دانشگاه صنعتی شاهرود
دانشکده علوم ریاضی
گروه ریاضی

پایان‌نامه کارشناسی ارشد

عنوان

کدهای کامل و موضوعات مربوط به آن

نگارش
عالیه محمدی

استاد راهنما
دکتر نادر جعفری‌راد

تیر ۱۳۹۱

دانشگاه صنعتی شاهرود

مدیریت تحصیلات تکمیلی

فرم شماره (۶)

بسمه تعالی

شماره :

تاریخ :

ویرایش :

فرم 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 **عالیه محمدی** رشته **ریاضی کاربردی** گرایش **گراف** تحت عنوان **کدهای کامل و موضوعات مربوط به آن**

که در تاریخ **۱۳۹۱.۴.۲۴** با حضور هیأت محترم داوران در دانشگاه صنعتی شاهرود برگزار گردید به شرح ذیل اعلام می گردد:

قبول (با درجه : بسیار خوب امتیاز ۱۸/۴۹) ☑	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 هیأت داوران	نام ونام خانوادگی	مرتبۀ علمی	امضاء
۱ـ استادراهنما	۱- دکتر نادر جعفری‌راد	دانشیار	
۲ـ استاد مشاور	ـــــــ	ـــــ	
۳ـ نماینده شورای تحصیلات تکمیلی	۱- دکتر علیرضا ناظمی	استادیار	
۴ـ استاد ممتحن	۱- دکتر بهزاد صالحیان	استادیار	
۵ ـ استاد ممتحن	۱- دکتر میثم علیشاهی	استادیار	

رئیس دانشکده : دکتر احمد زیره

دانشکده ریاضی - دانشگاه صنعتی شاهرود

قدردانی

سپاس بی کران پروردگار یکتا را که هستی مان بخشید و به طریق علم و دانش رهنمونمان شد و به هم نشینی با رهروان معرفت مفتخرمان نمود و خوشه چینی از علم و معرفت را روزیمان ساخت.

در این جا بر خود می دانم از استاد گرانقدرم جناب آقای دکتر نادر جعفری راد به پاس هدایت و راهنمایی اینجانب در طول انجام این پایان نامه و هم چنین از تمام اساتیدی که به نحوی افتخار شاگردی در محضر ایشان را داشتم تشکر و قدردانی کنم.

در پایان نیز از پدر و مادر عزیز و همسر مهربانم که در طول تحصیل همیشه مشوق بنده بوده اند کمال تشکر و سپاس گزاری را دارم.

تعهد نامه

اینجانب عا لیه محمدی به شماره دانشجویی **۸۹۰۴۱۳۴** دانشجوی دوره کارشناسی ارشد **رشته ریاضی کاربردی** دانشکده **علوم ریاضی** دانشگاه صنعتی شاهرود نویسنده پایان نامه **کدهای کامل و موضوعات مربوط به آن** تحت راهنمائی **دکترنادر جعفری راد** متعهد می شوم :

- تحقیقات در این پایان نامهتوسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است .
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « Shahrood University of Technology » به چاپ خواهد رسید .
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج ازپایان نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه ، در مواردی که از موجود زنده (یا بافتهای آنها) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

تاریخ ۹۱,۴,۲۶

امضای دانشجو عالیه محمدی

۹۱/٤/۲۶

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج ، کتاب ، برنامه های رایانه ای ، نرم افزار ها و تجهیزات ساخته شده است) متعلق به دانشگاه صنعتی شاهرود می باشد . این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود .
- استفاده از اطلاعات و نتایج موجود در پایان نامهبدون ذکر مرجع مجاز نمی باشد.

چکیده

مطالعه‌ی کدهای کامل به خاطر ساختار و ویژگی‌های جالب و خوبی که دارند از اهمیت خاصی برخوردار است.
در این پایان‌نامه ابتدا نگاهی کوتاه به تاریخچه‌ی نظریه‌ی کدگذاری انداخته و به بیان کاربرد این نظریه در علوم مختلف می‌پردازیم. در ادامه با خلاصه‌ای از مفاهیم مربوط به کدهای کامل آشنا می‌شویم و چند نوع کد کامل معرفی می‌کنیم. در پایان ساختار جدیدی از کدهای کامل با رتبه‌ی تام به نام α-کدهای نرمال را ارائه می‌دهیم که تا کنون ارائه نشده است. اما قبل از ارائه‌ی این ساختار باید با مفاهیم ضرایب فوریه و ابردوگان کد کامل آشنا شویم. در پایان نیز مثالی از کدهای کامل با رتبه تام به طول ۳۱ معرفی می‌شود.

واژه‌های کلیدی: کدهای کامل،کد کامل با رتبه‌ی تام، α- کدواژه، α- کد نرمال.

پیشگفتار

امروزه با پیشرفت قابل توجه در زمینه‌ی ارتباطات، نظریه اطلاعات و نظریه کدگذاری و با توجه به کاربرد وسیع مفاهیم موجود در ریاضیات در این رشته‌های جدید، زمینه‌ی مناسبی برای انجام تحقیقات کاربردی با استفاده از مفاهیم ریاضی در این حیطه وجود دارد. علاوه بر این نظریهی کدگذاری در بسیاری از علوم مورد استفاده قرار گرفته است که برخی از این کاربردها در داخل متن ذکر می‌شود. یکی از کاربردهای جذاب این نظریه در زمینهی ژنتیک و کدگشایی DNA است. در حقیقت نظریه کدگذاری با وجود جدید بودن، یکی از شاخه‌های پر کاربرد ریاضیات است که به سرعت در حال گسترش است. این شاخه از ریاضیات ابتدا در رشتههای مهندسی الکترونیک و مخابرات متولد شد و در حال حاضر یکی از مباحث مهم در رشتههای الکترونیک، مخابرات و کامپیوتر است.

آن‌چه در این پایان‌نامه بیان می‌شود بررسی کدهای کامل و مفاهیم مربوط به آن است. در این راستا با چند نوع کد کامل آشنا می‌شویم که از اهمیت زیادی برخوردارند و در نهایت ساختاری جدید از کدهای کامل با رتبه‌ی تام به نام $\alpha-$ کدهای نرمال، ارائه می‌دهیم.

فهرست مطالب

فصل ۱

تاریخچه و مفاهیم مقدماتی نظریه کدگذاری

۱.۱ مقدمه

قسمت وسیعی از اطلاعات که بر روی سیاره زمین مبادله می‌شوند، درقالب اعداد نشان داده شده‌اند. پیام های الکترونیکی، تلفن همراه، معاملههای بانکی، هدایت از راه دور ماهواره‌ها، انتقال تصاویر از راه دور، دیسک‌های CD یا DVD و غیره. در تمام این مثال‌ها اطلاعات به‌صورت دنباله‌ای از اعداد که به طور فیزیکی متناظر با علائم الکتریکی یا علائم دیگرند، ترجمه می‌شوند و یا گفته می‌شود کدگذاری شده‌اند. به صورت دقیق‌تر، اطلاعات در مجموع به شکل دنباله‌ای از ارقام دودویی (اعداد ۰ یا ۱) که بیت نیز نامیده می‌شوند، کدگذاری شده‌اند.
یک مسئله بزرگ در مخابره اطلاعات، خطاها هستند. کافی است که خراش کوچکی روی یک دیسک، یک اختلال در دستگاه، یا هر نوع پدیده پارازیت، پیام مخابره شده را با خطا همراه سازد، یعنی صفرها به طور ناگهانی به یک یا بالعکس تغییر کنند. بنابراین یکی از راههای بیشمار رهایی از این گونه اشکال، امکان کشف و حتی تصحیح چنین خطاهایی است. در این موارد نیازمند کدهای تصحیح کننده خطاها هستیم. مبنا و اساس عمل این کدها بدین صورت است که "کلمات" عددی رساننده پیام را طولانی می‌کنیم، به طریقی که قسمتی از بیت‌ها به عنوان بیت‌های کنترل به کار می‌روند. به عنوان مثال در صورت حساب‌های بانکی، یک حرف کلیدی

به یک شماره حساب افزوده می‌شود ، تا بتوان خطای یک انتقال را کشف کرد. به بیان دیگر فلسفه کدهای تصحیح کننده ایجاد پیام های اضافی است به طوری که هر کلمه از پیام به طریقی طولانی می‌شود که حاوی اطلاعاتی در مورد خود پیام باشد.
این بخش از ریاضیات یعنی نظریه کدگذاری از جبر پیشرفته برای دستیابی به اهداف خود استفاده می کند.

۲.۱   تاریخچه

همان‌طور که گفته شد کدگذاری یکی از شاخه‌های بسیار جالب و کاربردی ریاضیات است که همواره کاربردهای بسیاری در حوزه های گوناگون داشته است. در زمان جنگ جهانی دوم ریاضیدانان بسیاری با بکارگیری روش‌های کدگذاری پیچیده سعی در کد کردن داده های نظامی داشتند بگونه ای که طرف مقابل نتواند آنها را رمزگشایی کند. امروزه هم در حوزه های گوناگونی از جمله رایانه لزوم به‌کارگیری رمزهای پیچیده تر هم چنین امکان کشف و تصحیح خطا در پیام های دریافتی برای سیستم های ارتباطی گوناگون همچون شبکه‌های بی‌سیم باعث توجه بیشتری به این حوزه شده‌است.
در حقیقت نقش کدهای تصحیح کننده‌ی خطا در همان دوران اول کامپیوتر مطرح شده است که از آن زمان بیش از پنجاه سال می‌گذرد. اما به طور کلی بنیان‌گذار نظریه‌ی کدگذاری کسی به نام کلود شانون بود.
او نظریه ریاضی ارسال، دریافت، و ذخیره‌سازی بهینه‌ی داده‌ها و اطّلاعات را که به نظریه اطّلاعات معروف است ارائه کرد. در این نظریه، کلود شانون نحوه مدل‌سازی مسأله ارسال اطلاعات در کانال‌های مخابراتی را به‌صورت پایه‌ای بررسی کرده و مدلی کامل برای مدل‌سازی ریاضی منبع اطلاعات، کانال ارسال اطلاعات و بازیابی آن ارائه داده‌است.
کلود شانون [1]، ریاضی دان و دانش آموخته موسسه فناوری ماساچوست (ام. آی. تی) در سال

[1] Claude Shannon

۱۹۴۸، نظریه مهم خود را با عنوان نظریه ریاضی ارتباطات در مقالهای با همین نام عرضه کرد. در این مقاله، انتقال پیام، در نظامی ارتباطی (مثل تلفن یا تلگراف) که متشکل از فرستنده، رسانه، گیرنده و فرایندهای کدگذاری و کدگشایی است، تحلیل و توصیف آماری می‌شود و سه عامل مورد تاکید و توجه است:

۱- چگونگی کدگذاری پیام؛ ۲- وجود اختلال؛ و ۳- ظرفیت کانال. او مساله ارسال اطلاعات از یک منبع به یک مقصد را به کمک علم احتمالات بررسی و تحلیل نمود. دو نتیجه بسیار مهم، معروف به قضیه های شانون، عبارت اند از:

۱- حداقل میزان نرخی که می توان نرخ فشرده کردن اطلاعات یک منبع تصادفی اطلاعات را به آن محدود نمود برابر با آنتروپی آن منبع است؛ به‌عبارت‌دیگر نمی توان دنباله خروجی از یک منبع اطلاعات را با کمتر از آنتروپی آن منبع ارسال نمود.

۲- حداکثر میزان نرخی که می‌توان بر روی یک کانال مخابراتی اطلاعات ارسال نمود به نحوی که قادر به آشکارسازی اطلاعات در مقصد، با احتمال خطای در حد قابل قبول کم، باشیم، مقداری ثابت و وابسته به مشخصات کانال است، که به آن ظرفیت کانال می‌گوئیم. ارسال با نرخی بیشتر از ظرفیت یک کانال روی آن منجر به خطا می‌شود.

شایان ذکر است که تقریبا همزمان با شانون، **ریچارد همینگ** [۲] (۱۹۵۰) به تحقیق درباره امکان کشف و تصحیح خطا در پیام های دریافتی پرداخته‌است. به این ترتیب با کار این دو (بر آساس چارچوب مطرح شده توسط شانون) **نظریه کد گذاری** [۳] یا به طور دقیق تر ، **نظریه کدهای تصحیح کننده خطا** [۴] پایه‌گذاری شد.

می‌توان این گونه برداشت‌کرد که در حقیقت شانون نظریه کدگذاری را به دو قسمت **نظریه کد گذاری منبع** [۵] و **نظریه کد گذاری کانال** [۶] (کدهای تصحیح کننده خطا) تقسیم کرده‌است.

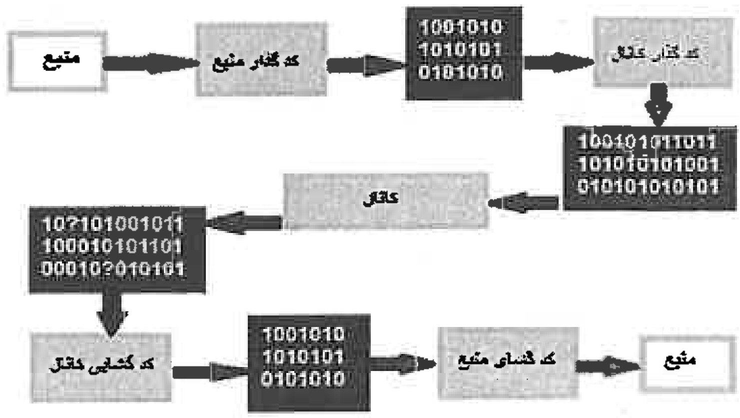
[۲] R. W. Hamming
[۳] Coding theory
[۴] Theory of Error-Correcting Codes
[۵] Source coding theory
[۶] Channel coding theory

نظریه کدگذاری شانون ادعا و به صورت نظری اثبات می کند که برای هر کانال، ماکزیمم نرخی وجود دارد که در آن نرخ می توان داده ها را به گونه ای که احتمال خطا صفر شود، مخابره کرد. این ماکزیمم نرخ به **ظرفیت کانال** [۷] مشهور شده است. علاوه بر این شانون اثبات می کند که تقریبا هر کد بسیار بزرگ، می تواند به این ظرفیت برسد. البته این اثبات، چگونگی ساخت این کدها و نحوه ی **کد گذاری** [۸] و **کد گشایی** [۹] آن‌ها را بیان نمی کند. در حقیقت یک کد تصادفی به اندازه ی دلخواه بزرگ ممکن است با استفاده از اصول فنی به خوبی اجرا شود ولی زمان‌های (پیچیدگی زمانی) کدگذاری و کدگشایی آن ممکن است بسیار بزرگ باشند. به این ترتیب (پس از کارهای شانون) یکی از اهداف اصلی نظریه کدگذاری، ساخت کدهایی شد که با پیچیدگی کدگذاری وکدگشایی قابل کنترل به ظرفیت کانال می‌رسند. از جمله موفقیت هایی که در نتیجه‌ی این تلاش‌ها حاصل شد، ساخت **کدهای توربو** [۱۰] در سال ۱۹۹۳بود. با ساخت این کدها، **کد گشایی تکراری** [۱۱] (که باعث اجرای عالی و پیچیدگی پایین گردید) مطرح شد.

آن چه با کار شانون از سال ۱۹۴۸ آغاز شد را به طور خلاصه می توان در شکل ۱.۱ دید. در فاصله زمانی ۱۹۴۸ تا ۱۹۹۳ (قبل از کدهای توربو) کدهایی با ساختار جبری از جمله کدهای خطی مطرح شدند. پس از آن کدهای خوبی مانند **رید مولر** [۱۲] و **کدهای پیچشی** [۱۳] ارائه شدند.

---

[۷] Capacity of channel
[۸] Encoding
[۹] Decoding
[۱۰] Turbo code
[۱۱] Iteration decoding
[۱۲] Reed-Muller
[۱۳] Convolutional codes



شکل ۱.۱: سیستم ارتباطی

۱.۲.۱ سیستم ارتباطی

همان طور که در شکل ۱.۱می بینید، در یک سیستم ارتباطی یک پیام (از منبع) ابتدا توسط کدگذار منبع، کدگذاری (رمزگذاری) می‌گردد (در شکل ۱.۱ الفبای کدگذاری میدان دودویی در نظر گرفته شده‌است ولی می‌تواند تغییر کند). حاصل این عمل، برداری به طول K است. سپس کدگذار کانال به این بردار با توجه به مدل کدگذاری کانال مورد نظر **افزونگی** [۱۴] اضافه می کند. که این افزونگی موجب می شود که کدگشایی کانال بتواند خطای حاصل از پارازیت کانال را در صورت امکان کشف و تصحیح کند. بردار جدید حاصل از مرحله کدگذاری کانال را **کدواژه** [۱۵] می نامند که عنصری متعلق به F_2^n (با فرض الفبای دودویی) است. به این ترتیب k را بعد (اندازه) کد و n را طول کد (طول کدواژه) می نامند. کدواژه از طریق کانال ارسال

[۱۴] Redundancy
[۱۵] Codeword

می‌گردد. کانال معمولا خواصی دارد که (این خواص) موجب تغییر سیگنال هایی که از کانال عبور می‌کنند، می‌گردند و آن‌ها را تحریف (خراب) می‌کند. یکی از مواردی که باعث تحریف کدواژه ارسالی می‌گردد وجود پارازیت (نوفه) در کانال است. در انتهای کانال گیرنده واژه‌ای را از کانال دریافت می‌کند که (با توجه به تغییرات رخ داده در پیام ارسالی در اثر پارازیت) ممکن است کدواژه نباشد. کدگشایی کانال، سعی خواهدکرد خطاهای احتمالی واژه ی دریافتی را در صورت امکان کشف و تصحیح کند و به این ترتیب محتمل ترین کدواژه (که به طور محتمل تر همان کدواژه ی ارسالی است) را به کدگشای منبع (رمزگشا) تحویل می‌دهد. کدگشای منبع نیز آن را رمزگشایی و پیام اصلی را از آن استخراج می کند. به مثال زیر توجه کنید.
مثال: عمل کپی کردن فیلم یا اطلاعات روی DVD را در نظر بگیرید. در این عمل، کامپیوتر به عنوان کدگذار منبع و کدگذار کانال عمل می‌کند. یعنی اطلاعات را به داده‌های دودویی تبدیل می‌کند و با توجه به مدل کدگذاری مورد استفاده افزونگی مورد نیاز را به آن اضافه می‌کند. سپس اطلاعات را روی DVD کپی می‌کند. در این جا DVD، کانال است. DVD ممکن است خراشیده یا کثیف گردد، به این ترتیب برخی از اطلاعات روی آن خراب خواهد شد. اجرا کننده‌ی DVD ($DVD\ player$) می تواند این داده‌ها را تعمیر کند و آن ها را بخواند (یعنی به آن عنوان کدگشای کانال و کدگشای منبع عمل می کند).

۳.۱ قضایا و تعاریف مقدماتی در نظریه کد گذاری

تعریف ۱.۳.۱. فرض کنید $A = \{a_1, ..., a_q\}$ یک مجموعه متناهی q عضوی باشد. چنین مجموعه‌ای را **الفبای کد** [۱۶] نامیده و هر عنصر A را یک نماد کد نامیم.

تعریف ۲.۳.۱. یک کلمه [۱۷] q نمادی به طول n روی A، دنباله ای مانند $w = w_1, ..., w_n$ است که برای هر i داشته باشیم: $w_i \in A$. گاه یک کلمه را به صورت بردار $w = (w_1, ..., w_n)$، نمایش

[۱۶] Code alphabet
[۱۷] Word

می‌دهند.

تعریف ۱.۳.۳. یک **کد** [۱۸] بلوکی q- نمادی به طول n روی مجموعه الفبای A، مجموعه‌ای ناتهی مانند C است که شامل کلماتی q- نمادی به طول یکسان n است.

تعریف ۱.۳.۴. به هر عنصر از C، یک **کدواژه** [۱۹] می‌گوییم. **وزن همینگ** [۲۰] یک کدواژه $c \in C$، یعنی $wt(c)$، تعداد مولفه های غیر صفر آن کدواژه است و **پشتیبان** [۲۱] کدواژه ی $c = (c_1, ..., c_n)$ مجموعه $supp(c) = \{i | c_i \neq 0\}$ است.

تعریف ۱.۳.۵. تعداد کدواژه‌های کد C را **اندازه کد** [۲۲] C نامیم و با $|C|$ نمایش می دهیم.

تعریف ۱.۳.۶. دو کد مانند C و C' را **کدهای معادل** [۲۳] گویند هرگاه کدواژه c. و جایگشت Π از مجموعه موقعیت‌های مولفه‌ها وجود داشته باشد به قسمی که:

$$C' = \Pi(C) + c.$$

که در آن:

$$\Pi(C) = \{\Pi(c) | c \in C\} \text{ و } \Pi((c_1, ..., c_n)) = (c_{\Pi(1)}, ..., c_{\Pi(n)}).$$

تذکر: معمولا الفبای کد یک میدان متناهی F_q از مرتبه q در نظر گرفته می‌شود.

تعریف ۱.۳.۷. یک کد روی الفبای $F_2 = \{0, 1\}$ یک **کد دودویی** [۲۴] نامیده می شود. لازم به‌ذکر است که F_2 همان $\mathbb{Z}_2$ می‌باشد.

[۱۸] Code
[۱۹] Codeword
[۲۰] Hamming weight
[۲۱] Support
[۲۲] Size of code
[۲۳] Equivalent codes
[۲۴] Binary code

تعریف ۸.۳.۱. فرض کنید x و y دو کلمه به طول n روی الفبای A باشند. منظور از **فاصله همینگ** [۲۵] بین x و y که با $d(x,y)$ نمایش داده می شود تعداد موقعیت‌هایی است که x و y در آن‌ها تفاوت دارند.

به عبارت‌دیگر اگر $x = x_1, ..., x_n$ و $y = y_1, ..., y_n$ آنگاه $d(x,y) = |\{i | x_i \neq y_i\}|$.

تعریف ۹.۳.۱. قاعده‌ای که پس از دریافت پیام غلط برای کشف و تصحیح خطا از آن استفاده می‌شود را **قاعده کدگشایی** [۲۶] نامیم.

در زیر دو قاعده کدگشایی را توضیح می‌دهیم:

۱- قاعده **کدگشایی حداکثر احتمال** [۲۷] (MLD): فرض کنیم کلمه x دریافت شود این قاعده آن را به c_x کد گشایی می‌کند هرگاه احتمال دریافت x به شرط ارسال c_x ماکزیمم باشد. یعنی:

$$P(x|c_x) = max\{P(x|c), c \in C\}.$$

دو نوع MLD وجود دارد: در نوع کامل آن اگر دو کدواژه c_x پیدا شوند که برای آن‌ها $P(x|c_x)$ ماکزیمم شود آن گاه به دلخواه یکی را انتخاب می‌کنیم.

در نوع ناقص آن در صورت بروز چنین مسئله ای، تقاضای ارسال مجدد می‌کنیم.

۲- قاعده **کدگشایی مینیمم فاصله** [۲۸] (NMD): فرض کنیم کلمه x دریافت شود، این قاعده آن را به c_x کد گشایی می‌کند هرگاه $d(x, c_x)$ مینیمم باشد، به‌عبارت‌دیگر:

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

مشابه قاعده ی قبل دو نوع NMD داریم که در حالت کامل آن اگر دو کدواژه c_x موجود باشند که $d(x, c_x)$ مینیمم باشد آن‌گاه یکی را به دلخواه انتخاب می‌کنیم و در نوع ناقص آن در صورت بروز چنین مساله‌ای تقاضای ارسال مجدد می‌کنیم.

---

[۲۵] Hamming distance
[۲۶] Decoding rule
[۲۷] Maximum likelihood decoding
[۲۸] Minimum distance decoding

مثال: فرض کنید کدواژه‌های کد $C = \{۰۰۰۰, ۰۰۱۱, ۰۱۱۰, ۱۰۰۰, ۱۱۰۰, ۰۰۰۱\}$ را از یک کانال ارسال می‌کنیم. کلمه $x = ۰۱۱۱$ دریافت می‌شود. می‌خواهیم با استفاده از قاعده کدگشایی مینیمم فاصله این کلمه را کدگشایی کنیم. مشاهده می‌شود برای دو کدواژه‌ی $c_۱ = ۰۰۱۱$ و $c_۲ = ۰۱۱۰$، $d(x, c_i)$ مینیمم است. در صورت استفاده از نوع ناقص این کدگشایی تقاضای ارسال مجدد می‌کنیم در غیر این‌صورت یکی از کدواژه‌های ۰۰۱۱ و ۰۱۱۰ را به دل‌خواه انتخاب می‌کنیم.

تعریف ۱۰.۳.۱. برای کد C **مینیمم فاصله** [۲۹] را با $d(C)$ نشان می‌دهیم و به صورت زیر تعریف می‌کنیم:

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

تعریف ۱۱.۳.۱. فرض کنیم t عددی طبیعی باشد، کد C را کدی t– **تصحیح کننده خطا** [۳۰] گوییم هر گاه با روش کد گشایی مینیمم فاصله ناقص قادر به تصحیح حداکثر t خطا باشیم. کد C را دقیقا t– تصحیح کننده خطا گوییم هر گاه C، t– تصحیح کننده خطا باشد اما $(t+۱)$– تصحیح کننده خطا نباشد.

مثال: کد $C = \{۰۰۰, ۱۱۱\}$ کدی ۱– تصحیح کننده خطاست اما ۲– تصحیح کننده خطا نیست. چون در هر یک از کدواژه‌های آن اگر یک خطا صورت گیرد قابل تصحیح است اما اگر دو خطا صورت گیرد قابل تصحیح نیست. مثلا اگر کدواژه "۰۰۰" ارسال شود و کدواژه "۱۰۰" دریافت شود این کدواژه با استفاده از قاعده کدگشایی مینیمم فاصله ناقص به صورت "۰۰۰" تصحیح می‌شود. اما اگر کدواژه "۰۰۰" ارسال شود و کدواژه "۱۱۰" دریافت شود با استفاده از روش مذکور به صورت "۱۱۱" تصحیح می‌شود.

قضیه ۱۲.۳.۱. [۶] کد C، کدی t– تصحیح کننده خطاست اگر و تنها اگر $d(C) \geq ۲t + ۱$.

[۲۹] Minimum distance
[۳۰] t- error-correcting

اثبات. " $\Rightarrow$ " فرض کنید $d(C) \geq ۲t+۱$ باشد. فرض می‌کنیم کد واژه c را ارسال کرده و کلمه x را دریافت کرده ایم و $d(x,c) \leq t$ (کلمه c را با حداکثر t خطا دریافت کرده‌ایم). حال فرض می‌کنیم $c' \neq c$ کدواژه‌ای دلخواه در C باشد، در این صورت داریم:

$$d(x,c') \geq d(c,c') - d(x,c) \geq ۲t+۱-t = t+۱ > d(x,c)$$

لذا به درستی x را به c کد گشایی می‌کنیم و در نتیجه C کدی t- تصحیح کننده خطاست.

