{j=1}^{\delta} C_{1+r(j-1)+\frac{r-2}{2}(q+1)},$$

جایی‌که $2 - (q+1) < \delta \leq 1$. دراین‌صورت $C^{\perp H} \subseteq C$.

اثبات. فرض کنید که کد C شامل کد دوگان هرمیتی نباشد و بنابر لم ۱.۲.۳، داریم: $Z \cap Z^{-q} \neq \emptyset$ دراین‌صورت دو عدد صحیح $k,l \in \left\{1 + 2 + \cdots + \frac{r+2}{2r}(q+1) - 2\right\}$ وجود دارند به‌طوری‌که:

$$1 + r(k-1) + \frac{r-2}{2}(q+1) \overset{rn}{\equiv} -\left[1 + r(l-1) + \frac{r-2}{2}(q+1)\right]_q$$

و این معادل است با

$$k + ql - \lambda \equiv 0 \ mod\ \lambda(q-1).$$

فرض کنید $r = 2s$ با مقادیر صحیح و $s \geq 1$. بنابراین $1 \leq l < \lambda(s+1) - 2$. ما l را به فرم $l = u\lambda + v$ بیان می‌کنیم، جایی‌که $0 \leq u \leq s$ و $0 \leq v \leq \lambda - 2$ (به جز برای مورد $u = v = 0$). دراین‌صورت دو حالت زیر را داریم که مورد بررسی قرار می‌دهیم:

۱ـ $0 \leq u \leq s$ و $1 \leq v \leq \lambda - 2$.
دراین‌صورت $k + l + (q-1)v - \lambda \equiv 0$ به پیمانه‌ی $\lambda(q-1)$ پس $l \leq k$ و $l \leq \frac{r+2}{2r}(q+1) - 2 \leq q - 1$ و این یعنی

$$k + l + (q-1)v - \lambda < (q-1) + (q-1) + (\lambda-2)(q-1) - \lambda = \lambda(q-2)$$

و این یک تناقض است.

۲ـ $s \leq u \leq ۱$ و $v = ۰$. بنا به رابطه‌ی (۱)، $k + l - \lambda \equiv ۰ \ mod \ \lambda(q-۱)$ اما $\lambda > ۱$ و $k + l - \lambda < ۲(q-۱) - \lambda < ۲(q-۱)$ و این نیز به تناقض منجر می‌شود و اثبات کامل است.

□

قضیه ۱.۳.۳. فرض کنید r یک مقسوم‌علیه زوج از $q+۱$ باشد و $r \neq q+۱$ و فرض کنید $n = \lambda(q-۱)$ که $\lambda = \frac{q+۱}{r}$ دراین‌صورت یک $[[n, n-۲d+۲, d]]_q$ ـ کد کوانتومی MDS وجود دارد جایی‌که

$$۲ \leq d \leq \frac{r+۲}{۲r}(q+۱) - ۱.$$

اثبات. فرض کنید $\varepsilon = w^{\lambda(q-۱)}$ جایی‌که w یک عنصر اولیه از $F_{q^۲}$ می‌باشد. فرض کنید C یک کد ε ـ دوری_ثابت از طول n روی $F_{q^۲}$ باشد و با مجموعه Z مشخص شود

$$Z = \bigcup_{j=۱}^{\delta} C_{۱+r(j-۱)+\frac{r-۲}{۲}(q+۱)}$$

جایی‌که $۲ - (q+۱) \leq \delta \leq \frac{r+۲}{۲r}(q+۱) - ۱$.
با استفاده از لم ۲.۳.۳، کد C شامل کد دوگان هرمیتی است و $dim(C) = n - \delta$. کران BCH برای کدهای دوری_ثابت، نشان می‌دهد که فاصله‌ی کد C حداقل $\delta + ۱$ می‌باشد. در این‌جا C یک کد دوری_ثابت با پارامترهای $[n, n-\delta, \geq \delta+۱]_{q^۲}$ است. حال با استفاده از ساختار هرمیتی ما یک کد کوانتومی با پارامترهای $[[n, n-۲\delta, \geq \delta+۱]]_q$ به‌دست می‌آوریم. با استفاده از کران سینگلتون برای کدهای کوانتومی ما یک $[[n, n-۲\delta, \delta+۱]]_q$ ـ کد به‌دست می‌آوریم که یک کد MDS کوانتومی می‌باشد. □

