دانشکده علوم‌ریاضی

رشته ریاضی‌کاربردی، گرایش رمز و کد

پایان‌نامه کارشناسی ارشد

نشاندن و پارتیشن‌بندی در کدهای کامل qـ آرایه‌ای

نگارنده: مهنا غفاری سبیل

استادان راهنما

دکتر عبدالله آل‌هوز
دکتر میثم علیشاهی

استاد مشاور

دکتر ابراهیم هاشمی

مهر ماه ۱۳۹۸

تقدیم

به پاس تعبیر عظیم و انسانی‌شان از کلمه ایثار،
به پاس عاطفه سرشار و گرمای امیدبخش وجودشان که در این سردترین روزگاران بهترین پشتیبان است،
به پاس قلب‌های بزرگشان که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می‌گراید و
به پاس محبت‌های بی‌دریغشان که هرگز فروکش نمی‌کند.
این پایان‌نامه را به پدر و مادر عزیزم تقدیم می‌نمایم.

سپاس‌گزاری

سپاس و ستایش مر خدای را جل و جلاله که آثار قدرت او بر چهره روز روشن، تابان است و انوار حکمت او در دل شب تار، درفشان. آفریدگاری که خویشتن را به ما شناساند و درهای علم را بر ما گشود و عمری و فرصتی عطا فرمود تا بدان، بنده ضعیف خویش را در طریق علم و معرفت بیازماید.
به امید آنکه توفیق یابم جز خدمت به خلق او نکوشم.

از اساتید فرهیخته و با کمالات؛ جناب آقای دکتر آل‌هوز و آقای دکتر علیشاهی که در کمال سعه صدر، با حسن‌خلق و فروتنی، از هیچ کمکی در این عرصه بر بنده دریغ ننمودند و زحمت راهنمایی این پایان‌نامه را بر عهده گرفتند؛
از استاد صبور و با تقوا؛ جناب آقای دکتر هاشمی، رئیس محترم دانشکده ریاضی، که زحمت مشاوره این پایان‌نامه را متقبل شدند و
از اساتید فرزانه و دلسوز؛ جناب آقای دکتر پورعیدی و خانم دکتر مغاری که زحمت داوری این پایان‌نامه را متقبل شدند، کمال تشکر و قدردانی را دارم.
از خداوند متعال برای شما اساتید گران‌قدر سلامتی و توفیق روزافزون در تمام عرصه‌های زندگی را خواستارم.

مهنا غفاری سبیل
مهر ماه ۱۳۹۸

تعهد نامه

اینجانب **مهنا غفاری سبیل** دانشجوی کارشناسی ارشد رشته **ریاضی‌کاربردی** ، **علوم‌ریاضی** دانشگاه شاهرود، نویسنده پایان‌نامه با عنوان**نشاندن و پارتیشن‌بندی در کدهای کامل** q**ـ آرایه‌ای** ، تحت راهنمایی دکتر **عبدالله آل‌هوز** و دکتر **میثم علیشاهی** متعهد می‌شوم:

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

مهنا غفاری سبیل
مهر ماه ۱۳۹۸

مالکیت نتایج و حق نشر

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

چکیده

مطالعه‌ی کدهای کامل به دلیل ساختار و ویژگی‌های جالب و خوبی که دارند از اهمیت خاصی برخوردار است و این کدها دارای کاربردهای زیادی در علم مخابرات می‌باشند. در این پایان‌نامه قصد داریم نشاندن و افراز ۱ـکدها و کدهای با وزن ثابت در کدهای کامل را مورد مطالعه قرار دهیم. نشان می‌دهیم که هر کد ۱ـ تصحیح‌گر خطا روی یک میدان متناهی را می‌توان در یک کد ۱ـکامل با طول بزرگ‌تر نشاند. نشاندن در اینجا بدین معناست که کد اصلی خود یک زیرکد از کد ۱ـکامل می‌باشد و می‌توان آن را به وسیله‌ی تکرارهای کوتاه به دست آورد. علاوه‌بر این، نتیجه به افرازها تعمیم داده می‌شود: هر افراز از فضای همینگ در کدهای ۱ـ تصحیح‌گر خطا را می‌توان در یک افراز از فضا با ابعاد بزرگ‌تر درون کدهای ۱ـکامل نشاند. برای افرازها، طول نشاندن، نزدیک به کران نظری موجود قبلی برای حالت‌های کلی و همچنین بهینه برای حالت دودویی می‌باشد. به‌علاوه، نشان خواهیم داد که هر کد qـ تایی با وزن ثابت ۳، با مینیمم فاصله‌ی ۴ و طول m، در یک کد ۱ـکامل qـ تایی از طول $n = \frac{q^m-1}{q-1}$ قابل نشاندن می‌باشد.

کلمات کلیدی: کد همینگ، کد کامل، افراز، نشاندن، کد ۱ـکامل، کد کامل غیرخطی، کدهای با وزن ثابت.

فهرست مطالب

فصل ۱

تعاریف و مفاهیم اولیه

۱.۱ گذری بر تاریخچه کد

نظریه‌ی کدگذاری[۱] مرهون مقاله معروف کلود شانون[۲] با موضوع ارسال قابل قبول اطلاعات روی کانال‌های مخابراتی پارازیت‌دار[۳] است که در سال ۱۹۴۸ مطرح شد. شانون اثبات کرد اگر نرخ ارسال اطلاعات کمتر از ظرفیت کانال باشد، مخابرات مطمئن قابل حصول خواهد بود، به شرطی که بتوان از کدگذاری و کدگشایی مناسبی در فرستنده و گیرنده استفاده کرد. از آن پس کارهای فراوانی به وسیله‌ی بسیاری از محققان به منظور دست‌یابی به یک کد خوب و با کدگذاری مناسب با پیش‌گامانی هم‌چون همینگ[۴]، گولای[۵] و دیگر محققان در اوایل دهه ۴۰ شروع شد و اکنون در سراسر دنیا به وسیله‌ی محققان زیادی در حال انجام می‌باشد.
پژوهش‌ها در دهه‌های ۵۰ و ۶۰ در زمینه‌ی کدگذاری، ابتدا به توسعه‌ی نظریه‌ی کدگذاری و کدگشایی با کارایی مناسب متمرکز بود. سپس در دهه‌ی ۷۰ بحث‌های پیاده‌سازی کدهای با قابلیت تشخیص خطا مطرح شد. دهه‌های ۸۰ و ۹۰ جهشی در نظریه کدگذاری به وجود آمد که به خصوص از لحاظ عملی قابل توجه بود و مهم‌ترین آن‌ها عبارتند از:

- استفاده از کدهای کانولوشنال دودویی[۶] و کدهای بلوکی[۷] با مدلاسیون مختلف،

[1] Coding theory
[2] Claude Shannon
[3] Noisy channel
[4] Hamming
[5] Golay
[6] Binary convolutional codes
[7] Block codes

- گسترش روش‌های کاربردی و کدگشایی نرم تخصصی برای کدهای بلوکی،
- ابداع روش‌های کدگشایی تکراری به صورت ورودی ـ نرم، خروجی ـ نرم برای کدهای بلوکی و کانولوشنال.

استفاده از این کاربردها در نظریه‌ی کدگذاری، انقلابی در سامانه‌های کدگشایی ایجاد کرد که به سهم خود به طراحی مودم‌های با نرخ بالا، سامانه‌های موبایل سلولی، مخابرات ماهواره‌ای و فضایی و ذخیره‌سازی پرچگال منجر شده است. شایان ذکر است که طراحی و تحلیل کدهای ذکر شده فوق نیاز به اطلاعات و پیش‌زمینه‌هایی در جبر خطی و نظریه احتمالات دارد. همچنین بسیاری از مهندسان بدون پرداختن به اصول طراحی و تحلیل آن‌ها به سمت پیاده‌سازی عملی چنین سامانه‌هایی سوق پیدا کردند.

پیدایش نظریه کدگذاری، یک حوزه‌ی مطالعاتی مرتبط با انتقال داده‌ها از طریق کانال‌های پارازیت‌دار و محافظت از آن‌ها در مقابل تحریف‌ها می‌باشد. در کمتر از نیم قرن، نظریه‌ی کدگذاری از نظر رشد، فوق‌العاده بوده است و کاربردهای گسترده‌ای در زمینه‌های علوم مختلف، به خصوص در علم مخابرات پیدا کرده است. لذا از نقطه نظر کاربردی طراحی کدهای خوب که کدگذاری و کدگشایی مناسبی داشته باشند حائز اهمیت می‌باشد.

پژوهشگران مختلفی بر آن شدند که کدهای نه لزوماً بلوکی را نیز مورد مطالعه قرار دهند که از مهم‌ترین این دسته کدها که اخیراً مورد مطالعه قرار گرفته‌اند می‌توان به: کدهای پیچشی[۸]، کدهای توربو[۹]، کدهای فضا ـ زمان[۱۰]، کدهای با ماتریس کنترل توازن کم ـ چگال[۱۱] و کدهای کوانتومی[۱۲] اشاره نمود.

یک رده مهم از کدهای خطی که اخیراً مورد توجه قرار گرفته و محققان بسیاری از نظریه کدگذاری برای انجام تحقیقات در این زمینه متمرکز شده‌اند، کدهای کامل می‌باشند که این کدها در حالت مرزی کران همینگ صدق می‌کنند، یعنی به تعداد $\frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i}$ کدواژه دارند، جایی‌که q بیانگر مرتبه‌ی میدان F_q است، n طول کد و d فاصله کد می‌باشد.

در این پایان‌نامه قصد داریم ضمن مطالعه و بررسی خواص بیشتری از این کدها، نشاندن و افراز برخی کدها در کدهای کامل را مورد بررسی قرار دهیم.

۲.۱ مفاهیم و تعاریف مقدماتی

در این بخش، مفاهیم و مطالب مورد استفاده از نظریه‌ی کدگذاری را بیان خواهیم کرد. مطالب این بخش غالباً برگرفته از مرجع [۱] است.

[8] Wrap codes
[9] Turbo codes
[10] Space- time codes
[11] Low- density parity check codes
[12] Quantum codes

تعریف ۱.۲.۱. فرض کنید A یک مجموعه‌ی qـعضوی به صورت $A = \{a_1, a_2, \ldots, a_q\}$ باشد. در این صورت مجموعه A را الفبای کد[13] می‌نامیم و هر یک از عناصر آن را سمبل (نماد) کد[14] گوییم.

تعریف ۲.۲.۱. یک کلمه qـتایی با طول n روی مجموعه A در حقیقت دنباله‌ای به شکل $w = w_1 w_2 \ldots w_n$ می‌باشد، جایی‌که برای هر $1 \leq i \leq n$ داریم $w_i \in A$. همچنین می‌توان هر کلمه qـتایی با طول n را به صورت برداری $w = (w_1, w_2, \ldots, w_n)$ نمایش داد.

تعریف ۳.۲.۱. کد بلوکی qـتایی[15] با طول n روی مجموعه‌ی A مجموعه‌ای ناتهی مانند C، متشکل از کلمات qـتایی می‌باشد که تمام کلمات آن از طول یکسان n می‌باشند. هر عنصر از مجموعه‌ی C را یک کدواژه[16] می‌نامیم.

تعریف ۴.۲.۱. تعداد کدواژه‌های کد C را اندازه کد می‌نامیم و با $|C|$ نمایش می‌دهیم.

تعریف ۵.۲.۱. هر کد بلوکی از طول n و اندازه M را یک (n, M)ـکد گویند.

تعریف ۶.۲.۱. نرخ (ارسال) اطلاعات[17] کد C به صورت نسبت $R(C) = \frac{k}{n}$ می‌باشد، جایی‌که k تعداد بیت‌های اطلاعات مفید ما می‌باشد و n تعداد بیت‌هایی است که کدگذار صرف کدگذاری اطلاعات و داده‌ها می‌کند، یعنی $n \geq k$ و به تعداد $n - k$ بیت اضافی در فرآیند کدگذاری اعمال شده است.
در واقع نرخ هر کد C به صورت نسبت تعداد بیت‌های پیام ارسالی به تعداد بیت‌های پیام کدگذاری شده می‌باشد.

ملاحظه ۱.۲.۱. نرخ کد C کمیتی برای اندازه‌گیری کارایی کد می‌باشد و کدهای با نرخ بالا از اهمیت ویژه‌ای در نظریه کدگذاری برخوردار می‌باشند. بالاترین نرخ کد برابر با $R(C) = 1$ می‌باشد و کدهایی که دارای نرخ ۱ می‌باشند، قابلیت تشخیص و تصحیح هیچ خطایی را ندارند، بنابراین از دیدگاه عملی کدهایی خوب هستند که در کنار کارایی بالا بتوانند قابلیت تشخیص و تصحیح خطای مناسبی نیز داشته باشند.

ملاحظه ۲.۲.۱. اکثر مواقع الفبای کد را یک میدان متناهی در نظر می‌گیرند، یعنی $A = F_q$.

- اگر $A = F_2$ باشد، کد دودویی[18] نامیده می‌شود.
- اگر $A = F_3$ باشد، کد سه‌تایی[19] نامیده می‌شود.

[13] Code alphabet
[14] Code symbol
[15] q- ary block code
[16] Code words
[17] Information rate
[18] Binary code
[19] Ternary code

◄ اگر $A = F_۴$ باشد، کد چهارتایی[۲۰] نامیده می‌شود.

مثال ۱.۲.۱. اگر $A = F_۲$ باشد، دراین صورت کد $C_۱ = \{۰۰۰, ۱۰۱, ۰۱۰, ۱۰۰, ۱۱۰\}$ یک (۵و۳)ـ کد دودویی است که طول کد برابر ۳ و اندازه کد برابر ۵ است و اگر $A = F_۳$ باشد، دراین صورت کد $C_۲ = \{۱۲۰۰, ۰۲۱۰\}$ یک (۲و۴)ـ کد سه‌تایی می‌باشد که طول کد ۴ و اندازه کد برابر ۲ است.

تعریف ۷.۲.۱. فرض کنید x و y دو کلمه به طول n روی الفبای A باشند. منظور از فاصله همینگ[۲۱] بین x و y که با $d(x, y)$ نمایش داده می‌شود، تعداد جایگاه‌هایی است که x و y در آن‌ها تفاوت دارند.
به عبارت دیگر اگر $x = x_۱, \ldots, x_n$ و $y = y_۱, \ldots, y_n$ ، آن‌گاه

$$d_H(x, y) = \Big|\Big\{i \,\big|\, x_i \neq y_i, ۱ \leq i \leq n\Big\}\Big|.$$

ملاحظه ۳.۲.۱. به راحتی می‌توان بررسی کرد که تعریف فوق از فاصله همینگ، تمام ویژگی‌های یک متر را دارا می‌باشد و اگر x و y و z کدواژه‌هایی از طول n در یک کد بلوکی باشند، همواره داریم:

◄ $۰ \leq d_H(x, y) \leq n$.

◄ $x = y \iff d_H(x, y) = ۰$.

◄ $d_H(x, y) = d_H(y, x)$.

◄ $d_H(x, z) \leqslant d_H(x, y) + d_H(y, z)$.