" $\Leftarrow$ " فرض می کنیم C، کدی t- تصحیح کننده خطا باشد.

فرض خلف: فرض می‌کنیم $d(C) \leq ۲t$ باشد. لذا دو کدواژه $c_۱$ و $c_۲$ موجودند که $d(c_۱,c_۲) \leq ۲t$.

ادعا می کنیم:

$$d(c_۱,c_۲) \geq t+۱.$$

برای اثبات این ادعا به برهان خلف عمل می‌کنیم: اگر $d(c_۱,c_۲) \leq t$ آنگاه با $d(c_۱,c_۲)$ تغییر می توان با ارسال $c_۱$، $c_۲$ را به اشتباه دریافت کرد. که این با t- تصحیح کننده خطا بودن C در تناقض است. لذا $t+۱ \leq d(c_۱,c_۲) \leq ۲t$.

فرض کنید $d(c_۱,c_۲) = d$ باشد. بدون کاستن از کلیت مساله فرض می‌کنیم $c_۱$ و $c_۲$ در d مکان اول متفاوت باشند و کلمه x را به صورت $x = x_۱,...,x_t,x_{t+۱},...,x_d,x_{d+۱},...,x_n$ در نظر می‌گیریم که $x_۱,...,x_t$ قسمتی از $c_۲$ و $x_{t+۱},...,x_d$ قسمتی از $c_۱$ و $x_{d+۱},...,x_n$ بین $c_۱$ و $c_۲$ مشترک است.

حال فرض می‌کنیم $c_۱$ کدواژه ارسالی و x کلمه دریافتی باشد، دراین‌صورت:

$$d(x,c_۲) = d-t \leq ۲t-t = t = d(x,c_۱)$$

چون فاصله x و $c_۱$ بیشتر از فاصله x و $c_۲$ است پس وقتی $c_۱$ ارسال و x دریافت می‌شود در صورت متفاوت بودن $d(x,c_۱)$ و $d(x,c_۲)$، x به اشتباه به $c_۲$ کدگشایی می‌شود و اگر $d(x,c_۱) = d(x,c_۲)$ باشد تقاضای ارسال مجدد می‌شود که در هر حالت متناقض با t- تصحیح کننده خطا بودن C است. لذا فرض خلف باطل می‌شود و $d(C) \geq ۲t+۱$. $\square$

تعریف ۱۳.۳.۱. مجموعه ناتهی V به همراه دو عمل "$+$" و "." را **فضای برداری** [۳۱] روی میدان F_q گوییم هرگاه برای $w, u, v \in V$ و برای $\lambda, \mu \in F_q$ داشته باشیم:

(i) $u + v \in V$.

(ii) $(u+v)+w = u+(v+w)$.

(iii) عنصری مانند $0 \in V$ وجود دارد که برای هر $v \in V$: $0 + v = v = v + 0$.

(iv) برای هر $u \in V$ عنصری از V موجود است که $(-u)$ نامیده‌می‌شود به قسمی که : $u+(-u) = (-u)+u = 0$.

(v) $u + v = v + u$.

(vi) $\lambda v \in V$.

(vii) $\lambda(u+v) = \lambda u + \lambda v$، $(\lambda+\mu)u = \lambda u + \mu u$.

$(viii)$ $(\lambda\mu)u = \lambda(\mu u)$.

(x) اگر ۱ یکان ضربی F_q باشد، آن‌گاه: $1u = u$.

مثال: برای میدان Z_2، $\{0000, 1010, 0101, 1111\}$ یک فضای برداری است.

قضیه ۱۴.۳.۱. [۵] زیر مجموعه‌ای ناتهی مانند C از فضای برداری V روی میدان F_q فضای برداری است اگر و تنها اگر:

$$\forall x, y \in C \text{ ، } \forall \lambda, \mu \in F_q \text{ ؛ } \lambda x + \mu y \in C$$

تعریف ۱۵.۳.۱. یک **ترکیب خطی** [۳۲] از بردارهای $v_1, ..., v_n$ در فضای برداری V روی میدان F_q عبارتی به صورت $\lambda_1 v_1 + ... + \lambda_n v_n$ است که برای هر $i = 1, 2, ..., n$، $\lambda_i \in F_q$ است.

مجموعه تمام بردارهای به طول n با درایه‌های متعلق به F_q را با F_q^n نشان می‌دهیم لذا

$$F_q^n = \{(\nu_1, ..., \nu_n); \nu_i \in F_q\}.$$

[۳۱] Vector space
[۳۲] Linear combination

به طور مثال $\mathbb{Z}_2^n = \{(\nu_1, ..., \nu_n); \nu_i \in \mathbb{Z}_2 = \{0, 1\}\}$.

تعریف ۱.۳.۱۶. فرض کنید V یک فضای برداری روی میدانF_q باشد. یک مجموعه از بردارها مانند $\{v_1, ..., v_r\}$ در V **مستقل خطی** [۳۳] هستند هر گاه رابطه $\lambda_1 v_1 + ... + \lambda_r v_r = 0$ نتیجه دهد $\lambda_1 = ... = \lambda_r = 0$. یک مجموعه که مستقل خطی نباشد وابسته خطی است.
یک مجموعه مستقل خطی که مولد نیز باشد **پایه** [۳۴] نامیده می‌شود.
تعداد عناصر یک پایه‌ی فضای V، **بعد فضا** [۳۵] V نامیده می‌شود و با $\dim(V)$ نمایش داده می‌شود.

تعریف ۱.۳.۱۷. فرض می‌کنیم V فضایی برداری بر روی میدان F_q باشد. یک **زیر فضا** [۳۶]ی V عبارت‌است‌از یک زیر مجموعه‌ی W از V که خود با اعمال جمع برداری و ضرب اسکالر روی V، یک فضای برداری بر روی F_q باشد.

تعریف ۱.۳.۱۸. فرض کنید S مجموعه‌ای از بردارهای فضای برداری V باشد. **زیر فضای پدید آمده** [۳۷] توسط S که با $\langle S\rangle$ یا $span(S)$ نمایش داده می‌شود عبارت‌است‌از اشتراک W از همه‌ی زیر فضاهای V که شامل S باشند.
هنگامی که S مجموعه‌ای متناهی از بردارها باشد، یعنی $S = \{\alpha_1, ..., \alpha_n\}$، W را زیر فضای پدید آمده توسط بردارهای $\alpha_1, ..., \alpha_n$ نیز می‌نامیم.

قضیه ۱.۳.۱۹. [۵] فرض کنیدV یک فضای برداری روی F_q باشد، اگر $dim(V) = k$ آن‌گاه $|V| = q^k$.

اثبات. فرض کنیم $\{v_1, ..., v_k\}$ پایه‌ای برای V باشد. لذا داریم:

$$V = \{\lambda_1 v_1 + ... + \lambda_k v_k | \lambda_i \in F_q\}.$$

[۳۳] Linearly independent
[۳۴] Basis
[۳۵] Dimention of space
[۳۶] Subspace
[۳۷] Spanning subspace

با توجه به تعداد حالت‌های ممکن برای λ_i ها داریم:

$$|V| = q^k.$$

□

تعریف ۲۰.۳.۱. برای دو بردار $v = (v_1, ..., v_n)$ و $w = (w_1, ..., w_n)$، **ضرب نقطه‌ای** [۳۸] این دو بردار به صورت $v.w = v_1w_1 + ... + v_nw_n$ تعریف می‌شود. دو بردار w و v متعامد نامیده می‌شوند هرگاه: $v.w = 0$.

تعریف ۲۱.۳.۱. فرض کنید V و W دو فضای برداری بر روی میدان F_q باشند. یک **تبدیل خطی** [۳۹] از V در W تابعی از V در W است که به ازای همه‌ی α ها و β ها از V و همه‌ی اسکالرهای c از F_q داشته باشیم:

$$T(c\alpha + \beta) = c(T\alpha) + T\beta.$$

تعریف ۲۲.۳.۱. فرض کنیم V و W دو فضای برداری بر روی میدان F_q، و T تبدیلی خطی از V در W باشد. فضای پوچ یا **هسته** [۴۰] T که با $\ker(T)$ نمایش داده می شود عبارت‌است‌از مجموعه‌ی همه‌ی بردارهای α از V با شرط $T\alpha = 0$.

هرگاه بعد V متناهی باشد، **رتبه** [۴۱] T که آن را با $rank(T)$ نمایش می‌دهیم بعد برد T است و پوچی T بعد فضای پوچ یا بعد هسته‌ی T است و با$(\dim(\ker(T))$ نمایش داده می‌شود.

قضیه ۲۳.۳.۱. [۵] فرض کنیم V و W دو فضای برداری بر روی میدان F_q، و T تبدیل خطی از V در W باشد. اگر بعد V متناهی باشد، آن گاه:

$$rank(T) + \dim(\ker(T)) = \dim(V)$$

تعریف ۲۴.۳.۱. فرض کنید $\varnothing \neq S \subseteq F_q^n$ باشد، **دوگان** [۴۲] S به صورت تعریف می‌شود:

---
[۳۸] Pointwise multiplication
[۳۹] Linear transformation
[۴۰] Kernel
[۴۱] Rank
[۴۲] Dual

$$S^{\perp} = \{v \in F_q^n; v.u = 0; \forall u \in S\}.$$

قضیه ۲۵.۳.۱. [۶] اگر $S \subseteq F_q^n$ آن‌گاه داریم:

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

اثبات. فرض کنید $dim\langle S\rangle = k$ و $\{v_1, ..., v_k\}$ یک پایه برای $\langle S\rangle$ باشد. اگر A ماتریس تشکیل شده توسط بردارهای $v_1, ..., v_k$ به عنوان سطرهای A باشد، آن‌گاه ماتریس تشکیل شده توسط بردارهای پایه $\langle S^{\perp}\rangle$ پایه‌ی فضای جواب دستگاه $AX = 0$ است. با به‌کاربردن قضیه ۲۳.۳.۱ به‌دست می‌آید:

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

□

تذکر: برای هر زیرمجموعه‌ی F_q^n مانند S، $S^{\perp}$ زیر فضایی از فضای برداری F_q^n است و $\langle S\rangle^{\perp} = S^{\perp}$.

تعریف ۲۶.۳.۱. هر زیر فضای برداری از F_q^n یک **کد خطی** [۴۳] به طول n روی میدان F_q نامیده می‌شود.

کدی که خطی نباشد **غیر خطی** [۴۴] است.

به‌طور مثال، $C = \{(\lambda, ..., \lambda) | \lambda \in F_q\}$ یک کد خطی است که کد تکرار نامیده می‌شود.

تعریف ۲۷.۳.۱. **دوگان کد خطی** [۴۵] C که با $C^{\perp}$نشان داده می شود، دوگان زیر فضای C در F_q^n است.

[۴۳] Linear code
[۴۴] Nonlinear
[۴۵] Dual of linear code

کد خطی C را **خود متعامد** [۴۶] گوییم هرگاه: $C \subseteq C^{\perp}$.

کد خطی C را **خود دوگان** [۴۷] گوییم هرگاه: $C = C^{\perp}$.

قضیه ۲۸.۳.۱. [۶] فرض کنید C کدی خطی به طول n روی F_q باشد. در این صورت داریم:

الف) اندازه‌ی C برابر است با: $|C| = q^{dim(C)}$. به‌عبارت‌دیگر: $dim(C) = \log_q^{|C|}$.

ب) $C^{\perp}$ کدی خطی است و $dim(C) + dim(C^{\perp}) = n$.

پ) $(C^{\perp})^{\perp} = C$

اثبات. الف) این قسمت قضیه بیان دیگر قضیه‌ی ۱۹.۳.۱ است.

ب) با توجه به تذکری که قبل از تعریف کد خطی بیان شد و قرار دادن C به جای S واضح است که $C^{\perp}$ یک کد خطی است و با توجه به قضیه‌ی ۲۵.۳.۱ داریم:

$$\dim(C) + \dim(C^{\perp}) = n.$$

پ) با استفاده از قسمت ب و قرار دادن $C^{\perp}$ به جای C داریم: $\dim(C) = \dim((C^{\perp})^{\perp})$. برای اثبات این قسمت از قضیه کافی است ثابت کنیم $C \subseteq (C^{\perp})^{\perp}$. فرض کنید $c \in C$. برای نشان دادن این‌که $c \in (C^{\perp})^{\perp}$ است، لازم است نشان دهیم که برای هر $x \in C^{\perp}$: $c.x = ۰$. چون $c \in C$ و $x \in C^{\perp}$، با توجه به تعریف $C^{\perp}$، نتیجه می‌شود که $c.x = ۰$. $\square$

تعریف ۲۹.۳.۱. ماتریس مولد [۴۸] یک کد خطی ماتریسی است که سطرهای آن پایه‌ای برای آن کد تشکیل دهند.

تعریف ۳۰.۳.۱. ماتریس کنترل توازن [۴۹] برای کد خطی C، ماتریسی است که سطرهای آن پایه‌ای برای $C^{\perp}$ تشکیل دهند.

---

[۴۶] Self-orthogonal

[۴۷] Self-dual

[۴۸] Generator matrix

[۴۹] Parity-check matrix

قضیه ۳۱.۳.۱. [۶] فرض کنید C یک کد خطی به طول n و بعد k، روی میدان F_q باشد و G ماتریس مولد آن باشد و $v \in F_q^n$. دراین‌صورت داریم:

الف) $v \in C^{\perp} \Longleftrightarrow v.G^T = 0$

ب) ماتریس $H_{(n-k)\times n}$، ماتریس کنترل توازن C است اگر و تنها اگر سطر های H مستقل خطی باشند و $H.G^T = 0$.

اثبات. الف) فرض کنید $v \in C^{\perp}$ ، دراین‌صورت ضرب v در تمام عناصر کد C برابر صفر است. اما چون سطرهای G پایه ای برای C تشکیل می دهند لذا ضرب v در هر سطر G نیز برابر صفر است و در نتیجه اگر r_i سطر i ام G باشد آن‌گاه: $v.r_i = 0$. در نتیجه: $v.G^T = 0$.

برعکس اگر $v.G^T = 0$ آن‌گاه v بر هر سطر G عمود است. اما سطرهای G پایه‌ای برای C می‌سازند، لذا ضرب v در هر کدواژه C صفر است یعنی: $v \in C^{\perp}$.

ب) فرض کنید $H_{(n-k)\times n}$ ماتریس کنترل توازن C است. دراین‌صورت به وضوح سطر های H مستقل خطی اند.

از طرفی چون سطرهای H پایه $C^{\perp}$ و سطرهای G پایه ی C هستند لذا حاصل‌ضرب هر سطر H در هر سطر G صفر است. یعنی $H.G^T = 0$.

برعکس فرض کنید $H.G^T = 0$. در این صورت بنا به قسمت قبل سطرهای H و در نتیجه فضای سطری H در $C^{\perp}$ قرار می‌گیرد. چون طبق فرض سطرهای H مستقل خطی اند لذا بعد فضای سطری H برابر است با $n-k$. اما بعد $C^{\perp}$ نیز $n-k$ است در نتیجه فضای سطری H برابر $C^{\perp}$ است. پس H ماتریس کنترل توازن است. □

قضیه ۳۲.۳.۱. [۶] فرض کنید C یک کد خطی و H ماتریس کنترل توازن آن باشد، دراین‌صورت:

الف) $d(C) \geq d$ اگر و تنها اگر هر $d-1$ ستون از H مستقل خطی باشند.

ب) $d(C) \leq d$ اگر و تنها اگر H، d ستون وابسته خطی داشته باشد.

اثبات. الف) فرض کنید $v = (v_1, ..., v_n) \in C$ یک کدواژه با وزن $m > 0$ باشد و فرض کنید

ستون‌های غیر صفر v عبارت‌اند از : $i_۱, ..., i_m$. دراین‌صورت:

$$v.H^T = ۰ \iff v \in C.$$

اما

$$v.H^T = \sum_{j=۱}^{n} v_{ij} c_{ij}^T$$

و c_{ij}^T ها ستون‌های H^T هستند در نتیجه یک کدواژه با وزن m در کد C موجود است اگروفقط اگر m ستون وابسته‌ی خطی در H داشته باشیم. فرض کنید مینیمم فاصله‌ی کد C برابر d باشد، بنا به استدلال فوق خواهیم داشت که ماتریس H دارای d ستون وابسته‌ی خطی است. اگر $d - ۱$ ستون از H وابسته‌ی خطی باشند آن‌گاه به‌طور معادل یک کدواژه با وزن $d - ۱$ در C خواهیم داشت که متناقض با این حقیقت است که $d(C) = d$. لذا هر $d - ۱$ ستون از H مستقل خطی‌اند.

برعکس فرض کنید هر $d - ۱$ ستون از H مستقل خطی باشند و $d(C) \leq d - ۱$. لذا فرض می‌کنیم c عضوی از C باشد که $wt(c) = m$ و $m \leq d - ۱$، پس m ستون وابسته‌ی خطی در m موجود است که این متناقض با فرض است که می‌گوید هر $d - ۱$ ستون از H مستقل خطی‌اند. پس داریم: $d(C) \geq d$.

ب) اثبات این قسمت دقیقا مشابه اثبات قسمت قبل است. □

قضیه ۱.۳.۳۳. [۶] اگر ماتریس G به شکل استاندارد $G = (I_k|X)$ ماتریس مولد یک کد خطی مانند C به طول n و بعد k باشد، آن‌گاه ماتریس کنترل توازن C به شکل $H = (-X^T|I_{n-k})$ است.

اثبات. به وضوح $H.G^T = ۰$. از طرفی سطرهای H مستقل خطی‌اند لذا بنابه قسمت دوم قضیه‌ی ۱.۳.۳۱، H ماتریس کنترل توازن است. □

تعریف ۳۴.۳.۱. فرض کنید C یک کد خطی به طول n روی F_q باشد و $u \in F_q^n$. **هم‌مجموعه** [۵۰] تعریف شده توسط u عباتست از: $u + C = \{u + v | v \in C\}$.

قضیه ۳۵.۳.۱. [۶] فرض کنید C یک کد خطی به طول n، بعد k و مینیمم فاصله d روی میدان متناهی F_q باشد. دراین‌صورت داریم:

(i) هر بردار F_q^n در یک هم‌مجموعه از C واقع است.

(ii) برای هر $u \in F_q^n$ داریم: $|C + u| = |C| = q^k$.

(iii) $u \in v + C$، آنگاه: $u + C = v + C$.

(iv) دو هم‌مجموعه یا مساوی هستند و یا اشتراکی ندارند.

(v) تعداد هم‌مجموعه های متمایز برای کد C برابر است با q^{n-k}.

(vi) $u - v \in C$ اگر و تنها اگر u و v در یک هم‌مجموعه واقع شوند.

از شرط (i) و (iv) نتیجه می‌شود که F_q^n توسط هم‌مجموعه های C افراز می‌شود.

تذکر: کدی به طول n و تعداد کدواژه‌های M و مینیمم فاصله d را یک (n, M, d)− کد می‌نامیم. و کدی خطی به طول n ، بعد k ، و مینیمم فاصله d را یک $[n, k, d]$− کد خطی نامیم.

تعریف $A_q(n, d)$: فرض کنید A مجموعه‌ای q عضوی موسوم به الفبا باشد که $q > 1$ است. برای اعداد n و d داده شده $A_q(n, d)$ بزرگ‌ترین مقدار M است که یک (n, M, d)− کد روی A موجود باشد.

یک (n, M, d)− کد که M آن ماکزیمم باشد را یک **کد بهینه** [۵۱] نامیم.

$B_q(n, d)$: بزرگ‌ترین مقدار q^k است که یک $[n, k, d]$− کد خطی موجود باشد.

قضیه ۳۶.۳.۱. [۶] برای q که توانی از یک عدد اول است و برای $1 \le d \le n$ داریم:

۱) $B_q(n, d) \le A_q(n, d) \le q^n$

---

[۵۰] Coset

[۵۱] Optimal code

۲) $B_q(n,1) = A_q(n,1) = q^n$

۳) $B_q(n,n) = A_q(n,n) = q$

تعریف ۳۷.۳.۱. برای کد خطی C روی میدان F_q **کد توسعه یافته** [۵۲] آن که با $\overline{C}$ نشان داده می‌شود عبارت‌است‌از:

$$\overline{C} = \{(c_1, ..., c_n, -\sum_{i=1}^{n} c_i) | (c_1, ..., c_n) \in C\}.$$

در حالت $q = 2$ مولفه اضافی $\sum c_i = -\sum c_i$ را مولفه کنترل توازن نامیم.

قضیه ۳۸.۳.۱. [۶] اگر C یک (n, M, d)– کد روی F_q باشد آن‌گاه $\overline{C}$ یک $(n+1, M, d')$ کد روی F_q است که در آن $d \leq d' \leq d+1$.

تعریف ۳۹.۳.۱. فرض کنید A مجموعه الفبا با اندازه q باشد. برای هر $u \in A^n$ **کره** [۵۳] به مرکز u و شعاع r عبارت‌است‌از:

$$s_A(u, r) = \{v \in A^n | d(u, v) \leq r\}.$$

تعریف ۴۰.۳.۱. نماد: برای اعداد $q > 1$ و $n \geq 1$ و $r \geq 0$، قرار می‌دهیم:

$$v(q, n, r) = \begin{cases} \sum_{i=0}^{r} \binom{n}{i} (q-1)^i & 0 \leq r \leq n \\ q^n & r > n \end{cases}$$

لم ۴۱.۳.۱. [۶] اگر A مجموعه‌ای q عضوی باشد آن‌گاه تعداد بردارهای یک کره به شعاع r در A^n برابراست با $v(n, q, r)$.

اثبات. فرض کنید $u \in A^n$ ثابت باشد، لذا:

$$s_A(u, r) = \{v \in A^n | d(u, v) \leq r\}$$

[۵۲] Extended code
[۵۳] Sphere

بنابراین فرض کنید $m \leq r$ باشد. اگر v برداری باشد که $d(u,v) = m$است آن‌گاه برای انتخاب v ابتدا $\binom{n}{m}$ حالت برای جایگاه‌های متمایز با u داریم. در هر یک از این جایگاه‌ها، $q-1$ عنصر می‌توان قرارداد تا با عنصر این جایگاه در u متمایز باشد. در نتیجه $\binom{n}{m}(q-1)^m$ حالت برای انتخاب v داریم لذا برای $r \leq n$ در مجموع $\sum \binom{n}{m}(q-1)^m$ حالت برای انتخاب v داریم. یعنی تعداد بردارهای کره‌ی فوق مساوی $v(q,n,r)$ می‌باشد. (برای حالت $r > n$، تعریف می‌کنیم $v(q,n,r) = q^n$.) □

قضیه ۴۲.۳.۱. [۶] (**کران پوششی کره** [۵۴]): برای اعداد صحیح $q > 1$ و $1 \leq d \leq n$ داریم:

$$A_q(n.d) \geq \frac{q^n}{\sum_{i=0}^{d-1}\binom{n}{i}(q-1)^i}$$

قضیه ۴۳.۳.۱. [۶] (**کران همینگ** [۵۵]):

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{n}{i}(q-1)^i}.$$

اثبات. فرض کنید $C = \{c_1, ..., c_M\}$ یک $(n,M,d)-$ کد بهینه روی الفبای q عضوی A باشد یعنی $M = A_q(n,d)$. و فرض کنید $e = \lfloor\frac{d-1}{2}\rfloor$ ، در این صورت کره هایی به مرکز c_i و شعاع e مجزا هستند (اشتراک ندارند) زیرا اگر به‌ازای $i \neq j$ ، $x \in s_A(c_i,e) \cap s_A(c_j,e)$، آن‌گاه داریم:

$$d(c_i,c_j) \leq d(c_i,x) + d(x,c_j) \leq 2e \leq d-1$$

و این تناقض است زیرا مینیمم فاصله کد C، d است و فاصله هیچ دو عضوی در C کمتر از d نیست. لذا کره‌های فوق مجزا هستند. در نتیجه داریم:

$$\cup_{i=1}^{e} s_A(c_i,e) \subseteq A^n$$

$$\Rightarrow Mv(n,q,e) \leq q^n \Rightarrow M \leq \frac{q^n}{v(n,q,e)} = \frac{q^n}{\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{n}{i}(q-1)^i}.$$

---

[۵۴] Spher- paking bound

[۵۵] Hamming bound

□

قضیه ۴۴.۳.۱. [۶](**کران گیلبرت ورشامو** [۵۶]) فرض کنید n و k و d اعداد صحیح باشند که $2 \leq d \leq n$ و $1 \leq k \leq n$ است. اگر

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k} \tag{1.1}$$

آنگاه یک $[n,k]$− کد خطی روی F_q وجود دارد که مینیمم فاصله آن حداقل d باشد.

اثبات. باید نشان دهیم که اگر رابطه ۱.۱ برقرار باشد آن‌گاه یک ماتریس از مرتبه $(n-k) \times n$، مانند H روی F_q وجود دارد به‌قسمی که هر $d-1$ ستون آن مستقل خطی است.
ماتریس H را به شکل زیر می‌سازیم: فرض کنید c_j ستون j ام H را نمایش می‌دهد. فرض می‌کنیم c_1 بردار غیر صفری در F_q^{n-k} باشد و c_2 برداری باشد که توسط c_1 تولید نشود. برای $2 \leq j \leq n$، فرض می‌کنیم c_j نیز برداری باشد که پدید آمده خطی توسط حداکثر $d-2$ بردار $c_1, \ldots, c_{j-1}$ نباشد. خاطر نشان می‌کنیم که تعداد بردارهای پدید آمده خطی توسط حداکثر $d-2$ بردار $c_1, \ldots, c_{j-1}$ $(2 \leq j \leq n)$ عبارت‌است‌از:

$\sum_{i=0}^{d-2} \binom{j-1}{i} (q-1)^i \leq \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}$

بنابراین بردار c_j $(2 \leq j \leq n)$ را همیشه می‌توان پیدا کرد.
ماتریس H ساخته‌شده از این روش یک ماتریس $(n-k) \times n$ است و هر $d-1$ ستون آن مستقل خطی هستند. فضای پوچ H یک کد خطی روی F_q به طول n است و مینیمم فاصله آن d و بعد آن حداقل k است. با درنظر گرفتن یک زیر فضای k− بعدی این فضا، کد خطی مورد نظر بدست می‌آید. □

[۵۶] Gilbert- Varshamov bound

فصل ۲
کدهای کامل

۱.۲ مقدمه

کدهای کامل دسته مهمی از کدها هستند و این اهمیت به خاطر خصوصیات جالب این کدها، کدگذاری و کدگشایی آسان آن‌ها است.
ما در این فصل ابتدا به تعریف کد کامل می‌پردازیم و تعاریف و مفاهیم مربوط به کدهای کامل را ارائه می‌دهیم. در ادامه چند نوع کد کامل را به همراه خصوصیات آن مورد بررسی قرارمی‌دهیم.
لازم به ذکر است که یک کد کامل ممکن است خطی یا غیرخطی باشد اما ما در این فصل توجه خود را به کدهای کامل خطی معطوف می‌کنیم. چون کدهای دودویی کاربرد بیشتری دارند و این امکان را به ما می‌دهند که ساختارشان را به کدهای q− نمادی تعمیم دهیم، بیشتر کدهای کامل دودویی را مورد مطالعه قرار می‌دهیم.