با در نظر گرفتن $r = ۲$ در قضیه‌ی ۱.۳.۳ یک کد MDS کوانتومی با پارامترهای $[[\frac{(q^۲-۱)}{۲}, \frac{(q^۲-۱)}{۲-۲d+۲}, d]]_q$ به‌دست می‌آوریم جایی‌که $۲ \leq d \leq q$، اما زمانی‌که r یک مقسوم‌علیه زوج از $q+۱$ باشد و $r \neq ۲$ باشد یک کد کوانتومی با پارامترهای $[[\lambda(q-۱), \lambda(q-۱) - ۲d + ۲, d]]_q$ وجود دارد جایی‌که $\frac{(q+۱)}{۲} + ۱ \leq d \leq \frac{(q+۱)}{۲} + \lambda - ۱$ این کدها در مجموع مینیمم فاصله‌ی نسبتاً بزرگی دارند. [۱۸] را ببینید.
ما می‌توانیم $r = ۲$ و $r \neq ۲$ را به هم ارتباط داده و کدهای MDS بیشتری با این ساختار به‌دست آوریم.

مثال ۱.۳.۳. فرض کنید $q = ۱۹$. با استفاده از قضیه‌ی ۱.۳.۳ می‌توانیم ۴ کد کوانتومی MDS با پارامترهای زیر بسازیم:

$$[[۹۰,۶۴,۱۴]]_{۱۹} \ , \ [[۹۰,۶۶,۱۳]]_{۱۹} \ , \ [[۹۰,۶۸,۱۲]]_{۱۹} \ , \ [[۹۰,۷۰,۱۱]]_{۱۹}$$

مثال ۲.۳.۳. فرض کنید $q = ۲۳$. با استفاده از قضیه‌ی ۱.۳.۳ چند کد کوانتومی MDS در جدول زیر مشخص شده‌اند:

جدول ۱.۳: کدهای MDS کوانتومی جدید

λ	r	n	$[[n,k,d]]_q$
2	12	44	$[[44,20,13]]_{23}$
3	8	66	$[[66,42,13]]_{23}$
3	8	66	$[[66,40,14]]_{23}$
4	6	88	$[[88,64,13]]_{23}$
4	6	88	$[[88,62,14]]_{23}$
4	6	88	$[[88,60,15]]_{23}$
6	4	132	$[[132,108,13]]_{23}$
6	4	132	$[[132,106,14]]_{23}$
6	4	132	$[[132,104,15]]_{23}$
6	4	132	$[[132,102,16]]_{23}$
6	4	132	$[[132,100,17]]_{23}$

حالت دوم: $n=\lambda(q-1)$ که λ یک مقسوم‌علیه از $q+1$ است و r فرد می‌باشد.
در [۱۸] مؤلف حالتی را که r یک مقسوم‌علیه زوج از $q+1$ می‌باشد را بررسی می‌نماید اما اکنون r یک مقسوم‌علیه فرد از $q+1$ می‌باشد. در این قسمت ما این مسئله را بررسی کرده و یک کلاس جدید از کدهای MDS کوانتومی را معرفی می‌نماییم.
فرض کنید $r=\frac{(q+1)}{gcd(v,q+1)}$ فرد باشد برای هر $v\in\{1,2,\ldots,q\}$ و $\varepsilon=\omega^{v(q-1)}$ و $\lambda=\frac{(q+1)}{r}$.
با استفاده از کدهای ε ـ دوری ـ ثابت ما کدهای MDS کوانتومی q ـ تایی از طول $\lambda(q-1)$ را طراحی می‌کنیم. واضح است که مجموعه‌ی دایره‌بر q^2 شامل $1+jr+\frac{r-1}{2}(q+1)$ به‌پیمانه‌ی rn تنها یک عنصر $1+jr+\frac{r-1}{2}(q+1)$ را دارد و

$$C_{1+jr+\frac{r-1}{2}(q+1)}=\left\{1+jr+\frac{r-1}{2}(q+1)\right\},$$

که $0\leq j\leq\frac{r+1}{2r}(q+1)$.