تعریف ۸.۲.۱. علاوه‌بر طول و اندازه کد، پارامتر مهم دیگر فاصله کد[۲۲] است. برای کد C که شامل حداقل دو کدواژه می‌باشد فاصله‌ی کد C، که با نماد $d(C)$ نمایش داده می‌شود، به صورت زیر تعریف می‌شود:

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

تعریف ۹.۲.۱. هر کد بلوکی که طول آن n، اندازه آن M و فاصله همینگ آن d باشد را یک (n, M, d)ـ کد می‌نامیم. در این حالت n و M و d را پارامترهای کد C می‌نامند.

---

[20] Quaternary code
[21] Hamming distance
[22] Distance of a code

تعریف ۱.۲.۱.۱۰. دو قاعده‌ی کدگشایی که معمولاً برای کدگشایی کدها در حالت کلی مورد استفاده قرار می‌گیرند به صورت زیر می‌باشند:

۱. قاعده‌ی کدگشایی مینیمم فاصله[۲۳] (MDD) بدین‌صورت می‌باشد که کدواژه‌های کد C در یک کانال ارتباطی پارازیت‌دار ارسال می‌شود و ما کلمه x را دریافت می‌کنیم، در این صورت قاعده کدگشایی مینیمم فاصله کلمه x را به کدواژه c_x کدگشایی می‌کند، هرگاه فاصله‌ی (همینگ) بین x و c_x در بین تمام کدواژه‌های کد C مینیمم مقدار ممکن باشد، یعنی داشته باشیم:

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

دو نوع قاعده MDD داریم:
در نوع کامل آن اگر دو کدواژه c_x موجود باشند که $d_H(x, c_x)$ مینیمم باشد، آن‌گاه یکی را به دلخواه انتخاب می‌کنیم. در نوع غیرکامل آن در صورت بروز چنین مسئله‌ای تقاضای ارسال مجدد می‌کنیم.

۲. در قاعده‌ی کدگشایی ماکزیمم احتمال[۲۴] (MLD) کدواژه‌های کد C از طریق یک کانال پارازیت‌دار ارسال می‌گردد و ما کلمه‌ی x را دریافت می‌کنیم، دراین صورت قاعده کدگشایی ماکزیمم احتمال کلمه x را به کدواژه c_x کدگشایی می‌کند هرگاه احتمال کانال ارسال برای c_x ماکزیمم باشد، یعنی داشته باشیم:

$$p\Big(x\text{دریافت}\,\Big|\,c_x\text{ارسال}\Big) = max\Big\{p\Big(x\text{دریافت}\,\Big|\,c_x\text{ارسال}\Big)\,\Big|\,c \in C\Big\}.$$

مشابه قاعده‌ی قبل دونوع قاعدهMLD داریم:
در نوع کامل آن اگر دو کدواژه c_x پیدا شوند که برای آن‌ها $p(x|c_x)$ ماکزیمم باشد آن‌گاه به دلخواه یکی را انتخاب می‌کنیم. در نوع غیرکامل آن در صورت بروز چنین مسئله‌ای درخواست ارسال مجدد می‌کنیم.

تعریف ۱.۲.۱.۱۱. برای عدد صحیح مثبت u، گوییم کد C یک کد uـتشخیص‌گر خطا[۲۵] می‌باشد، هرگاه اگر در کدواژه‌های کد C، حداقل یک خطا و حداکثر uـخطا رخ دهد، در این صورت کلمه حاصل کدواژه‌ای از کد C نباشد (خطا تشخیص داده شود).

[23] Minimum distance decoding
[24] Maximum likelihood decoding
[25] u- error detecting code

کد C را دقیقاً uـ تشخیص‌گر خطا گوییم هرگاه کد C یک کد uـ تشخیص‌گر خطا باشد ولی $(u+1)$ـ تشخیص‌گر خطا نباشد.

تعریف ۱.۲.۱. برای عدد صحیح مثبت u، گوییم کد C یک کد uـ تصحیح‌گر خطا[۲۶] می‌باشد، هرگاه روش کدگشایی مینیمم فاصله غیرکامل[۲۷] $(IMDD)$ قادر به تصحیح حداکثر uـ خطا باشد. کد C را دقیقاً uـ تصحیح‌گر خطا گوییم، هرگاه کد C یک کد uـ تصحیح‌گر خطا باشد ولی $(u+1)$ـ تصحیح‌گر خطا نباشد.

مثال ۱.۲.۱. کد $C=\{000, 111\}$ کدی ۱ـ تصحیح‌گر خطا می‌باشد ولی ۲ـ تصحیح‌گر خطا نیست. چون در هر یک از کدواژه‌های آن یک خطا صورت گیرد قابل تصحیح می‌باشد ولی اگر دو خطا صورت گیرد قابل تصحیح نیست. به طور مثال اگر کدواژه ”000 “ ارسال شود و کلمه ” 001 “ دریافت گردد این کدواژه با استفاده از قاعده‌ی کدگشایی مینیمم فاصله غیرکامل به صورت ”000 “ تصحیح می‌شود. اما اگر کدواژه ” 000 “ ارسال شود و کلمه ”011 “ دریافت گردد، قاعده کدگشایی مینیمم فاصله غیرکامل به اشتباه به کدواژه ” 111” کدگشایی می‌نماید. لذا کد C فوق دقیقاً ۱ـ تصحیح‌گر خطا می‌باشد.

قضیه ۱.۲.۱. کد C یک کد uـ تصحیح‌گر خطا می‌باشد اگر و تنها اگر $d(C)\geq 2u+1$.

برهان. ابتدا فرض کنیم $d(C)\geq 2u+1$ می‌باشد. فرض می‌کنیم کدواژه‌ی $c\in C$ ارسال شود و با اعمال حداکثر u خطا کلمه‌ی x دریافت شود، یعنی داشته باشیم $d_H(x,c)\leq u$. حال برای کدواژه مجزا از c مانند c' داریم؛

$$1\leq d_H(c,c')\leq d_H(c,x)+d_H(x,c'),$$

آن‌گاه

$$d_H(x,c')\geq d_H(c,c')-d_H(c,x)\geq (2u+1)-u=u+1.$$

لذا قاعده‌ی $IMDD$ کلمه x را به درستی به کدواژه‌ی $c\in C$ کدگشایی کرده و در نتیجه کد C یک کد uـ تصحیح‌گر خطا می‌باشد.

حال فرض می‌کنیم کد C یک کد uـ تصحیح‌گر خطا باشد و به برهان خلف فرض می‌کنیم $d(C)<2u+1$، در این صورت $d(C)\leq 2u$. لذا کدواژه‌های مجزای c و c' در کد C موجودند که $d_H(c,c')=d(C)\leq 2u$.

حال ادعا می‌کنیم که $d_H(c,c')\geq u+1$، زیرا در غیر این صورت $d_H(c,c')<u+1$ باشد آن‌گاه $d_H(c,c')\leq u$، یعنی با اعمال uـ خطا کدواژه‌ی c به کدواژه‌ی c' می‌تواند تبدیل شود که با تعریف uـ تشخیص‌گری کد در تناقض است. لذا فرض خلف باطل و ادعا ثابت می‌شود که $d_H(c,c')\geq u+1$، بنابراین

$$u+1\leq d_H(c,c')=d(C)\leq 2u.$$

[26] u- error correcting code
[27] Incomplete MDD

بدون از دست دادن کلیت مسئله فرض کنیم که کدواژه‌های c و c' در d مؤلفه‌ی اول تفاوت دارند، جایی که $d = d(C) = d_H(c, c')$ بنابراین اگر کلمه‌ی x به صورت زیر دریافت شود؛

$$x = x_1, \ldots, x_u, x_{u+1}, \ldots, x_d, \ldots, x_{d+1}, \ldots, x_n,$$

که $x_1, \ldots, x_u$ قسمتی از c' و $x_{u+1}, \ldots, x_d$ قسمتی از c و $x_{d+1}, \ldots, x_n$ بین c و c' مشترک است، آن‌گاه داریم

$$d_H(x, c') = d - u \leq u = d_H(x, c).$$

حال دو حالت مختلف داریم؛

۱. اگر $d_H(x, c') = d_H(x, c)$، در این صورت قاعده‌ی کدگشایی $IMDD$ درخواست ارسال مجدد کرده و تصحیح خطا اتفاق نمی‌افتد.

۲. اگر $d_H(x, c') < d_H(x, c)$، در این صورت قاعده‌ی کدگشایی $IMDD$ کلمه‌ی x را به اشتباه به کدواژه‌ی c' کدگشایی می‌کند،

که هر دو حالت فوق با uـ تصحیح‌گر خطا بودن کد C در تناقض است، بنابراین فرض خلف باطل و باید داشته باشیم $d(C) \geq 2u + 1$. □

تعریف ۱.۲.۱۳. مجموعه ناتهی V به همراه دو عمل "$+$" و "$.$" را فضای برداری[۲۸] روی میدان F_q گوییم، هرگاه برای $u, v, w \in V$ و $\lambda, \mu \in F_q$ داشته باشیم:

۱. $u + v \in V$.

۲. $(u + v) + w = u + (v + w)$.

۳. عنصری مانند $\circ \in V$ وجود دارد که برای هر $v \in V$ داریم $\circ + v = v = v + \circ$.

۴. برای هر $u \in V$، عنصری از V موجود است که $(-u)$ نامیده می‌شود به قسمی که

$$u + (-u) = (-u) + u = \circ.$$

۵. $u + v = v + u$.

۶. برای هر $v \in V$ و $\lambda \in F_q$، $\lambda.v \in V$.

۷. برای هر $\lambda \in F_q$ و $v, w \in V$ داریم $\lambda.(v + w) = \lambda v + \lambda w$.

۸. برای هر $\lambda, \mu \in F_q$ و $v \in V$ داریم $(\lambda\mu).v = \lambda.(\mu v)$.

۹. اگر عنصر ۱ همانی ضربی F_q باشد، آن‌گاه $1.v = v$.

[28] Vector space

ملاحظه ۴.۲.۱. زیرمجموعه‌ی ناتهی مانند W از فضای برداری V روی میدان F_q زیرفضایی از V می‌باشد اگر و تنها اگر داشته باشیم:

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

تعریف ۱۴.۲.۱. یک ترکیب خطی [۲۹] از بردارهای $v_۱, \ldots, v_n$ در فضای برداری V روی میدان F_q عبارتی به صورت $\lambda_۱ v_۱ + \cdots + \lambda_n v_n$ می‌باشد به طوری‌که برای هر $i = ۱, ۲, \ldots, n$، داشته باشیم $\lambda_i \in F_q$.

مجموعه‌ی تمام بردارهای به طول n با درایه‌های متعلق به F_q را با $F_q^{\,n}$ نمایش می‌دهیم، یعنی داریم

$$F_q^{\,n} = \Big\{ v = (v_۱, \ldots, v_n) \,|\, v_i \in F_q \,, \forall\, ۱ \leq i \leq n \Big\}.$$

تعریف ۱۵.۲.۱. فرض کنیم V یک فضای برداری روی میدان F_q و S یک زیرمجموعه‌ی ناتهی از V باشد. در این صورت گوییم S یک مجموعه‌ی مستقل‌خطی [۳۰] می‌باشد، هرگاه برای عناصر $\lambda_۱, \ldots, \lambda_n \in F_q$ اگر

$$\lambda_۱ v_۱ + \lambda_۲ v_۲ + \cdots + \lambda_n v_n = ۰,$$

آن‌گاه داشته باشیم:

$$\lambda_۱ = \lambda_۲ = \cdots = \lambda_n = ۰.$$

مجموعه‌ای که مستقل‌خطی نباشد، وابسته‌خطی نامیده می‌شود.

تعریف ۱۶.۲.۱. یک مجموعه‌ی مستقل‌خطی که برای فضای برداری V مولد نیز باشد پایه‌ی [۳۱] فضای برداری V نامیده می‌شود.

تعریف ۱۷.۲.۱. تعداد عناصر پایه‌ی فضای برداری V روی میدان F را بعد [۳۲] فضای برداری نامیده و آن را با نماد $dim_F V$ نمایش می‌دهیم.

تعریف ۱۸.۲.۱. یک کد خطی [۳۳] از طول n روی میدان F_q، یک زیرفضایی از فضای برداری $F_q^{\,n}$ می‌باشد.

کدی که خطی نباشد، کد غیرخطی [۳۴] نامیده می‌شود.

مثال ۳.۲.۱. نمونه‌هایی از کدهای خطی را به صورت زیر داریم:

۱. $C = \Big\{ (\lambda, \ldots, \lambda) \,|\, \lambda \in F_q \Big\}$، یک کد خطی است که کد تکرار [۳۵] نامیده می‌شود.

[29] Linear combination
[30] Linearly independent
[31] Basis
[32] Dimension
[33] Linear code
[34] Nonlinear
[35] Repeat code

۲. $C = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱۱\}$، یک کد خطی است که $(q = ۲)$ می‌باشد.

۳. $C = \{۰۰۰, ۱۲۰, ۲۱۰\}$، یک کد خطی است که $(q = ۳)$ می‌باشد.

تعریف ۱.۲.۱۹. فرض کنید x یک کلمه در ${F_q}^n$ باشد. وزن همینگ[۳۶] کلمه x که با نماد $wt(x)$ نمایش داده می‌شود، برابر با تعداد مؤلفه‌های غیرصفر کلمه x تعریف می‌شود. به عبارت دیگر:

$$wt(x) = d(x, ۰),$$

جایی‌که ۰ کلمه‌ی صفر در F_q^n می‌باشد؛ $۰ = (۰, ۰, \ldots, ۰) \in F_q^n$.
برای هر عضو $x \in F_q$ وزن همینگ را می‌توانیم به صورت زیر تعریف کنیم:

$$wt(x) = d(x, ۰) = \begin{cases} ۱, & x \neq ۰ \\ ۰, & x = ۰. \end{cases}$$

در این صورت همواره خواهیم داشت:
$\forall\, x \in F_q^n,\ x = (x_۱, x_۲, \ldots, x_n);\ wt(x) = \sum_{i=۱}^{n} wt(x_i) = wt(x_۱) + \cdots + wt(x_n).$

قضیه ۱.۲.۲. فرض کنیم C یک کد خطی روی میدان متناهی F_q باشد. در این صورت همواره داریم: $d(C) = wt(C)$.

تعریف ۱.۲.۲۰. ماتریس مولد[۳۷] کد خطی C، ماتریسی است که سطرهای آن پایه‌ای برای کد خطی C می‌باشد.

تعریف ۱.۲.۲۱. فرض کنیم C یک کد خطی در ${F_q}^n$ باشد. دوگان[۳۸] کد C که با نماد $C^{\perp}$ نمایش داده می‌شود، برابر با مکمل متعامد C در ${F_q}^n$ می‌باشد، یعنی

$$C^{\perp} = \{v \in {F_q}^n \,|\, v.c = ۰,\ \forall c \in C\}.$$

تعریف ۱.۲.۲۲. ماتریس کنترل توازن[۳۹] کد خطی C، ماتریسی است که سطرهای آن پایه‌ای برای دوگان کد C، یعنی $C^{\perp}$ می‌سازند.