۲.۲ مفاهیم اولیه

تعریف ۱.۲.۲. یک کد q− نمادی که دارای

$$\frac{q^n}{\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{n}{i}(q-1)^i}$$

کدواژه باشد را یک **کد کامل** [1] نامند. به عبارت دیگر کد کامل کدی است که اندازه آن برابر با کران بالای همینگ است.

لذا یک کد کامل بیشترین تعداد کدواژه را خواهد داشت یعنی:

$$|C| = A_q(n,d) = \frac{q^n}{\sum_{i=0}^{e=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i}.$$

از رابطه بالا و با درنظرگرفتن آن‌چه در اثبات قضیه ۴۳.۳.۱ (کران همینگ) آمده‌است داریم:

$$q^n = |C|. \sum_{i=0}^{e} \binom{n}{i}(q-1)^i = |C|.v(n,q,e)$$

$$\Rightarrow |A^n| = |C|.v(n,q,e)$$

و همان‌طور که در اثبات قضیه مذکور گفته شد، $v(n,q,e)$ تعداد بردارهای یک کره به مرکزیت c_i و شعاع e است، لذا خواهیم داشت:

$$A^n = \bigcup_{i=1}^{|C|} s_A(c_i, e)$$

حال اگر اجتماع کره‌های مجزا به مرکزیت اعضای C و به شعاع e را با $k(C)$ نمایش دهیم آن‌گاه: $A^n = k(C)$.

پس می‌توان تعریفی جدید معادل با تعریف اول برای یک کد کامل به‌صورت زیر ارائه‌داد:

کد C به عنوان زیر مجموعه‌ای از A^n کامل است هرگاه $k(C) = A^n$ و برای هر دو بردار x, y، $k(x) \cap k(y) = \varnothing$.

به‌عبارت‌دیگر کد C کامل است هرگاه A^n با کره‌هایی به مرکزیت اعضای C و شعاع e افراز شود.

اگر یک کد با مینیمم فاصله ۳ و در نتیجه کدی ۱− تصحیح کننده خطا باشد آنگاه $e = 1$ لذا تعریف قبل معادل است با این که: کد C کامل است اگر برای هر بردار $z \in A^n$ ، دقیقا یک بردار $x \in C$ وجود داشته‌باشد به‌طوری‌که x و z حداکثر در یک مولفه متفاوت باشند، به‌عبارت‌دیگر $d(z,x) \leq 1$.

[1] Perfect code

همان‌طور که گفته‌شد یک کد کامل لزوماً کدی خطی نیست. اما ما در این فصل توجه خود را به کدهای کامل خطی معطوف می‌کنیم. به مثال زیر توجه کنید.
مثال: فرض کنید $C^{(n-1)/2}$ یک کد کامل به‌طول $2^m - 1 = \frac{n-1}{2}$، $m \geq 2$ باشد و λ یک تابع دل‌خواه از $C^{(n-1)/2}$ به مجموعه‌ی $\{0,1\}$ باشد. برای $x = (x_1, ..., x_{(n-1)/2}) \in A^{(n-1)/2}$ فرض کنید $|x| = x_1 + ... + x_{(n-1)/2}$ (در مبنای دو) باشد. دراین‌صورت اگر برای هر $y, y' \in C^{(n-1)/2}$ داشته‌باشیم $\lambda(y) + \lambda(y') \neq \lambda(y + y')$ آن‌گاه مجموعه‌ی

$$V^n = \{(x+y, |x| + \lambda(y), x) : x \in A^{(n-1)/2}, y \in C^{(n-1)/2}\}$$

یک کد کامل غیر خطی به‌طول n است که به **کد واسیلو** [2] معروف است.

تعریف ۲.۲.۲. رتبه کد کامل: بعد زیر فضای پدید آمده از عناصر یک کد کامل مانند C، رتبه C نامیده‌شده و با $rank(C)$ نمایش داده‌می‌شود.
یک کد کامل مانند C، به طول n دارای رتبه تام است هرگاه $rank(C) = n$. در این‌صورت کد C را یک **کد کامل با رتبه تام** [3] نامند.

تعریف ۳.۲.۲. هسته یک کد کامل: هسته یک کد کامل مانند C روی Z_2، مجموعه تناوب‌های C است و با $\ker(C)$ نمایش داده‌می‌شود.

$$\ker(C) = \{p \in Z_2^n | p + C = C\}$$

$$p + C = \{p + c | c \in C\}.$$

تذکر: لازم به‌ذکر است که وقتی کد C خطی است اگر $p + C = C$ آن‌گاه $p \in C$ در نتیجه $\ker(C) = C$.

[2] Vasil'ev code
[3] Full rank perfect code

قضیه ۴.۲.۲. [۱۰] کدهای کامل غیر بدیهی به طول n فقط با سه مشخصه‌ی زیر وجود دارند:

۱) $d = ۳; n = \frac{q^m - ۱}{q - ۱}; m \geq ۱$ ؛ $q = p^k$ که p عددی اول است،

۲) $d = ۷; n = ۲۳; q = ۲$؛

۳) $d = ۵; n = ۱۱; q = ۳$.

در مورد اول که $d = ۳$ و $n = \frac{q^m - ۱}{q - ۱}$ است، ساختارهای زیادی از کدهای کامل مخصوصا برای حالت دودویی وجود دارد. از حالا به بعد هرگاه از کدهای کامل صحبت می‌کنیم و مشخصات دقیق آن را ذکر نمی‌کنیم منظورمان کدهای کامل دودویی با مینیمم فاصله $d = ۳$ است. در زیر چند نوع کد کامل را به همراه خصوصیات آن‌ها مورد بررسی قرار می‌دهیم.

۳.۲ کد همینگ دودویی

برای تعریف کد همینگ که در سال ۱۹۴۹ توسط ریچارد همینگ ارائه شد، ابتدا قضیه ۳۲.۳.۱ را یادآوری می‌کنیم.

اگر H ماتریس کنترل توازن یک کد خطی به طول n باشد آن‌گاه این کد دارای مینیمم فاصله d است اگرو فقط اگر هر $d - ۱$ ستون از H مستقل خطی باشند و d ستون وابسته خطی در H وجود داشته باشند.

اکنون می‌خواهیم یک دسته از کدهای کامل دودویی با مینیمم فاصله ۳ بسازیم.

با استفاده از اثبات قضیه گیلبرت ورشامو که در فصل اول به آن اشاره شد، برای هر عدد طبیعی m باید بردارهایی دودویی به طول m داشته باشیم که در قضیه بالا برای $d = ۳$ صدق کنند. برای این منظور باید یک ماتریس کنترل توازن بسازیم به‌طوری‌که هر دو ستون آن مستقل خطی باشند و سه ستون وابسته خطی نیز درآن وجود داشته‌باشند.

در این مورد به جز بردار تماما صفر $o^m = (۰, ..., ۰)$، می‌توانیم تمام بردارهای فضای $F_۲^m$ را درنظر بگیریم.

در نتیجه دسته ای از کدهای با فاصله ۳ خواهیم داشت که با ماتریس کنترل توازنشان تعریف می شوند.

این کد، کد همینگ نامیده می‌شود و با $Ham(m,2)$ یا H^n نمایش داده‌می‌شود.

پس در نهایت کد همینگ دودویی را به صورت زیر تعریف می‌کنیم:

تعریف ۲.۳.۱. فرض کنید $m \geq 2$ عددی صحیح باشد. **کد همینگ دودویی** [۴] یک کد خطی دودویی به‌طول $n = 2^m - 1$، با ماتریس کنترل توازن H است که ستون‌های آن تمام بردارهای غیر صفر F_2^m است که هر دو ستون آن مستقل خطی می‌باشند و آن را با $Ham(m,2)$ نشان می‌دهیم.

تذکر: خاطر نشان می‌شود که سطرهای H مستقل خطی هستند چون H شامل تمام m ستون با وزن ۱ می‌باشد. بنابراین H یک ماتریس کنترل توازن می‌باشد.

۲.۳.۱ مشخصات کد همینگ دودویی

گزاره ۲.۳.۲. [۶] بعد کد همینگ دودویی، یعنی $dim(H^n)$، برابر است با: $k = n - \log_2(n+1)$.

اثبات. می دانیم اگر بعد یک کد مانند C برابر k باشد ماتریس مولد آن کد ماتریسی $k \times n$ و ماتریس کنترل توازن آن $(n-k) \times n$ است. چون:

$$n = dim\langle C\rangle + dim\langle C^{\perp}\rangle = k + dim\langle C^{\perp}\rangle$$

خواهیم داشت

$$dim\langle C^{\perp}\rangle = n - k.$$

حال ماتریس کنترل توازن کد همینگ فوق از مرتبه‌ی $m \times (2^k - 1)$ است. درنتیجه داریم:

$$n - dim\langle H^n\rangle = m \Rightarrow dim\langle H^n\rangle = n - m$$

[۴] Binary Haming code

و از آن‌جا که:

$$n = 2^m - 1 \Rightarrow 2^m = n + 1 \Rightarrow m = \log_2(n+1)$$

لذا داریم:

$$dim(H^n) = n - \log_2(n+1).$$

$\square$

لذا پارامترهای کد همینگ دودویی به صورت زیر است:

$$[n = 2^m - 1; k = 2^m - 1 - m = n - \log_2(n+1); d = 3]$$

گزاره ۳.۳.۲. [۶] کد همینگ کدی ۱− تصحیح کننده خطاست.

اثبات. همان‌طور که می‌دانیم در کد همینگ مینیمم فاصله برابر ۳ است لذا بنا به قضیه ۱۲.۳.۱ این کد ۱− تصحیح کننده خطاست. $\square$

گزاره ۴.۳.۲. [۶] کد همینگ دودویی، کامل است.

اثبات. چون کد همینگ کدی خطی است لذا تعداد کدواژه‌های آن برابراست‌با:

$$|H^n| = 2^k = 2^{2^m-1-m}$$

حال با درنظرگرفتن کران همینگ داریم:

$$|H^n| = \frac{q^n}{\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{n}{i}(q-1)^i} = \frac{2^n}{\sum_{i=0}^{1}\binom{n}{i}} = \frac{2^n}{n+1} = \frac{2^{2^m-1}}{2^m} = 2^{2^m-1-m}$$

در نتیجه اندازه‌ی این کد در کران بالای همینگ صدق کرده و لذا این کد کامل است. $\square$

گزاره ۵.۳.۲. [۶] کدهای همینگ دودویی به طول یکسان معادلند.

اثبات. به‌وضوح برای یک طول ثابت با جابه‌جایی ستون‌های یکی از ماتریس‌های کنترل توازن، ماتریس کنترل توازن کد دیگر به‌دست می‌آید، پس این دو کد معادل هستند. $\square$

۲.۳.۲ مثال هایی از کد های همینگ دودویی به طول ۷

سه کد همینگ متفاوت به طول ۷ را در زیر نمایش می‌دهیم:

(۱) کد همینگ می‌تواند به شکل استاندارد باشد که دراین‌صورت سه ستون آخر ماتریس کنترل توازن آن، ماتریس همانی با رتبه ۳ است، برای مثال ماتریس کنترل توازن به شکل زیر است:

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

۱) کد C به طول n را دوری گویند اگر برای هر کدواژه $x=(x_1,...,x_n)$ ، $(x_2,x_3,...,x_n,x_1)$ نیز عضوی از C باشد.

کد همینگ H^7 با ماتریس کنترل توازن به فرم دوری، به صورت زیر نمایش داده می‌شود:

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

فرض کنید $B=(y_1,...,y_n)$ و $A=(x_1,...,x_n)$ دو بردار باشند: اگر $x_n > y_n$ باشد آن‌گاه $A>B$ و اگر $x_n = y_n$ باشد آنگاه y_{n-1} و x_{n-1} را مقایسه می‌کنیم و ...

در این صورت A و B از **ترتیب الفبایی** [5] نامیده می شود.

۳) ماتریس کنترل توازن کد همینگ به ترتیب الفبایی به شکل زیر است:

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

۳.۳.۲ کد گشایی کد همینگ دودویی

برای کد گشایی کد همینگ $Ham(m,2)$ با ماتریس کنترل توازن H به صورت زیر عمل می‌کنیم:

۱) با دریافت $s(w)$ ، w را به شکل زیر به‌دست می‌آوریم: $s(w)=w.H^T$.

۲)اگر $s(w)=0$ آن‌گاه w کدواژه ارسالی است.

۳)اگر $s(w)$ نمایش دودویی عدد $1 \le j \le 2^r - 1$ باشد آن‌گاه برداری را به‌صورت $e_j =$

[5]Lexicographic order

$(\circ, \dots, \circ, ۱, \circ, \dots, \circ)$ درنظر می‌گیریم که ۱ در مکان j ام قرار دارد. در نتیجه $w + e$ کدواژه ارسالی خواهدبود.

به عنوان مثال اگر کد همینگ $Ham(۳, ۲)$ ، کدی با ماتریس کنترل توازن از مرتبه الفبایی باشد، برای کدگشایی بردار $w = ۱۰۰۱۰۰۱$ داریم:

$$s(w) = w.H^T = ۰۱۰$$

اما ۰۱۰ نمایش دودویی عدد ۲ است. لذا $e_۲ = ۰۱۰۰۰۰۰$ بردار خطا خواهدبود. پس کدواژه ارسالی به شکل زیر به‌دست خواهدآمد:

$$w + e = ۱۰۰۱۰۰۱ + ۰۱۰۰۰۰۰ = ۱۱۰۱۰۰۱$$

۴.۲ کد سیمپلکس

تعریف ۱.۴.۲. دوگان کد همینگ دودویی $Ham(m, ۲)$، **کد سیمپلکس** [۶] دودویی نامیده می‌شود و گاهی با $S(m, ۲)$ نمایش داده می‌شود.

گزاره ۲.۴.۲. [۱۰] ۱) اگر G ماتریس مولد کد سیمپلکس $S(m, ۲)$ باشد، برای هر بردار غیر صفر $v \in F_۲^m$، دقیقا $۲^{m-۱} - ۱$ ستون مانند c از G وجود دارد به‌قسمی‌که $v.c = ۰$.

۲) هر کد واژه غیر صفر از $S(m, ۲)$ دارای وزن $۲^{m-۱} = \frac{n+۱}{۲}$ است.

اثبات. ۱) فرض کنید v بردار غیر صفر در $F_۲^m$ باشد ابتدا نشان می‌دهیم مجموعه بردارهای $F_۲^m$ که بر v عمود هستند ($\{v\}^\perp$) یک زیر فضا از $F_۲^m$ است که دارای بعد $m - ۱$ است.

طبق قضیه‌ی ۱۴.۳.۱ برای این‌که نشان دهیم $\{v\}^\perp$ زیرفضای $F_۲^m$ است باید نشان‌دهیم برای هر $x, y \in \{v\}^\perp$، $x + y \in \{v\}^\perp$ است.

فرض می‌کنیم $x, y \in \{v\}^\perp$ دل‌خواه باشند، داریم:

---

[۶] Simplex code

$(x+y).v = x.v + y.v = \circ + \circ = \circ \Rightarrow x + y \in \{v\}^{\perp}$

می‌دانیم فضای تولید شده توسط v، یعنی $\langle v\rangle$، دارای بعد یک است و بنا به قضیه ۲۵.۳.۱ داریم:

$dim\langle v\rangle + dim\{v\}^{\perp} = m \Rightarrow dim\{v\}^{\perp} = m - ۱$

پس $\{v\}^{\perp}$ زیر فضایی از $F_۲^m$ با بعد $m-۱$ است. در نتیجه بنا به قضیه ۱۹.۳.۱ و با توجه به این که محاسبات بر مبنای دو است، $\{v\}^{\perp}$ دارای $۲^{m-۱}$ عضو و $\langle v\rangle$ دارای دو عضو است.

از آن‌جا که G ماتریس کنترل توازن کد سیمپلکس و ماتریس کنترل توازن کد همینگ است لذا بنا به تعریف کد همینگ، ستون‌های G شامل تمام بردارهای غیر صفر $F_۲^m$ هستند یعنی G شامل $۲^m - ۱$ ستون است که بردار v و تمام بردارهای $\{v\}^{\perp}$ به جز بردار تماما صفر را شامل می‌شود. پس دقیقا به تعداد $۲^{m-۱} - ۱$ ستون در G مانند c وجود دارد که $c.v = \circ$.

۲) با توجه به قسمت قبل تعداد ستون‌هایی از G مانند c به طوری که $c.v = \circ$ باشد برابراست‌با $۲^{m-۱} - ۱$، پس $v.G$ دارای $۲^{m-۱} - ۱$ مولفه صفر است و از آن‌جا که $v.G$ به طول $۲^m - ۱$ است پس تعداد مولفه های ۱ در $v.G$ که همان وزن $v.G$ است برابر است با:

$wt(v.G) = ۲^m - ۱ - ۲^{m-۱} + ۱ = ۲^m - ۲^{m-۱} = ۲^{m-۱}.$

با کمی دقت پی می بریم که $v.G$ به ازای هر v در $F_۲^m$، ترکیب خطی از سطرهای G است و چون G ماتریس مولد کد سیمپلکس است پس به ازای هر v در $F_۲^m$، $v.G$ برداری غیّر صفر در کد سیمپلکس $s(m,۲)$ است.

در نتیجه همان‌طور که در بالا گفته‌شد وزن هر بردار غیر صفر در $s(m,۲)$ برابر با، $۲^{m-۱}$ است و چون $n = ۲^m - ۱$ است پس داریم: $\frac{n+۱}{۲} = ۲^{m-۱}$. □

۵.۲ کد همینگ q- نمادی

تعریف ۱.۵.۲. فرض کنید $m \geq ۲$ عددی صحیح باشد و q توانی از یک عدد اول باشد، یک کد خطی روی F_q که ماتریس کنترل توازن آن حاوی m سطر و n ستون است، به‌طوری‌که

n بیشترین تعداد ممکن ستون‌هایی است که هیچ دو ستونی وابسته خطی نباشند را یک **کد همینگ q- نمادی** [۷] به طول n نامیده و با $Ham(m,q)$ نمایش میدهیم.

قضیه ۲.۵.۲. [۸] در کد همینگ $Ham(m,q)$ داریم:

$$n = \frac{q^m - 1}{q - 1}.$$

اثبات. برای هر $u \in F_q^m$ قرار می‌دهیم: $m_u = \{\lambda u | \lambda \in F_q - \{0\}\}$ لذا به ازای هر u، $|m_u| = q - 1$.
فرض کنید دو مجموعه m_u و m_v دارای اشتراک باشند یعنی بردار x موجود است که $x \in m_u \bigcap m_v$.
در این صورت اسکالرهای λ_1 و λ_2 موجودند که $x = \lambda_1 u = \lambda_2 v$

$$x \in m_u \cap m_v \Rightarrow \exists \lambda_1, \lambda_2; x = \lambda_1 u = \lambda_2 v$$

نشان می‌دهیم $m_u \subseteq m_v$. فرض کنید $y \in m_u$ باشد در نتیجه:

$$\exists \lambda_3; y = \lambda_3 u = \lambda_3 \lambda_1^{-1} \lambda_1 u = \lambda_3 \lambda_1^{-1} \lambda_2 v = \lambda v$$

به‌طور مشابه می توان نشان داد $m_v \subseteq m_u$. در نتیجه $m_u = m_v$.
بنابراین مجموعه‌های فوق یا اشتراک ندارند و یا در صورت داشتن اشتراک مساوی هستند. از طرفی هر عضو $F_q^m - \{0\}$ در یکی از این مجموعه‌ها قرار دارد پس مجموعه‌های فوق $F_q^m - \{0\}$ را افراز می‌کنند. اما هر یک از این مجموعه‌ها $q - 1$ عضو دارد و $F_q^m - \{0\}$ دارای $q^r - 1$ عضو است. پس تعداد این مجموعه‌ها برابر است با $\frac{q^m - 1}{q - 1}$. □

بنابراین گزاره‌ی زیر حاصل می‌شود.

گزاره ۳.۵.۲. [۱۰] برای کدهای $Ham(m,q)$ داریم:

۱) همه کدهای همینگ q- نمادی به‌طول یکسان معادل هستند.
۲) کد $Ham(m,q)$ یک $\left[\frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} - m, 3\right]$ - کد است.
۳)کد همینگ $Ham(m,q)$ ، کامل است.

[۷] q-ary Hamming code

۶.۲ کد گلی

کدهای گلی در سال ۱۹۴۰ توسط **گلی** [۸] ارائه شد. کدهای گلی مثال‌هایی از کدهای کامل هستند.

۱.۶.۲ کد گلی دودویی توسعه یافته

تعریف ۱.۶.۲. فرض کنید G یک ماتریس ۲۴ × ۱۲ و به‌شکل زیر باشد. $G=(I_{12}|A)$ که I_{12} ماتریس همانی ۱۲ × ۱۲ و A نیز ماتریس ۱۲ × ۱۲ زیر است.

$$A=\begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0\\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1\\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1\\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0\\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1\\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1\\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1\\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0\\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0\\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0\\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}$$

یک کد خطی دودویی با ماتریس مولد G **کد گلی توسعه یافته** [۹] نامیده می‌شود و با G_{24} نمایش داده می‌شود.

گزاره ۲.۶.۲. [۱۰] (i) طول G_{24}، ۲۴ و بعد آن ۱۲ است.

(ii) یک ماتریس کنترل توازن برای G_{24} ماتریس ۲۴ × ۱۲ زیر است: $H=(A|I_{12})$.

(iii) کد G_{24} خود دوگان است پس $G_{24}=G_{24}^{\perp}$.

(iv) یک ماتریس کنترل توازن دیگر برای G_{24} ماتریس ۲۴ × ۱۲ زیر است:

$H'=(I_{12}|A)(=G)$.

(v) یک ماتریس مولد دیگر برای G_{24} ماتریس ۲۴ × ۱۲ زیر است: $G'=(A|I_{12})(=H)$.

---

[۸] Golay

[۹] Extended Golay code

(vi) وزن هر کدواژه در $G_{۲۴}$ مضربی از ۴ است.

(vii) کد $G_{۲۴}$ ، کدواژه با وزن ۴ ندارد بنابراین مینیمم فاصله $G_{۲۴}$، $d = ۷$ است.

$(viii)$ کد $G_{۲۴}$ دقیقا ۳− تصحیح کننده خطاست.

اثبات. (i) این قسمت با توجه به تعریف $G_{۲۴}$ واضح است.

(ii) با توجه به قضیه ۳۳.۳.۱ چون ماتریس مولد C یعنی G به‌شکل استاندارد $(I_{۱۲}|A)$ است لذا ماتریس کنترل توازن C، هم‌چنین با توجه به این که محاسبات بر مبنای دو است و A ماتریسی متقارن است لذا ماتریس کنترل توازن C به شکل $H = (A|I_{۱۲})$ است.

(iii) خاطر نشان می‌کنیم که سطرهای G بر هم عمود هستند یعنی اگر r_i و r_j دو سطر دلخواه از G باشند آن گاه $r_i.r_j = ۰$.

این نتیجه می‌دهد که $G_{۲۴} \subseteq G_{۲۴}^{\perp}$.

از طرف دیگر چون $G_{۲۴}$ و $G_{۲۴}^{\perp}$ هر دو دارای بعد ۱۲ هستند پس باید $G_{۲۴} = G_{۲۴}^{\perp}$ باشد.

(iv) یک ماتریس کنترل توازن $G_{۲۴}$ ،یک ماتریس مولد $G_{۲۴}^{\perp} = G_{۲۴}$ است، و G چنین ماتریس است، پس G ماتریس کنترل توازن $G_{۲۴}$ نیز هست.

(v) یک ماتریس مولد $G_{۲۴}$، یک ماتریس کنترل توازن $G_{۲۴}^{\perp} = G_{۲۴}$ است و H چنین ماتریسی است، پس H ماتریس مولد دیگری برای $G_{۲۴}$ است.

(vi) فرض کنید v کدواژه‌ای در $G_{۲۴}$ باشد. می‌خواهیم نشان دهیم که وزن همینگ v، یعنی $wt(v)$، مضربی از ۴ است. خاطر نشان می‌کنیم که v ترکیب خطی از سطرهای G است. فرض کنیم r_i سطر i ام G باشد.

ابتدا فرض می‌کنیم v یکی از سطر□های G است. چون سطرها دارای وزن ۸ و ۱۲ هستند پس وزن v مضربی از ۴ است.

در گام بعد فرض می‌کنیم v جمع دو سطر مختلف از G باشد یعنی $v = r_i + r_j$.

می‌دانیم $G_{۲۴}$ خود دوگان است، یعنی $G_{۲۴} = G_{۲۴}^{\perp}$ است و در قضیه‌ای داریم که اگر x و y دو

کدواژه از کد دودویی خود دوگان باشند و وزن x و y مضربی از ۴ باشد آن‌گاه وزن $x+y$ نیز مضربی از ۴ است. پس چون هر دو سطر G مثل r_i و r_j مضربی از ۴ هستند پس $v = r_i + r_j$ نیز مضربی از ۴ است. گذشته از این می‌توان هر دو سطر G را با هم جمع کرد دراینصورت مشاهده میشود که وزن مجموع هر دو سطر مضربی از ۴ است.

در ادامه به راحتی به استقرا ثابت می‌شود که وزن هر $v \in G_{24}$ مضربی از ۴ است.

(vii) توجه کنید که وزن سطر آخر G برابر ۸ است. با درنظر گرفتن این حقیقت و قسمت (vi) نتیجه می‌گیریم که ۸ یا $d = 4$ است.

فرض می‌کنیم G_{24} یک کدواژه مانند v داشته باشد که $wt(v) = 4$ است. v را به‌صورت $(v_1.v_2)$ می‌نویسیم که v_1 برداری به طول ۱۲ و ساخته‌شده از ۱۲ مولفه اول v و v_2 برداری به طول ۱۲ باشد که از ۱۲ مولفه دوم v ساخته شده‌است.دراین‌صورت یکی از موارد زیر اتفاق می‌افتد.