لم ۳.۳.۳. فرض کنید $r=\frac{(q+1)}{gcd(v,q+1)}$ برای هر $v\in\{1,2,\ldots,q\}$ فرد باشد. فرض کنید $n=\lambda(q-1)$ و $\lambda=\frac{(q+1)}{r}$. حال فرض کنید C یک کد ε ـ دوری ـ ثابت از طول n روی F_{q^2} باشد که به‌صورت زیر تعریف می‌شود:

$$Z=\bigcup_{j=1}^{\delta}C_{1+r(j-1)+\frac{r-1}{2}(q+1)},$$

جایی‌که $1\leq\delta\leq\frac{r+1}{2r}(q+1)-2$. در این‌صورت $C^{\perp H}\subseteq C$.

اثبات. فرض کنید که C شامل کد دوگان هرمیتی نباشد، دراین‌صورت $Z \cap Z^{-q} \neq \emptyset$. از این‌رو دو عدد صحیح k و l وجود دارند که $k,l \in \{۱,۲,\ldots,\frac{r+۱}{۲r}(q+۱)-۲\}$ به‌طوری‌که

$$۱+r(k-۱)+\frac{r-۱}{۲}(q+۱) \equiv -\left[۱+r(l-۱)+\frac{r-۱}{۲}(q+۱)\right]_q \mod rn$$

که معادل است با این‌که

$$k+ql \equiv ۰ \mod \lambda(q-۱). \qquad (۱.۳)$$

حال $r=۲s+۱$ که $s \geq ۱$ و مقدار s عدد صحیح می‌باشد، دراین صورت $۱ \leq l \leq \lambda(s+۱)-۲$. ما l را به فرم $l=u\lambda+v$ می‌نویسیم جایی‌که $۰ \leq u \leq s$ و $۰ \leq v \leq \lambda-۲$ (به جز برای حالت $u=v=۰$) دو حالت زیر را داریم که مورد بررسی قرار می‌دهیم.

۱_ $۰ \leq u \leq s$ و $۰ \leq v \leq \lambda-۲$.
با استفاده از رابطه‌ی (۱.۳) داریم:

$$k+l+(q-۱)v \equiv ۰ \mod \lambda(q-۱)$$

حال با توجه به‌این‌که $l \leq k$ و $l \leq \frac{r+۱}{۲r}(q+۱)-۲ \leq q-۱$. در نتیجه داریم:

$$k+l+(q-۱)v < (q-۱)+(q-۱)+(\lambda-۲)(q-۱) = \lambda(q-۱)$$

و این یک تناقض است.

۲_ $۱ \leq u \leq s$ و $v=۰$.
با استفاده از رابطه (۱.۳) داریم:

$$k+l \equiv ۰ \mod \lambda(q-۱)$$

اما $k+l < ۲(q-۱)$ و $\lambda > ۱$ و این یک تناقض است و اثبات کامل می‌شود.

□

قضیه ۲.۳.۳. فرض کنید r یک مقسوم علیه فرد از $q+۱$ باشد و $n=\lambda(q-۱)$ و $\lambda=\frac{(q+۱)}{r}$. دراین‌صورت یک کد MDS کوانتومی با پارامترهای $[[n,n-۲d+۲,d]]_q$ وجود دارد جایی‌که $۲ \leq d \leq \frac{r+۱}{۲r}(q+۱)-۱$.

اثبات. $\varepsilon = w^{\lambda(q-۱)}$ جایی‌که w یک عنصر اولیه از $F_{q^۲}$ می‌باشد. فرض کنید C یک کد ε ـدوری_ثابت از طول n روی $F_{q^۲}$ باشد که به‌صورت زیر تعریف می‌شود:

$$Z = \bigcup_{j=۱}^{\delta} C_{۱+r(j-۱)+\frac{r-۱}{۲}(q+۱)}$$

جایی‌که $۲ - (q+۱) \leq \delta \leq \frac{r+۱}{۲r}$ ۱.
با استفاده از لم ۳.۳.۳، C شامل کد دوگان هرمیتی می‌باشد و $dim(C) = n - \delta$ و $d(C) \geq$ $\delta + ۱$. بنابراین C یک کد ε ــ دوری‌ــ ثابت با پارامترهای $[n, n-\delta, \geq \delta+۱]_q$ می‌باشد. حال با استفاده از کران سینگلتون برای کدهای کوانتومی یک $[[n, n-۲\delta, \delta+۱]]_q$ ــ کد به‌دست می‌آوریم که یک کد MDS کوانتومی می‌باشد. □