قضیه ۱.۲.۳. فرض کنیم C یک (n, k) ـ کد خطی روی میدان F_q باشد و H ماتریس کنترل توازن کد C باشد، در این صورت

$$v \in C \iff vH^T = ۰.$$

[36] Hamming weight
[37] Generator matrix
[38] Dual
[39] Parity check matrix

قضیه ۴.۲.۱. فرض کنیم C یک (n,k)ـ کد خطی و H ماتریس کنترل توازن آن باشد، دراین صورت خواهیم داشت:

- $d(C) \geq d$ اگر و تنها اگر هر $d-1$ ستون از H مستقل‌خطی باشند.
- $d(C) \leq d$ اگر و تنها اگر H، دارای d ستون وابسته‌خطی باشد.

برهان. فرض کنیم $v = (v_1, v_2, \ldots, v_n)$ یک کلمه با وزن همینگ e باشد و $e \leq n$. بدون از دست دادن کلیت مسئله، فرض کنیم $v_{i_1}, v_{i_2}, \ldots, v_{i_e} \neq 0$. لذا برای هر $i \notin \{i_1, i_2, \ldots, i_e\}$ ، داریم $v_i = 0$. فرض کنیم e_i ستون iام ماتریس کنترل توازن H باشد. حال اگر کلمه v با وزن همینگ e بخواهد متعلق به کد C باشد، بنابر قضیه (۳.۲.۱) داریم: $v.H^T = 0 \iff v \in C$. لذا

$$0 = v.H^T = v_{i_1}.e_{i_1}^T + v_{i_2}.e_{i_2}^T + \cdots + v_{i_e}.e_{i_e} = 0.$$

حال اگر بخواهیم کلمه‌ای با وزن همینگ e متعلق به کد C باشد، معادل با این است که $e_{i_1}, e_{i_2}, \ldots, e_{i_e}$ وابسته خطی باشند. لذا با توجه به بالا، فاصله‌ی کد C حداقل d می‌باشد اگر و تنها اگر هر $d-1$ ستون از H مستقل خطی باشند. اگر d ستون از H وابسته‌ی خطی باشند، در این صورت کلمه (کدواژه‌ای) با وزن همینگ d در کد C قرار گرفته و در نتیجه بنابر تعریف فاصله‌ی کد C، داریم $d(C) \leq d$. □

ملاحظه ۵.۲.۱. اهمیت و دلیل ترجیح کدهای خطی بر کدهای غیرخطی را می‌توان در موارد زیر خلاصه نمود:

۱. با توجه به این‌که یک کد خطی فضای برداری می‌باشد، با استفاده از یک پایه می‌تواند به طور کامل به دست آید، لذا کارکردن با کدهای خطی آسان‌تر از کدهای غیرخطی می‌باشد.

۲. روش‌های کدگذاری و کدگشایی کدهای خطی نسبت به کدهای غیرخطی سریع‌تر و آسان‌تر می‌باشد.

۳. در کد خطی فاصله کد با مینیمم وزن همینگ کدواژه‌های غیرصفر آن برابر است.

تعریف ۲۳.۲.۱. فرض کنیم C یک کد qـتایی با پارامترهای (n,m,d) باشد. در این صورت مینیمم فاصله نسبی کد C را با $\delta(C)$ نمایش داده و به صورت زیر تعریف می‌کنیم:

$$\delta(C)_{n\to\infty} = \frac{d-1}{n}.$$

مثال ۴.۲.۱. فرض کنیم یک کد تکراری دودویی به صورت $C = \{۰۰\ldots۰, ۱۱\ldots۱\}$ داشته باشیم، از آن‌جایی که $\delta(C) = \frac{d-۱}{n} = \frac{n-۱}{n}$، بنابراین مینیمم فاصله‌ی نسبی برابر با ۱ می‌شود و زمانی‌که $\delta(C) = ۱$ است مناسب می‌باشد و قابلیت تشخیص و تصحیح خطا بالا می‌باشد.

تعریف ۲۴.۲.۱. فرض کنیم کد C با مجموعه‌ی الفبای A باشد و $|A| = q > ۱$ و مقادیر n و d مشخص باشند. در این صورت عدد $A_q(n,d)$ ماکزیمم اندازه ممکن برای M است که یک (n,M,d)ـ کد روی الفبای qـ عنصری A موجود باشد.

تعریف ۲۵.۲.۱. یک (n,M,d)ـ کد که در آن $M = A_q(n,d)$ باشد را یک کد بهینه[۴۰] می‌نامیم.

مثال ۵.۲.۱. چون $C_۱ = \{۰۰۰, ۱۰۱, ۰۱۱\}$ یک $(۳,۳,۲)$ـ کد دودویی و $C_۲ = \{۰۰۰, ۱۰۱, ۰۱۱, ۱۱۰\}$ یک $(۳,۴,۲)$ـ کد دودویی می‌باشند، لذا طبق تعریف کد بهینه می‌توان گفت که کد $C_۱$ بهینه نمی‌باشد.

تعریف ۲۶.۲.۱. فرض کنید A یک الفبای qـ عنصری باشد $(|A| = q > ۱)$ در این صورت برای هر بردار $u \in A^n$ جایی‌که $A^n = \Big\{u = (u_۱, u_۲, \ldots, u_n) \,|\, u_i \in A\Big\}$ و هر عدد صحیح $r \geq ۰$، گوی n بعدی به شعاع r و مرکز u با نماد $S_A(u,r)$ نمایش داده می‌شود و به صورت زیر تعریف می‌شود:

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

تعریف ۲۷.۲.۱. فرض کنیم $q > ۱$ و $r \geq ۰$ و n اعداد صحیح باشند. دراین صورت عدد $V_q^n(r)$ را به صورت زیر تعریف می‌کنیم:

$$V_q^n(r) = \begin{cases} \sum_{m=۰}^{r} \binom{n}{m}(q-۱)^m, & ۰ \leq r \leq n \\ q^n, & r \geq n. \end{cases} \qquad (۱.۱)$$

گزاره ۱.۲.۱. برای هر عدد صحیح $r \geq ۰$، گوی n بعدی با شعاع r در A^n دارای دقیقاً $V_q^n(r)$ بردار می‌باشد، جایی‌که A الفبای qـ عنصری می‌باشد. $(|A| = q > ۱)$

برهان. فرض کنید $u \in A^n$ یک بردار دلخواه باشد. تعداد بردارهای $v \in A^n$ را می‌شماریم که برای آن‌ها داشته باشیم $d(u,v) = m$، جایی‌که m یک عدد طبیعی یا صفر می‌باشد. برای این‌که بردارهای u و v دارای فاصله m باشند، بایستی دقیقاً در m جایگاه متفاوت باشند، لذا m جایگاه بردار v بایستی متفاوت از u در نظر گرفته شود. برای انتخاب این m جایگاه، $\binom{n}{m}$

[40] Optimal code

حالت متمایز داریم. در هر یک از این جایگاه‌ها، $q-1$ عنصر می‌توان قرار داد تا با عنصر این جایگاه در u متمایز باشد. لذا برای $0 \leq r \leq n$ در مجموع $\sum_{m=0}^{r} \binom{n}{m}(q-1)^m$ حالت برای انتخاب v داریم. یعنی تعداد بردارها برابر $V_q^n(r)$ می‌باشد.
حال در حالت $r \geq n$، بایستی گوی n بعدی $S_A(u,r)$ برابر با کل A^n باشد و در این حالت به تعداد $|A^n|$، یعنی q^n عنصر دارد. □

تعریف ۲۸.۲.۱. کد $C \subset F^n$ یک ۱ـ کد نامیده می‌شود، اگر همسایگی کدواژه‌ها مجزا باشد.
۱ـ کد، یعنی کدی که می‌تواند حداقل یک خطا را تصحیح کند.

تعریف ۲۹.۲.۱. ۱ـ کد $P \subset F^n$ کد ۱ـ کامل نامیده می‌شود، اگر $\Omega(P) = F^n$ باشد.

تعریف ۳۰.۲.۱. ماتریس کنترل توازن کد خطی qـ تایی H با این ویژگی که ستون‌های آن بردارهای غیرصفر است و از فضای برداری ${F_q}^m$ جایی‌که $m \geq 2$ می‌باشد ساخته شده‌اند، کد همینگ[41] q ـ تایی نامیده می‌شود که گاهی با $H_{q,m}$ نمایش داده می‌شود و دارای پارامترهای q و m می‌باشد و هر کدواژه از طول n می‌باشد و در حالت $q=2$ کد همینگ دودویی نامیده می‌شود.

مثال ۶.۲.۱. فرض کنیم $Ham(2,3)$ یک کد همینگ از طول ۷ باشد، در این‌صورت ماتریس کنترل توازن آن به شکل زیر می‌باشد:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

که در آن $m=3$ و $q=2$ می‌باشد. از آن‌جایی که H شامل همه ستون‌های m از کدواژه‌های با وزن ۱ می‌باشد و با توجه به این‌که ستون‌های صفر وجود ندارند و هیچ دو ستونی از H، 0 نیست. بنابراین هر دوستون از H مستقل‌خطی‌اند. چون فاصله‌ی کد همینگ $d=3$ می‌باشد، بنابر قضیه‌ی (۱.۲.۱) و قضیه‌ی (۴.۲.۱) داریم که کد همینگ دودویی دقیقاً ۱ـ تصحیح‌گر خطا می‌باشد.

تعریف ۳۱.۲.۱. کد C یک کد ۱ـ کامل[42] qـ تایی است، اگر برای هر $x \in {F_q}^n$ $(A^n = {F_q}^n)$، یک کدواژه منحصر به‌فرد $c \in C$ موجود باشد به طوری‌که $d(x,c) \leq 1$ باشد.
کدهای ۱ـ کامل qـ تایی با طول n وجود دارد اگر $n = \frac{(q^m-1)}{(q-1)}$، جایی‌که $m \geq 2$ می‌باشد و حداقل فاصله در کد ۱ـ کامل qـ تایی برابر با ۳ است.

[41] Hamming code
[42] 1 -Perfect code

مثال ۷.۲.۱. کدهای همینگ با طول $n = \frac{q^m-1}{q-1}$ وجود دارند، جایی‌که $m \geq 2$ می‌باشد، که در آن هر کدواژه از اندازه n می‌باشد و حداقل فاصله $d = 3$ می‌باشد، کد ۱ـ کامل qـ تایی می‌باشد. به دلیل این‌که $d(C) = 3$ است، بنابراین دقیقاً ۱ـ تصحیح‌گر خطا می‌باشد. کد همینگ $Ham(2,3)$ در مثال (۶.۲.۱) را در این مورد می‌توان در نظر گرفت.

تعریف ۳۲.۲.۱. کد $C \subset F^m$، نشانده شده در کد $P \subset F^n$ نامیده می‌شود، اگر C را بتوان از P با استفاده از جایگشت دادن مؤلفه‌ها و کوتاه کردن‌های مکرر به دست آورد، یعنی

$$C = \Big\{ x \in F^m \,|\, (x, a_{m+1}, \ldots, a_n) \in s(P_i) \Big\},$$

جایی‌که $a_{m+1}, \ldots, a_n$ عناصری ثابت می‌باشند و s جایگشت مؤلفه‌ای می‌باشد.

تعریف ۳۳.۲.۱. مجموعه $(C_1, \ldots, C_k)$ متشکل از کدها را یک افراز از فضای برداری F^m گوییم، هرگاه برای هر $i \neq j$،

- $C_i \cap C_j = \varnothing$ باشد.
- $\bigcup_{i=1}^{k} C_i = F^m$.

تعریف ۳۴.۲.۱. یک افراز $(C_1, \ldots, C_k)$ از F^m در افراز $(P_1, \ldots, P_t)$ از F^n، جایی‌که $k \leq t$ نشانده می‌شود، هرگاه برای برخی از عناصر ثابت $a_{m+1}, \ldots, a_n$ و جایگشت مؤلفه‌ای s تساوی

$$C_i = \Big\{ x \in F^m \,|\, (x, a_{m+1}, \ldots, a_n) \in s(P_i) \Big\},$$

برای هر $1 \leq i \leq k$ صادق باشد.

فصل ۲

نشاندن و افراز در کدهای کامل qـ تایی

۱.۲ مقدمات و نمادگذاری

مطالعه‌ی کدهای کامل یکی از جالب‌ترین موضوعات در نظریه کدگذاری می‌باشد، که ما در این فصل توجه خود را به نشاندن و افراز در کدهای کامل که به نوبه‌ی خود یکی از کاربردهای قابل توجه و کاربردی است معطوف می‌کنیم. ابتدا تعاریف و مفاهیم مربوط به کدهای کامل را ارائه می‌دهیم. در ادامه به چند لم و قضیه‌ی مرتبط با کدهای کامل می‌پردازیم و نهایتاً قضیه‌ی مهم در مورد افراز کدهای کامل را ارائه خواهیم داد. هدف از این بررسی نشان دادن این است که هر ۱ـ کد، یعنی کدی که می‌تواند حداقل یک خطا را تصحیح کند، زیرکدی از کد ۱ـ کامل با طول بزرگ‌تر می‌باشد. علاوه‌بر این، یک افراز از فضای همینگ[1] در ۱ـ کدها می‌تواند در یک افرازی از فضایی با بعد بالاتر در کدهای ۱ـ کامل نشانده شود. در مرجع [۲] اثبات شده است که هر کد دودویی از طول m می‌تواند در یک کد ۱ـ کامل دودویی از طول $n = ۲^m - ۱$ نشانده شود.

در مرجع [۱۳] مسئله فوق برای حالت سه‌تایی به صورت زیر اثبات شده است: هرسه‌تایی از ۱ـ کدها با طول m را می‌توان در یک کد ۱ـ کامل سه‌تایی با طول $n = \frac{۳^m - ۱}{۲}$ نشاند.

همچنین در مرجع [۱۳] کدها در یک میدان متناهی با تعداد عناصر $q > ۳$ در نظر گرفته شده‌اند و عبارت زیر برای آن‌ها اثبات شده است:

[1] Hamming space

هر ۲ـ کد qـ تایی از طول m می‌تواند در یک کد ۱ـ کامل qـ تایی با طول $n = \frac{q^m-1}{q-1}$ نشانده شود. این محدودیت که کد نشانده شده می‌بایست حداقل ۲ خطا را تصحیح بکند یک محدودیت اساسی می‌باشد تا جایی‌که، تمام ۱ـ کدها، ۲ـ کد نمی‌باشند. دلیل این محدودیت این است که روش پیشنهادی در مرجع [۲] برای حالت‌های کلی قابل استفاده نمی‌باشد: مؤلفه‌هایی که باید در کد ۱ـ کامل خطی تبدیل گردند تا زیرکد مدنظر ایجاد شود در حالت $q > ۳$ می‌توانند اشتراک داشته باشند (ملاحظه (۱.۴.۲) را ببینید).
برای جلوگیری از این مشکل اصلاحاتی را برای این روش پیشنهاد خواهیم داد. از نمادگذاری و تکنیک‌های اثبات مرجع [۲] با سه تفاوت اساسی پیروی می‌کنیم.
تفاوت اول، در نمادگذاری ما از حروف یونانی به جای حروف معمولی استفاده می‌کنیم، تعریف پایه‌ای i مؤلفه‌ی خطی را ما در حالت معمول به کار می‌بریم که در مرجع [۱۱] می‌توانید ببینید، در حالی‌که خاصیت مدنظر در لم (۵.۳.۲) بیان شده است (این تعریف براساس این خاصیت در نگاه اول ممکن است که در حالت qـ تایی خیلی پیچیده به نظر بیاید).
تفاوت دوم، بیان و فرمول‌بندی گزاره اساسی ما که بخش اصلی و اساسی اثبات قضیه‌ی بنیادین ما می‌باشد، متفاوت از لم اساسی در حالت دودویی می‌باشد (همان‌طور که در بالا نیز اشاره کردیم روش پیشنهادی در حالت دودویی در حالت کلی کار نمی‌کند، ملاحظه (۱.۴.۲) را ببینید).
تفاوت سوم، ما قضیه‌ای در مورد افراز نشاندن اضافه کرده‌ایم که برای تمام qها از جمله $q = ۲$ جدید می‌باشد.