مورد یک: $wt(v_1) = 0$ و $wt(v_2) = 4$. این مورد نمی‌تواند اتفاق بیفتد چون با نگاهی به ماتریس مولد G، می‌توان دید که تنها بردار با این مشخصات، بردار تماما صفر است که وزن صفر دارد.

مورد دو: $wt(v_1) = 1$ و $wt(v_2) = 3$. در این مورد نیز با نگاهی به ماتریس G ، v باید یکی از سطرهای G باشد که باز هم تناقض است چون هیچ یک از سطرهای G داراری وزن ۴ نیستند.

مورد سه: $wt(v_1) = 2$ و $wt(v_2) = 2$. پس v باید جمع دو سطر از G باشد. به آسانی می توان دید که با جمع هیچ دوسطری از G ، $wt(v_2)$ برابر با ۲ نخواهد شد.

مورد چهار: $wt(v_1) = 3$ و $wt(v_2) = 1$. چون G' نیز بنا بر قسمت (v) ماتریس مولدی برای G_{24} است پس v باید سطری از G' باشد که به‌وضوح متناقض با این حقیقت است که وزن هیچ سطری از G' برابر ۴ نیست.

مورد پنجم: $wt(v_1) = 4$ و $wt(v_2) = 0$. این مورد نیز مشابه مورد اول است ولی در این مورد G' را به جای G بکار می‌بریم.

در تمام موارد فوق تناقض ایجاد می‌شود. لذا در تمام این موارد حالت $d = 4$ غیر ممکن است. بنابراین $d = 8$ است.

$(viii)$ می‌دانیم در $G_{۲۴}$ ، $d = ۸$ است لذا با توجه به قضیه ۱۲.۳.۱ $G_{۲۴}$ کدی دقیقا ۳- تصحیح کننده خطاست. □

تعریف ۳.۶.۲. فرض کنید $\widehat{G}$ ماتریس ۲۳ × ۱۲ زیر باشد: $\widehat{G} = (I_{۱۲}|\widehat{A})$

که $I_{۱۲}$ ماتریس همانی ۱۲ × ۱۲ و $\widehat{A}$ ماتریس ۱۱ × ۱۲ بدست‌آمده از ماتریس A با حذف ستون آخر A است.

کد خطی دودویی با ماتریس مولد $\widehat{G}$ **کد گلی دودویی** [۱۰] نام دارد و با $G_{۲۳}$ نمایش داده می‌شود.

تذکر: به‌عبارت‌دیگر کد گلی دودویی می‌تواند به‌عنوان کد بدست آمده از $G_{۲۴}$ با حذف مولفه آخر هر کدواژه تعریف شود.

گزاره ۴.۶.۲. [۸] (i) طول $G_{۲۳}$ برابر ۲۳ و بعد آن ۱۲ است.

(ii) یک ماتریس کنترل توازن برای $G_{۲۳}$ ، ماتریس ۲۳ × ۱۱ زیر است: $\widehat{H} = (\widehat{A}^T|I_{۱۱})$.

(iii) $G_{۲۴}$ کد توسعه یافته $G_{۲۳}$ است.

(iv) مینیمم فاصله $G_{۲۳}$ ، $d = ۷$ است.

(v) کد $G_{۲۳}$ کد کامل دقیقا ۳ - تصحیح کننده خطاست.

اثبات. (i) با توجه به این‌که $G_{۲۳}$ کدی خطی است لذا با توجه به تعریف واضح است که طول هر کدواژه در آن ۲۳ و بعد آن ۱۲ است.

(ii) با توجه به قضیه ۳۳.۳.۱ چون ماتریس مولد $G_{۲۳}$ یعنی $\widehat{G}$ به شکل استاندارد $(I_{۱۲}|\widehat{A})$ است لذا ماتریس کنترل توازن آن به‌شکل $\widehat{H} = (-\widehat{A}^T|I_{n-k}) = (\widehat{A}^T|I_{۱۱})$ است.

(iii) با توجه به تعریف کد توسعه یافته می‌دانیم که مولفه آخر یا مولفه کنترل توازن هر کد توسعه یافته وقتی در مبنای ۲ محاسبه می‌کنیم، برابر با مجموع مولفه‌های کد اصلی است. از آن جا که تمام مولفه‌های کد $G_{۲۳}$ باید ترکیب‌های خطی سطرهای ماتریس مولد یعنی $\widehat{G}$ باشند و مولفه‌های کد $G_{۲۴}$ باید ترکیب خطی سطرهای G باشند با مقایسه $\widehat{G}$ و G و انجام محاسبات

[۱۰] Binary Golay code

ساده می‌بینیم G یک ستون بیشتر از $\widehat{G}$ دارد و هر مولفه این ستون جمع تمام مولفه‌های سطر متناظر است.

حال اگر ترکیب خطی هر کدام از سطرهای G را هم درنظر بگیریم باز هم مشاهده می‌کنیم که مولفه آخر هر سطر جمع تمام مولفه‌های سطر متناظر است.

پس در G_{24} مولفه آخر هر کدواژه جمع تمام مولفه‌های آن کدواژه است پس G_{24} کد توسعه یافته کد G_{23} است.

(iv) بنا به قضیه ۳۸.۳.۱ مربوط به کدهای توسعه یافته، فرض کنید d مینیمم فاصله در C و d' مینیمم فاصله در $\overline{C}$ باشد، اگر مولفه اضافه شده به تمام کدواژه‌ها با هم یکسان باشد آن‌گاه $d' = d$ و در غیر این صورت $d' = d + 1$.

در مورد G_{24} چون مولفه‌ی اضافه شده به هر کدواژه گاهی صفر و گاهی یک است پس $d' = d + 1$ است. و قبلا ثابت شد که برای G_{24}، $d' = 8$ است، پس باید $d = 7$ باشد.

(v) با توجه به قسمت قبل که دیدیم که در G_{23} ، $d = 7$ است و بنا به قضیه ۱۲.۳.۱، G_{23} یک کد دقیقا ۳- تصحیح کننده خطاست. حال ثابت می کنیم G_{23} کامل است:

چون G_{23} کدی خطی و دودویی است پس داریم:

$$|G_{23}| = 2^k = 2^{12}$$

حال با توجه به رابطه‌ی

$$|G_{23}| = \frac{q^n}{\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor} \binom{n}{i}(q-1)^i} \frac{2^{23}}{\sum_{i=0}^{3} \binom{23}{i}} = \frac{2^{23}}{2048} = \frac{2^{23}}{2^{11}} = 2^{12}$$

مشخص می‌شود که G_{23} در کران همینگ صدق کرده ودر نتیجه کدی کامل است. $\square$

تعریف ۵.۶.۲. کد گلی سه‌سه‌ای توسعه یافته که با G_{12} نمایش داده می‌شود، یک کد خطی سه‌سه‌ای با ماتریس مولد $G = (I_6|B)$ است.که B ماتریس 6×6 زیر است:

$$B = \begin{pmatrix} ۰ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۲ & ۲ & ۱ \\ ۱ & ۱ & ۰ & ۱ & ۲ & ۲ \\ ۱ & ۲ & ۱ & ۰ & ۱ & ۲ \\ ۱ & ۲ & ۲ & ۱ & ۰ & ۱ \\ ۱ & ۱ & ۲ & ۲ & ۱ & ۰ \end{pmatrix}$$

تذکر: هر کد خطی که با کد بالا معادل باشد کد گلی سهسهای نامیده میشود.
مشابه روندی که در اثبات مشخصات کد گلی دودویی بکاررفت به‌آسانی میتوان بررسی کرد که $G_{۱۲}$ یک کد سه‌سه‌ای خود دوگان است و یک $[۱۲,۶,۶]$- کد خطی است.

تعریف ۶.۶.۲. کد گلی سه‌سه‌ای که با $G_{۱۱}$ نمایش داده می‌شود کدی خطی است که از حذف مولفه‌ی آخر کدواژه‌های $G_{۱۲}$ به وجود می‌آید.

تذکر: با بررسی ستون آخر ماتریس مولد $G_{۱۲}$ می‌توان فهمید که هر مولفه‌ی در این ستون قرینه‌ی مجموع تمام مولفه‌های سطر متناظر (در مبنای سه) است. پس می‌توان گفت $G_{۱۲}$ کد توسعه یافته $G_{۱۱}$ است.
می‌خواهیم نشان دهیم که $G_{۱۱}$ یک $[۱۱,۶,۵]$ - کد سه‌سه‌ای است.
با توجه به این که $G_{۱۲}$ یعنی کد توسعه یافته $G_{۱۱}$ یک $[۱۲,۶,۶]$- کد است پس بنا به قضیه ۳۸.۳.۱، $G_{۱۱}$ باید دارای طول ۱۱ و بعد ۶ باشد و اگر تمام مولفه‌هایی که به آخر هر کدواژه در $G_{۱۲}$ اضافه می‌شوند یکسان باشند، مینیمم فاصله $G_{۱۲}$ و $G_{۱۱}$ برابر است اما از آنجا که مولفه‌های آخر هر کدواژه در $G_{۱۲}$ یکسان نیستند پس مینیمم فاصله $G_{۱۱}$ از مینیمم فاصله ی $G_{۱۲}$ یکی کمتر است در نتیجه در $G_{۱۱}$ ، $d = ۵$ است.
برای بررسی کامل بودن $G_{۱۱}$، چون $G_{۱۱}$ کدی سه‌سه‌ای خطی با بعد ۶ است پس داریم:

$$|G_{۱۱}| = ۳^{۶}$$

از طرفی طبق کران همینگ داریم:

$$|G_{11}| = \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i} = \frac{3^{11}}{\sum_{i=0}^{2} \binom{11}{i} 2^i} = \frac{3^{11}}{1 + (11 \times 2) + (55 \times 4)} = \frac{3^{11}}{243} = \frac{3^{11}}{3^5} = 3^6$$

لذا G_{11} در کران همینگ صدق کرده و در نتیجه کدی کامل است.

فصل ۳
کدهای کامل با رتبه‌ی تام

۱.۳ مقدمه

تا این‌جا با چند نوع کد کامل خطی آشنا شدیم. در حال حاضر بیش از بیست ساختار از کدهای غیر خطی وجود دارد. ولی هنوز حتی برای طول‌های کوچک مانند $n = ۱۵$ نیز دسته‌بندی صورت نگرفته‌است. اولین ساختار یک کد کامل غیر خطی توسط **واسیلو** [۱] ارائه شد. پژوهشگران دیگری نیز مانند **زینو** [۲] و **سلوا** [۳]، با ارائه‌ی ساختارهای نسبتاً خوب در این کار سهیم بودند.

در این‌جا ما کدهای کاملی را که رتبه ی تام دارند درنظر خواهیم گرفت. مفهومی که در ادامه توضیح داده خواهدشد.

نتیجه‌ی اصلی ما در این فصل ارائه‌ی ساختار جدید از کدهای کامل با رتبه‌ی تام است. این کدها α- کدهای نرمال نامیده می‌شوند. برای ارائه‌ی این ساختار از ابر دوگان کد کامل استفاده خواهیم کرد، مفهومی که در بخش بعد توضیح داده می‌شود. مزیت این ساختار این‌است که این کدها مطابق تعریف به‌آسانی ساخته می‌شود و با استفاده از این ساختار یافتن مثال‌هایی از کدهای کامل با رتبه ی تام آسان است. در انتهای این فصل ما یک مثال از کدهای کامل با رتبه‌ی تام به طول ۳۱ و هسته‌ای با بعد ۲۱ ارائه می‌دهیم.

قبل از پرداختن به کدهای کامل با رتبه تام مفاهیم اولیه و مورد نیاز این مبحث را مورد بررسی

[۱] vasil'ev
[۲] Zinov'ev
[۳] Solov'eva

قرارمی‌دهیم.

۲.۳ مفاهیم اولیه

یک کد کامل دودویی۱− تصحیح کننده خطا، به‌طول n، زیر مجموعه‌ای از Z_2^n مانند C است که در مشخصه‌ی زیر صدق می‌کند:
برای هر عنصر $x = (x_1, x_2, ..., x_n)$ از Z_2^n، عنصر یکتای $c = (c_1, c_2, ..., c_n)$ از C وجود دارد، به‌قسمی که x و c حداکثر در یک مکان با هم اختلاف داشته‌باشند.
با توجه به این که کد C، کد کامل دودویی ۱− تصحیح کننده‌ی خطا است پس بنا قضیه‌ی ۱۲.۳.۱، کد C دارای مینیمم فاصله‌ی ۳ است. حال با استفاده از کران همینگ در قضیه‌ی ۴۳.۳.۱ داریم:

$$|C| = \frac{2^n}{\sum_{i=0}^{1} \binom{n}{i}} = \frac{2^n}{\binom{n}{0} + \binom{n}{1}} = \frac{2^n}{n+1} = \frac{2^n}{2^{\log(n+1)}} = 2^{n-\log(n+1)}$$

برای هر عدد صحیح t، حداقل یک کد کامل به‌طول $n = 2^t - 1$ وجود دارد با توجه به کدهای همینگ دودویی که در فصل قبل توضیح داده شد، این کدها دارای طول $n = 2^t - 1$ هستند و هم‌چنین می‌توان دید که طول n برای هر کد کامل دودویی همیشه برابر $n = 2^t - 1$ است که در آن t عددی صحیح است. با توجه به این‌که در این فصل با کدهای ۱− تصحیح کننده‌ی خطا که دارای مینیمم فاصله‌ی ۳ هستند سروکار داریم و بنا به قضیه‌ی ۴.۲.۲ کدهای کامل به طول n فقط با سه مشخصه‌ی زیر وجود دارند:

$d = 3; n = \frac{q^m - 1}{q - 1}; m \geq 1$ ؛ $q = p^k$ که p عددی اول است،

$d = 7; n = 23; q = 2$ ؛

$d = 5; n = 11; q = 3$

که در میان این سه دسته تنها کدهای دسته‌ی اول هستند که مینیمم فاصله‌ی آنها ۳ است، پس طول n برای هر کد کامل با مینیمم فاصله‌ی ۳ همیشه برابر $n = \frac{q^t - 1}{q - 1}$ است که در حالت

دودویی $n = ۲^t - ۱$ است.

می‌دانیم کد همینگ به‌طول $n = ۲^t - ۱$، کدی است با ماتریس کنترل توازن H که از مرتبه‌ی $t \times n$ است و ستون‌هایش تمام بردارهای دودویی غیر صفر به طول t است. کدهای همینگ، کدهای خطی کامل هستند.

همان‌طور که در فصل دوم گفته شد رتبه‌ی یک کد کامل C، $rank(C)$ ، بعد زیر فضای پدید آمده از عناصر یا کدواژه‌های C روی میدان $\mathbb{Z}_۲$ است.

یادآوری می‌کنیم که هسته‌ی یک کد کامل C، یعنی $\ker(C)$، مجموعه‌ی تناوب‌های p از C است:

$$\ker(C) = \{p \in \mathbb{Z}_۲^n \mid p + C = C\}$$

$$p + C = \{p + c | c \in C\}$$

هسته‌ی یک کد کامل همیشه زیر فضایی از $\mathbb{Z}_۲^n$ است، زیرا:

$$\forall a, b \in \ker(C), a + b \in \ker(C)$$

$$a + b = (a_۱, ..., a_n) + (b_۱, ..., b_n) = (c_۱, ..., c_n)$$

حال اگر $(t_۱, ..., t_n) \in C$ باشد:

$$(c_۱, ..., c_n) + (t_۱, ..., t_n) = ((a_۱, ..., a_n) + (b_۱, ..., b_n) + (t_۱, ..., t_n)) \in C$$

پس $(c_۱, ..., c_n) \in ker(C)$.

حال اگر کدواژه‌ی $(۰, ..., ۰)$ متعلق به C باشد، آن‌گاه هسته زیر مجموعه‌ی C است، زیرا:

$$\forall (x_۱, ..., x_n) \in ker(C) \text{ ، } (x_۱, ..., x_n) + (۰, ..., ۰) = (x_۱, ..., x_n) \in C$$

پس تمام اعضای $ker(C)$ عضو C هستند، در نتیجه $ker(C) \subseteq C$.

همان‌طور که می دانیم وزن یک کدواژه مانند c، یعنی $w(c)$، تعداد مؤلفه‌های غیر صفر c است و پشتیبان کدواژه $c = (c_۱, ..., c_n)$ مجموعه‌ی زیر است:

$$supp(c) = \{i | c_i \neq ۰\}$$

دو کد C و C' معادلند اگر کدواژه‌ی c. و جایگشت Π از مجموعه‌ی موقعیت‌های مؤلفه‌ها وجود داشته‌باشد، به‌قسمی که:

$$C' = \Pi(C) + c.$$

که در آن:

$$\Pi(C) = \{\Pi(c) | c \in C\} \text{ و } \Pi((c_۱, ..., c_n)) = (c_{\Pi(۱)}, ..., c_{\Pi(n)})$$

قبلاً گفته شد که یک کد سیمپلکس به طول $n = ۲^t - ۱$ یک زیر فضای خطی S از $\mathbb{Z}_۲^n$ است با این مشخصه که هر کدواژه غیر صفر S دارای وزن $\frac{(n+۱)}{۲}$ است. و ماتریس H که سطرهایش مجموعه‌ای از بردارهای پایه برای S تشکیل می‌دهند، یک ماتریس مولد برای کد سیمپلکس S است. اگر بعد S معادل t باشد، دراین‌صورت ماتریس H یک ماتریس $t \times n$ خواهد بود، بنابراین H یک ماتریس کنترل توازن کد همینگ C نامیده می‌شود و داریم:

$$C = \{c \in \mathbb{Z}_۲^n | Hc^T = ۰\}.$$

با معرفی یک مفهوم، برای تعریف $\alpha-$ کلمه یا $\alpha-$ کدواژه آماده می‌شویم.

فرض کنید $H = (s_{ij})$ یک ماتریس مولد برای S باشد، کدواژه‌ی $s_H(\alpha_۱, ..., \alpha_t)$ که $\alpha_\nu \in \{۰, ۱, *\}$ برای $\nu = ۱, ۲, ..., t$، نمایشی برای کدواژه‌ی $(t_۱, ...t_n) \in \mathbb{Z}_۲^n$ است به‌طوری‌که برای $i = ۱, ۲, ..., n$ داریم:

$$t_i = \begin{cases} ۱ & s_{ri} = \alpha_r, \forall r \in \{۱, ..., t\}, \alpha_r \neq * \\ ۰ & o.w \end{cases}$$

این مفهوم را با یک مثال توضیح می‌دهیم.

مثال . (۱)فرض کنید H ماتریس زیر باشد:

$$H = \begin{pmatrix} ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{pmatrix}$$

سطرهای H کد سیمپلکس S به طول ۷ و بعد ۳ را تولید می‌کند. کدواژه‌ی $(۰, ۰, ۰, ۰, ۱, ۰, ۱)$ متناظر با کدواژه‌ی $s_H(۱, *, ۱)$ خواهد بود ، $s_H(۰, *, *)$ متناظر با کدواژه‌ی $(۱, ۱, ۱, ۰, ۰, ۰, ۰)$ و $s_H(۰, ۱, ۱)$ متناظر با کدواژه‌ی $(۰, ۰, ۱, ۰, ۰, ۰, ۰)$ خواهد بود.

به‌طور مثال برای کدواژه‌ی $s_H(۱, *, ۱)$ می‌بینیم که مؤلفه‌ی اول وسوم آن۱ ومؤلفه‌ی دوم آن $*$ است. حال ستون‌های ماتریس H را بررسی می‌کنیم (هفت ستون داریم) ستون‌هایی را که مؤلفه ی اول وسوم آن ۱ است را انتخاب می‌کنیم و مؤلفه‌ی دوم که $*$ است بدین معنی است که در مؤلفه‌ی دوم مجازیم صفر یا یک داشته باشیم. با بررسی ستون‌های H می‌بینیم که فقط در ستون پنجم و هفتم مؤلفه‌ی اول و سوم، ۱ داریم، پس در کدواژه‌ی متناظر با $s_H(۱, *, ۱)$ مکان‌های پنجم و هفتم را یک و بقیه را صفر قرار می‌دهیم، لذا داریم: $(۰, ۰, ۰, ۰, ۱, ۰, ۱)$.

اگر حداقل برای دو عدد صحیح $i, j \in \{۱, ۲, ..., t\}$ داشته باشیم $\alpha_i = ۱$ و $\alpha_j = *$ ، آن‌گاه کدواژه $s_H(\alpha_۱, \alpha_۲, ..., \alpha_t)$ یک α–**کدواژه** [۴] برای ماتریس مولد H از کد سیمپلکس S نامیده می‌شود. مجدداً یادآوری می‌کنیم که S یک کد سیمپلکس به‌طول $n = ۲^t - ۱$ و با بعد t است. در مثال بالا $s_H(۱, *, ۱)$ یک α– کدواژه است اما $s_H(۰, *, *)$ و $s_H(۰, ۱, ۱)$، α– کدواژه نیستند.

توجه کنید که هر سطر در ماتریس H نیز یک α -کدواژه خواهد بود. سطر اول H، متناظر با α– کدواژه‌ی $s_H(۱, *, *)$، سطر دوم آن متناظر با α– کدواژه‌ی $s_H(*, ۱, *)$ و سطر سوم متناظر با α– کدواژه‌ی $s_H(*, *, ۱)$ خواهد بود.

مشخصه‌ی اصلی و سودمند α -کدواژه‌های $s_H(\alpha_۱, \alpha_۲, ..., \alpha_t)$ این‌است که می‌توان آن‌ها را با بعضی از سطرهای ماتریس H که ماتریس مولد یک کد سیمپلکس است جمع بست و یک ماتریس مولد برای یک کد سیمپلکس دیگر بدست آورد. از جمع α – کدواژه‌ی $s_H(۱, *, ۱)$ با سطر دوم ماتریس H، ماتریس زیر به‌دست خواهد آمد که یک ماتریس مولد برای یک کد

[۴] α-word

سیمپلکس دیگر است.

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

باید خاطرنشان کرد که H_1 می‌تواند از ماتریس H با جایگشت ستون‌های ۵ و ۷ بدست آید و هم‌چنین با جمع بستن هر $\alpha-$ کدواژه‌ی H با هر سطر از H ماتریس مولد برای یک کد سیمپلکس بدست نمی‌آید. به‌عنوان مثال با جمع بستن $\alpha-$ کدواژه‌ی $s_H(1,*,1)$ با سطر اول یا سوم ماتریس H، ماتریس مولد هیچ کد سیمپلکسی به‌دست نمی‌آید چون ماتریس به‌دست آمده حداقل دارای دو ستون یکسان یا وابسته‌ی خطی خواهد بود که بنا به آن‌چه قبلاً در تعریف کد همینگ گفته شد، باید هر دو ستون از ماتریس کنترل توازن کد همینگ مستقل خطی باشد. در ادامه خواهیم گفت از جمع بستن کدام یک از $\alpha-$ کدواژه‌ها با کدام سطرهای ماتریس مولد یک کد سیمپلکس، ماتریس مولد برای یک کد سیمپلکس دیگر به‌دست خواهد آمد. ♣

اکنون چهار لم اساسی برای کدواژه های $s_H(\alpha_1, ..., \alpha_t)$ ارائه خواهد شد که سه لم اول نتیجه‌ی مستقیم از تعریف این کدواژه‌ها هستند.

لم ۳.۲.۱. [۲] فرض کنید H یک ماتریس مولد برای یک کد سیمپلکس باشد. در این صورت پشتیبان دو کدواژه‌ی $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ و $a' = s_H(\alpha'_1, \alpha'_2, ..., \alpha'_t)$ مجزا هستند اگر و تنها اگر حداقل یک عنصر $i_0 \in \{1, 2, ..., t\}$ وجود داشته باشد به‌طوری‌که:

$$\alpha'_{i_0} \neq * \text{ ، } \alpha_{i_0} \neq * \text{ و } \alpha'_{i_0} \neq \alpha_{i_0}$$

اثبات. عبارت بالا بدین معنی است که حداقل یک i_0 موجود باشد که $\alpha_{i_0} = 1$ و $\alpha'_{i_0} = 0$ یا برعکس $\alpha'_{i_0} = 1$ و $\alpha_{i_0} = 0$ و بقیه‌ی مؤلفه‌های a و a' با هم برابر باشند. اگر $\{j_1, j_2, ..., j_r\}$ ستون‌های صفر از سطر i_0 و $\{j_1, j_2, ..., j_s\}$ ستون‌های یک از سطر i_0 در ماتریس H باشند، آن‌گاه مجموعه‌های $\{j_1, j_2, ..., j_r\}$ و $\{j_1, j_2, ..., j_s\}$ کاملاً مجزا هستند و $r + s = n$.

برای نوشتن پشتیبان کدواژه‌ی a، موقعیت‌های $j_1, ..., j_s$ امکان یک شدن و برای پشتیبان

کدواژه‌ی a' موقعیت‌های $j_1, ..., j_r$ امکان یک شدن دارند پس اعضای پشتیبان a از مجموعه‌ی $\{j_1, ..., j_s\}$ و اعضای پشتیبان a' از مجموعه‌ی $\{j_1, ..., j_r\}$ انتخاب می‌شود. چون این دو مجموعه کاملاً مجزا هستند، لذا پشتیبان a و a' نیز مجزا هستند. □

لم ۲.۲.۲.۳. [۲] اگر دو α− کدواژه ی متفاوت $a' = s_H(\alpha'_1, \alpha'_2, ..., \alpha'_t)$ و $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ در شرط زیر صدق کنند:

$$\alpha_i \neq * \Rightarrow \alpha'_i = \alpha_i \forall i = 1, 2, ...t \tag{1.3}$$

آن‌گاه پشتیبان a به طور محض شامل پشتیبان a' است.