با استفاده از قضیه‌ی ۲.۳.۳ ما می‌توانیم کدهای MDS کوانتومی با پارامترهای

$$[[\lambda(q-۱), \lambda(q-۱) - ۲d + ۲, d]]_q$$

را بسازیم جایی‌که $۱ - \frac{\lambda}{۲} + \frac{(q+۱)}{۲} \leq d \leq \frac{(q+۱)}{۲}$.
این کلاس از کدهای MDS کوانتومی مینیمم فاصله‌ی نسبتاً بزرگی دارند.

مثال ۳.۳.۳. فرض کنید $q = ۱۷$. با استفاده از قضیه‌ی ۲.۳.۳، می‌توانیم ۴ کد MDS جدید بسازیم که در جدول ۳ــ۲ مشخص شده‌اند.

جدول ۲.۳: کدهای MDS کوانتومی جدید

λ	r	n	$[[n,k,d]]_q$
2	9	32	$[[32,16,9]]_{17}$
6	3	96	$[[96,80,9]]_{17}$
6	3	96	$[[96,78,10]]_{17}$
6	3	96	$[[96,76,11]]_{17}$

مثال ۴.۳.۳. فرض کنید $q = ۲۹$. با استفاده از قضیه‌ی ۲.۳.۳ چند کد MDS کوانتومی جدید ساخته‌ایم که در جدول ۳ــ۳ مشخص می‌باشند.

جدول ۳.۳: کدهای MDS کوانتومی جدید

λ	r	n	$[[n,k,d]]_q$
2	15	56	$[[56,28,15]]_{29}$
6	5	168	$[[168,140,15]]_{29}$
6	5	168	$[[168,138,16]]_{29}$
6	5	168	$[[168,136,17]]_{29}$
10	3	280	$[[280,252,15]]_{29}$
10	3	280	$[[280,250,16]]_{29}$
10	3	280	$[[280,248,17]]_{29}$
10	3	280	$[[280,246,18]]_{29}$
10	3	280	$[[280,244,19]]_{29}$

مراجع

[1] A. Ashikhmin and E. Kill, Non-binary quantum stabilizer codes, *IEEE Trans. Inf. Theory*, **47**(7) (2001), 306–3072.

[2] N. Aydin, I. Siap and D.J. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, *Des. Codes Cryptogr.*, **24** (2001), 313–326.

[3] J. Bierbrauer and Y. Edel, Quantum twisted codes, *J. Comb. Des.*, **8**(3) (2000), 174–188.

[4] E. J. Candes, J. K. Romberg and T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete Fourier information, *IEEE Trans. Inform. Theory*, **52**(8) (2006), 489–509.

[5] I. Duursma and R. Kotter, Error-locating pairs for cyclic codes, *IEEE Trans. Inform. Theory*, **40** (1994), 1108–1121.

[6] P. F. Frenkel, Simple proof of Chebotarevs theorem on roots of unity, arXiv:math/032398.

[7] D. Goldstein, R. M. Guralnick and I.M. Isaacs, Inequalities for finite group permutation modules, *Trans. Amer. Math. Soc.*, **10** (2005), 4017–4042.

[8] B. Hurley and T. Hurley, System of MDS codes from units and idempotents, *Discrete Math.*, **335** (2014), 81–89.

[9] B. Hurley and T. Hurley, Paraunitary matrices and group rings, *Int. J. Group Theory*, **1**(1) (2014), 31–56.

[10] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu and C. H. Oh, Graphical nonbinary quantum error-correcting codes, *Phys. Rev. A.*, **78**(1) (2001), 1–11.

[11] T. Hurley, Group rings and rings of matrices, *Int. J. Pure Appl. Math.*, **31**(3)(2006), 319–335.

[12] L. Jin and C. Xing, A construction of new quantum MDS codes, *IEEE Trans. Inf. Theory*, **65**(5) (2014), 2921–2925.

[13] L. Jin, S. Ling, J. Luo and C. Xing, Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, *IEEE Trans. Inf. Theory*, **56**(9) (2010), 4735–4740.