اکنون به بیان تعدادی از نمادگذاری‌ها و تعاریف می‌پردازیم.

- F بیانگر میدان گالوا[۲] $GF(q)$ از مرتبه‌ی q می‌باشد و داریم؛ $GF(q) = (۰, \alpha^۰, \alpha^۱, \ldots, \alpha^q)$.
- F^m یک مجموعه mتایی روی میدان F است و آن را به عنوان فضای برداری روی میدان F درنظر می‌گیرند. عناصر F^m را با حروف یونانی نشان خواهیم داد.
- $\dot{F}^m := F^m \setminus \{۰\}$، جایی که ۰^m کلمه mتایی صفر می‌باشد.
- $n := ۲^m - ۱$ و $n > m$.
- هر زیرمجموعه‌ی غیر تهی $C \subset F^m$ را به عنوان یک کد qـ تایی از طول m در نظر می‌گیریم.
- مجموعه‌ی $\mathcal{A}$ شامل تمام m تایی‌هایی از F^m می‌باشد که اولین مؤلفه غیرصفر آن برابر ۱ است .

[2] Galois field

◄

$$n \stackrel{\text{df}}{=} |\mathcal{A}| = \frac{q^m - ۱}{q - ۱}.$$

◄ تقاطع مجموعه $\mathcal{A}$ با زیرفضای دو بعدی از F^m تحت عنوان یک خط تعبیر می‌شود و اندازه هر خط $q+۱$ است. مجموعه‌ی خطوط به همراه مجموعه‌ی نقاط $\mathcal{A}$ تشکیل یک ساختار تقاطع را می‌دهند که به این ساختار هندسه تصویری[۳] $PG(m-۱,q)$ گویند.

◄ تقاطع مجموعه‌ی $\mathcal{A}$ با زیرمجموعه ۳ بعدی F^m را صفحه می‌نامند.

◄

$$\Pi \stackrel{\text{df}}{=} \left\{\pi^{(۱)}, \pi^{(۲)}, \ldots, \pi^{(m)}\right\} \stackrel{\text{df}}{=} \left\{(۱,۰,\ldots,۰),(۰,۱,۰,\ldots,۰),\ldots,(۰,\ldots,۰,۱)\right\},$$

پایه اساسی در F^m می‌باشد.

◄ عناصر F^n را با علامت خطی بالای مؤلفه‌های اندیس‌دار عناصر مجموعه‌ی $\mathcal{A}$ نشان می‌دهیم. ما فرض می‌کنیم که m مؤلفه‌ی اول دارای اندیس‌های $\pi^{(۱)}, \pi^{(۲)}, \ldots, \pi^{(m)}$ هستند، در حالی‌که $n-m$ مؤلفه‌ی دیگر به صورت ثابت و دلخواه می‌باشند.

◄ $\{e^{-\delta}\}_{\delta\in\mathcal{A}}$ یک پایه اساسی در F^n است که در آن $\bar{e}^{(\pi^{(i)})} = \left(\pi^{(i)}, ۰^{(n-m)}\right)$، جایی‌که $۰^{(n-m)}$ همه‌ی بردارهای صفر از طول $n-m$ است.

◄ برای هر $\alpha = (\alpha_۱, \ldots, \alpha_m) \in F^m$ تعریف می‌کنیم:

$$\bar{\alpha} \stackrel{\text{df}}{=} (\alpha, ۰^{n-m}) \in F^n,$$

علاوه‌بر این داریم:

$$\bar{\alpha} = \sum_{i=۱}^{m} \alpha_i \bar{e}^{(\pi^{(i)})}.$$

◄ همسایگی $\Omega(M)$ یک مجموعه‌ی $M \subset F^n$، مجموعه‌ای از بردارها در فاصله‌ی ۱ تا M می‌باشد.

◄ کد همینگ H_m از طول n، مجموعه‌ای از بردارهای $\bar{c} \in F^n$ تعریف می‌کنیم که در رابطه‌ی زیر صدق می‌کند:

$$\sum_{\alpha\in\mathcal{A}} \bar{c}_\alpha \alpha = ۰^m. \qquad (۱.۲)$$

[3] Projective geometry

- $$supp(\bar{c}) = \Big\{\delta \in \mathcal{A} \,|\, \bar{c}_\delta \neq \circ\Big\}.$$

- $$T \stackrel{\text{df}}{=} \Big\{\bar{c} \in H_m \,|\, |supp(\bar{c})| = ۳\Big\}.$$

- $$T_\delta \stackrel{\text{df}}{=} \Big\{\bar{c} \in T \,|\, \bar{c}_\delta = ۱\Big\}.$$

- δ مؤلفه‌ی خطی، که آن را با نماد R_δ نمایش می‌دهیم به صورت $R_\delta = \langle T_\delta \rangle$ تعریف می‌کنیم. منظور از δ مؤلفه‌ی یک کد همینگ، هر هم‌دسته‌ای از δ مؤلفه‌ی خطی می‌باشد که زیرمجموعه‌ای از کد همینگ می‌باشد.

- برای هر l از $\dot{F}^m$، i مؤلفه‌ی خطی از H را برای هر $\alpha \in F^m \setminus \langle l \rangle$، به صورت زیر تعریف می‌کنیم؛

$$R_l := \Big\{\bar{c} \in H \,|\, c_\alpha = c_{\alpha+l}\Big\},$$

توجه داشته باشید که R_l یک زیرکد خطی از H برای هر l می‌باشد.

۲.۲ کدهای کامل و کدهای همینگ

کدهای کامل دسته مهمی از کدها هستند که در حالت مرزی کران همینگ صدق می‌کنند. در اواخر دهه‌ی ۱۹۴۹ ریچارد همینگ به این نکته پی‌برد که تکامل بیشتر کامپیوترها نیاز به قابلیت اطمینان بیشتری دارند، به‌خصوص توانایی تشخیص و تصحیح خطاها را داشته باشد. در آن زمان ماتریس کنترل توازن برای تشخیص خطا مورد استفاده قرار می‌گرفت ولی نتوانست هیچ خطایی را تصحیح کند. او کدهای همینگ را که دسته‌ای مهم از کدهای کامل می‌باشند و ۱ـ تصحیح‌گر خطا می‌باشند را طراحی نمود و با ادامه تحقیقات روی کدهای همینگ، این کدها به کدهای ۱ـ تصحیح‌گر خطا و ۲ـ تصحیح‌گر خطا تعمیم داده شد. کدهای همینگ به طور گسترده‌ای در محاسبات، ارتباطات و دیگر کاربردها از جمله؛ فشرده‌سازی اطلاعات و کدهای توربو کاربرد دارد. اکنون به اثبات قضیه‌ی کران همینگ[۴] می‌پردازیم و در ادامه تعاریف و مفاهیم مربوط به کدهای کامل را ارائه می‌دهیم.

[4] Hamming bound

قضیه ۱.۲.۲. فرض کنیم $q > ۱$ عددی صحیح و n و d اعدادی صحیح باشند، به گونه‌ای که $۱ \leq d \leq n$ داشته باشیم آن‌گاه همواره داریم:

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=۰}^{\lfloor \frac{d-۱}{۲} \rfloor} \binom{n}{i}(q-۱)^i}.$$

برهان. فرض کنیم A یک الفبای qـعنصری باشد $(|A| = q > ۱)$ و $C = \{c_۱, c_۲, \ldots, c_M\}$ یک کد بهینه باشد، یعنی داشته باشیم $M = A_q(n,d)$.
با فرض $e = \lfloor \frac{d-۱}{۲} \rfloor$، گوی‌های n بعدی به مرکز کدواژه‌های C_i $(۱ \leq i \leq M)$ و به شعاع e، دو به دو مجزا می‌باشند. یعنی $S_A(c_i, e)$ دو به دو مجزا می‌باشند، لذا داریم:

$$\bigcup_{i=۱}^{M} S_A(c_i, e) \subseteq A^n,$$

چون $S_A(c_i, e)$ دو به دو مجزایند، آن‌گاه:

$$\Big|\bigcup_{i=۱}^{M} S_A(c_i, e)\Big| = \sum_{i=۱}^{M} |S_A(c_i, e)| \leq q^n = |A^n|,$$

اما از قبل بنابر گزاره (۱.۲.۱) می‌دانیم که $S_A(c_i, e) = V_q^n(e)$. لذا داریم:

$$M. \sum_{i=۰}^{e} \binom{n}{i}(q-۱)^i \leq q^n.$$

چون کد C بهینه است، بنابراین $M = A_q(n,d)$، در نتیجه خواهیم داشت:

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=۰}^{\lfloor \frac{d-۱}{۲} \rfloor} \binom{n}{i}(q-۱)^i}.$$

□

تعریف ۱.۲.۲. یک کد qـتایی که تعداد کدواژه‌های آن برابر با مرز کران همینگ می‌باشد را یک کد کامل[۵] می‌نامند. در واقع یک کد کامل دارای

$$\frac{q^n}{\sum_{i=۰}^{\lfloor \frac{d-۱}{۲} \rfloor} \binom{n}{i}(q-۱)^i},$$

کدواژه می‌باشد. لذا یک کد کامل بیشترین تعداد کدواژه را خواهد داشت، یعنی

$$|C| = A_q(n,d) = \frac{q^n}{\sum_{i=۰}^{\lfloor \frac{d-۱}{۲} \rfloor} \binom{n}{i}(q-۱)^i}.$$

[5] Perfect code

بنابر رابطه بالا و با در نظر گرفتن اثبات قضیه کران همینگ داریم:

$$q^n = |C|.\sum_{i=۰}^{\lfloor \frac{d-۱}{۲} \rfloor} \binom{n}{i}(q-۱)^i = |C|.V_q^n(e) \quad \Rightarrow \quad |A^n| = |C|.V_q^n(e).$$

همان‌طور که در اثبات قضیه گفته شد $V_q^n(e)$ تعداد بردارهای یک گوی به مرکزیت C_i و شعاع e است، لذا خواهیم داشت:

$$A^n = \bigcup_{i=۱}^{|C|} S_A(c_i, e),$$

بنابراین اجتماع گوی‌های مجزا به مرکزیت اعضای C و به شعاع e برابر با A^n می‌باشد.
کد C به عنوان زیرمجموعه‌ای از A^n کامل است، هرگاه اجتماع گوی‌های مجزا به مرکزیت اعضای C و به شعاع e برابر با A^n باشد و اگر این اجتماع گوی‌ها را با $K(C)$ نمایش دهیم، لذا برای هر دو بردار $z, y \in K(C)$ داریم $K(z) \cap K(y) = \varnothing$.
به عبارت دیگر کد C کامل است هرگاه A^n با گوی‌های به مرکزیت اعضای C و به شعاع e افراز گردد. اگر یک کد با مینیمم فاصله ۳ و در نتیجه کدی ۱ـ تصحیح‌گر خطا باشد، آن‌گاه $e = ۱$ می‌باشد.

مثال ۱.۲.۲. موارد زیر نمونه‌هایی از کدهای کامل می‌باشند:

* کد $C = {F_q}^n$ باشد، در این‌صورت داریم: $M = |C| = q^n$.
* کد دودویی $C = \{۰, ۱\}$.
* اگر کد C کدی با اندازه $(M = |C| = ۱)$ باشد، لذا در این‌صورت کد C یک کد کامل می‌باشد.
* کدهای تکراری، به طور مثال کد $C = \left\{۰۰۰ \dots ۰, ۱۱ \dots ۱\right\}$.

کدهای همینگ، مشهورترین کدهای تصحیح‌گر خطا می‌باشند، این کدها خطی و کامل بوده و دقیقاً ۱ـ تصحیح‌گر خطا می‌باشند، به طوری‌که یک (n, k, d) ـ کدخطی qـ تایی است، جایی‌که $n = \frac{q^m - ۱}{q - ۱}$ و $k = n - m$ و چون کدهمینگ یک کد کامل می‌باشد لذا $d = ۳$ می‌باشد و داریم؛

$$(\frac{q^m - ۱}{q - ۱}, \frac{q^m - ۱}{q - ۱} - m, ۳),$$

در فصل ۳ روند ساختار ماتریس کنترل توازن را توضیح داده‌ایم.

قضیه ۲.۲.۲. برای کدهای همینگ دودویی داریم؛

- ✓ همه‌ی کدهای همینگ دودویی که با یک طول به دست می‌آیند هم‌ارز می‌باشند.
- ✓ بعد کد همینگ دودویی با m سطر، $k = ۲^m - ۱ - m$ است.
- ✓ فاصله‌ی کدهمینگ دودویی $d = ۳$ است، جایی‌که دقیقاً ۱ــ تصحیح‌گر خطا می‌باشد.
- ✓ کد همینگ دودویی، کد کامل است.

ملاحظه ۱.۲.۲. بنابر تعریف (۶.۲.۱) و تعریف (۲۳.۲.۱) خواهیم داشت؛

$$R(c) = ۱ - \frac{m}{n}.$$
$$\delta(c) = \frac{۲}{n}.$$

بنابراین $R(c)$ به سمت ۱ و $\delta(c)$ به سمت ۰ میل می‌کند و می‌توان دید که دقیقاً ۱ــ تصحیح‌گر خطا می‌باشد.

۳.۲ ساختار تبدیل

شهودی‌ترین روش برای ساختن یک کد ۱ــ کامل غیرخطی بدین صورت می‌باشد که با یک کد همینگ H_m شروع کرده و یک مجموعه‌ی منتخب از کدواژه‌ها مانند $S \subset H_m$ به یک مجموعه‌ی دیگری از کلمات مانند S' تغییر دهیم، به گونه‌ای که کد حاصل، یعنی

$$C = \Big(H_m \backslash S\Big) \cup S',$$

هم‌چنان یک کد ۱ــ کامل باقی بماند.
این ایده از جهت‌های مختلف به منظور ساختن کدهای ۱ــ کامل دودویی تعمیم یافته است (مرجع [۵] را ببینید). در مرجع [۴] اتزیون یکی از این تکنیک‌ها را برای ساختن کدهای ۱ــ کامل استفاده کرده است و در اینجا برای بیان نشاندن و افراز در کدهای کامل qــ تایی می‌توان از این تکنیک بهره‌مند شد.
فرض کنیم $GF(q) = \{۰, \alpha^۰, \alpha, \ldots, \alpha^{q-۲}\}$ باشد، جایی‌که α یک عنصر اولیه است و e_i برداری یکه از طول n می‌باشد که در آن همه‌ی مؤلفه‌ها برابر با صفر می‌باشند جز مؤلفه‌ی iام که برابر ۱ می‌باشد. فرض کنیم C یک کد ۱ــ کامل qــ تایی باشد و $C + \alpha^j e_i$ گرفته شده از C باشد و T_i بیانگر زیرفضای تولید شده توسط بردارهای ۳ تایی که مؤلفه‌ی iام آن‌ها ۱ است و برای برخی $x_i \in C$، $T_i + x_i \subseteq C$ باشد. قصد داریم تبدیل را به عنوان فرآیندی که همدسته‌ی[۶] $T_i + x_i$ با

[۶] Coset

همدسته‌ی $T_i + x_i + \alpha^j e_i$ جایگزین می‌کند، معرفی نماییم. در نتیجه کد C' را به صورت زیر تعریف می‌کنیم؛

$$C' = \Big(C \setminus (T_i + x_i)\Big) \cup \Big(T_i + x_i + \alpha^j e_i\Big),$$

جایی‌که $i \in \{۱, ۲, \ldots, n\}$ و $j \in \{۰, ۱, \ldots, q-۲\}$ می‌باشند.