اثبات. فرض کنید رابطه ی ۱.۳ برقرار باشد دراین‌صورت در موقعیت‌هایی که $\alpha_i = *$ است باید داشته باشیم $\alpha'_i = 1$ یا $\alpha'_i = 0$ که در آن $i = 1, ..., t$. ما فرض می‌کنیم $\alpha'_i = 1$. دراین‌صورت پشتیبان a' شامل موقعیت ستون‌هایی است که در جاهایی که a صفر است صفر، و جاهایی که a یک یا ستاره است یک باشد. لذا پشتیبان a علاوه بر اعضای پشتیبان a' شامل موقعیت های صفر به جای ستاره نیز می‌باشد. پس پشتیبان a به طور محض شامل پشتیبان a' است. □

برای هر کدواژه‌ی $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ ، V_a که در لم بعد از آن استفاده شده، به‌صورت زیر تعریف می‌شود:

$$V_a = \{(B_1, ..., B_t) \in \mathbb{Z}_2^t | \beta_i = \alpha_i if \alpha_i \neq *\}$$

لم ۳.۲.۲.۳. [۲] برای هر کدواژه‌ی $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ داریم :

$$s_H(\alpha_1, \alpha_2, ..., \alpha_t) = \sum_{(\beta_1, ..., \beta_t) \in V_a} s_H(\beta_1, ..., \beta_t).$$

اثبات. فرض می‌کنیم a در موقعیت‌های $i_1, ..., i_t$ ستاره باشد لذا V_a شامل اعضایی است که به‌جای ستاره در این موقعیت‌ها صفر یا یک دارند ودر بقیه‌ی جاها مانند a باشند، پس V_a دارای 2^t عضو خواهد بود. از آن‌جا که بنا بر لم ۲.۲.۳، پشتیبان a شامل پشتیبان تمام اعضای V_a است اگر

b عضوی دلخواه از V_a باشد آن‌گاه چون b فاقد ستاره است لذا فقط یکی از ستون‌های H در مشخصات b صدق کرده و b فقط در یک مکان یک است. پس پشتیبان هر عضو V_a فقط دارای یک عضو است. پس عدد 2^t همان تعداد یک‌های کدواژه‌ی a یا تعداد اعضای پشتیبان a است که از اجتماع 2^t عضو پشتیبان اعضای V_a به دست می‌آید، پس هر کدواژه‌ی a از حاصل‌جمع تمام اعضای V_a به‌دست خواهد آمد:

$$s_H(\alpha_1, \alpha_2, ..., \alpha_t) = \sum_{(\beta_1,...,\beta_t)\in V_a} s_H(\beta_1, ..., \beta_t).$$

□

اگر در مثال (۱)، $a = s_H(1, *, 1)$ را به‌عنوان یک کدواژه از ماتریس H در نظر داشته باشیم، داریم:

$$V_a = \{(1, 1, 1), (1, 0, 1)\}$$

$$s_H(1, *, 1) = s_H(1, 0, 1) + s_H(1, 1, 1)$$

$$(0, 0, 0, 0, 1, 0, 1) = (0, 0, 0, 0, 0, 0, 1) + (0, 0, 0, 0, 1, 0, 0).$$

تذکر: خاطر نشان می‌کنیم که هر کدواژه‌ی $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ به‌طوری‌که برای $i = 1, 2, ..., t$، $\alpha_i \neq *$ وزنی برابر یک دارد زیرا در غیراین‌صورت حداقل دو ستون در H داریم که همانند a است، یعنی حداقل دو ستون H با هم برابرند، و این غیر ممکن است، زیرا H ماتریس کنترل توازن کد همینگ دودویی است و طبق تعریف، ستون‌های ماتریس کنترل توازن کد همینگ دودویی یعنی $H_{t\times n}$، تمام بردارهای ناصفر $\mathbb{Z}_2^t$ هستند که هیچ دو ستونی وابسته‌ی خطی نباشند.
اکنون لم زیر مستقیماً از لم ۱.۲.۳ و ۳.۲.۳ نتیجه می‌شود.

لم ۴.۲.۳. [۲] وزن هر کدواژه ی $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ همیشه برابر 2^p است که در آن p تعداد مؤلفه‌های α_i در کدواژه‌ی a است که $\alpha_i = *$.

اثبات. طبق لم ۳.۲.۳ کدواژه‌ی a جمع ۲^p عنصر V_a است که ستاره ندارد پس وزن a مجموع وزن‌های این ۲^p عنصر است که طبق تذکر بالا هر یک دارای وزن یک می‌باشد، لذا وزن a برابر ۲^p می‌باشد. □

برای توضیح بیشتر لم بالا، اگر در مثال (۱)، $a = s_H(*, ۱, *)$ را به عنوان کدواژه‌ای برای H در نظر بگیریم آن‌گاه داریم:

$$s_H(*, ۱, *) = s_H(۱, ۱, ۱) + s_H(۰, ۱, ۱) + s_H(۱, ۱, ۰) + s_H(۰, ۱, ۰)$$

$$(۰, ۱, ۱, ۰, ۰, ۱, ۱) =$$

$$(۰, ۰, ۰, ۰, ۰, ۰, ۱) + (۰, ۰, ۱, ۰, ۰, ۰, ۰) + (۰, ۰, ۰, ۰, ۰, ۱, ۰) + (۰, ۱, ۰, ۰, ۰, ۰, ۰)$$

لذا وزن $s_H(*, ۱, *)$ برابر $۲^p = ۲^۲ = ۴$ است.

کدواژه‌ی $s_H(\alpha_۱, \alpha_۲, ..., \alpha_t)$ یک α–**کدواژه ابتدایی** [۵] از مرتبه i است اگر

$$\alpha_j = \begin{cases} * & j = i \\ ۰ \, or \, ۱ & j \neq i \end{cases}.$$

طبق لم ۴.۲.۳ چون هر α– کدواژه‌ی ابتدایی فقط یک مؤلفه ی ستاره دارد پس دارای وزن ۲ است.

تذکر: دو α– کدواژه‌ی ابتدایی که دارای مرتبه‌ی یکسان هستند دارای پشتیبان دو به دو مجزا هستند زیرا دو α– کدواژه‌ی ابتدایی که مرتبه‌ی یکسان دارند حداقل در یک مؤلفه غیر ستاره متفاوتند، در غیراین‌صورت دو کدواژه دقیقاً یکسان هستند، پس طبق لم ۱.۲.۳ این کدواژه‌ها پشتیبان مجزا دارند.

لم ۵.۲.۳. [۲] اگر $\alpha_i. = *$ آن‌گاه α -کدواژه ی $a = s_H(\alpha_۱, \alpha_۲, ..., \alpha_t)$ را می توان به‌صورت مجموع منحصر بفردی از α– کدواژه‌های ابتدایی از مرتبه‌ی i. نوشت که این α– کدواژه‌ها پشتیبان دو به دو مجزا دارند.

---

[۵] Primitive α– word

اثبات. هر α− کدواژه را می‌توان به‌صورت زیر نوشت:
اگر $\alpha_v = *$ آن‌گاه داریم:

$$s_H(\alpha_1, ..., \alpha_t) = s_H(\alpha'_1, ..., \alpha'_t) + s_H(\alpha''_1, ..., \alpha''_t)$$

که در آن اگر $j \neq v$، آن‌گاه داریم $\alpha'_j = \alpha''_j = \alpha_j$ و اگر $j = v$ آن‌گاه: $\alpha'_v = 0$ و $\alpha''_v = 1$. این رابطه نشان می‌دهد که هر α -کدواژه با وزن $w \geq 4$، یا با حداقل دو ستاره را می‌توان به صورت جمع دو α -کدواژه با پشتیبان دو به دو مجزا با وزن $\frac{w}{2}$ نوشت، زیرا وقتی که α -کدواژه‌ای با حداقل دو ستاره یا با وزن $w \geq 4$ را به صورت مجموع دو α -کدواژه با یک ستاره کمتر می‌نویسیم، با کمتر شدن یک ستاره، وزن به $\frac{w}{2}$ کاهش می‌یابد. اگر a دارای p ستاره باشد، آن‌گاه داریم:

$$w = 2^p \Longrightarrow 2^{p-1} = \frac{2^p}{2} = \frac{w}{2}$$

با ادامه‌ی روند بالا، در هر مرحله یک ستاره کمتر می‌شود. در نتیجه هر α− کدواژه را می‌توان به‌صورت جمع α - کدواژه‌های ابتدایی از رتبه‌ی i. نوشت (اگر a در موقعیت i. ستاره داشته باشد) هم‌چنین بنا به تذکر قبل خواهیم داشت که این α -کدواژه‌های ابتدایی پشتیبان دوبه‌دو مجزا دارند. □

برای فهم بیشتر مثال (۱) را در نظر می‌گیریم در این‌صورت خواهیم داشت:

$$s_H(*, 1, *) = s_H(*, 1, 1) + s_H(*, 1, 0)$$

$$(0, 1, 1, 0, 0, 1, 1) = (0, 0, 1, 0, 0, 0, 1) + (0, 1, 0, 0, 0, 1, 0)$$

یا

$$s_H(*, 1, *) = s_H(1, 1, *) + s_H(0, 1, *)$$

$$(0, 1, 1, 0, 0, 1, 1) = (0, 0, 0, 0, 0, 1, 1) + (0, 1, 1, 0, 0, 0, 0)$$

لذا α-کدواژه $s_H(*, ۱, *)$ را به دو صورت می‌توان به دو صورت میتوان بهصورت مجموع α-کدواژههای ابتدایی نوشت که همانطور که مشاهده میشود این کدواژههای ابتدایی پشتیبان مجزا دارند.

لم ۶.۲.۳. [۲] فرض کنید H ماتریس مولد یک کد سیمپلکس به‌طول $n = ۲^t - ۱$ و بعد t باشد و $a = s_H(\alpha_۱, \alpha_۲, ..., \alpha_t)$ یک α - کدواژه‌ی ابتدایی برای H از مرتبه ی i باشد. اگر سطر i ام H، یعنی h_i را با سطر $a + h_i$ جایگزین کنیم آن‌گاه ماتریس H'، ماتریس مولد کد سیمپلکس S' بدست خواهدآمد به‌طوری‌که $H' = \Pi(H)$.
که Π جابه‌جایی دو ستون متعلق به پشتیبان کدواژه a را نشان می‌دهد.

اثبات. هر ستون H را به‌صورت $(\beta_۱, \beta_۲, ..., \beta_i, ..., \beta_t)^T$ در نظر می‌گیریم و کدواژه‌ی a را با سطر i ام ماتریس H جمع می‌کنیم، حال اگر ستون $(\beta_۱, \beta_۲, ..., \beta_i, ..., \beta_t)$ متعلق به پشتیبان a باشد، آن‌گاه داریم:

$$b = (\beta_۱, \beta_۲, ..., \beta_i, ..., \beta_t)^T \Longrightarrow b' = (\beta_۱, \beta_۲, ..., \beta_i + ۱, ..., \beta_t)^T$$

در غیر این‌صورت $b \to b$. چون $\alpha_i = *$ پس موقعیت ستون b' نیز به پشتیبان a تعلق دارد. زیرا اگر $\alpha_i = *$ و بقیه‌ی α_j ها صفر و یک باشند، آن‌گاه وقتی a به سطر i ام H اضافه می‌شود فقط در ستون‌هایی تغییر ایجاد می‌شود که جزء پشتیبان a باشند. در این ستون‌ها تمّام مؤلفه‌ها با مؤلفه‌های a یکسان هستند غیر از مؤلفه‌ی i ام که می‌تواند صفر یا یک باشد که اگر مولفه‌ی i ام ستون‌های متعلق به پشتیبان a صفر باشد آن‌گاه با اضافه کردن a به سطر i ام H، این مولفه یک می‌شود (و بالعکس) که در این‌صورت باز هم در مشخصه‌ی α - کدواژه صدق کرده و در پشتیبان a قرار می‌گیرد. واضح است که H' از جابه جایی دو ستون از H که در پشتیبان a قرار دارند بدست می‌آید زیرا با جمع a با سطر i ام H، تغییر فقط در مولفه‌ی i ام ستون‌های متعلق به پشتیبان a صورت می‌گیرد. یکی از این دو ستون دارای مؤلفه‌ی i ام ۱ است که با اضافه شدن a به صفر تبدیل می‌شود و دیگری دارای مؤلفه ی i ام صفر است، که با اضافه شدن a به

یک تبدیل می‌شود و بقیه‌ی مؤلفه‌های این دو ستون یکسان هستند، پس می‌توان گفت این دو ستون جابهجا می شوند و ماتریس H' به‌وجود می‌آید. $\square$

برای توضیح بیشتر، در مثال (۱) دیدیم که با جمع بستن α- کدواژه‌ی ابتدایی از رتبه‌ی ۲، یعنی $a = s_H(1,*,1)$، با سطر دوم ماتریس H، ماتریس H_1 بدست آمد که ماتریس مولد کد سیمپلکس S_1 است. ماتریس H_1 با جابه‌جایی ستون‌های پنجم و هفتم ماتریس H که متعلق به پشتیبان a هستند نیز بدست می‌آید.

لم ۷.۲.۳. [۲] فرض کنید H ماتریس مولد یک کد سیمپلکس به طول $n = 2^t - 1$ و بعد t باشد و $a = s_H(\alpha_1, \alpha_2, ..., \alpha_t)$ یک α- کدواژه از H باشد که $\alpha_{i_0} = *$ است. اگر سطر i_0 ام از H، یعنی h_{i_0} را با سطر $a + h_{i_0}$ جایگزین کنیم آن‌گاه ماتریس H'، ماتریس مولد کد سیمپلکس S' بدست می آید. ماتریس H' از H با دنباله‌ای از تعویض ستون‌های متعلق به پشتیبان α- کدواژه a به‌دست خواهد آمد.

اثبات. این لم همان لم ۶.۲.۳ است با این تفاوت که در لم ۶.۲.۳، a یک α- کدواژه ابتدایی است ولی در این‌جا a بیش از یک ستاره دارد. پس از لم ۵.۲.۳ کمک گرفته آن را به صورت جمع چند α- کدواژه ابتدایی از سطح i_0 نوشته و لم ۶.۲.۳ را بکار می‌بریم. $\square$

تذکّر: اگر $a = s_H(*,1,*)$ یک α-کدواژه ابتدایی از H و از مرتبه i باشد h'_i سطر i ام ماتریس H' باشد، آن‌گاه:

$$h'_i = \begin{cases} a + h_i & i = i_0 \\ h_i & ow \end{cases} \qquad (۲.۳)$$

نتیجه ۸.۲.۳. [۲] فرض کنیدH ماتریس مولد یک کد سیمپلکس S به طول $n = 2^t - 1$ و بعد t باشد و برای $i = 1, ..., t$، h_i سطر i ام ماتریس H را نمایش می‌دهد. اگر برای یک مقدار

$i = ۱, ۲, ..., t$ کدواژه‌های $s_H(\alpha_{i_\nu ۱}, ..., \alpha_{i_\nu t})$، $\alpha-$ کدواژه‌های H باشند، به‌طوری‌که $\alpha_{i_\nu i} = *$ برای $\nu = ۱, ..., r$ آن‌گاه:

$$(\{h_۱, ..., h_t\} \setminus \{h_i\}) \cup \left\{ h_i + \sum_{\nu=۱}^{r} s_H(\alpha_{i_\nu ۱}, ..., \alpha_{i_\nu t}) \right\} \qquad (۳.۳)$$

یک مجموعه از بردارهای پایه برای یک کد سیمپلکس به طول n خواهد بود.

اثبات. با توجه به لم ۵.۲.۳، هر کدواژه $a = s_H(\alpha_۱, ..., \alpha_t)$ را می توان به‌صورت مجموع $\alpha-$ کدواژه‌ی ابتدایی از رتبه‌ی i نوشت که پشتیبان دو به دو مجزا دارند. حال با توجه به لم ۷.۲.۳ اگر $a = s_H(\alpha_۱, ..., \alpha_t)$ یک $\alpha-$ کدواژه از H با $\alpha_i = *$ باشد وسطر i ام از H یعنی h_i را با $a + h_i$ جایگزین کنیم آن‌گاه ماتریس H' مولد کد سیمپلکس S' به‌دست خواهد آمد.
پس عبارت $a + h_i = \sum_{\nu=۱}^{r} s_H(\alpha_{i_\nu ۱}, ..., \alpha_{i_\nu t}) + h_i$ مطابق لم بالا معادل سطر i ام $a + H$ یا همان سطر i ام H' خواهد بود و عبارت $\{h_۱, ..., h_t\} \setminus \{h_i\}$ سطرهای مشترک بین H و H' را نمایش می‌دهد، هم‌چنین عبارت ۳.۳ نمایشی از ماتریس H' است که در لم ۷.۲.۳ به آن اشاره شده است. بنابراین H' ماتریس مولد کد سیمپلکس S' به طول n خواهد بود. □

اگر مثال (۱) را در نظر بگیریم و $a = s_H(*, ۱, *)$، $\alpha-$ کدواژه‌ای برای ماتریس H باشد، آن‌گاه $\alpha-$ کدواژه‌ی $s_H(*, ۱, *)$ متناظر با کدواژه‌ی $(۰, ۱, ۱, ۰, ۰, ۱, ۱)$ است و مطابق لم ۷.۲.۳ اگر آن را با سطرهای اول و سوم ماتریس H جمع کنیم آن‌گاه داریم:

$$a + h_۱ = (۰, ۱, ۱, ۱, ۱, ۰, ۰) \text{ و } a + h_۳ = (۱, ۱, ۰, ۰, ۱, ۱, ۰)$$

و عبارت ۳.۳ به صورت:

$$(\{h_۱, h_۲, h_۳\} \setminus \{h_۱, h_۳\}) \cup \{h_۱ + a, h_۳ + a\} = \{h'_۱, h_۲, h'_۳\}$$

نوشته می‌شود. در نتیجه ماتریس زیر بدست می‌آید که ماتریس مولد کد سیمپلکس S' است:

$$H' = \begin{pmatrix} ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ \end{pmatrix}.$$

همان‌طور که گفته شد فضای دوگان $F^{\perp}$ از یک زیر فضای F از $\mathbb{Z}_2^n$ به‌صورت زیر تعریف می‌شود:

$$F^{\perp} = \{x \in \mathbb{Z}_2^n | f.x = f_1x_1 + f_2x_2 + ... + f_nx_n = 0(mod2), \forall f \in F\}.$$

یک α– زیر فضای G از $\mathbb{Z}_2^n$، زیرفضایی از $\mathbb{Z}_2^n$ است، به‌قسمی که $G^{\perp}$ توسط α– کدواژه‌های کد سیمپلکس S با ماتریس مولد ثابت H تولید شود.

با توجه به تعریف، هر کد همینگ یک α– زیر فضا از $\mathbb{Z}_2^n$ است زیرا همان‌طور که می‌دانیم کد سیمپلکس دوگان کد همینگ دودویی است و H ماتریس مولد S و ماتریس کنترل توازن کد همینگ است و سطرهای H که α– کدواژه برای H هم هستند، S یا دوگان همینگ را تولید می‌کنند.

مثال. (۲) فرض کنید H همان ماتریس مثال ۱ و G ماتریس زیر باشد:

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

فضای پوچ ماتریس G را که با $N(G)$ نمایش میدهیم مجموعه همه‌ی ماتریس‌های ستونی X است به طوری‌که: $G.X = 0$. برای بدست آوردن X داریم:

$$G. \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = 0 \Longrightarrow \left\{ \begin{array}{c} x_4 + x_5 + x_6 + x_7 = 0 \\ x_2 + x_3 + x_6 + x_7 = 0 \\ x_1 + x_3 + x_5 + x_7 = 0 \\ x_5 + x_7 = 0 \Rightarrow x_5 = x_7 \\ x_2 + x_3 = 0 \Rightarrow x_2 = x_3 \end{array} \right\}$$

اکنون چهار حالت زیر را در نظر می گیریم.

$$1) \begin{cases} x_5 = x_7 = 0 \\ x_2 = x_3 = 0 \end{cases} \Rightarrow X = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$۲)\begin{cases} x_۵ = x_۷ = ۱ \\ x_۲ = x_۳ = ۱ \end{cases} \Rightarrow X = \begin{bmatrix} ۱ \\ ۱ \\ ۱ \\ ۱ \\ ۱ \\ ۱ \\ ۱ \end{bmatrix}$$

$$۳)\begin{cases} x_۵ = x_۷ = ۰ \\ x_۲ = x_۳ = ۱ \end{cases} \Rightarrow X = \begin{bmatrix} ۱ \\ ۱ \\ ۱ \\ ۰ \\ ۰ \\ ۰ \\ ۰ \end{bmatrix}$$

$$۴)\begin{cases} x_۵ = x_۷ = ۱ \\ x_۲ = x_۳ = ۰ \end{cases} \Rightarrow X = \begin{bmatrix} ۰ \\ ۰ \\ ۰ \\ ۱ \\ ۱ \\ ۱ \\ ۱ \end{bmatrix}$$

پس داریم:

$$N(G) = \{(۰,۰,۰,۰,۰,۰,۰),(۱,۱,۱,۱,۱,۱,۱),(۰,۰,۰,۱,۱,۱,۱),(۱,۱,۱,۰,۰,۰,۰)\}$$

که $N(G)$ یک $\alpha-$ زیر فضای $\mathbb{Z}_۲^۷$ است، زیرا اولاً: $N(G)$ زیر فضایی از $\mathbb{Z}_۲^۷$ است (جمع هر دو عضو از $N(G)$ در $N(G)$ قرار دارد).

دوماً: $N(G)^{\perp}$ که همان فضای سطری G است توسط $\alpha-$ کدواژه های کد سیمپلکس S با ماتریس مولد H تعریف شده در مثال ۱ به‌وجود می‌آید و به‌ازای هر $\alpha-$ کدواژه‌ی S مانند a (از جمله سطرهای H) اگر $a.N(G) = ۰$ آن‌گاه $a \in N(G)^{\perp}$. ولی فضای $L = \{(۰,۰,۰,۰,۰,۰,۰),(۱,۱,۱,۰,۰,۰,۰)\}$ یک $\alpha-$ زیر فضا از $\mathbb{Z}_۲^۷$ نیست زیرا $(۱,۱,۰,۰,۰,۰,۰) \in L^{\perp}$ است اما توسط هیچ یک از $\alpha-$ کدواژه‌های S به وجود نمی‌آید. ♣

۱.۲.۳ ابردوگان کد کامل

فرض کنید C یک کد کامل به طول n شامل کدواژه‌ی $\bar{o}=(\circ,\circ,...,\circ)$ باشد و $V=\ker(C)^{\perp}$.
فرض کنید $p_\circ=\circ, p_1, p_2, ..., p_s$ نماینده‌های هم‌مجموعه‌های $\ker(C)$ در C باشند که:

$$C=\ker(C)\cup(p_1+\ker(C))\cup...\cup(p_s+\ker(C)) \qquad (۴.۳)$$

و $\frac{|C|}{|\ker(C)|}=s+1$. پس $s=2^{n-\log(n+1)-k}-1$ و هم‌چنین برای هر $i=\circ,...,s$ داریم $p_i\in C$.
حال فرض کنیم σ یک نگاشت خطی از $\ker(C)^{\perp}$ به $\mathbb{Z}_2^s$ باشد که:

$$\sigma(u)=(u.p_1,...,u.p_s), u\in\ker(C)^{\perp}$$

حال **ابردوگان** [۶] C^* از C را که زیر فضایی از $\mathbb{Z}_2^n\times\mathbb{Z}_2^s$ است به‌صورت زیر تعریف می‌کنیم:

$$C^*=\{(u|\sigma(u))|u\in V\}$$

فرض کنیم G ماتریسی باشد که سطرهای آن $g_1, g_2, ..., g_{n-k}$ بردارهای پایه برای فضای دوگان هسته‌ی C، یعنی V باشند.
حال ماتریس $(n-k)\times s$ ، $T=(t_{ij})$ را به‌صورت زیر تعریف می‌کنیم:

$$t_{ij}=g_ip_j; j=1,...,s; i=1,...,n-k$$

سطرهای ماتریس افزوده‌ی $(G|T)$ ابردوگان کد کامل C را تولید می‌کنند.
گاهی اوقات سطرهای این ماتریس افزوده را با $(g_i|t(g_i))$ یا $(g_i|t_i)$ برای $i=1,2,...,n-k$ نمایش می‌دهیم و ترکیب خطی سطرها را نیز به شکل زیر می‌نویسیم:

$$t(g_\lambda)=\lambda_1t_1+...+\lambda_{n-k}t_{n-k}$$

$$g_\lambda=\lambda_1g_1+...+\lambda_{n-k}g_{n-k}$$

[۶] Superdual

که $\lambda = (\lambda_1, ..., \lambda_{n-k})$.

در ادامه قضیه‌ی مهم ابردوگانی به بیان این مطلب می‌پردازد که ماتریس افزوده‌ی $(G|T)$ ابردوگان کد کامل بیان شده در معادله‌ی ۴.۳ را تولید می‌کند اگر و تنها اگر در چهار شرط که به شرط های ابردوگانی معروف هستند، صدق کند. برای اثبات این قضیه آشنایی با مفهوم ضرایب فوریه ضروری است.

ضرایب فوریه

برای هر زیر مجموعه از $\mathbb{Z}_2^n$ مانند C چند جمله‌ای $C(x_1, ..., x_n)$ به‌صورت زیر تعریف می‌شود:

$$C(x_1, ..., x_n) = \sum_{(c_1,...,c_n)\in C} x_1^{c_1}...x_n^{c_n}$$

و مجموعه‌ای از چندجملهایها را به‌صورت زیر تعریف می‌کنیم:

$$y_u(x_1, ..., x_n) = \frac{1}{2^n}\prod_{i=1}^n (1 + x_i)^{1-u_i}(1 - x_i)^{u_i} \text{ ؛ } u = (u_1, ..., u_n) \in \mathbb{Z}_2^n$$

هر چندجملهای $C(x_1, ..., x_n)$ یک بسط منحصر بفرد به شکل زیر دارد:

$$C(x_1, ..., x_n) = \sum_{u\in\mathbb{Z}_2^n} A_u y_u(x_1, ..., x_n) \tag{۵.۳}$$

که عناصر A_u برای $u \in \mathbb{Z}_2^n$ اعداد حقیقی هستند.

مشاهده می‌شود که:

$$y_u(x_1, ..., x_n)y_s(x_1, ..., x_n) = \begin{cases} y_u(x_1, ..., x_n) & u = s \\ 0 & ow \end{cases} \tag{۶.۳}$$

ضرایب A_u که $u \in \mathbb{Z}_2^n$ است را در معادله‌ی ۵.۳ **ضرایب فوریه** [۷] مجموعه ی C نامیم.

فرض کنید $S_1(0)$ نمایش مجموعه‌ی کدواژه‌ها با وزن حداکثر ۱ باشد زیرمجموعه‌ی C از $\mathbb{Z}_2^n$ که کدی ۱− تصحیح کننده خطاست یک کد کامل به طول n نامیده می‌شود، اگر وتنها اگر:

[۷] Fourier coefficients

$$C + S_1(0) = \mathbb{Z}_2^n$$

یا به طور معادل:

$$C(x_1, ..., x_n)S_1(0)(x_1, ..., x_n) = 2^n y_0(x_1, ..., x_n) = \prod_{i=1}^{n}(1 + x_i)$$

تقریبا تمام ضرایب فوریه A_u از $S_1(0)$ غیر صفر هستند به استثناء A_u ها به‌قسمی که: $w(u) = \frac{n+1}{2}$.