[14] O. M. Baksalary, D. S. Bernstein and G. Trenkler, On the equality between rank and trace of an idempotent matrix, *Appl. Math. Comput.*, **217** (2010), 4076–4080.

[15] R. E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, 2003.

[16] L. Wang and S. Zhu, New quantum MDS codes derived from constacyclic codes, *Quantum Inf. Process*, **14** (2015), 881–889.

[17] X. Kai, S. Zhu and P. Li, Constacyclic codes and some new quantum MDS codes, *IEEE Trans. Inf. Theory*, **60**(4) (2014), 2080–2085.

[18] X. Kai and S. Zhu, New quantum MDS codes from negacyclic codes, *IEEE Trans. Inf. Theory*, **59**(2) (2013), 1193–1197.

واژه‌نامه فارسی به انگلیسی

اول ژرمین . . . . . Germain prime
اول . . . . . Prime
اولیه . . . . . Primitive
توان . . . . . Power
تشخیص خطا . . . . . Error-detecting
تصحیح خطا . . . . . Error-correcting
جداگانه . . . . . Separable
چندجمله‌ای . . . . . Polynomial
خودتوان . . . . . Idempotent
خودمتعامد . . . . . Self-orthogonal
دوری . . . . . Cyclic
طول . . . . . Length
فاصله . . . . . Distance
کد دوگان . . . . . Dual code
کدهای خطی . . . . . Linear codes
کدهای ثابت ـ دوری . . . . . Constacyclic codes
کدهای کلاسیک . . . . . Classical codes
کران سینگلتون . . . . . Singleton bound
کوانتوم . . . . . Quantum
ماتریس کنترل توازن . . . . . Parity check matrix
ماتریس فوریه . . . . . Fourier matrix
ماتریس مولد . . . . . Genarator matrix
میدان متناهی . . . . . Finite field
یکه . . . . . Unit

واژه‌نامه انگلیسی به فارسی

کدهای کلاسیک ..... Classical codes
کدهای ثابت‌ـدوری ..... Constacyclic codes
دوری ..... Cyclic
فاصله ..... Distance
کد دوگان ..... Dual code
تصحیح خطا ..... Error-correcting
تشخیص خطا ..... Error-detecting
میدان متناهی ..... Finite fields
ماتریس فوریه ..... Fourier matrix
ماتریس مولد ..... Generator matrix
اول اصلی ..... Germain prime
خودتوان ..... Idempotent
طول ..... Length
کدهای خطی ..... Linear codes
ماتریس کنترل توازن ..... Parity check matrix
چندجمله‌ای ..... Polynomial
توان ..... Power
اول ..... Prime
اولیه ..... Primitive
کوانتوم ..... Quantum
جداگانه ..... Seperable
خودمتعامد ..... Self-orthogonal
کران سینگلتون ..... Singleton bound
یکه ..... Unit

Abstract

In this thesis, some algebraic systems are considered which enables us to construct some new classe of maximum distance separable (MDS) codes. The methods use unit and idempotent schemes. Quantum maximum-distance-separable (MDS) codes form an important class of quantum codes. It is very hard to construct quantum MDS codes with relatively large minimum distance. In this thesis, based on classical constacyclic codes, we construct two classes of quantum MDS codes with parameters $[\,[\lambda(q-1), \lambda(q-1)-2d+2, d]\,]_q$ where $2 \leq d \leq \frac{(q-1)}{2} + \lambda - 1$ and $q+1 = \lambda r$ with r even, and

$[\,[\lambda(q-1), \lambda(q-1)-2d+2, d]\,]_q$ where $2 \leq d \leq \frac{(q-1)}{2} + \frac{\lambda}{2} - 1$ and $q+1 = \lambda r$ with r odd. The quantum MDS codes exhibited here have parameters better than the ones available in the literature.

Keywords: Constacyclic codes; Quantum codes; MDS codes; Unit; Idempotent.

Shahrood University of Technology

Faculty Of Mathematical Sciences

MSc Thesis in: Cryptography and Coding

On some properties of quantum maximum-distance-separable (MDS) codes

By: Amir Karimi

Supervisor

Dr. Abdollah Alhevaz

Advisor

Dr. Ebrahim Hashemi

October 2019