گزاره ۱.۳.۲. کد qـ تایی همینگ H_m از طول $n = \frac{q^m - ۱}{q - ۱}$ داده شده است، فرض کنیم $T_i, x_i \in H_m$، آن‌گاه $C' = \big(H_m \setminus (T_i + x_i)\big) \cup \big(T_i + x_i + \alpha^j e_i\big)$ برای هر $i \in \{۱, ۲, \ldots, n\}$ و $j \in \{۰, ۱, \ldots, q-۲\}$ یک کد ۱ـ کامل qـ تایی غیرخطی است.

برهان. می‌توان دید که C' غیرخطی است، کد C' دارای تعداد کدواژه‌هایی به اندازه q^{n-m} می‌باشد، که مطلوب ما می‌باشد. به برهان خلف فرض کنیم که مینیمم فاصله ۳ نباشد و فرض کنید که $c \in H_m \setminus (T_i + x_i)$ باشد به طوری‌که برای برخی $y \in T_i + x_i + \alpha^j e_i$، $d(c, y) \leq ۲$ باشد. پس $d(y - c, ۰) \leq ۲$ و $y - c \in H_m + \alpha^j e_i$ و این بدین معنی است که $y - c \in T_i + \alpha^j e_i$ می‌باشد، از آن‌جایی که که کلمه‌های با وزن کمتر یا مساوی ۲ در $H_m + \alpha^j e_i$ دقیقاً کلمات $v + \alpha^j e_i$ هستند، جایی‌که v یک ۳تایی است که شامل α^j در مؤلفه‌ی iام آن می‌باشد یا زمانی که $v = ۰$ باشد.
لذا $y \in T_i + \alpha^j e_i + c = T_i + \alpha^j e_i + x_i$ می‌باشد یا به عبارت دیگر $c \in T_i + x_i$ می‌باشد، ولی $c \in H_m \setminus (T_i + x_i)$ می‌باشد، بنابراین فرض خلف باطل و مینیمم فاصله هنوز ۳ است. □

با اثبات گزاره بالا تبدیلی ساختیم که به وسیله‌ی آن می‌توانیم کد ۱ـ کامل qـ تایی دیگری داشته باشیم، به گونه‌ای که می‌توانیم $T_۱ + x_۱$ را با $T_۱ + x_۱ + \alpha^{j_۱} e_۱$ و $T_۲ + x_۲$ را با $T_۲ + x_۲ + \alpha^{j_۲} e_۲$ و ... و $T_m + x_m$ با $T_m + x_m + \alpha^{j_m} e_m$ جایگزین نماییم. ما می‌توانیم این کار را انجام دهیم اگر $T_i + x_i$ و $T_k + x_k$ برای همه‌ی $k \neq i$ همیشه مجزا باشند.

حال به بیان چند لم و قضیه می‌پردازیم که ما را برای پرداختن به موضوع نشاندن و افراز در کدهای کامل qـ تایی یاری می‌نمایند.

لم ۱.۳.۲. برای هر $\bar{z}$ از F^n ثابت می‌شود که

$$\Omega(R_l + \bar{z}) = \Omega(R_l + \bar{z} + \bar{e}^{(l)}).$$

برهان. بدون از دست دادن کلیت مسئله، فرض کنیم $\bar{z} = ۰^n$. بنابراین فرض می‌کنیم که $\bar{z} = ۰^n$ و $\bar{e}^{(۰^m)} := ۰^n$ نمادگذاری می‌کنیم و از آن‌جایی که $\bar{e}$ یک پایه‌ی طبیعی برای F^n

می‌باشد خواهیم داشت:

$$\Omega(R_l) = \bigcup_{\kappa\in F^m} (R_l + \bar{e}^{(\kappa)}) = \bigcup_{\kappa\in F^m} (R_l + \bar{e}^{(l)} + \bar{e}^{(\kappa+l)}) = \bigcup_{\lambda\in F^m} ((R_l + \bar{e}^{(l)}) + \bar{e}^{(\lambda)})$$
$$= \Omega(R_l + \bar{e}^{(l)}).$$

زیرا برای هر $\kappa \in F^m$ داریم که $\bar{e}^{(l)} + \bar{e}^{(\kappa)} + \bar{e}^{(\kappa+l)} \in R_l$ می‌باشد. □

لم ۲.۳.۲. هر عنصر $\bar{C}$ از $\langle R_l, R_\kappa\rangle$، برای هر $\alpha \in F^m \setminus \langle l, \kappa\rangle$، در ترکیب خطی

$$c_\alpha + c_{\alpha+l} + c_{\alpha+\kappa} + c_{\alpha+l+\kappa} = ۰, \qquad (۲.۲)$$

صدق می‌کند.

برهان. بنابر تعریف R_l داریم؛

$$R_l := \Big\{\bar{c} \in H \,|\, c_\alpha = c_{\alpha+l}\Big\},$$

که R_l یک زیرکد خطی از H برای هر l می‌باشد و

$$R_\kappa := \Big\{\bar{c} \in H \,|\, c_\alpha = c_{\alpha+\kappa}\Big\},$$

که R_κ یک زیرکد خطی از H برای هر κ می‌باشد، عناصر R_l و R_κ در رابطه‌ی (۲.۲) صدق می‌کند. بنابراین عناصر آن‌ها در فضای‌خطی رابطه‌ی (۲.۲) نیز صدق می‌کند. □

لم ۳.۳.۲. برای هر $l, \kappa \in \dot{F}^m$ با فاصله‌ی حداقل ۳ از ۰^m و l مؤلفه‌ی $R_l + \bar{l} + \bar{e}^{(l)}$ و κ مؤلفه‌ی $R_\kappa + \bar{\kappa} + \bar{e}^{(\kappa)}$ مجزا هستند و شامل ۰^n نیستند.

برهان. به دلایل عمومی جبری کافی است نشان دهیم که $\bar{w} = \bar{l} + \bar{e}^{(l)} + \bar{\kappa} + \bar{e}^{(\kappa)}$ به $\langle R_l, R_\kappa\rangle$ متعلق نیست.
فرض کنید j یک مؤلفه‌ی غیرصفر از $l+\kappa$ باشد و آن‌گاه $\pi^{(j)}$ اندیس مؤلفه‌ی غیرصفر $\bar{w}$ خواهد بود. اندیس‌های مؤلفه‌های غیرصفر دیگر متعلق به $\Pi \cup \{l, \kappa\}$ می‌باشند. اما از آن‌جایی که فاصله‌های متضاد بین $\kappa, l, ۰^m$ و $l + \kappa$ کمتر از ۳ نیست، اندیس‌های $\pi^{(j)} + l$، $\pi^{(j)} + \kappa$ و $\pi^{(j)} + l + \kappa$ به $\Pi \cup \{l, \kappa\}$ متعلق نیست. بنابراین داریم؛

$$w_{\pi^{(j)}} + w_{\pi^{(j)}+l} + w_{\pi^{(j)}+\kappa} + w_{\pi^{(j)}+l+\kappa} = ۱ + ۰ + ۰ + ۰ = ۱.$$

با استفاده از لم (۲.۳.۲) خواهیم داشت؛ $\bar{w} \notin \langle R_l, R_\kappa \rangle$. حال با استدلال مشابه می‌توان نشان داد که $R_l + \bar{l} + \bar{e}^{(l)}$ و $R_\kappa + \bar{\kappa} + \bar{e}^{(\kappa)}$ شامل $\circ^m$ نیستند. □

قضیه ۱.۳.۲. فرض کنید $C \subset F^m$ یک ۱ـ کد باشد که شامل $\circ^m$ می‌باشد و $\dot{C} := C \setminus \{\circ^m\}$. پس مجموعه

$$P(C) := \left(H \setminus \bigcup_{l \in \dot{C}} (R_l + \bar{l} + \bar{e}^{(l)}) \right) \cup \left(\bigcup_{l \in \dot{C}} (R_l + \bar{l}) \right),$$

یک کد ۱ـ کامل در F^n می‌باشد. بنابراین

$$C = \left\{ l \in F^m \,|\, (l, \circ^{n-m}) \in P(C) \right\} \qquad (۳.۲)$$

می‌باشد.

برهان. با توجه به تعریفی که از کد همینگ داشتیم، می‌توان نوشت:

$$H = \left\{ \bar{c} \in \{\circ, ۱\}^n \,\middle|\, \sum_{\alpha \in \dot{F}^m} c_\alpha \alpha = \circ^m \right\}$$

و $\bar{l} + \bar{e}^{(l)}$ به ازای هر l متعلق به H است؛ بنابراین برای هر l، $R_l + \bar{l} + \bar{e}^{(l)} \subset H$ می‌باشد. بنابر لم (۳.۳.۲) مجموعه‌های $R_l + \bar{l} + \bar{e}^{(l)}, l \in \dot{C}$ متقابلاً مجزا می‌باشند. از آن‌جایی که زیرمجموعه‌ای از کد ۱ـ کامل می‌باشند، دارای همسایگی‌های مجزا نیز می‌باشند. با استفاده از لم (۱.۳.۲) درستی این مطلب را می‌توان مشاهده کرد. لذا دیدیم که $P(C)$ یک کد ۱ـ کامل می‌باشد. به آسانی می‌توان دید که؛

- در کد H فقط یک کلمه به فرم $(\alpha, \circ^{n-m})$ وجود دارد که همه‌ی کلمه صفر می‌باشد. بنابراین فقط $\bar{l}$ به این فرم در $R_l + \bar{l}$ است، به طوری‌که؛

** اگر برای برخی $\kappa \in F^m$ داشته باشیم؛ $(\kappa, \circ^{n-m}) \in R_l + \bar{l}$، چون R_l خود زیرکد خطی از H می‌باشد و $l \in \dot{C}$ می‌باشد و طبق فرض نیز داریم؛ $\dot{C} := C \setminus \{\circ^m\}$ پس $\kappa = l$ می‌باشد. در واقع فرض می‌کنیم که $\bar{\kappa} = (\kappa, \circ^{n-m}) \in R_l + \bar{l}$ باشد، پس $\bar{\kappa} + \bar{l} \in R_l \subset H$ می‌باشد. بنابر $(*)$ ما داریم $\bar{\kappa} + \bar{l} = \circ^n$، بنابراین ادعای $(**)$ ثابت می‌شود.
از $(*)$ و $(**)$ نتیجه می‌گیریم که رابطه‌ی (۳.۲) مفهوم ضمنی تعریف $P(C)$ می‌باشد.

□

لم ۴.۳.۲. برای هر $\bar{z} \in F^n$ ثابت می‌شود که برای هر $\mu \in F$ داریم:

$$\Omega(R_\delta + \bar{z}) = \Omega(R_\delta + \bar{z} + \mu \bar{e}^{(\delta)}).$$

برهان. بدون از دست دادن کلیت مسئله، کافی است این جمله برای $\bar{z} = \circ^n$ ثابت شود. در مرجع [۱۱] نشان داده شده است که $(H_m \backslash R_\delta) \cup (R_\delta + \mu \bar{e}^{(\delta)})$ برای هر $\mu \in F$ یک کد ۱ـ کامل است. با استفاده از مفاهیم کد ۱ـ کامل همسایگی مجموعه‌های R_δ و $R_\delta + \mu \bar{e}^{(\delta)}$ با هم برابرند. پس حکم درست است. □

لم ۵.۳.۲. فرض کنید $\delta \in \mathcal{A}$ می‌باشد. هر کلمه‌ی $\bar{c}$ از R_δ در رابطه‌ی

$$\sum_{\alpha \in \mathcal{L}} \bar{c}_\alpha l(\alpha) = \circ, \tag{۴.۲}$$

برای همه‌ی توابع خطی l از F^m تا F صدق می‌کند به طوری‌که $l(\delta) = \circ$ و برای همه‌ی خطوط $\mathcal{L}$ شامل δ می‌باشد.

برهان. از آن‌جایی که R_δ یک زیرمجموعه از کد همینگ است، هر کدام از عناصر $\bar{c}$ در رابطه‌ی (۱.۲) صدق می‌کند. لذا رابطه‌ی

$$\sum_{\alpha \in \mathcal{A}} \bar{c}_\alpha l(\alpha) = \circ, \tag{۵.۲}$$

برای تمام توابع خطی l برقرار است. حال فرض کنید که $l(\delta) = \circ$ و خط $\mathcal{L}$ شامل δ را در نظر بگیرید. بنابراین نقاط غیرصفر هر بردار از T_δ شامل $\mathcal{L}$ خواهد بود یا با $\mathcal{L}$ در یک عنصر δ اشتراک خواهد داشت. برای حالت دوم رابطه‌ی (۴.۲) بدیهی است، در حالت اول به صورت بدیهی از رابطه‌ی (۵.۲) پیروی می‌کند. چون این رابطه برای هر عنصر T_δ برقرار است، با توجه به خطی بودن، این رابطه برای هر عنصر محدوده خطی T_δ برقرار است، همان‌طور برای محدوده R_δ برقرار است. □

لم ۶.۳.۲. فرض کنید $\delta, \kappa \in \mathcal{A}$ هستند. هر عنصر $\bar{c}$ از محدوده‌ی خطی $\langle R_\delta, R_\kappa \rangle$ در رابطه‌ی

$$\sum_{\alpha \in \mathcal{B}} \bar{c}_\alpha l(\alpha) = \circ, \tag{۶.۲}$$

برای همه‌ی توابع خطی l از F^m تا F به طوری‌که $l(\delta) = l(\kappa) = \circ$ می‌باشند و برای همه‌ی صفحات $\mathcal{B}$ که شامل δ و κ هستند، صدق می‌کند.

برهان. ابتدا حالت $\bar{c} \in R_\delta$ را در نظر بگیرید. رابطه‌ی (۴.۲) همه‌ی خطوط شامل δ و $\mathcal{B}$ را به طور خلاصه بیان کرده است و رابطه‌ی (۶.۲) را به دست می‌آوریم، بنابراین عناصر R_δ و به طور مشابه عناصر R_κ، در رابطه‌ی (۶.۲) صدق می‌کنند. با توجه به خاصیت خطی بودن، عناصر $\langle R_\delta, R_\kappa \rangle$ در رابطه‌ی (۶.۲) صدق می‌کنند. □

۴.۲ نشاندن درون کد ۱ـ کامل

گزاره ۱.۴.۲. فرض کنید که δ و κ از F^m هر دو از یک شروع شده و فاصله‌ی بین آن‌ها حداقل ۳ است. بنابراین δ مؤلفه‌ی $R_\delta + \bar{\delta} - \bar{e}^{(\delta)}$ و κ مؤلفه‌ی $R_\kappa + \bar{\kappa} - \bar{e}^{(\kappa)}$ از هم مجزا می‌باشند.