اکنون از معادله ی ۶.۳ قضیه زیر به‌دست می‌آید.

قضیه ۹.۲.۳. [۳] یک زیر مجموعه از $\mathbb{Z}_2^n$ مانند C به‌طول $2^{n-\log(n+1)}$ یک کد کامل ۱− تصحیح کننده‌ی خطا ست اگر و تنها اگر ضرایب فوریه A_u $(u \in \mathbb{Z}_2^n \setminus \{0\})$ از C برای u هایی که $w(u) \neq \frac{n+1}{2}$ است، معادل صفر باشد.

اکنون نشان می‌دهیم چطور ضرایب فوریه هر کد C با استفاده از مجموعه‌ی نماینده هممجموعههای $\ker(C)$ بدست می آید.

اگر C کد تعریف شده در معادله‌ی ۴.۳ باشد. با داشتن ضرب نقطه‌ای و برای هر $u \in \mathbb{Z}_2^n$ داریم:

$$A_u = |\{p \in C | p.u = 0\}| - |\{p \in C | p.u = 1\}| \tag{۷.۳}$$

و برای تمام $u \in \mathbb{Z}_2^n$ که $A_u \neq 0$ داریم:

$$p \in \ker(C) \Longleftrightarrow p.u = 0 \tag{۸.۳}$$

بنابراین:

$$\ker(C) = (span\{u \in \mathbb{Z}_2^n | A_u \neq 0\})^{\perp} \tag{۹.۳}$$

$$\ker(C)^{\perp} = span\{u \in \mathbb{Z}_2^n | A_u \neq 0\} \tag{۱۰.۳}$$

از معادله‌ی۸.۳ بدست می‌آوریم که اگر برای تعدادی بردار $u \in \mathbb{Z}_2^n$ داشته باشیم $A_u \neq 0$ آن گاه برای هر $p \in p_i + ker(C)$ داریم $p.u = p_i.u$.

حال اگر $u \notin \ker(C)^{\perp}$ آن‌گاه ضرایب فوریه A_u معادل صفر است.

و اگر $u \in \ker(C)^{\perp}$ آن‌گاه ضرایب فوریه A_u به نماینده‌ی هم‌مجموعه $\ker(C)$ در C وابسته است یعنی:

$$u \in \ker(C)^{\perp} \Longrightarrow A_u = |\ker(C)| \left(s + 1 - 2\sum_{i=1}^{s} p_i.u \right) \tag{11.3}$$

که در آن s در معادله ی ۴.۳ بدست می‌آید.

لم ۱۰.۲.۳. [۳] برای هر کد C فضای دوگان $\langle C \rangle$ برابر است با هسته‌ی σ:

$$\langle C \rangle^{\perp} = \{u \in \ker(C)^{\perp} | \sigma(u) = 0\}$$

اثبات. کدواژه‌ی u در $\langle C \rangle^{\perp}$ است اگر وتنها اگر برای هر $p \in C$ داشته باشیم $u.p = 0$ یا به‌طور معادل اگر وتنها اگر:

$$u.p_i = 0 \text{ ،} i = 1, 2, ..., s$$

□

$Im(\sigma)$، یعنی دامنه ی نگاشت σ به صورت زیر تعریف می شود:

$$Im(\sigma) = \{(t_1, ..., t_s) \in \mathbb{Z}_2^s | (t_1, ..., t_s) = \sigma(u), u \in ker(C)^{\perp}\}$$

با مشاهدات ابتدایی جبر خطی و از لم بالا نتیجه می‌گیریم که:

نتیجه ۱۱.۲.۳. [۳] فرض کنید C کدی کامل به طول n باشد و σ به‌صورت بالا تعریف شود. بعد دامنه‌ی σ به‌صورت زیر به‌دست می‌آید:

$$dim(Im(\sigma)) = n - dim(ker(C)) - dim(\langle C \rangle^{\perp})$$

و لم زیر نتیجه‌ی مستقیم معادله‌ی ۱۱.۳ است.

لم ۱۲.۲.۳. [۳] برای $u \in \mathbb{Z}_2^n$ ضرایب فوریه‌ی A_u از کد کامل C برابر است با:

$$A_u = |\ker(C)|\,(s + 1 - 2w(\sigma(u)))$$

پس برای $u \in ker(C)^{\perp}$ ، $A_u = 0$ اگر وتنها اگر $w(\sigma(u)) = \frac{s+1}{2}$.

قضیه ۱۳.۲.۳. [۳](ابردوگانِی) ماتریس افزوده $(G|T)$ از دو ماتریس G و T ابردوگان یک کد کامل به طول n و هسته‌ای با بعد k را تولید می کند اگر و فقط اگر در چهار شرط زیر صدق کند:

(۱) G یک ماتریس $(n-k) \times n$ و T یک ماتریس $(n-k) \times s$ باشد که $s = 2^{n-\log(n+1)-k} - 1$ است.

(۲) اگر $wt(g_\lambda) \neq \frac{n+1}{2}$ آن‌گاه $wt(t(g_\lambda)) = \frac{s+1}{2}$.

(۳) یک مجموعه از $n-k$ ترکیب خطی از سطرهای $f_1, ..., f_{n-k}$ در فضای سطری G وجود دارد، به‌طوری که برای $i = 1, ...n-k$ داشته باشیم:

$$wt(\sigma(f_i)) \neq \frac{s+1}{2}$$

(۴) مجموعه‌ٔستون‌های ماتریس T ⃞ همراه ستون صفر تناوب غیر صفر ندارد.

این چهار شرط به **شرط های ابردوگانی** [۸] معروف هستند.

اثبات. "$\Rightarrow$": برای هر ماتریس افزوده‌ی $(G|T)$ با سطر های $(g_i|t_i)$ شرط های ۳ و ۴ معادلند. حال فرض کنیم دو ماتریس G و T داریم که در چهار شرط بالا صدق کنند. کد C را به‌صورت زیر تعریف می‌کنیم:

$$C = \{\overline{c} \in \mathbb{Z}_2^n | G\overline{c}^T \in col(T) \bigcup \{\overline{0}^T\}\} \tag{۱۲.۳}$$

[۸] Superdual conditions

رتبه‌ی ماتریس G برابر $n-k$ و تمام s ستون T متفاوت هستند، بنا به شرط ۱ و با محاسبات جبر خطی تعداد کدواژه‌های C برابر است با:

$$|C| = 2^{n-(n-k)}.(s+1) \Longrightarrow |C| = 2^{n-\log(n+1)} \qquad (۱۳.۳)$$

اکنون ضرایب فوریه $A_u = A_u(C)$، $u \in \mathbb{Z}_2^n$ از مجموعه‌ی C را در نظر می‌گیریم و ثابت می‌کنیم:

$$A_u(C) \neq 0 \Longrightarrow w(u) \in \{0, \frac{n+1}{2}\}$$

از قضیه ۹.۲.۳ در مبحث ضرایب فوریه و معادله ۱۳.۳ نتیجه می‌شود که C کدی کامل است.
ابتدا خاطر نشان می‌کنیم که با توجه به معادله ؟؟(۱۱□□ هر عضو هسته C در فضای دوگان فضای سطری ماتریس G واقع است و با توجه به شرط ۴ ستونهای ماتریس T همراه ستون صفر تناوب غیر صفر ندارد لذا فضای سطری G دقیقاً فضای دوگان هسته C است و از معادله‌ی ۸.۳ نتیجه می‌شود که برای هر ضریب فوریه غیر صفر $A_u(C)$ از C ، u به فضای دوگان هسته C متعلق است. پس نتیجه می‌گیریم که u یک ترکیب خطی از سطرهای ماتریس G است و پس داریم:

$$A_u(C) \neq 0 \Longrightarrow u = \sum_{i=1}^{n-k} \lambda_i g_i \qquad (۱۴.۳)$$

که $g_1, ..., g_{n-k}$ سطرهای ماتریس G هستند.
با توجه به این که $s = 2^{n-k-\log(n+1)} - 1$ است، $s+1$ هم‌مجموعه مجزا از $\ker(C)$ در C داریم.
اگر $p_0, p_1, ..., p_s$ نماینده هم‌مجموعه‌های هسته C در C باشند که $p_0 = \bar{0}$ آن گاه Gp_i برابر یکی از ستون‌های T است و برای سطر i ام از T یعنی t_i داریم:

$$t_i = (g_i.p_1, ..., g_i.p_s); i = 1, ..., n-k \qquad (۱۵.۳)$$

با توجه به این حقیقت و آنچه در بالا مشاهده میشود نتیجه میگیریم که $(G|T)$ ابردوگان کد کامل C که در معادله ی ۱۲.۳ تعریف شد را تولید می‌کند.
از معادلهی ۱۵.۳ به دست می‌آوریم:

$\sum_{i=1}^{n-k} \lambda_i t_i = \left(\left(\sum_{i=1}^{n-k} \lambda_i g_i \right) .p_1, \ldots, \left(\sum_{i=1}^{n-k} \lambda_i g_i \right) .p_s \right)$

$\Longrightarrow u = \sum_{i=1}^{n-k} \lambda_i g_i \Longrightarrow \sigma(u) = \sum_{i=1}^{n-k} \lambda_i t_i$

با توجه به آن‌چه در معادله‌ی ۱۱.۳ مبحث ضرایب فوریه به آن اشاره شد، اگر $u \in ker(C)^\perp$ آن‌گاه داریم:

$$A_u = |ker(C)|(s + 1 - 2 \sum_{i=1}^{s} p_i.u) \qquad (۱۶.۳)$$

با توجه به لم ۱۲.۲.۳ نتیجه می‌شود که:

$$A_u(C) = |ker(C)|(s + 1 - 2w(\sigma(u)) \qquad (۱۷.۳)$$

با در نظر گرفتن معادلات ۱۴.۳ و ۱۷.۳ و شرط (۲) بدست می‌آوریم:

$$A_u(C) \neq 0 \Longrightarrow w(\sigma(u)) \neq \frac{s+1}{2}; u = \sum_{i=1}^{n-k} \lambda_i g_i \Longrightarrow w(u) \in \{0, \frac{n+1}{2}\}$$

از قضیه‌ی ۹.۲.۳ در ضرایت فوریه نتیجه می‌شود که C کد کامل ۱− تصحیح کننده‌ی خطاست.

" $\Leftarrow$ " اکنون نشان می‌دهیم اگر C کد کامل دودویی ۱− تصحیح کننده‌ی خطا باشد آن‌گاه ماتریس توازن $(G|T)$ مربوط به کد C در شرایط قضیه صدق می‌کند.

با در نظر گرفتن مسائل مربوط به بعد زیر فضاهای فضاهای برداری شرط ۱ برقرار است.

اگر شرط ۴ نادرست باشد هسته‌ی C دقیقاً فضای دوگان فضای سطری ماتریس G را شامل نمی‌شود.

پس شرط ۴ باید درست باشد و در نتیجه شرط ۳ نیز باید درست باشد. با توجه به لم ۱۲.۲.۳ و معادله‌ی ۱۰.۳ شرط (۳) درست است چون G ماتریسی با فضای سطری برابر فضای دوگان هسته‌ی C است.

اثبات درستی شرط ۲: اگر u متعلق به فضای سطری G باشد، از تعریف ماتریس G می‌دانیم که $u \in ker(C)^\perp$. ممکن است از معادله‌ی ۱۱.۳ برای محاسبه‌ی ضرایب فوریه $A_u(C)$ از C استفاده

کنیم، در این صورت به‌دست می‌آوریم: اگر $w(\sigma(u)) \neq \frac{s+1}{2}$ آن‌گاه $A_u(C) \neq 0$.
از قضیه‌ی ۹.۲.۳ در ضرایب فوریه نتیجه می‌شود که $w(u) = \frac{n+1}{2}$. بنابراین شرط ۲ نیز درست است. $\square$

کد C که توسط ماتریس افزوده $(G|T)$ ایجاد می‌شود، اجتماع هم‌مجموعه‌های فضای پوچ ماتریس G یعنی D خواهد بود.

$$C = D\bigcup(p_1+D)\bigcup(p_2+D)\bigcup\dots\bigcup(p_s+D) \tag{۱۸.۳}$$

که $D = \{c \in \mathbb{Z}_2^n|; G.c = 0\}$ و با توجه به تعریف ماتریس T، Gp_i^T برای $i = 1,\dots,s$ ، i امین ستون ماتریس T است.
با توجه به اینکه سطرهای G پایه‌ای برای $\ker(C)^\perp$ هستند پس با توجه به تعریف فضای پوچی، فضای پوچی G یعنی D با $\ker(C)$ برابر است.
اکنون مفهوم ابردوگانی با یک مثال توضیح داده می‌شود.

مثال . (۳) ماتریس افزوده $(G|T)$ را به صورت زیر در نظر می گیریم:

$$(G|T) = \left(\begin{array}{ccccccccccccccc|ccc}
0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0\\
0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&1&0&0\\
1&1&0&0&1&0&1&0&1&0&1&1&1&0&1&0&1&0\\
1&0&1&1&0&0&1&1&0&0&1&0&1&0&1&0&0&1
\end{array}\right)$$

در این مورد $n = 15$ ، $k = 9$ و $s = 3$ است. فرض کنید $g_1, g_2, \dots, g_6$ سطرهای G باشند.
G یک ماتریس $(n-k)\times n$ یعنی 6×15 و H یک ماتریس $(n-k)\times s$ یعنی 6×3 است و داریم:

$$s = 2^{n-\log(n+1)-k} - 1 = 2^{15-\log 16-9} - 1 = 3$$

پس شرط (۱) برقرار است.

واضح است که ستون‌های ماتریس T به همراه ستون صفر دارای تناوب غیر صفر نیستند.

یعنی اگر k_1 ، k_2 و k_3 ستون‌های ماتریس T باشند عنصری غیر صفر مانند p در $\mathbb{Z}_2^t$ یافت نمی‌شود که برای هر k_i که $i = 1, 2, 3$ است داشته باشیم: $p + k_i = k_j$. پس شرط (۴) نیز برقرار است.
با انجام محاسبات ساده می‌توان دید شرط (۳) نیز برقرار است.
اما برای بررسی شرط (۲) خاطر نشان می‌کنیم که چهار سطر g_1, g_2, g_3 و g_i برای $i = 4, 5, 6$ مولدی برای یک کد سیمپلکس است و هم‌چنین سطرهای g_1, g_2, g_3 و $g_4 + g_5 + g_6$ نیز مولد یک کد سیمپلکس هستند و چون هر کدواژه غیر صفر در کد سیمپلکس به‌طول n دارای وزن $\frac{n+1}{2}$ است لذا هر ترکیب خطی از این سطرها درنظر بگیریم دارای وزن است.
بنابر آن‌چه گفتیم باید کدواژهای p_1, p_2, p_3 از $\mathbb{Z}_2^n$ وجود داشته باشند به‌طوری که:

$$Gp_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, Gp_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, Gp_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

حال فرض کنید D فضای پوچی ماتریس G باشد. مجموعه:

$$C = D \bigcup (p_1 + D) \bigcup (p_2 + D) \bigcup (p_3 + D)$$

یک کد کامل خواهد بود و ماتریس افزوده‌ی $(G|T)$ ابردوگان کد کامل C را تولید خواهد کرد.
♣

گزاره ۱۴.۲.۳. [۲] رتبه کد کامل C مربوط به یک ابردوگان $(G|T)$ برابر است با :

$$n - rank(G) + rank(T).$$

اثبات. فرض کنیم که C همان کد تعریف شده در معادله ۱۸.۳ باشد و k_i ستون i اُم T را نمایش دهد. فرض کنیم رتبه T معادل t و مجموعه ستون‌های $k_{i_1}, \ldots, k_{i_t}$ از T یک پایه برای فضای ستونی T تشکیل دهند. چون G دارای رتبه ماکزیمال است پس کدواژه‌های $p_{i_1}, \ldots, p_{i_t}$ وجود دارد که $Gp_{i_v}^T = k_{i_v}$ برای $v = 1, 2, \ldots, t$. اگر $q_1, \ldots, q_k$ که $k = n - rank(G)$، مجموعه بردارهای

پایه برای فضای پوچ D از ماتریس G را نمایش دهد آن‌گاه $p_{i_1},\dots,p_{i_t}$ و $q_1,\dots,q_k$ که $i=1,\dots,s$ مستقل خطی هستند.

فرض کنید $k_i=\sum_{v=1}^{t}\lambda_v k_{i_v}$ ، پس داریم:

$$G(p_i-\sum_{v=1}^{t}\lambda_v p_{i_v})^T=Gp_i^T-\sum_{v=1}^{t}\lambda_v Gp_{i_v}^T=k_i-\sum_{v=1}^{t}\lambda_v k_{i_v}=0$$

نتیجه می‌شود که هر ترکیب خطی از $p_1,\dots,p_s$ با کلمات D را می‌توان به‌صورت ترکیب خطی از یک کلمه در فضای پوچی G که D است و یک ترکیب خطی از کلمات $p_{i_1},\dots,p_{i_t}$ نوشت.

و چون $\langle C\rangle$ شامل چنان ترکیبات خطی است پس حکم نتیجه می‌شود و داریم:

$$dim(\langle C\rangle)=k+t=n-rank(G)+rank(T)$$

□

۳.۳ α- کدهای نرمال

فرض کنید H_1 و H_2 ماتریس‌های مولد کدهای سیمپلکس S_1 و S_2 به طول‌های $n=2^t-1$ و $s=2^r-1$ و بعدهای به ترتیب t و r باشند .فرض کنید G_1 و G_2 دو ماتریس باشند به‌قسمی که سطرهای این ماتریسها α- کدواژههای به ترتیب H_1 و H_2 باشند که G_1 یک ماتریس از مرتبهی $r\times n$ و G_2 یک ماتریس از مرتبهی $t\times s$ است.

حال G و T را بهصورت زیر درنظر میگیریم:

$$G=\begin{pmatrix}H_1\\G_1\end{pmatrix},T=\begin{pmatrix}G_2\\H_2\end{pmatrix}\qquad(۱۹.۳)$$

پس G از مرتبه $(t+r)\times n$ و T ماتریسی از مرتبه $(t+r)\times s$ است.

دو ماتریس G و T به صورت بالا داده شده‌اند. یک **α-کد**[۹] C مجموعه ای از کدواژه های c به طول n است به قسمی که Gc^T یا برابر ستون صفر باشد یا به مجموعه ستون‌های ماتریس T

[۹] α–code

متعلق است.

دو ماتریس G_1 و G_2 به‌صورت زیر مفروض هستند:

$$G_1 = \begin{pmatrix} s_{H_1}(\alpha_{11}, \dots, \alpha_{1t}) \\ \vdots \\ s_{H_1}(\alpha_{r1}, \dots, \alpha_{rt}) \end{pmatrix}$$

$$G_2 = \begin{pmatrix} s_{H_1}(\alpha_{11}, \dots, \alpha_{1r}) \\ \vdots \\ s_{H_1}(\alpha_{t1}, \dots, \alpha_{tr}) \end{pmatrix}$$

می‌گوییم ماتریس‌های:

$$\tilde{G_1} = \begin{pmatrix} \alpha_{11}, \dots, \alpha_{1t} \\ \vdots \\ \alpha_{r1}, \dots, \alpha_{rt} \end{pmatrix}^T$$

$$\tilde{G_2} = \begin{pmatrix} \alpha_{11}, \dots, \alpha_{1r} \\ \vdots \\ \alpha_{t1}, \dots, \alpha_{tr} \end{pmatrix}$$

ماتریس‌های تعریف شده برای $\alpha-$ کد هستند. خاطر نشان می‌کنیم که هر-دو ماتریس $t \times r$ هستند.

قضیه ۳.۳.۱. [۲] یک $\alpha-$ کد با ماتریس های تعریف شده $\tilde{G_1}$ و $\tilde{G_2}$، کد کامل با رتبه تام است اگر در چهار شرط زیر صدق کند.

(a)سطر های G مستقل خطی باشند.

(b) اگر در یک موقعیت (i,j) از ماتریس تعریف شده $\tilde{G_2}$، ستاره وجود نداشته باشد آنگاه در موقعیت (i,j) ماتریس تعریف شده $\tilde{G_1}$ ستاره داشته باشیم.

(c) پشتیبان سطر های ماتریس G_2 دو به‌دومجزا هستند.

(d) هر ستون $\tilde{G}_2$ حداقل یک درایه غیر ستاره دارد.

بنابراین اگر این چهار شرط صادق باشد هسته C، فضای دوگان فضای سطری ماتریس G یا فضای پوچی ماتریس G خواهد بود و دارای بعد $n-(r+t)$ است:

$$dim(ker(C)) = n-(r+t)$$

یک α- کد که در چهار شرط بالا صدق کند یک **α-کد نرمال** [۱۰] نامیده می‌شود.

مثال . (۴) ماتریس‌های زیر مفروض هستند:

$$\tilde{G}_1 = \begin{pmatrix} 0 & * & * & 1 & * & 1 \\ 1 & 0 & * & * & 0 & * \\ * & 1 & 0 & * & * & 0 \\ * & * & 1 & 0 & 1 & * \end{pmatrix}$$

$$\tilde{G}_2 = \begin{pmatrix} * & 0 & 1 & * & 1 & * \\ * & * & 0 & 1 & * & 1 \\ 1 & * & * & 0 & 0 & * \\ 0 & 1 & * & * & * & 0 \end{pmatrix}$$

با بررسی مختصر مشاهده می‌شود شرط های b و d برقرار هستند زیرا هر مولفه‌ی غیر ستاره در $\tilde{G}_2$ با یک مولفه ستاره در $\tilde{G}_1$ متناظر است و هر ستون از $\tilde{G}_2$ شامل حداقل یک درایه غیر ستاره است. شرط c هم برقرار است چون بنا به لم ۱.۲.۳ دو سطر دلخواه j و k پشتیبان دو به دو مجزا دارند اگر و تنها اگر:

$$\exists i; \alpha_{ji} \neq *, \alpha_{ki} \neq * \Longrightarrow \alpha_{ji} \neq \alpha_{ki}$$

که α_{ji} مولفه i ام سطر j ام و α_{ki} مولفه iام سطر k ام است.

با مقایسه هر دو سطر دلخواه حداقل در یک مولفه هر دو سطر غیر ستاره هستند و با هم برابر نیستند. پس هر دو سطر دارای پشتیبان دو به دو مجزا هستند.

اگر H_1 را ماتریس مولد یک کد سیمپلکس از مرتبه 15×4 درنظر بگیریم که ستونهای آن تمام بردارهای غیرصفر F_2^4 هستند و α-کدواژههای این ماتریس را با توجه به ستونهای ماتریس $\tilde{G}_1$

---

[۱۰] Normal α-code

زیر آن بنویسیم آنگاه با محاسبات ساده مشخص می‌شود که سطرهای G مستقل خطی هستند.
پس شرط a نیز برقرار است.
پس α– کد C یک α– کد نرمال به طول $n = ۱۵$ خواهد بود بنابراین C یک کد کامل با رتبه تام است.
ماتریس $G_۱$ دارای شش سطر است و بعد هسته C برابر ۵ خواهد بود.
زیرا:

$$n-(r+t) = ۱۵-(۶+۴) = ۵$$

♣

در حقیقت این‌که هر α– کد، ممکن است α– کد نرمال نباشد، واضح است ولی از قضیه بالا نتیجه می‌شود که هر α– کد نرمال یک کد کامل خواهد بود.
اکنون اثبات قضیه ۱.۳.۳ را ارائه خواهیم کرد که شامل دو گام اصلی است.
گام اول بررسی این حقیقت است که ماتریس افزوده $(G|T)$ در شرایط ابردوگانی صدق می‌کند. در نتیجه C یک کد کامل است. در گام دوم اثبات می‌کنیم که این کد کامل دارای رتبه تام است.

اثبات. اثبات این قضیّه در گام‌های زیادی ارائه می گردد.
گام ۱: اثبات می‌کنیم که شرط b و c شرط پنجمی را نیز نتیجه می‌دهد:
e) در هر سطر از $G_۲$ حداقل دو درایه غیر ستاره وجود دارد.
برای اثبات این حقیقت خاطرنشان می کنیم که تمام سطرهای $G_۲$، α– کدواژه هستند پس هر سطر $G_۲$ حداقل ۱ درایه غیر ستاره دارد.
برهان خلف: فرض می‌کنیم یک سطر در $G_۲$ وجود دارد که دقیقاً یک درایه غیر ستاره دارد که در ستون i ام ظاهر شده است چون تمام کدواژه‌های $G_۲$ پشتیبان دو به دو مجزا دارند، طبق لم ۱.۲.۳، با در نظر گرفتن هر دو سطر باید یک موقعیت موجود باشد که در آن هر دو سطر غیر

ستاره و با هم متفاوت باشند.

چون تمام مولفه‌های سطر مذکور جز ستون i ام آن ستاره هستند پس باید مولفه‌های ستون i ام بقیه‌ی سطرها غیر ستاره و با ستون i ام این سطر متفاوت باشند دراین‌صورت طبق شرط (b) باید تمام درایه‌های ستون i ام در $\tilde{G_2}$ ستاره باشد که چون سطرهای G_1، α- کدواژه هستند پس تمام ستون‌های $\tilde{G_2}$ از جمله ستون i ام نیز α- کدواژه است پس نمی‌تواند تمام مولفه‌هایش ستاره باشد.

پس فرض خلف باطل می‌شود و در هر سطر از $\tilde{G_2}$ حداقل دو درایه غیر ستاره وجود دارد.

اکنون شرایط ابردوگانی را بررسی می‌کنیم.

گام ۲، بررسی شرط (ii) ابردوگانی: اگر $w(g_\lambda) \neq \frac{n+1}{2}$ آن‌گاه $w(t(g_\lambda)) = \frac{s+1}{2}$.

یعنی برای هر ترکیب خطی $(g|t)$ از سطرهای $(G|T)$ اگر وزن g برابر $\frac{n+1}{2}$ نباشد آن‌گاه وزن t باید برابر $\frac{s+1}{2}$ شود.

فرض می‌کنیم $(g_i|t_i)$ برای $i = 1, \ldots, t+r$ ، سطر i ام از $(G|T)$ را نمایش دهد.

اگر $(g|t)$ ترکیب خطی از t سطر اول $(G|T)$ باشد باتوجه به تعریف G، ترکیب خطی t سطر اول G که با g نمایش داده می‌شود، ترکیب خطی از سطرهای H_1 است و چون H_1 مولد کد سیمپلکس S_1 است پس g یک کدواژه در S_1 خواهد بود.

زیرا:

$$G = \begin{pmatrix} H_1 \\ G_1 \end{pmatrix}_{(t+r)\times n}.$$

و با توجه به آن چه در تعریف کد سیمپلکس گفته شد، g دارای وزن $\frac{n+1}{2}$ است.