برهان. بردار تفاضل $\bar{c} = (\bar{\delta} - \bar{e}^{(\delta)}) - (\bar{\kappa} - \bar{e}^{(\kappa)})$ را در نظر بگیرید.
فقط کافی است نشان دهیم که $\bar{c} \notin \langle R_\delta, R_\kappa \rangle$. همچنین نشان خواهیم داد که $\bar{c}$ در رابطه‌ی (۶.۲) صدق نمی‌کند. توجه کنید که اولین عنصر $\bar{c}$ صفر است و $c_\pi^{(i)} \neq 0$ می‌باشد، اگر و تنها اگر $\delta_i \neq \kappa_i$ باشد. در بین مؤلفه‌های دیگر (که از Π نمی‌باشند)، $\bar{c}$ دقیقاً دارای دو جایگاه غیرصفر δ, κ می‌باشد. حال تعدادی i درنظر بگیرید، به طوری‌که $c_\pi^{(i)} \neq 0$ باشد. توجه کنید که $\pi^{(i)}, \delta$ و κ مستقل‌خطی هستند. (یک ترکیب خطی غیر بدیهی از δ و κ در اولین مکان غیرصفر خواهند بود یا یک مضربی از $\delta - \kappa$ می‌باشند، که حداقل دارای سه مکان غیرصفر است و در نتیجه با $\pi^{(i)}$ مطابقت نمی‌کند). از این‌رو صفحه‌ی یکتای $\mathcal{B}$ وجود دارد که شامل $\pi^{(i)}, \delta, \kappa$ است.
حال نشان می‌دهیم که $\pi^{(i)}, \delta$ و κ تنها نقاط $\mathcal{B}$ هستند که $\bar{c}$ در آن‌ها برابر صفر نیست. در واقع فرض کنید که $\beta = h\pi^{(i)} + a\delta + b\kappa \in \mathcal{A}$ است. اگر $a + b \neq 0$ باشد، پس $\beta_1 \neq 0$ است و در این‌صورت $\beta \in \{\delta, \kappa\}$ است یا $c_\beta = 0$ می‌گردد. اگر $a + b = 0$ باشد، لذا $a\delta + b\kappa = a(\delta - \kappa)$ و بنابراین با فرض دانستن گزاره بالا، این ترکیب شامل حداقل ۳ نقطه غیرصفر خواهد بود. دراین مورد β دارای حداقل ۲ مکان غیرصفر است و به Π متعلق نخواهد بود. بنابراین $c_\beta = 0$ است. لذا یک تابع خطی l را در نظر می‌گیریم به طوری‌که $l(\delta) = l(\kappa) = 0 \neq l(\pi^{(i)})$ و می‌بینیم که رابطه‌ی (۶.۲) نمی‌تواند یک جمع غیرصفر داشته باشد و $\alpha = \pi^{(i)}$. □

مثال ۱.۴.۲. فرض کنید $q = 5, m = 4$، $\delta = (1,3,3,3), \kappa = (1,1,0,1)$ باشند. لذا

$$\bar{c} = (\bar{\delta} - \bar{e}^{(\delta)}) - (\bar{\kappa} - \bar{e}^{(\kappa)}) = (0,2,3,2,0,\ldots,0,4,0,\ldots,0,1,0,\ldots,0).$$

می‌باشد که در آن ۴ و ۱، به ترتیب δ امین و κ امین مکان می‌باشند. $i = 2$ در نظر بگیرید، بنابراین $c_\pi(i) = 2 \neq 0$. بردارهای $\pi^{(2)} = (0,1,0,0)$. $\delta = (1,3,3,3)$ و $\kappa = (1,1,0,1)$ مستقل‌خطی می‌باشند، پس آن‌ها با هم صفحه $\mathcal{B}$ را مشخص می‌کنند. توجه کنید که مکان‌های دیگر در $\bar{c}$ غیرصفر هستند، به طوری‌که $\pi^{(3)} = (0,0,1,0)$ است و $\pi^{(4)} = (0,0,0,1)$ و آن‌ها متعلق به $\mathcal{B}$ نیستند، زیرا آن‌ها ترکیب خطی از $\delta, , \pi^{(2)}$ و κ نیستند. یک تابع خطی l روی F^m به صورت $l(\delta) = l(\kappa) = 0 \neq l(\pi^{(2)})$ تعریف می‌کنیم.
برای مثال $l(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_2 + \alpha_3 - \alpha_1$ است. اکنون می‌بینیم که (۶.۲) برقرار نمی‌باشد. تنها جمع غیرصفر در سمت چپ برابر ۲ است، بنابراین $\bar{c} \notin (R_\delta, R_\kappa)$.

ملاحظه ۱.۴.۲. با فرض این‌که δ و κ با ۱ شروع می‌شوند، لازم است که در گزاره (۱.۴.۲) برای $q > ۳$ باشد. به طور مثال فرض کنید که $\kappa = (t, t^۲, t^۲) = t(۱, t, t) = t\gamma, \delta = (۱, ۱, ۱)$ که در آن $t^۲$ از اختلاف ۱ و t است، بنابراین $(q \geq ۴)$. لذا بردارهای $\bar{\delta}$ و $\bar{\kappa}$ با فاصله‌ی ۱ از مؤلفه‌ی δام، $R_\delta + \bar{\delta} - \bar{e}^{(\delta)}$ و مؤلفه‌ی γام، $R_\gamma + \bar{\kappa} - t\bar{e}^{(\gamma)}$ به ترتیب از کد همینگ می‌باشند. به آسانی می‌توان دید که مؤلفه‌های غیرصفر $\bar{c} = (\bar{\delta} - \bar{e}^{(\delta)}) - (\bar{\kappa} - t\bar{e}^{(\gamma)})$ و γ بنابر تفاضل $\delta, \pi^{(۳)}, \pi^{(۲)}, \pi^{(۱)}$ متعلق به صفحه می‌باشند. بنابراین چون این تفاضل از کد همینگ می‌باشد، می‌بینیم که در رابطه‌ی (۶.۲) صدق می‌کند. به راحتی می‌توان نتیجه گرفت که مؤلفه‌های متناظر با هم اشتراک دارند.

قضیه ۱.۴.۲. فرض کنید $C \subset F^{m-۱}$ یک ۱ـ کد باشد.
مجموعه‌ی $\dot{C}$ را بدین‌صورت تعریف می‌کنیم: $\dot{C} \stackrel{\text{df}}{=} \{(۱, x) \,|\, x \in c\}$. بنابراین مجموعه‌ی

$$P(C) \stackrel{\text{df}}{=} \left(H_m \Big\backslash \bigcup_{\delta \in \dot{C}} (R_\delta + \bar{\delta} - \bar{e}^{(\delta)}) \right) \cup \left(\bigcup_{\delta \in \dot{C}} (R_\delta + \bar{\delta}) \right),$$

یک کد ۱ـ کامل در F^n می‌باشد و علاوه‌بر آن ،

$$C = \Big\{ x \in F^{m-۱} \,|\, (۱, x, \circ^{n-m}) \in P(C) \Big\}. \tag{۷.۲}$$

برهان. به یاد داریم که کد همینگ از طول n به صورت مجموعه‌ای از بردارهای $\bar{c} \in F^n$ تعریف می‌شود و برای هر $\delta \in \mathcal{A}$، داریم $\bar{\delta} - \bar{e}^{(\delta)} \in H_m$. این بدین معنی است که برای هر δ، داریم $R_\delta + \bar{\delta} - \bar{e}^{(\delta)} \subset H_m$. مطابق با گزاره (۱.۴.۲) مجموعه‌های $R_\delta + \bar{\delta} - \bar{e}^{(\delta)}$ برای هر $\delta \in \dot{C}$ مجزا هستند. در نتیجه آن‌ها زیرمجموعه‌ی کد ۱ـ کامل هستند، همچنین همسایگی‌های آن‌ها مجزا می‌باشد. با توجه به لم (۴.۳.۲) می‌بینیم که $P(C)$ یک کد ۱ـ کامل می‌باشد.
برای اثبات (۷.۲) باید توجه کرد که $\bar{C} = (\alpha, \circ^{n-m}) \in H_m$ و بیان می‌دارد که $\alpha = \circ^m$ که از تعریف کد همینگ پیروی می‌کند. نهایتاً نشان می‌دهیم که اگر برای برخی $x \in F^{m-۱}$ داشته باشیم؛ $(۱, x, \circ^{n-m}) \in R_\delta + \bar{\delta}$، آن‌گاه $(۱, x) = \delta$. در واقع اگر $(۱, x, \circ^{n-m})$ باشد، بنابراین $(۱, x, \circ^{n-m}) - \bar{\delta} \in R_\delta \subset H_m$ می‌باشد، که در آن برای $(۱, x) = \delta$ ثابت می‌شود. □

قضیه ۲.۴.۲. فرض کنید $(C_۱, \ldots, C_k)$ یک افراز از $F^{m-۱}$ به ۱ـ کدها باشد. آن‌گاه یک افراز $(P_۱, \ldots, P_{q^m})$ از F^n به کدهای ۱ـ کامل از طول $n = \frac{(q^m - ۱)}{q - ۱}$ وجود دارد که تساوی

$$C_j = \{ x \in F^{m-۱} \,|\, (۱, x, \circ^{n-m}) \in P_j \}, \tag{۸.۲}$$

برای هر $j = ۱, \dots, k$ برقرار می‌باشد.

برهان. فرض کنید برای هر α از F^m، H_α هم‌دسته‌ای از کدهای همینگ باشد که شامل $\bar{\alpha}$ می‌باشد و از آن‌جایی که

$$\bar{\alpha} = \sum_{i=۱}^{m} \alpha_i \bar{e}^{(\pi^{(i)})}$$

می‌باشد و $\bar{e}^{(\pi^{(i)})}$ پایه‌ی اساسی از F^n است، بنابراین مجموعه‌ی $\{H_\alpha\}_\alpha \in F^m$ افرازی از F^n است. حال فرض کنید k بردار مجزای $y_۱, \dots, y_k$ از $F^{m-۱}$ انتخاب کنیم و توجه کنید که برای هر $j = ۱, \dots, k$، $\alpha_j = (۰, y_j)$ می‌باشد. با استفاده از قضیه‌ی (۱.۴.۲) به جای کد H_{α_j} با $P_j \overset{\text{df}}{=} p(C_j - y_j) + \bar{\alpha}_j$ کار می‌کنیم. در این‌صورت بنابر قضیه‌ی (۱.۴.۲) خواهیم داشت:

$$P_j = \left(H_m \Big\backslash \bigcup_{\delta \in \dot{C} - \alpha_j} (R_\delta + \bar{\delta} - \bar{e}^{(\delta)}) \right) \cup \left(\bigcup_{\delta \in \dot{C} - \alpha_j} (R_\delta + \bar{\delta}) \right) + \bar{\alpha}_j.$$

به طورکلی رابطه‌ی (۸.۲) بسط رابطه‌ی (۷.۲) می‌باشد. حال چیزی که باقی می‌ماند این است که باید دیگر هم‌دسته‌های کد همینگ را جایگزین کنیم تا این‌که افراز را به دست آوریم.
بنابر تعریف P_j، $j \leq k$ می‌باشد، P_j با این هم‌دسته‌های کد همینگ اشتراک دارد: به‌گونه‌ای که با $H_{\alpha_j} = H_m + \bar{\alpha_j}$ و به ازای هر x از C_j، با $H_{(۱,x)}$، که دارای مؤلفه‌ی مشترک $R_\delta + \bar{\delta} + \bar{\alpha}_j$ با P_j می‌باشد، جایی‌که $\delta = (۱, x) - \alpha_j$ می‌باشد.
حال فرض کنید O_x با حذف این مؤلفه از $H_{(۱,x)}$ به دست آید و با جایگزین کردن مؤلفه‌ی متناظر از H_{α_j} خواهیم داشت:

$$O_x \overset{\text{df}}{=} \left(H_{(۱,x)} \backslash (R_\delta + \bar{\delta} + \bar{\alpha}_j) \right) \cup \left(R_\delta + \bar{\delta} + \bar{\alpha}_j - \bar{e}^{(\delta)} \right).$$

می‌بینیم که کدهای P_j و O_x، به تعداد $|C_j| + ۱$ می‌باشند، چون $x \in C_j$ است و به تعداد $|C_j|$، x داریم و از روی آن‌ها کد ساختیم و اسم آن‌ها O_x می‌باشد و تعداد O_x به اندازه C_j است و یک P_j هم داریم، بنابراین تعداد کل آن‌ها برابر با $|C_j| + ۱$ می‌باشد و متقابلاً مجزا هستند و داریم؛

$$P_j \cup \bigcup_{x \in C_j} O_x = H_{\alpha_j} \cup \bigcup_{x \in C_j} H_{(۱,x)}.$$

پس کدهای P_j، برای هر $j = ۱, \dots, k$ همراه با کدهای O_x، که $x \in F^{m-۱}$ می‌باشد و کدهای H_α جایی‌که α با ۱ شروع نمی‌شود و با همه‌ی α_jها به ازای هر $j = ۱, \dots, k$ متفاوت است، یک افراز از F^n را تشکیل می‌دهند. همان‌طور که در بالا اشاره شد رابطه‌ی (۸.۲) اثبات شد. □

توجه کنید که چون تعداد k از کدها در افراز اصلی می‌تواند به نسبت تا حدودی بزرگ باشد، تا $q^{m-۱}$، طول n که برای آن عمل نشاندن ممکن باشد نمی‌تواند کوچک باشد: تعداد

$(q-۱)n+۱$ از کدهای کامل در افراز به دست آمده نمی‌تواند کوچکتر از $q^{m-۱}$ باشد. بنابراین $n \geq \frac{q^{m-۱}-۱}{q-۱}$ می‌باشد و می‌توان دید که ساختار ما یک نشاندن با تقریباً طول مینیمم $\frac{q^m-۱}{q-۱}$ می‌باشد. با استفاده از روشی مشابه در قضیه (۲.۴.۲) و بر اساس نتایج مرجع‌های [۲] و [۱۳] می‌توان نشاندن‌های با طول مینیمم به ترتیب برای حالت‌های $q=۲$ و $q=۳$ ارائه کرد.

با کمی افزایش طول نشاندن، نتایج مرجع [۲] تعمیم داده می‌شود (هر ۱ـ کد دودویی می‌تواند در یک کد ۱ـ کامل نشانده شود) و همچنین برخی از نتایج مرجع [۱۳] تعمیم داده می‌شود (هر ۱ـ کد سه‌تایی یا ۲ـ کد qـ تایی می‌تواند در یک کد ۱ـ کامل نشانده شود). سرانجام، توجه کنیم که قضیه (۲.۴.۲) کلی‌ترین حالت بیان شده برای تعمیم قضیه (۱.۴.۲) می‌باشد. همان‌طور که در مرجع [۲] بیان شده است، نتایج کلاسیک مرجع‌های [۱۶] و [۶] در مورد نشاندن در سیستم‌های سه‌تایی اشتاینر[۷] و سیستم‌های چهارتایی اشتاینر می‌توانند به عنوان حالت‌های خاصی از این قضیه باشند .

[7] Steiner

فصل ۳

نشاندن کدهای با وزن ثابت در کدهای کامل qـ تایی

۱.۳ مقدمه

در این فصل با توجه به این‌که بحث اصلی و مورد توجه ما نشاندن کدهای با وزن ثابت در کدهای کامل qـ تایی می‌باشد، بنابراین در ابتدا مفاهیم اولیه مورد نیاز را بیان می‌نماییم و در ادامه به بررسی نشاندن کدهای با وزن ثابت در کدهای کامل qـ تایی می‌پردازیم.
در مرجع [۲] نشان داده شده است که، هر کد دودویی با طول m و مینیمم فاصله ۳ در برخی کدهای ۱ـ کامل دودویی با طول $n = ۲^m - ۱$ نشانده می‌شود.
در مرجع [۱۳] نشان داده شده است که، هر کد دودویی با طول $m+k$ و مینیمم فاصله $۳k+۳$ در کد ۱ـ کامل دودویی با طول $n = ۲^m - ۱$ نشانده می‌شود و این‌که هر کد ۳تایی با طول m و مینیمم فاصله ۳ در برخی کدهای ۱ـ کامل ۳تایی با طول $n = \frac{۳^m - ۱}{۲}$ نشانده می‌شود.
همچنین در مرجع [۱۳] اثبات شده است که هر کد qـ تایی با طول m و مینیمم فاصله ۵ در برخی کدهای ۱ـ کامل qـ تایی با طول $n = \frac{q^m - ۱}{q - ۱}$ نشانده می‌شود.
در مرجع [۸] اثبات شده است که هر کد qـ تایی با طول $m - ۱$ و مینیمم فاصله ۳ در برخی کدهای ۱ـ کامل با طول $n = \frac{q^m - ۱}{q - ۱}$ نشانده می‌شود.
در مرجع [۱۳] قابلیت نشاندن کدهای qـ تایی که با مینیمم فاصله ۵ ساخته شده‌اند نشان

داده شده است.
در این فصل نشان می‌دهیم که هر کد qـ تایی با وزن ثابت از وزن ۳ و مینیمم فاصله ۴ و طول m در کد ۱ـ کامل qـ تایی با طول $n = \frac{q^m-1}{q-1}$ نشانده می‌شود و بنابر مرجع [۸]، ما با معرفی محدودیت‌های اضافی، حداقل فاصله کد را کاهش می‌دهیم.

۲.۳ مفاهیم اولیه

به یاد داریم F_q یک میدان متناهی از مرتبه‌ی q و ${F_q}^n$ فضای برداری متشکل از تمام nـ تایی‌های روی F_q باشد:

$$ {F_q}^n = \Big\{ x = (x_1, \dots, x_n) \,|\, x_i \in F_q \Big\}. $$

بنابراین ${F_q}^n$ فضای برداری از بعد n روی میدان F_q می‌باشد. در فصل قبل بیان کردیم یک کد C کد ۱ـ کامل qـ تایی نامیده می‌شود، اگر برای هر $x \in {F_q}^n$ یک کدواژه منحصربه فرد $c \in C$ موجود باشد، به طوری‌که $d(x,c) \leq 1$.
کدهای ۱ـ کامل qـ تایی غیربدیهی با طول n وجود دارد، اگر $n = \frac{(q^m-1)}{(q-1)}$ باشد، جایی‌که $m \geq 2$ می‌باشد و حداقل فاصله‌ی کد ۱ـ کامل qـ تایی برابر با ۳ است که به صورت زیر اثبات می‌کنیم.

قضیه ۱.۲.۳. فرض کنیم $C \subseteq {F_q}^n$ یک کد ۱ـ کامل باشد، در این صورت فاصله کد C برابر با ۳ می‌باشد.

برهان. فرض کنیم $C \subseteq {F_q}^n$ یک کد ۱ـ کامل باشد. ابتدا نشان می‌دهیم که $d(C) \geq 3$. به برهان خلف، فرض کنیم $d(C) < 3$، یعنی $d(C) \leq 2$ و لذا کد C دارای دو کدواژه مانند

$$ x = (\dots, \alpha, \dots, \beta, \dots) \in C $$
$$ y = (\dots, \alpha', \dots, \beta', \dots) \in C, $$

می‌باشد به گونه‌ای که $\alpha \neq \alpha'$ و $\beta \neq \beta'$ و $d(x,y) = 2$. حال عنصر

$$ z = \{\dots, \alpha', \dots, \beta, \dots\} \in {F_q}^n, $$

در نظر بگیرید. به وضوح $d(z,x) = 1 = d(z,y)$، که این مطلب با تعریف کد ۱ـ کامل تناقض دارد. لذا فرض خلف باطل و بایستی داشته باشیم $d(C) \geq 3$.
حال ثابت می‌کنیم $d(C) \leq 3$. برای این منظور فرض کنیم $y = (y_1, y_2, \dots, y_n) \in C$ کدواژه

دلخواهی از کد C باشد. حال بردار $x \in {F_q}^n$ را به صورت زیر تعریف می‌کنیم:

$$x = (x_۱, x_۲, y_۳, \ldots, y_n) \in {F_q}^n,$$

جایی‌که $x_۱ \neq y_۱$ و $x_۲ \neq y_۲$. در این صورت واضح است که $d(x, y) = ۲$.
حال چون C کدی ۱ــ کامل می‌باشد، لذا کدواژه‌ای مانند $c \in C$ (به صورت منحصربه‌فرد) موجود است به گونه‌ای که $d(x, c) \leq ۱$. لذا داریم:

$$d(y, c) \leq d(y, x) + d(x, c) \leq ۲ + ۱ = ۳.$$

بنابراین $d(C) \leq ۳$ و اثبات کامل می‌شود.

□

دو کد $C_۱, C_۲ \subseteq {F_q}^n$ معادلند، هرگاه بردار $v \in {F_q}^n$ و ماتریس تک جمله‌ای[1] M (ماتریسی است که دقیقاً در هر سطر و ستون یک درایه غیرصفر دارد) از مرتبه n روی میدان F_q موجود باشند به طوری‌که $C_۲ = \{(v + cM) : c \in C_۱\}$.

فرض می‌کنیم که بردار صفر متعلق به کد باشد. حال با توجه به این‌که کدهای ۱ــ کامل غیرخطی‌اند و یک کد، خطی نامیده می‌شود اگر شامل زیرفضای خطی F_q باشد. کدهای ۱ــ کامل qــ تایی خطی که با طول n در حد هم‌ارزی یکتا هستند، کدهای همینگ qــ تایی نامیده می‌شوند. از فصل ۲ به یاد داریم که کد همینگ با طول $n = \frac{(q^m - ۱)}{(q - ۱)}$ می‌باشد که با $H_{q,m}$ نمایش داده می‌شوند و $m \geq ۲$ است و دارای پارامترهای q و m می‌باشد که هر کدواژه از اندازه n است و حداقل فاصله $d(c) = ۳$ می‌باشد.
کد همینگ را با استفاده از ماتریس کنترل توازن می‌سازیم و از آن‌جایی که در میدان F_q کار می‌کنیم و $F_q = \{\bar{۰}, \bar{۱}, \ldots, \overline{q - ۱}\}$ می‌باشد و $|F_q| = ۱$ است، اگر یک بردار mــ تایی روی F_q بخواهیم بسازیم، برای هر یک از آن‌ها q انتخاب داریم و در کل q^m حالت داریم و چون ماتریس کنترل توازن باید مستقل خطی باشد بردار صفر را خارج می‌کنیم، بنابراین $q^m - ۱$ بردار mــ تایی غیرصفر روی F_q داریم. ابتدا بردار اول را از F_q در نظر می‌گیریم. حال بردار دوم را بایستی به گونه‌ای در F_q در نظر بگیریم که بردار اول و بردار دوم مستقل خطی باشند، برای این منظور بردار دوم نباید در فضای تولید شده توسط بردار اول واقع شده باشد، یعنی نباید مضربی از بردار اول باشد و $۱, ۲, \ldots, q - ۱$ مضرب اسکالر می‌باشند، در نتیجه از تعداد $q^m - ۱$ بردار، $q - ۱$ بردار از محدوده‌ی انتخاب ما حذف می‌گردد و این بردارهای mــ تایی باقی‌مانده را در ستون‌های ماتریس می‌چینیم که طول آن‌ها m بود (تعداد سطرها) و بنابراین داریم؛

$$\frac{q^m - ۱}{q - ۱} = n\,,\ \frac{q^m - ۱}{q - ۱} - m = M,$$

[1] Monomial

در نتیجه یک ماتریس کنترل توازن با بعد m خواهیم داشت. از آن‌جایی که مجموع ابعاد یک کد با کد دوگان آن برابر با n می‌باشد، می‌توان به این نتیجه رسید؛

$$k = dim\, C = n - m.$$

در مرجع‌های [۴،۹،۱۵،۱۸] اثبات شده است که حداقل q^{qcn} یک عدد کافی برای کدهای ۱ـ کامل q تایی با طول n است.
وزن کلمه $x \in F_q^{\,n}$ برابر با فاصله بین x و ۰ می‌باشد. کد C دارای یک وزن ثابت k است، به شرط این‌که $x \in C$ باشد، بنابراین وزن کلمه x برابر با k می‌باشد.
فرض کنید $n_1 \leq n_2$ و $C_1 \subseteq F_q^{\,n_1}$ و $C_2 \subseteq F_q^{\,n_2}$ باشد. کدواژه‌های کد C_1 را با اضافه کردن صفر به انتهای کدواژه‌ها طولانی کرده و به طول n_2 می‌رسانیم، اگر همه کدواژه‌های طولانی شده در C_1 متعلق به C_2 باشد، در این صورت C_1 در C_2 نشانده می‌شود. توجه کنید که در C_2، $n_2 - n_1$ مؤلفه‌ی آخر همه کدواژه‌ها صفر می‌باشد، که با حذف کردن $n_2 - n_1$ صفر آخر کدواژه‌ها باز به کد C_1 می‌رسیم که در واقع می‌گوییم C_1 در C_2 به طور دقیق نشانده می‌شود. در این‌جا منظور ما از نشاندن، نشاندن به طور دقیق می‌باشد.

مثال ۱.۲.۳. فرض کنیم دو کد زیر مفروض باشند.
$C_1 = \{۱۱, ۰۱, ۱۰\}$ با $n_1 = ۲$ و $C_2 = \{۱۱۰۰, ۰۱۰۰, ۱۰۰۰, ۰۰۰۰, ۱۱۰۱, ۱۱۱۱\}$ با $n_2 = ۴$.
کدواژه‌هایی از کد C_2 که در انتهای آن‌ها $n_2 - n_1 = ۲$ صفر وجود دارد را مشخص نموده و ۲ صفر انتهای این کدواژه‌ها را حذف می‌کنیم و داریم؛ $C_2 = \{۱۱, ۰۱, ۱۰, ۰۰\}$. بنابراین کد C_1 در کد C_2 نشانده می‌شود. ولی این نشاندن به طور دقیق نیست، چون اگر بخواهیم به طور دقیق باشد باید کد C_1 هم دارای کدواژه‌ی $\{۰۰\}$ نیز باشد. زیرا اگر ۲ صفر انتهای کدواژه $\{۰۰۰۰\}$ را حذف کنیم، $\{۰۰\}$ تولید می‌شود که در کد C_1 وجود ندارد.

۳.۳ نشاندن کدهای با وزن ثابت در کدهای کامل qـ تایی

ماتریس کنترل توازن $H = [h_1, h_2, \ldots, h_n]$ از کد همینگ $H_{q,m}$ با طول $n = \frac{q^m - ۱}{q - ۱}$، شامل n جفت ستون مستقل‌خطی است که بردارهای h_i، $i \in \{۱, \ldots, n\}$. ${h_i}^T$ بردار ستون‌های انتقال یافته متعلق به ${F_q}^m$ می‌باشد، جایی‌که $i \in \{۱, \ldots, n\}$ است.
فرض می‌کنیم که ستون‌های H به صورت ثابت و دلخواه مرتب شده‌اند. با توجه به تعریفی که از هندسه‌ی تصویری در فصل ۲ داشتیم: مجموعه‌ی خطوط به همراه مجموعه‌ی نقاط $\mathcal{A}$ تشکیل یک ساختار تقاطع را می‌دهند، که به این ساختار هندسه‌ی تصویری گویند. حال

براساس تعریف هندسه تصویری مجموعه‌ی ${F_q}^m \setminus \{\circ\}$ هندسه‌ی تصویری $PG_{m-1}(q)$ از ابعاد $m-1$ روی میدان F_q تولید می‌کند. در این هندسه نقاط به صورت ستون‌های H می‌باشند. نقاط i و j و k روی یک خط مستقیم هستند اگر ستون‌های متناظر این نقاط یعنی h_i، h_j و h_k وابسته‌خطی باشند. خط مستقیم بین x و y را با $l_{x,y}$ نمایش می‌دهیم و $P_{x,y,z}$ صفحه تولید شده با ۳ نقطه غیرخطی x، y و z می‌باشد.

فرض کنیم $x = (x_1, \ldots, x_n) \in {F_q}^n$، مفروض باشد. پس نقاط غیرصفر بردار x در مجموعه‌ی $PG_{m-1}(q)$ مطابق ستون‌های $supp(x) = \{i \,|\, x_i \neq \circ\}$ می‌باشد. نقاط هندسه‌ی‌تصویری ماتریس کنترل توازن H وستون‌های H مطابق مؤلفه‌های فضای ${F_q}^n$ است. می‌گوییم که نقطه i متعلق به مجموعه‌ی $supp(x)$ است، اگر مؤلفه‌های نقطه i متعلق به مجموعه‌ی $supp(x)$ باشد.

یک بردار از وزن ۳ از کد همینگ $H_{q,m}$، یک سه‌تایی نامیده می‌شود. به پیروی از مرجع [۱۱]، زیرفضای تولید شده توسط مجموعه‌ی همه ۳ تایی‌هایی از کد $H_{q,m}$ که مؤلفه‌ی iام آن یک می‌باشد در نظر می‌گیریم و این زیرفضا را با R_i نمایش می‌دهیم و مجموعه‌ی $R_i + u$ مؤلفه iام از کد همینگ $H_{q,m}$ نامیده می‌شود. m ستون مستقل‌خطی از ماتریس کنترل توازن H از کد همینگ $H_{q,m}$ با طول $n = \frac{q^m-1}{q-1}$ انتخاب می‌کنیم، فرض کنید $\{h_1, h_2, \ldots, h_m\}$ ستون‌هایی باشند که انتخاب کرده‌ایم. حال $\Lambda \subset {F_q}^m$ یک کد qـ تایی با وزن ثابت از وزن ۳ با مینیمم فاصله ۴ و طول m در نظر بگیرید. فرض کنید Λ حاوی t بردار $(\lambda_1, \lambda_2, \ldots, \lambda_t)$ است، به طوری‌که وزن هر کدام برابر با ۳ می‌باشد. فاصله بین دو بردار متفاوت در $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_t\}$ حداقل ۴ است.