بطور مشابه اگر $(g|t)$ ترکیب خطی باشد که هیچ یک از t سطر اول در آن نباشد t کدواژه‌ای در کد سیمپلکس S_2 است (با توجه به اینکه $T = \begin{pmatrix} G_2 \\ H_2 \end{pmatrix}_{(t+r)\times s}$) که طول هر کدواژه در آن s است پس وزن t برابر $\frac{s+1}{2}$ خواهد بود.

فقط مورد زیر باقی می‌ماند:

$$(g|t) = \sum_{v=1}^{b}(g_{i_v}|t_{i_v}) + \sum_{v=1}^{a}(g_{t+j_v}|t_{t+j_v}) \qquad (۲۰.۳)$$

که $i_1, i_2, ..., i_b \in \{1, 2, ..., t\}$ و $j_1, j_2, ..., j_a \in \{1, 2, ..., r\}$.

یعنی $(g|t)$ ترکیب خطی از چند سطر از سطرهای $1, 2, ..., t$ و چند سطر از سطرهای $t+1, ..., t+r$ باشد، که دو احتمال وجود خواهد داشت. در اولی معلوم می‌شود که وزن t برابر $\frac{s+1}{2}$ است و در مورد دوم وزن g برابر $\frac{n+1}{2}$ خواهد شد.

مورد اول: برای هر $i \in \{i_1, i_2, ..., i_b\}$ در ماتریس $G\tilde{_2}$ یک ستاره در تقاطع سطر i ام و ستون j ام حداقل برای یک $j(i) \in \{j_1, ..., j_a\}$ وجود دارد.

در این مورد برای هر $i \in \{i_1, i_2, ..., i_b\}$ ابتدا کدواژه t_i را با کدواژه $t_{t+j(i)}$ جمع می‌کنیم.

یعنی اگر در سطر i ام $G\tilde{_2}$ در ستون j ام ستاره وجود دارد سطر $j(i)$ ام از H_2 را با سطر i ام G_2 که α - کدواژه H_2 است جمع می کنیم که در این صورت با توجه به لم ۷.۲.۳ و اینکه t_i ها که سطرهای G_2 هستند، طبق شرط (c) پشتیبان دوبدو مجزا دارند، ماتریس H_2 با H'_2 جایگزین می شود که H'_2 از H_2 با دنباله‌ای از جایگشت ستون‌ها بدست می‌آید که H'_2 مولد یک کد سیمپلکس به‌طول s است و با توجه به معادله‌ی ۲۰.۳ و سطر j ام از H'_2 که $j \notin \{j(i_v)|v = 1, ..., b\}$ معادل سطر j ام H_2 است.

با توجه به آن‌چه در تعریف کد سیمپلکس گفته شد تمام کدواژه‌ها در این کد سیمپلکس وزنی معادل $\frac{s+1}{2}$ خواهند داشت.

مورد دوم: یک $i = i_x$ در مجموعه $i_1, ..., i_b$ وجود دارد به‌قسمی که در ماتریس $G\tilde{_2}$ در تقاطع ستون j ام و سطر i_x به ازای هر $j \in \{j_1, ..., j_a\}$ یک غیر ستاره وجود دارد.

در این مورد با توجه به شرط (b) قضیه در ماتریس $G\tilde{_2}$ در تقاطع سطر i_x ام و ستون‌های $j_1, ..., j_a$ ستاره وجود خواهد داشت.

حال اگر سطر g_{i_x} از H_1 را با سطر $g_{i_x} + \sum_{\mu=1}^{a} g_{t+j_\mu}$ جایگزین کنیم مثل این است که سطر g_{i_x}

را با تمام α - کد واژه‌های ابتدایی از درجه i_x جمع کرده ایم که طبق نتیجه‌ی ۸.۲.۳ با این جایگزینی یک ماتریس مولد برای کد سیمپلکس S' به طول n به وجود می‌آید.
پس g در معادله‌ی ۲۰.۳ به‌صورت زیر خواهد بود:

$$\sum_{j_\mu \in \{i_1,...,i_b\} \setminus \{i_x\}} g_{i_\mu} + \left(g_{i_x} + \sum_{\mu=1}^{a} g_{t+j_\mu}\right)$$

بنابراین g به کد سیمپلکس S' تعلق دارد. در نتیجه وزن آن معادل $\frac{n+1}{2}$ خواهد بود.
تا اینجا شرط (ii) از شرایط ابردوگانی ثابت شد.
گام ۳، بررسی شرط (iv) ابردوگانی: ثابت می‌کنیم که مجموعه ستون‌های ماتریس $T_{(r+t)\times s}$ همراه ستون صفر تناوب غیر صفر مانند p ندارند:

$$p = (p_1, ..., p_t, p_{t+1}, ..., p_{t+r})^T \neq (0, ..., 0)^T$$

واضح است که اگر بردار $(1, ..., 1)$ را به یک بردار دو دویی به‌طول s و وزن w اضافه کنیم و به پیمانه دو حساب کنیم برداری با وزن $s - w$ خواهیم داشت.
اکنون از این حقیقت استفاده می‌کنیم که: هر سطر ماتریس G_2^* با توجه به شرط (e) حداقل دو درایه غیر ستاره دارد، با استفاده از لم ۴.۲.۳ (وزن هر α- کدواژه برابر 2^p است که p تعداد ستاره‌هاست)، با وجود دو درایه‌ی غیر ستاره در هر سطر G_2^* وزن هر سطر G_2 به $\frac{w}{4}$ کاهش می‌یابد و از آن‌جا که حداکثر وزن هر سطر در G_2، برابر s است، پس داریم:

$$w < \frac{s}{4} \leq \frac{s+1}{4} \Longrightarrow w \leq \frac{s+1}{4}$$

در کدواژه‌ی p که در بالا داده شده فرض می‌کنیم برای یک $i = 1, ..., t$، $p_i = 1$.
تعداد ستون‌های با درایه ۱ در سطر شماره i از ماتریس G_2 کمتر از نصف تعداد ستون هاست چون وزن هر سطر حداکثر $\frac{s+1}{4}$ است. اگر کدواژه p را به همه ستون‌ها اضافه کنیم چون $p_i = 1$ است مثل این‌است که سطر i ام G_2 را با کدواژه ی $(1, ..., 1)$ جمع کرده‌ایم پس تعداد ستون‌های با درایه یک در کدواژه‌ی حاصل بیشتر از نصف تعدا ستون‌هاست. پس این کدواژه نمی تواند

سطری از $G_{۲}$ باشد.

لذا اگر $p_i = ۱$ آن‌گاه p نمی‌تواند تناوب باشد.

تنها احتمالی که برای تناوب p باقی می‌ماند این‌است که $p_i = ۰$ برای تمام $i = ۱, ..., t$.

اکنون دوباره t سطر اول ماتریس T را در نظر می‌گیریم. می‌دانیم t_i ها $\alpha-$ کدواژه‌های $H_{۲}$ هستند $t_i = s_H(\alpha_{۱}, ..., \alpha_r)$.

فرض کنید که $\alpha_{i_\mu} \neq *$ برای $\mu = ۱, ..., a$ و $\alpha_{i_\mu} = *$ برای $\mu = a + ۱, ..., t$.

مجموعه‌ی M_i از ستون‌های $b = (\beta_{۱}, ..., \beta_r)^T$ از ماتریس $H_{۲}$ را در نظر بگیرید به‌قسمی که ستون زیر، ستونی از ماتریس T باشد:

$$(۰...۰۱۰...۰|\beta_{۱}...\beta_r)^T$$

که مولفه‌ی یک در سطر i ام است.

ستون b از ماتریس $H_{۲}$ در M_i است اگر و فقط اگر $\beta_j = \alpha_j$ برای j هایی که $\alpha_j \neq *$. چون $p_i = ۰$، $i = ۱, ..., t$، پس هر تناوب p از مجموعه ستون‌های T وقتی به ستون‌های T اضافه می شود، مجموعه ستون‌های M_i را به داخل خودش می‌نگارد. نتیجه می‌گیریم که اگر $\alpha_j \neq *$ آن‌گاه $p_j = ۰$.

با استفاده از شرط (d) در قضیه؛ که در هر ستون حداقل یک درایه غیر ستاره دارد نتیجه می‌گیریم که $p_j = ۰$ برای هر $j = t + ۱, ..., t + r$. بنابراین هیچ تناوب غیرصفری برای ستون‌های ماتریس T وجود ندارد و شرط (iv) ابردوگانی ثابت شد.

با استفاده از یک مثال می‌توان قسمت دوم این اثبات را بهتر توضیح داد.

در مثال (۱) اگر H را $H_{۲}$ فرض کنیم و $G_{۲}^{\sim}$ را به‌صورت زیر فرض کنیم:

$$G_{۲}^{\sim} = \begin{pmatrix} ۱ & * & ۰ \\ * & ۰ & ۱ \\ ۰ & ۱ & * \end{pmatrix}$$

در این صورت تمام شرایط قضیه برقرار است و ماتریس T به صورت زیر خواهد بود:

$$T = \begin{pmatrix} * & * & ۰ & ۱ & ۰ & ۱ & ۰ \\ ۱ & * & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۰ & * & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{pmatrix}$$

که $\alpha_{۳\mu} \neq *$ ، $\mu = ۱,۲$ و $\alpha_{۳۳} = *$.

حال مجموعه $M_۳$ شامل ستون های $\begin{pmatrix} ۰ \\ ۱ \\ ۱ \end{pmatrix}$ و $\begin{pmatrix} ۰ \\ ۱ \\ ۰ \end{pmatrix}$ است که ستون‌های $\begin{pmatrix} ۰ \\ ۰ \\ ۱ \\ ۰ \\ ۱ \\ ۱ \end{pmatrix}$ و $\begin{pmatrix} ۰ \\ ۰ \\ ۱ \\ ۰ \\ ۱ \\ ۰ \end{pmatrix}$ ستون‌های T هستند.

ستون b در $M_۳$ قرار دارد اگر و فقط اگر $\alpha_۱ = \beta_۱$ و $\alpha_۲ = \beta_۲$ که $\alpha_۱ = ۰$ و $\alpha_۲ = ۱$ و هر دو غیر ستاره هستند.

همان‌طور که توضیح داده شد با جمع هر تناوب از ستون‌های T با هر ستون از T، ستون‌های $M_۳$ به داخل خودش نگاشته می‌شود. پس چون $\alpha_۱$ و $\alpha_۲$ مولفه‌های غیر ستاره هستند، $p_۴$ و $p_۵$ باید صفر باشند.

با درنظر گرفتن $M_۲$ و پیش گرفتن روند بالا بدست می‌آید $p_۵ = ۰$ و $p_۶ = ۰$. در نتیجه $p_۴$ و $p_۵$ و $p_۶$ باید صفر باشند.

گام ۴ ، بررسی شرط (iii) ابردوگانی: $t + r$ سطر مستقل خطی $f_۱, ..., f_{t+r}$ از فضای سطری G وجود دارد که:

$$w(t(f_i)) \neq \frac{s + ۱}{۲}; i = ۱, ..., t + r.$$

فرض می‌کنیم که $(g_i|t_i)$ ، $i = ۱, ..., t + r$ ، سطر i ام از ماتریس افزوده $(G|T)$ را نمایش دهد. و هر سطر از ماتریس $H_۲$ را به شکل t_{t+j} ، $j = ۱, ..., r$، در نظر می‌گیریم.

طبق شرط (d) قضیه هر ستون از $G_۲^*$ حداقل یک درایه غیر ستاره دارد پس حداقل یک سطر $f(j)$ از ماتریس $G_۲^*$ وجود دارد که در ستون j شامل یک عنصر غیر ستاره $\alpha_{f(j)j}$ است. اگر

$\alpha_{f(j)j} = ۱$ آنگاه سطر $f(j)$ ام از $G_۲$ در مکان‌هایی یک است سطر j ام از $H_۲$ یک باشد وچون بنا به شرط (e) در سطر $f(j)$ ام از $\tilde{G_۲}$ حداقل دو درایه غیر ستاره داریم، بنا به لم ۲.۲.۳ پشتیبان سطر j ام از ماتریس $H_۲$ پشتیبان سطر $f(j)$ ام ازماتریس $G_۲$ را شامل می‌شود.
حال در این مورد اگر $\alpha_{f(j)j} = ۰$ آن‌گاه سطر $f(j)$ ام از $G_۲$ در مکان هایی یک است که سطر j ام از $H_۲$ صفر باشد.

پس پشتیبان سطر $f(j)$ ام ماتریس $G_۲$ از پشتیبان سطر j ام ماتریس $H_۲$ مجزا است.
در هر دو مورد داریم:

$$w(t_{f(j)} + t_{t+j}) \neq \frac{s+۱}{۲}$$

چون سطر t_{t+j} سطری از ماتریس $H_۲$ است پس کدواژه‌ای در کد سیمپلکس $s_۲$ است. پس وزن آن برابر $\frac{s+۱}{۲}$ است و سطر $t_{f(j)}$ سطری از ماتریس $G_۲$ است و بنابه آن‌چه در گام ۳ گفته شد هر سطر $G_۲$ وزنی کمتر مساوی $\frac{s+۱}{۴}$ دارد.
در نتیجه با جمع دو سطر $t_{f(j)}$ و t_{t+j} وزن $t_{f(j)} + t_{t+j}$ در حالت اول که پشتیبان سطر j ام از ماتریس $H_۲$ شامل پشتیبان سطر $f(j)$ ام ماتریس $G_۲$ است، کمتر از $\frac{s+۱}{۲}$ است.
در حالت دوم که پشتیبان این دو سطر مجزا است بیشتر از $\frac{s+۱}{۲}$ است.
پس در هر دو حالت داریم:

$$w(t_{f(j)} + t_{t+j}) \neq \frac{s+۱}{۲} \tag{۲۱.۳}$$

سطرهای زیر که در فضای سطری ماتریس G هستند مستقل خطی اند:

$$g_۱, g_۲, ..., g_t, g_{f(۱)} + g_{t+۱}, g_{f(۲)} + g_{t+۲}, ..., g_{f(r)} + g_{t+r} \tag{۲۲.۳}$$

چون بنا به شرط (a) سطرهای G مستقل خطی هستند درنتیجه جمع سطرهای مستقل خطی باز هم مستقل خطی خواهند بود.
تمام کدواژه‌های $t_۱, ..., t_t$ بنا به آن‌چه در گام سوم گفته شد وزنی کمتر مساوی $\frac{s+۱}{۴}$ و لذا کمتر

از $\frac{s+1}{2}$ دارد.

و از آن‌جا که $t(g_1) = t_1$ و $t(g_2) = t_2$ و ... و $t(g_t) = t_t$ و $t(g_{f(1)} + g_{t+1}) = t_{f(1)} + t_{t+1}$ و ... و $t(g_{f(r)} + g_{t+r}) = t_{f(r)} + t_{t+r}$ و وزن همه‌ی آن‌ها مخالف $\frac{s+1}{2}$ است.

در نتیجه مجموعه کدواژه‌های معادله ی ۲۲.۳ در شرط (iii) ابردوگانی صدق می‌کنند.

گام ۵: اثبات می‌کنیم C کدی کامل است.

درستی شرط (i) ابردوگانی واضح است پس درستی تمام شرایط ابردوگانی ثابت شد بنابراین C یک کد کامل با ابردوگان $(G|T)$ است.

میدانیم هسته C فضای پوچ ماتریس G است. با استفاده از فرع یا گزاره‌ی ۱۴.۲.۳ بدست می آوریم که اگر ماتریس T رتبه تام داشته باشد آن‌گاه C کد کامل با رتبه تام است.

گام ۶: اثبات می‌کنیم T دارای رتبه تام است.

بنا به شرط (c) پشتیبان سطرهای ماتریس G_2 دو بدو مجزا هستند بنا براین این t سطر مستقل خطی هستند .

r سطر ماتریس H_2 نیز مستقل خطی هستند چون H_2 ماتریس مولد کد سیمپلکس S_2 است.

برای نشان دادن اینکه سطرهای ماتریس T مستقل خطی اند کافی است که نشان دهیم که هیچ ترکیب خطی از سطرهای G_2 با هیچ ترکیب خطی سطرهای H_2 برابر نیست.

برهان خلف: فرض می‌کنیم ترکیب خطی ناصفری از سطرهای G_2 با ترکیب خطی از سطر های H_2 برابر است.

بدون کاستن از کلیت مسئله و برای ساده سازی مفهوم فرض می‌کنیم که جمع v سطر اول H_2 با جمع سطرهای R زیرمجموعه‌ی سطرهای ماتریس G_2 برابر است.

$$\sum_{t\in R} t = \sum_{i=1}^{v} t_{t+i} \qquad (۲۳.۳)$$

فرض می‌کنیم A مجموعه‌ی α- کدواژه های $s_H(\alpha_1, ..., \alpha_r)$ را نمایش می‌دهد به‌قسمی که:

$$\alpha_i = \begin{cases} 0 \; or \; 1 & i = 1, ..., v \\ * & i = v+1, ..., r \end{cases}$$

و وزن کدواژه‌های دودویی $(\alpha_1,...,\alpha_v)$ یک عدد صحیح فرد است. چون تمام α– کدواژه‌های A از مکان v به بعد ستاره هستند و برای اینکه یکی نباشند و باید حداقل در یکی از موقعیت‌های غیر ستاره با هم تفاوت داشته باشند که در این صورت بنا به لم ۱.۲.۳، α– کدواژه‌های A پشتیبان دوبه‌دو مجزا دارند.

چون محاسبات به پیمانه دو انجام می‌گیرد، سمت راست معادله‌ی ۲۳.۳ را برابر مجموع α–کدواژه‌های A به‌دست می‌آوریم:

$$\sum_{i=1}^{v} t_{t+i} = \sum_{a\in A} a$$

برای نوشتن کدواژه‌ی معادل α– کد واژه های a متعلق به A که تا مکان v ام صفر و یک و از مکان v ام به بعد ستاره است و تعداد یک‌ها فرد است، مکان‌هایی یک است که در مشخصات a تا مکان v ام صدق کند.

اگر α– کدواژه‌ی $a = s_H(0,1,*)$، از ماتریس H، که در مثال ۱ ارائه شده است را در نظر بگیریم برای نوشتن کدواژه‌ی معادل آن ستون‌هایی در آن یک است که سطر اول صفر و سطر دوم یک باشد که با درنظر گرفتن H، (۰۱۱۰۰۰۰) کدواژه‌ی معادل آن است و برای نوشتن کدواژه‌ی معادل $a' = s_H(1,0,*)$ ستون‌هایی را یک قرار می‌دهیم که سطر اول آن یک و سطردوم آن صفر باشد. با توجه به H ، (۰۰۰۱۱۰۰) کد واژه‌ی معادل آن است با جمع این دو کدواژه، کدواژه (۰۱۱۱۱۰۰) حاصل می‌شود.

با توجه به این‌که a و a' هر دو در شرایط مجموعه A صدق می‌کنند و مکان اول و دوم آن غیر ستاره است پس سطر اول و دوم ماتریس H را با هم جمع می‌کنیم کدواژه‌ی حاصل باید در موقعیت‌هایی یک باشد که تعداد یک‌ها در ستون‌های مربوط فرد باشد. که این معادل جمع تمام کدواژه‌های معادل α– کدواژه‌های است که تا مکان دوم آن صفر و یک باشد و تعداد یک‌ها فرد باشد. پس جمع v سطر اول ماتریس H_2 معادل این است که تمام α– کدواژهایی را که تا مکان v ام صفر و یک هستند و تعداد یک ها فرد است، با هم جمع کنیم. چون فرض شده که

تمام سطرهای ماتریس $G_۲$ پشتیبان دو به دو مجزا دارند، پس هر مکان i حداکثر در یکی از پشتیبان‌های کدواژه‌های R ظاهر می‌شود.

بنابراین جمع کدواژه‌های مجموعه‌ی R با جمع کدواژه‌های مجموعه A برابر است، لذا برای هر $t \in R$ داریم:

$$supp(t) \subseteq \bigcup_{a\in A} supp(a); \forall t \in R \qquad (۲۴.۳)$$

اکنون نشان می‌دهیم که برای هر $t \in R$ یک $a \in A$ به‌طور منحصر به‌فرد وجود دارد به‌طوری‌که:

$$supp(t) \subseteq supp(a) \qquad (۲۵.۳)$$

برهان خلف: فرض کنید $j, j' \in supp(t)$ وجود دارد به‌قسمی که $j \in supp(a)$ و $j' \in supp(a')$ که $a = s_{H_۲}(\alpha_۱, ..., \alpha_r)$ و $a' = s_{H_۲}(\alpha'_۱, ..., \alpha'_r)$ دو α − کدواژه متفاوت در مجموعه A هستند. اگر t، α−کدواژه‌ی $t = s_H(\beta_۱, ..., \beta_r)$ باشد آن‌گاه برای این‌که
$supp(t) \subseteq supp(a) \bigcup supp(a')$ باشد t باید در مکان‌هایی که a و a' متفاوتند ستاره باشد. یعنی اگر $\alpha_i \neq \alpha'_i$ برای $i = ۱, ..., v$ آن‌گاه $\beta_i = *$ درغیراینصورت اگر دراین مکان ها
$\beta_i = ۱$ یا $\beta_i = ۰$ باشد آن‌گاه طبق لم ۱.۲.۳ پشتیبان t از پشتیبان a یا پشتیبان a' مجزا است.
لذا t در مکانهایی که a و a' متفاوت هستند ستاره و در مکان‌هایی که $\alpha_i = \alpha'_i$ است $\beta_i = \alpha_i = \alpha'_i$ برای $i = ۱, ..., v$.

چون وزن هر دو کدواژه دودویی $(\alpha_۱, ..., \alpha_v)$ و $(\alpha'_۱, ..., \alpha'_v)$ فرد است، بدترین حالت این است که هر دو دارای وزن یک باشند. که در این صورت برای اینکه دو کدواژه یکسان نباشند این یک ها در دو مکان مختلف قرار می‌گیرند پس اختلاف در دو مؤلفه است یا اینکه یکی سه مولفه‌ی یک و یکی از آن‌ها یک مولفه‌ی یک داشته باشد. که باز هم در بدترین حالت که دو مولفه یک در یک ستون زیر هم باشند این دو کدواژه دو اختلاف خواهند داشت پس حداقل دو تا از β_i برای $i = ۱, ..., v$ باید ستاره باشد. به‌طور کلی با بررسی تمام حالات a و a' به طوری که از مکان

۱ تا v صفر و یک باشد و تعداد یک ها در این مکان ها فرد باشد، متوجه می شویم که اختلاف a و a' همیشه عددی زوج است پس تعداد ستاره‌های t از موقعیت‌های ۱ تا v تعدادی زوج است. از این مطلب نتیجه می‌گیریم که یک $(\alpha_1, ..., \alpha_r)$ در پشتیبان t وجود دارد که وزن $(\alpha_1, ..., \alpha_v)$ عددی زوج است پس $(\alpha_1, ..., \alpha_r)$ به اجتماع پشتیبان‌های کدواژه‌های A متعلق نیست که این با معادله ۲۴.۳ در تناقض است بنابراین برای هر $t \in R$ یک $a \in A$ منحصر به‌فرد وجود دارد به‌طوری که معادله ۲۵.۳ درست باشد.

اگر R_a، برای $a = s_H(\alpha_1, ..., \alpha_t) \in A$، مجموعه کدواژه‌های $t \in R$ را که در معادله ۲۵.۳ صدق می‌کند نمایش دهد آن‌گاه با توجه به لم ۲.۲.۳ برای این‌که پشتیبان t در پشتیبان a قرار بگیرد باید مکان‌هایی که a غیر ستاره است، a و t یکسان باشند و این یعنی برای $i = 1, ..., v$ داریم:

$$t = s_H(\beta_1, ..., \beta_t) \in R_a \Longrightarrow \beta_i = \alpha_i \qquad (۲۶.۳)$$

با توجه به این حقیقت که کدواژه‌های ماتریس G_2 پشتیبان دو به دو مجزا دارند پس t اعضای R_a نیز پشتیبان مجزا دارند. که با توجه به معادله ۲۵.۳ داریم:

$$\forall t \in R_a; supp(t) \subseteq supp(a)$$

پس پشتیبان اعضای R_a ، پشتیبان a را افراز می‌کنند یعنی

$$\bigcup_{t \in R_a} supp(t) = supp(a)$$

و چون همان‌طور که گفته شد t ها پشتیبان دوبه‌دو مجزا دارند داریم:

$$a = \sum_{t \in R_a} t$$

که برای هر $a \in A$ داریم:

$$R_a = \{t \in R | supp(t) \subseteq supp(a)\}.$$

خاطر نشان می کنیم که اگر $a = s_{H_۲}(\alpha_۱, ..., \alpha_t) \in R_a$ و $t = s_{H_۲}(\alpha'_۱, ..., \alpha'_t) \in A$ آن‌گاه برای $i = ۱, ..., v$ هر داریم:

$$\alpha_i = \alpha'_i.$$

با توجه به لم ۳.۲.۳ هر α- کدواژه را می‌توان به‌صورت مجموع تمام کدواژه‌هایی نوشت که در مکان‌هایی که α- کدواژه غیر ستاره است با آن برابر باشد. و در مکان‌های ستاره یا صفر باشند یا یک. پس $a \in A$ را می‌توان به‌صورت زیر نوشت:

$$a = s_{H_۲}(\alpha_۱, ..., \alpha_t) = \sum s_{H_۲}(\alpha'_۱, ..., \alpha'_t)$$

که این جمع روی مجموعه s_a است که مجموعه تمام کدواژه‌های $(\alpha'_۱, ..., \alpha'_t)$ است که:

$$\alpha'_i = \begin{cases} \alpha_i & i = ۱, ..., v \\ ۰ or ۱ & i = v + ۱, ..., t \end{cases} \tag{۲۷.۳}$$

حال اگر $t \notin R$، $t = s_{H_۲}(\beta_۱, ..., \beta_t)$ $\alpha-$ کدواژه‌ای در مجموعه سطرهای ماتریس $G_۲$ باشد و اگر $t_a = s_{H_۲}(\alpha'_۱, ..., \alpha'_t)$ کدواژه‌ای در s_a مربوط به کدواژه a باشد، هر $a \in A$ را می‌توان به‌صورت مجموع چند کدواژه در R نوشت که R نیز زیر مجموعه‌ی سطرهای ماتریس $G_۲$ است.
پس هر $a \in A$ را می‌توان به صورت مجموع چند کدواژه در $G_۲$ نوشت و از آن‌جا که پشتیبان سطرهای $G_۲$ دو به دو مجزا هستند و t نیز سطری در $G_۲$ است، پس پشتیبان $t \notin R$ و $a \in A$ مجزا هستند و با توجه به این‌که a را می‌توان به‌صورت مجموع تمام $t_a \in s_a$ نوشت پس باید پشتیبان t_a ها و t مجزا باشند. در نتیجه طبق لم ۱.۲.۳ داریم:

$$\beta_i \neq *; \alpha'_i \neq * \text{ و } \beta_i \neq \alpha'_i$$

برای حداقل یک $i \in \{۱, ۲, ..., t\}$. چون این عبارت باید برای تمام $t_a \in s_a$ درست باشد و با توجه به این‌که a و t طبق لم ۱.۲.۳، حداقل باید در یکی از موقعیت‌های $i = ۱, ..., v$ که a غیر ستاره است با t تفاوت داشته باشد و از آن‌جا که در معادله ۲۷.۳ داریم: $\alpha'_i = \alpha_i; i = ۱, ..., v$ به‌دست

می‌آوریم لذا برای حداقل یک $i \in \{۱, ..., v\}$ داشته باشیم:

$$i \in \{۱, ..., v\}; \beta_i \neq \alpha_i' \beta_i \neq *; \alpha_i' \neq * \tag{۲۸.۳}$$

اکنون اثبات می‌کنیم که از این حقیقت نتیجه می‌شود:

$$\forall i = ۱, ..., v; \beta_i \neq *.$$

ابتدا موردی را در نظر می‌گیریم که $\beta_i = ۱$ برای تعدادی فرد i در مجموعه $\{۱, ۲, ..., v\}$. دراین‌صورت دقیقاً یک α-کدواژه $a = s_{H_۲}\{\alpha_۱, ..., \alpha_t\} \in A$ وجود دارد به‌قسمی که برای $i = ۱, ..., v$:

$$\alpha_i = \begin{cases} ۱ & \beta_i = ۱ \\ ۰ & els \end{cases}$$

اگر برای $i = ۱, ..., v$، $\beta_i \neq ۱$ آن‌گاه β_i باید صفر یا ستاره باشد دراین‌صورت در مکان‌هایی که t و a غیر ستاره هستند با هم برابرند لذا طبق لم ۱.۲.۳ پشتیبان t و a دارای اشتراک بوده و مجزا نیستند و چون هر a را می توان به‌صورت جمع کدواژه‌های $t' \in R_a$ نوشت پس نتیجه می‌گیریم که حداقل یک کدواژه $t' \in R_a$ وجود دارد به‌قسمی که پشتیبان t و t' دارای اشتراک ناتهی هستند.

از آن‌جا که t و t' هر دو کدواژه‌هایی در $\tilde{G_۲}$ هستند و این اشتراک بین پشتیبان t و t' با شرط (c) در تناقض است چون طبق شرط (c) ، t و t' باید دارای پشتیبان‌های مجزا باشند.

بنابراین اگر $t \notin R$ آن‌گاه β_i باید برای تعداد زوج $i \in \{۱, ۲, ..., v\}$ معادل یک باشد.

حال فرض می‌کنیم کدواژه $t = s_{H_۲}\{\beta_۱, ..., \beta_t\}$ عضوی از R باشد به‌طوری که برای تعداد زوج $i = ۱, ..., v$، $\beta_i = ۱$ باشد و برای حداقل یک درایه $\beta_{i_۰}$ برای $i_۰ = ۱, ..., v$ ستاره باشد. سپس برای هر نقطه $(\alpha_۱, ..., \alpha_r)$ داریم:

$$\alpha_i = \begin{cases} ۱ & \beta_i = ۱ \\ ۱ & i = i_۰ \\ ۰ & els \end{cases}$$

که $i = ۱, ..., v$ است. اگر $\beta_i \neq *$ باشد، آن‌گاه $\alpha_i = \beta_i$ برای $i = v+۱, ..., r$، است دراین‌صورت $(\alpha_۱, ..., \alpha_r)$ به پشتیبان t متعلق است زیرا طبق لم ۲.۲.۳ درتمام موقعیت‌هایی که t غیر ستاره است داریم:

$$\alpha_i = \beta_i; i = ۱, ..., v$$

پس $(\alpha_۱, ..., \alpha_r)$ به پشتیبان t تعلق دارد و چون برای $i = ۱, ..., v$ ، $\alpha_i \neq *$ و:

$$\alpha_i = \begin{cases} ۱ & \beta_i = ۱ \\ ۱ & i = i_\circ \\ \circ & els \end{cases}$$

یعنی به تعداد فردی یک برای مؤلفه های $۱, ..., v$ وجود دارد پس $a' = s_{H_۲}(\alpha'_۱, ..., \alpha'_t) \in A$ وجود دارد که:

$$\alpha'_i = \begin{cases} \alpha_i & i = ۱, ..., v \\ * & i = v+۱, ..., r \end{cases}$$

در نتیجه $(\alpha_۱, ..., \alpha_r)$ به پشتیبان تعدادی $t' \in R_a$ تعلق دارد.

پس نقطه $(\alpha_۱, ..., \alpha_r)$ به پشتیبان t و تعدادی $t' \in R_a$ تعلق دارد که با شرط (c) در تناقض است چون همان‌طور که گفته شد t و t' سطرهایی از $G_۲$ هستند و طبق شرط (c) سطرهای $G_۲$ دارای پشتیبان مجزا هستند. پس برای $i_\circ = ۱, ..., v$ ، $\beta_{i_\circ} = *$ وجود ندارد.

بنابراین ثابت کرده‌ایم که اگر ترکیب خطی از سطرهای ماتریس $G_۲$ وجود داشته باشد که با جمع v سطر اول ماتریس $H_۲$ برابر باشد آن‌گاه برای هر $\alpha-$ کدواژه $t = s_{H_۲}(\alpha_۱, ..., \alpha_t)$ در مجموعه سطرهای ماتریس $G_۲$ داریم:

$$\alpha_i \neq *; \forall i = ۱, ..., v \qquad (۲۹.۳)$$

که این یعنی در تمام سطرهای $G_۲^\sim$ درایه v ستون اول مخالف ستاره هستند پس طبق شرط (b) نتیجه می‌شود، v ستون اول تمام سطرهای ماتریس $G_۲^\sim$ ستاره است. که دراین‌صورت چون ستون‌های $G_۲^\sim$ سطرهای $G_۱$ هستند پس تمام درایه‌های v سطر اول $G_۱$ ستاره هستند پس v

سطر اول $G_{۱}$، α- کدواژه نیستند که این متناقض با فرض مسأله است که گفته شد سطرهای $G_{۱}$، α- کدواژه‌های ماتریس مولد کد سیمپلکس $S_{۱}$ است. نتیجه می‌گیریم که هیچ ترکیب خطی از سطرهای $G_{۲}$ با هیچ ترکیب خطی از سطرهای ماتریس $H_{۲}$ برابر نیست. بنابراین ماتریس T دارای رتبه کامل است و این گام از اثبات به پایان می رسد.

گام آخر از اثبات قضیه:

در گام پنجم اثبات شد که C یک کد کامل است. با توجه به شرط (a) سطرهای ماتریس G مستقل خطی‌اند پس ماتریس G دارای رتبه کامل است. بنابراین با استفاده از گزاره ۱۴.۲.۳ در گام ششم به‌دست آوردیم که C یک کد کامل با رتبه تام است. حال اثبات قضیه کامل شد. □

باید خاطرنشان کنیم که در خیلی از موارد خاص اثبات مستقیم این حقیقت که یک α- کد نرمال دارای رتبه تام است، آسان است. برای مثال اگر تمام α- کدواژه‌های ماتریس $G_{۲}$ دارای وزن کم باشند به‌طوری‌که جمع این کدواژه‌ها وزنی کمتر از $\frac{s+۱}{۲}$ داشته باشند یا هر سطر ماتریس $G_{۲}^{\sim}$ حداقل دارای دو درایه یک باشد.

توجه کنید که باید بین مفاهیم α-کدهای کامل با رتبه تام و α- کدهای نرمال تمایز قائل شویم. α-کدهای نرمال، کدهای کاملی با رتبه تام هستند ولی ممکن است کدی کامل با رتبه تام یافت شود که α-کد نرمال نباشد.

۴.۳ مثال‌ها

ابتدا می‌خواهیم نشان دهیم که دو ماتریس زیر از مرتبه $t \times t$ برای $t \geq ۵$ در شرایط قضیه‌ی قبل صدق می‌کنند و ماتریس‌های تعریف شده یک α- کد هستند:

$$G_{۱}^{\sim} = \begin{pmatrix} ۱ & * & * & \dots & * & ۰ \\ ۰ & ۱ & * & \dots & * & * \\ * & ۰ & ۱ & \dots & * & * \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ * & * & * & \dots & ۰ & ۱ \end{pmatrix}, G_{۲}^{\sim} = \begin{pmatrix} * & ۱ & ۱ & \dots & ۱ & ۰ & * \\ * & * & ۱ & \dots & ۱ & ۱ & ۰ \\ ۰ & * & * & \dots & ۱ & ۱ & ۱ \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ ۱ & ۱ & ۱ & \dots & ۰ & * & * \end{pmatrix} \qquad (۳۰.۳)$$

بنابراین این ماتریس‌ها می‌توانند برای ساختن کدهای کامل با رتبه تام به‌طول $n = ۲^t - ۱$ و با هسته‌ای از بعد $n - ۲t$ استفاده شوند. با مشاهده دو ماتریس می‌بینیم هر درایه غیر ستاره ماتریس $G_۳^\sim$ در موقعیت (i,j) با یک درایه ستاره در موقعیت (i,j) از ماتریس $G_۲^\sim$ متناظر است پس شرط (b) برقرار است و هم‌چنین هر ستون از $G_۳^\sim$ شامل حداقل یک درایه غیرستاره است پس شرط (d) نیز برقرار است.

با مقایسه هر دو سطر از ماتریس $G_۳^\sim$ می‌بینیم حداقل یک موقعیت وجود دارد که دو سطر ستاره نباشند و با هم متفاوت باشند یعنی یکی صفر و یکی یک باشد (با توجه به این‌که محاسبات به پیمانه‌ی ۲ انجام می‌شود) بنابراین شرایط لم ۱.۲.۳ برقرار است و هر دو سطر ماتریس $G_۲$ پشتیبان دوبه‌دو مجزا دارند، پس شرط (c) نیز برقرار است. اکنون ثابت می‌کنیم که شرط (a) نیز درست است.

فرض کنیم $h_۱, h_۲, ..., h_t$ و $r_۱, r_۲, ..., r_t$ به ترتیب سطرهای ماتریس $H_۱$ و $G_۱$ را نمایش دهند. معادله زیر را در نظر بگیرید:

$$\lambda_۱ h_۱ + \lambda_۲ h_۲ + ... + \lambda_t h_t + \mu_۱ r_۱ + \mu_۲ r_۲ + ... + \mu_t r_t = ۰ \qquad (۳۱.۳)$$

می‌بینیم که تمام ستون‌های ماتریس $G_۳^\sim$ یک درایه یک در سطر j ام و برای بعضی j ها، یک صفر در سطر $j + ۱$ ام دارند.

می‌دانیم ماتریس $H_۱$ ماتریس مولد کد سیمپلکس $S_۱$ است و هم‌چنین ماتریس کنترل توازن کد کامل همینگ است.

با توجه به تعریف کد همینگ دودویی، ستون‌های ماتریس کنترل توازن این کد همه‌ی بردارهای غیر صفر $F_۲^t$ هستند. بنابراین در ماتریس $H_۱$ که ماتریس کنترل توازن یک کد همینگ دودویی است برای هر $j = ۱, ..., t$، ستونی مثل i با وزن یک وجود دارد که درایه یک آن در سطر j ام قرار دارد. حال از ساختار ماتریس $G_۳^\sim$ و با توجه به این‌که سطر j ام ماتریس $G_۱$، α- کدواژهای از $H_۱$ است که متناظر با α-کدواژهی ستون j ام ماتریس $G_۳^\sim$ است، نتیجه می‌شود که تنها

سطر ماتریس G_1 که یک مولفه‌ی یک در ستون i ام دارد، سطر j ام است. بنابراین در معادله ۳۱.۳عبارت زیر باید درست باشد:

$$\lambda_j = 1 \Longleftrightarrow \mu_j = 1 \qquad (۳۲.۳)$$

حال فرض می‌کنیم:

$$\mu_i = \begin{cases} 1 & if i \in \{i_1, ..., i_q\} \\ 0 & else, \end{cases} \qquad (۳۳.۳)$$

که $i_1 > i_2 > ... > i_q$.

اکنون ستون j ام ماتریس H_1 را در نظر میگیریم که در سطرهای i برای $i_2 \leq i \leq i_1$، دارای یک است و مولفه سایر سطرها صفر است. چون سطرهای ماتریس G_1، $\alpha-$ کدواژه متناظر با مجموعه ستون‌های ماتریس G_2^γ هستند، در میبابیم که تنها سطر ماتریس G_1 در میان سطرهای r_{i_v} برای $v = 1, ..., q$، که دارای یک مولفه یک در ستون j ام است، سطر i_1 ام است زیرا وقتی فقط سطرهای iام برای $i_2 \leq i \leq i_1$، در ستون jام دارای مولفه یک باشد لذا سطر i_1ام دارای مولفه‌ی یک و سطر بعد مولفه صفر خواهد داشت و با توجه به ستون‌های ماتریس G_2^γ فقط ستون i_1ام دارای مولفه یک در سطر i_1 ام و مولفه ی صفر در سطر بعد است و چون سطرهای G_1، $\alpha-$ کدواژه‌های ماتریس G_2^γ هستند لذا تینها سطر در سطرهای G_1 که دارای مولفه یک در ستون j ام است سطر i_1 ام خواهد بود. حال اگر در سطر iام از ستون j ام دارای یک باشیم آن‌گاه ستونی با وزن یک وجود خواهد داشت که تنها مولفه یک آن در سطر i ام است. بنابراین با توجه به آن‌چه گفته شد نتیجه می‌گیریم در عبارت سمت چپ معادله ۳۱.۳ مولفه موقعیت j ام به شکل زیر خواهد بود:

$$\mu_{i_1} + \lambda_{i_1} + \lambda_{i_2} \equiv 1, (mod 2)$$

که با توجه به معادله ۳۲.۳ و ۳۳.۳، λ_z برای $i_2 < z < i_1$، برابر صفر است. هم‌چنین داریم: $\mu_{i_1} = \lambda_{i_1} = \lambda_{i_2} = 1$. در نتیجه مولفه j ام عبارت سمت چپ معادله ۳۱.۳ هرگز صفر نمی‌شود.

لذا سطرهای G مستقل خطی هستند و شرط (a) از قضیه ۱.۳.۳نیز برقرار است.
اگر در این مثال قرار دهیم $t = ۵$ آن‌گاه مثالی از یک کد کامل با رتبه‌ی تام به طول ۳۱ و هسته‌ای با بعد ۲۱ خواهیم داشت. در واقع ما در بالا گزاره زیر را اثبات کردیم.

گزاره ۱.۴.۳. [۲] α-کدهای بدست آمده از ماتریس‌ها تعریف شده‌ی معادله ۳۰.۳، کدهای کامل با رتبه تام به‌طول $n = ۲^t - ۱$ و هسته ای از بعد $n - ۲t$ برای $t = ۵, ۶, ۷, ...$ هستند.

برای $t = ۴$ ماتریس‌های معادله ۳۰.۳ در شرایط قضیه ۱.۳.۳ صدق نمی‌کنند. **وردی** [۱۱] و **استرگارد** [۱۲]ثابت کردند که کد کامل به‌طول ۱۵ و با هسته‌ای از بعد بزرگ‌تر یا مساوی ۶ وجود ندارد. با این وجود همان‌طور که قبلا توسط **مالیوجین** [۱۳] با محاسبات کامپیوتر به‌دست آمد که کدهای کامل به‌طول ۱۵ و با هسته‌ای از بعد ۵ وجود دارند. کد کامل ارائه شده در مثال ۴ نیز کد کامل با رتبه تام با همین پارامترها است.
قابل ذکر است که می‌توان با محاسبات ساده دستی مشاهده کرد که α- کدهای نرمال به‌طول ۱۵ و با هسته‌ای از بعد ۶ وجود ندارد. اثبات عدم وجود کدهای کامل با این پارامترها خیلی پیچیده است ولی می‌توانید در منبع [۷] به این اثبات مراجعه کنید.
خاطر نشان می‌کنیم که برای تمام α-کدهای نرمال به‌طول ۱۵ و با هسته‌ای از بعد ۵، ستاره‌های ماتریس‌های تعریف شده فقط باید در موقعیت‌های که در ماتریس‌های معادله‌ی ۳۰.۳ تعریف شده باشند.
مثال دیگر از کدهای کامل با رتبه‌ی تام با جابه‌جایی نقش G و T در ابردوگان ارائه می‌شود.
اگر ما هر α- کد نرمال مانند C را با ابردوگانی که در معادله ۱۹.۳ تعریف شده است در نظر بگیریم، دراین‌صورت ماتریس افزوده

$$(T|G) = \left(\begin{array}{c|c} H_۲ & G_۱ \\ G_۲ & H_۱ \end{array} \right) \qquad (۳۴.۳)$$

[۱۱] Vardy
[۱۲] Ostergard
[۱۳] Malyugin

نیز می‌تواند برای تعریف کد کامل با رتبه تام مانند C' استفاده شود. این کد شامل کدواژه‌هایی مانند c' است که Tc'^T مساوی ستون صفر یا مساوی یکی از ستون‌های ماتریس G است.
تعداد سطرهای ماتریس T به اندازه تعداد سطرهای ماتریس G و برابر $n-\dim(\ker(C))$ است.
زیرا هسته‌ی C همان فضای دوگان فضای سطری ماتریس G است. پس خواهیم داشت:

$$\dim(\ker(C)) = n - (rank(G)) = n - (r+t) \Longrightarrow r+t = n - \dim(\ker(C)) \qquad (۳۵.۳)$$

با توجه به تعریف دو ماتریس G و T، هر دو ماتریس دارای $r+t$ سطر هستند لذا می‌توانیم بگوییم هر دو دارای $n-\dim(\ker(C))$ سطر هستند. هم‌چنین تعداد ستون‌های ماتریس T برابر طول کد C' است با توجه به معادله ۳۵.۳ و این که $n = ۲^t - ۱$ در نتیجه $t = \log(n-۱)$ است، به صورت زیر محاسبه می‌شود.

$$n' = s = ۲^r - ۱ = ۲^{n-\dim(\ker(C))-t} - ۱ = ۲^{n-\dim(\ker(C))-\log(n-۱)} - ۱$$

این که سطرهای ماتریس T توسط فضای دوگان هسته C' تولید می شود، قطعی نیست چون مجموعه ستون‌های ماتریس G با ستون صفر ممکن است تناوب داشته باشد. اما در هر صورت داریم:

$$\dim(\ker(C')) \geq n' - rank(T) = n' - n + \dim(\ker(C))$$

در مورد کد ارائه شده در مثال ۴، با تغییر در نقش G و T کد کامل با رتبه تام C' را به‌طول $n' = ۶۳$ و با هسته‌ای از بعد حداکثر ۵۴ خواهیم داشت و ماتریس افزوده معادله ۳۴.۳ ابر دوگان کد C' را تولید می‌کند.

مراجع

[1] R. W. Hamming, (1950)," Error Detecting and Error Correcting Codes", **The Bell System Technical Journal**, 26:147–160.

[2] O. Heden, (2009), "Full rank perfect codes and $\alpha-$ kernels", **Discrete Math**, 309:2202–2216. 44, 45, 46, 47, 49, 50, 62, 64, 83

[3] O. Heden, (2008), "Perfect codes from the dual point of view I", **Discrete Math**, 308:6141–6156. 56, 57, 58

[4] O. Heden,(2010), "On kernel of perfect codes", **Discrete Math**, 310: 3052–3055.

[5] K. Hoffman and R. Kunze, (1971), "**Linear Algebra**", Prentice-Hall. 11, 12, 13

[6] S. Ling and C. P. Xing, (2004), "**Coding theory**", Cambridge University Press, New York. 9, 14, 15, 16, 17, 18, 19, 20, 21, 26, 27

[7] P. R. J. Ostergard and A. Vardy, (2004), "Resolving the existence of full-rank tilings of binary Hamming space", **SIAM Journal on Discrete Methodes**, 18: 382–387.

[8] G. Sanders, (2004), "Perfect Codes", **Journal of Combinatorial Theory**, Series B: 1–8. 31, 35

[9] C. E. Shannon, (1948), "A mathematical theory of communication", **Bell System Technical**, 27: 379–423, 623–656.

[10] F. L. Solov'eva, (2004), "**On perfect codes and related topics** " , Com^{2}Mac Lecture Note, , Korea. 25, 29, 31, 32

[11] M. Villanueva i Gay, (2001), "On rank and kernel of perfect codes", PhD thesis, University of UAB.

واژه‌نامه فارسی به انگلیسی

α–کد	α–code
α–کدواژه	α–word
α–کدواژه ابتدایی	primitive α– word
α–کد نرمال	normal α– code
t–تصحیح کننده خطا	t–error-correcting
ابردوگان	superdual
افزونگی	redundancy
الفبای کد	code alphabet
اندازه کد	size of code
بعد فضا	dimention of space
پایه	basis
پشتیبان	support
تبدیل خطی	linear transformation
ترکیب خطی	linear combination
دوگان مجموعه	dual of set
دوگان کد خطی	dual of linear code
رتبه	rank
رتبه کد کامل خطی	rank of linear perfect code
زیر فضا	subspace
زیرفضای پدید آمده	spanning subspace
شرط های ابردوگانی	superdual conditions
ضرایب فوریه	Fourier coefficients
ضرب نقطه ای	pointwise multiplication
ظرفیت کانال	capacity of channel
فاصله همینگ	Hamming distance
فضای برداری	vector space
قاعده کدگشایی	decoding rule
کد	code
کدواژه	codeword
کد بهینه	optimal code
کد توربو	Turbo code

کد توسعه یافته	extended code
کد خطی	linear code
کد خود دوگان	self-dual code
کد خود متعامد	self-orthogonal code
کد دودویی	binary code
کد سیمپلکس	simplex code
کد کامل	perfect code
کد کامل با رتبه تام	full rank perfect code
کدگذاری	encoding
کدگشایی	decocing
کدگشایی حداکثر احتمال	maximum likelihood decoding
کدگشایی مینیمم فاصله	minimum distance decoding
کدگشایی تکراری	iteration decoding
کد گولای	Golay code
کد گولای توسعه یافته	extended Golay code
کد گولای دودویی	binary Golay code
کدهای پیچشی	convolutional codes
کدهای معادل	equivalent codes
کد واسیلو	Vasil'ev code
کد همینگ	Hamming code
کد همینگ دودویی	binary Hamming code
کد همینگ $q-$ نمادی	$q-$ary Hamming code
کران پوششی کره	sphere-paking bound
کران گیلبرت ورشامو	Gilbert-Varshamov bound
کران همینگ	Hamming bound
کره	sphere
کلمه یا واژه	word
ماتریس کنترل توازن	parity-check matrix
ماتریس مولد	generator matrix
مرتبه الفبایی	Lexicographic order
مینیمم فاصله	minimum distance
نظریه اطلاعات	information theory
نظریه کدگذاری	coding theory
نظریه کدگذاری کانال	channel coding theory
نظریه کدگذاری منبع	source coding theory
نظریه کدهای تصحیح کننده خطا	theory of error-correcting code
وزن همینگ	Hamming weight
هسته	kernel
هم مجموعه	coset

واژه‌نامه انگلیسی به فارسی

α–code	α–کد
α–word	α–کدواژه
q–ary Hamming code	کد همینگ q– نمادی
t–error-correcting	t–تصحیح کننده خطا
binary code	کد دودویی
binary Golay code	کد گولای دودویی
binary Hamming code	کد همینگ دودویی
basis	پایه
capacity of channel	ظرفیت کانال
channel coding theory	نظریه کدگذاری کانال
code	کد
code alphabet	الفبای کد
codeword	کدواژه
coding theory	نظریه کدگذاری
convolutional codes	کدهای پیچشی
coset	هم مجموعه
decocing	کدگشایی
decoding rule	قاعده کدگشایی
dimention of space	بعد فضا
dual of linear code	دوگان کد خطی
dual of set	دوگان مجموعه
encoding	کدگذاری
equivalent codes	کدهای معادل
extended Golay code	کد گولای توسعه یافته
full rank perfect code	کد کامل با رتبه تام
Fourier coefficients	ضرایب فوریه
generator matrix	ماتریس مولد
Gilbert-Varshamov bound	کران گیلبرت ورشامو
Golay code	کد گولای
Hamming bound	کران همینگ
Hamming code	کد همینگ
Hamming weight	وزن همینگ

نظریه اطلاعات	information theory
کدگشایی تکراری	iteration decoding
هسته	kernel
مرتبه الفبایی	Lexicographic order
کد خطی	linear code
ترکیب خطی	linear combination
تبدیل خطی	linear transformation
کدگشایی حداکثر احتمال	maximum likelihood decoding
مینیمم فاصله	minimum distance
کدگشایی مینیمم فاصله	minimum distance decoding
α–کد نرمال	normal $\alpha-$ code
کد بهینه	optimal code
ماتریس کنترل توازن	parity-check matrix
کد کامل	perfect code
ضرب نقطه ای	pointwise multiplication
α–کدواژه ابتدایی	primitive $\alpha-$ word
رتبه	rank
رتبه کد کامل خطی	rank of linear perfect code
افزونگی	redundancy
کد خود دوگان	self-dual code
کد خود متعامد	self-orthogonal code
کد سیمپلکس	simplex code
اندازه کد	size of code
زیرفضای پدید آمده	spanning subspace
کره	sphere
کران پوششی کره	sphere-paking bound
نظریه کدگذاري منبع	source coding theory
زیر فضا	subspace
ابردوگان	superdual
شرط های ابردوگانی	superdual conditions
پشتیبان	support
نظریه کدهای تصحیح کننده خطا	theory of error-correcting code
کد توربو	Turbo code
کد واسیلو	Vasil'ev code
فضای برداری	vector space
کلمه یا واژه	word

Abstract

Resently, utilizing perfect codes have been magnificently of interest for many researchers and application. In this project we first study basic and elementary concepts in the coding theory and then investigate perfect codes, related topics and type of perfect codes. Finally construct full rank perfect codes, the so-called normal $\alpha-$ codes, by first finding the superdual of the perfect code and we gave an example of full rank perfect code of length 31.

Keywords: *Perfect code, Full rank perfect code, $\alpha-$word, Normal $\alpha-$ word.*

Shahrood University of Technology
Facualty of Methematical Sciences
Department of Mathematics

MS.C. Thesis

On perfect codes and related topics

By:
Aliye Mohamadi

Supervisor:
Professor N. Jafarirad

Jul 2012