برای هر بردار $\lambda_s = (\lambda_{s_1}, \lambda_{s_2}, \ldots, \lambda_{s_m})$ از طول m، یک بردار u_s از طول n نظیر می‌کنیم، جایی‌که $s \in \{1, \ldots, t\}$ می‌باشد. قرار می‌دهیم

$$\mu_s hi_s = \lambda_{s_1} h_1 + \lambda_{s_2} h_2 + \cdots + \lambda_{s_m} h_m,$$

جایی‌که $\mu_s \in F_q$ و $i_s \in \{m+1, m+2, \ldots, n\}$ می‌باشد.

آنگاه داریم؛

$$u_s = (\lambda_{s_1}, \lambda_{s_2}, \ldots, \lambda_{s_m}, \circ, \ldots, \circ, -\mu_s, \circ, \ldots, \circ),$$

نقاط غیرصفر u_s متعلق به $\{1, 2, \ldots, m\} \cup \{i_s\}$ است.

از آن‌جایی که کد همینگ $H_{q,m}$ شامل فضای پوچ H می‌باشد، بنابر تعریف فضای پوچ داریم؛ $N(H) = \{c \in {F_q}^n \,|\, cH^T = \circ\} = C$ و همچنین با استفاده از قضیه (۳.۲.۱) خواهیم داشت: $u_s H^T = \circ$، بنابراین داریم $u_s \in H_{q,m}$.

توجه می‌کنیم که برای هر $\circ \neq x \in F^n$، یک h_i یکتا چنان وجود دارد که $x \in \langle h_i \rangle$ باشد. به عبارت دیگر $x = \gamma h_i$. لذا هر xای در n انتخاب کنیم داریم؛

$$\forall\, h_i \neq h_j, \langle h_i \rangle \cap \langle h_j \rangle = \{\circ\} \Rightarrow |\bigcup_{i=1}^{n} \langle h_i \rangle| = 1 + (q-1) \times n \leq |F^m| = q^m \Rightarrow n \leq \frac{q^m - 1}{q-1}.$$

ولی با توجه به این‌که در کد همینگ $n = \frac{q^m-۱}{q-۱}$ می‌باشد، بنابراین

$$\bigcup_{i=۱}^{n} \langle h_i \rangle = F^m.$$

لذا هر بردار $x \in F^n$ که در نظر بگیریم، x متعلق به مجموعه ستون‌های $\{h_۱, h_۲, \ldots, h_m\}$ نمی‌باشد. بنابر قضیه‌ی (۴.۲.۱) می‌توانیم نتیجه بگیریم که در اینجا هر دو ستون مستقل‌خطی می‌باشند و اگر اشتراک داشته باشند وابسته‌ی‌خطی می‌شوند. بنابراین توانستیم از بردارهایی به طول m در کد Λ خانواده‌ای از مؤلفه‌ها را به صورت زیر از کد همینگ $H_{q,m}$ با طول $n = \frac{q^m-۱}{q-۱}$ بسازیم؛

$$R_{i_۱} + u_۱, R_{i_۲} + u_۲, \ldots, R_{i_t} + u_t.$$

یک خانواده از این مؤلفه‌های $R_{i_۱} + u_۱, R_{i_۲} + u_۲, \ldots, R_{i_t} + u_t$ از یک کد همینگ $H_{q,m}$ را قابل قبول[۲] می‌نامیم، اگر تساوی $(R_{i_r} + u_r) \cap (R_{i_s} + u_s) = \varnothing$ برای هر $r, s \in \{۱, ۲, \ldots, t\}$ و $r \neq s$ برقرار باشد (مرجع [۱۴] را ببینید).
درادامه اثبات خواهیم کرد که گروهی از مؤلفه‌های ساخته شده از کد همینگ $H_{q,m}$ مذکور در فوق قابل قبول است.

در مرجع [۵] اتزیون[۳] و وردی[۴] پیشنهاد دادند که روش اصلی ساختن یک خانواده قابل قبول از کد همینگ دودویی را تغییر دهند. آن‌ها کدهای ۱ـ کامل ساختند که براساس این ساختار پیشنهادی بود. در مرجع [۱۳] این روش پیشنهادی به کدهای qـ تایی تعمیم داده شده است. قابل قبول بودن مورد مذکور برای خانواده‌ای از مؤلفه‌ها از کد همینگ $H_{q,m}$ که پایه‌ای برای تعمیم روش اتزیون و وردی می‌باشد در مرجع [۵] آمده است و در مرجع [۱۳] پیشنهاد داده شده است.

قضیه ۱.۳.۳. فرض کنید $s \in \{۱, ۲, \ldots, t\}$ باشد، همواره داریم $u_s \notin R_{i_s}$.

برهان. تعریف R_i را به صورت زیر داشتیم؛

$$R_i = \Big\{ x \in H_{q,m} \,|\, x_i = ۱, w(x) = ۳ \Big\}, x = \{x_۱, x_۲, \ldots, x_n\} \in F_q^n$$

و $supp(x) = \Big\{ i \,|\, x_i \neq ۰ \Big\}$ و همچنین داریم

$$u_s = (\lambda_{s_۱}, \lambda_{s_۲}, \ldots, \lambda_{s_m}, ۰, \ldots, ۰, -\mu_s, ۰, \ldots, ۰),$$

برای u_s داریم $supp(u_s) = \{۱, ۲, \ldots, m\} \cup \{i_s\}$. اگر $u_s \in R_{i_s}$ باشد، در این صورت u_s در مکان i_sام باید ۱ باشد. کد Λ شامل t بردار است که وزن هر کدام برابر ۳ است. در نتیجه h_{i_s} یک

[2] admissible
[3] Etzion
[4] Vardy

ترکیب خطی از ۳ ستون مجموعه‌ی $\{h_1, h_2, \ldots, h_m\}$ است و داریم $h_{i_s} = c_1 h_{l_1} + c_2 h_{l_2} + c_3 h_{l_3}$، جایی‌که $l_1, l_2, l_3 \in \{1, \ldots, m\}$ می‌باشد. بنابراین اگر به برهان خلف فرض کنیم؛ یک ترکیب خطی از h_x و h_{i_s} به صورت زیر در مجموعه‌ی $\{h_1, h_2, \ldots, h_m\} \setminus \{h_x\}$ بیافتد، در نتیجه خواهیم داشت؛

$$\alpha h_x + \beta h_{i_s} \in \{h_1, h_2, \ldots, h_m\} \setminus \{h_x\}.$$

از آن‌جایی که ستون‌های $\{h_1, h_2, \ldots, h_m\}$ مستقل‌خطی‌اند، لذا مستقل‌خطی بودن مجموعه $\{h_1, h_2, \ldots, h_m\}$ را نقض می‌کند. پس برای هر $x \in \{1, 2, \ldots, m\}$، هیچ ترکیب خطی از ستون‌های h_x و h_{i_s} متعلق به $\{h_1, h_2, \ldots, h_m\} \setminus \{h_x\}$ نیست.
بنابر قضیه‌ی ۱ در مرجع [۱۳] داریم ؛ اگر R_iای را در نظر بگیریم می‌دانیم که در R_i، u_i برابر با ۱ می‌باشد، چون در R_i مؤلفه‌ی iام برابر ۱ است و هر چیزی که در R_i انتخاب می‌شود باید این خاصیت را داشته باشد. حال با استفاده از این قضیه داریم؛ h_{i_s} یک ترکیب خطی از ۳ ستون مجموعه‌ی $\{h_1, h_2, \ldots, h_m\}$ می‌باشد و خود h_{i_s} هیچ یک از این ۳ ستون نیست و اگر $u_s \in R_{i_s}$ باشد، یک yای در مجموعه‌ی $\{1, \ldots, m\}$ وجود دارد که غیر از x و i می‌باشد و ترکیب خطی $\alpha h_x + \beta h_{i_s} = h_y$ وابسته‌ی‌خطی می‌شوند، در صورتی‌که این ۳ ستون نمی‌توانند وابسته‌ی‌خطی باشند، زیرا مستقل خطی بودن را نقض می‌کند. در نتیجه $u_s \notin R_{i_s}$. □

قضیه ۲.۳.۳. یک خانواده از مؤلفه‌های $R_{i_1} + u_1, R_{i_2} + u_2, \ldots, R_{i_t} + u_t$ از کد همینگ $H_{q,m}$ از طول n قابل قبول است.

برهان. فرض کنیم u کدواژه و R_i مجموعه باشد، بنابراین مؤلفه‌ی $R_{i_r} + u_r$ را به صورت زیر تعریف می‌کنیم؛

$$R_{i_r} + u_r = \Big\{ a + u_r \,|\, a \in R_{i_r} \Big\}.$$

حال به برهای خلف فرض می‌کنیم که؛

$$x \in (R_{i_r} + u_r) \cap (R_{i_s} + u_s)$$

باشد.
بنابر تعریف مؤلفه‌ی $R_{i_r} + u_r$ داریم؛

$$x \in R_{i_r} + u_r \longrightarrow \exists\, r_{i_r} \in R_{i_r} \quad s.t \quad x = r_{i_r} + u_r.$$
$$x \in R_{i_s} + u_s \longrightarrow \exists\, r_{i_s} \in R_{i_s} \quad s.t \quad x = r_{i_s} + u_s.$$

و لذا خواهیم داشت؛

$$u_r - u_s \in R_{i_r} + R_{i_s} \longrightarrow u_r - u_s = -(r_{i_r} - r_{i_s}) = -r_{i_r} + r_{i_s} \in R_{i_r} + R_{i_s}.$$

اگر x به اشتراک تعلق داشته باشد، بنابراین $u_r - u_s \in R_{i_r} + R_{i_s}$ می‌باشد ولی اشتراک تهی می‌باشد و $u_r - u_s \notin R_{i_r} + R_{i_s}$.
حال فرض کنید $r, s \in \{۱, ۲, \ldots, t\}$ و $r \neq s$ باشد، پس نشان می‌دهیم که

$$(R_{i_r} + u_r) \cap (R_{i_s} + u_s) = \varnothing. \qquad (۱.۳)$$

کافی است که ثابت کنیم؛

$$u_r - u_s \notin R_{i_r} + R_{i_s}. \qquad (۲.۳)$$

از قبل می‌دانیم که در واقع فاصله بین هر λ_r و λ_s حداقل ۴ می‌باشد $(d(\lambda_r, \lambda_s) = ۴)$، لذا حالت‌های زیر را در نظر می‌گیریم؛

حالت ۱. ابتدا فرض کنیم $d(\lambda_s, \lambda_r) \geq ۵$ باشد، در این‌صورت از ماتریس کنترل توازن کد همینگ H از طول $n = \frac{(q^m - ۱)}{(q-۱)}$، m ستون مستقل‌خطی انتخاب می‌کنیم. فرض کنیم که ستون‌های $\{h_۱, h_۲, \ldots, h_m\}$ را انتخاب کرده‌ایم و $(\Lambda \cup \{\vec{۰}\}) \subset {F_q}^m$ یک کد با t بردار غیرصفر $(\lambda_۱, \lambda_۲, \ldots, \lambda_t)$ باشد، که فاصله‌ی بین هر دو بردار متمایز از مجموعه‌ی $\Lambda = \{\lambda_۱, \lambda_۲, \ldots, \lambda_t\}$ بزرگ‌تر یا مساوی ۵ می‌باشد. برای هر بردار $\lambda_s = (\lambda_{s_۱}, \lambda_{s_۲}, \ldots, \lambda_{s_m})$ از طول m یک بردار u_s از طول n نظیر می‌کنیم، جایی‌که $s \in \{۱, \ldots, t\}$ می‌باشد.
قرار می‌دهیم

$$\mu_s hi_s = \lambda_{s_۱} h_۱ + \lambda_{s_۲} h_۲ + \cdots + \lambda_{s_m} h_m,$$

جایی‌که $\mu_s \in F_q$ و $i_s \in \{m+۱, m+۲, \ldots, n\}$ می‌باشد و

$$u_s = (\lambda_{s_۱}, \lambda_{s_۲}, \ldots, \lambda_{s_m}, ۰, \ldots, ۰, -\mu_s, ۰, \ldots, ۰),$$

نقاط غیرصفر u_s متعلق به $\{۱, ۲, \ldots, m\} \cup \{i_s\}$ است.
از آن‌جایی که کد همینگ $H_{q,m}$ شامل فضای پوچ H می‌باشد، آن‌گاه $u_s H^T = ۰$، بنابراین داریم $u_s \in H_{q,m}$. بنابراین توانستیم از بردارهایی به طول m در کد Λ خانواده‌ای از مؤلفه‌های

$$R_{i_۱} + u_۱, R_{i_۲} + u_۲, \ldots, R_{i_t} + u_t,$$

از کد همینگ $H_{q,m}$ از طول $n = \frac{q^m - ۱}{q-۱}$ بسازیم.

حالت ۲ . حال فرض کنیم که $d(\lambda_s, \lambda_r) = ۴$.

با استفاده از قضیه‌ی ۲ در مرجع [۱۳] برای درستی رابطه‌ی (۲.۳) کافی است ثابت کنیم که نقاط غیرصفر $u_r - u_s$ شامل برخی نقاط مثل x می‌باشد که بر روی خط راست $l_{i_r i_s}$ واقع نمی‌شوند و به طوری‌که هیچ نقطه دیگری (متفاوت با x و i_r و i_s) در این نقاط غیرصفر متعلق

به صفحه‌ی $P_{xi_ri_s}$ نیست. نقاط غیرصفر $u_r - u_s$ متعلق به $\{۱,۲,\ldots,m\} \cup \{i_r\} \cup i_s$ می‌باشد. فرض کنیم که یک xای متعلق به نقاط غیرصفر $u_r - u_s$ وجود داشته باشد، به طوری‌که روی خط راست $l_{i_ri_s}$ نیست، پس دارای این ویژگی می‌باشد که هیچ یک از i_r و i_s نمی‌باشد. چون اگر i_r یا i_s بود، در در این صورت x روی خط $l_{i_ri_s}$ می‌افتاد، در نتیجه $x \in \{۱,۲,\ldots,m\}$ می‌باشد. با توجه به قضیه‌ی ۲ در مرجع [۱۳] ما بایستی x را طوری انتخاب نماییم که هیچ ترکیب خطی از ستون‌های h_x, h_{i_r} و h_{i_s} متعلق به $\{h_۱, h_۲, \ldots, h_m\} \backslash \{h_x\}$ نباشد. چون اگر x در این مجموعه بیافتد، روی خط قرار می‌گیرد و h_x هم روی خط $l_{i_ri_s}$ می‌افتد، در حالی که نباید روی خط باشد.

حالت ۲.۱ . فرض کنید که اشتراک نقاط غیرصفر (λ_r) و نقاط غیرصفر (λ_s) شامل دو نقطه باشد، به طوری‌که

$$supp(\lambda_r) \cap supp(\lambda_s) = \{x_۱, x_۲\}. \qquad (۳.۳)$$

وزن (λ_r) و (λ_s) برابر با ۳ است و فاصله بین دو بردار برابر با ۴ می‌باشد. لذا دو ستون $h_{x_۱}$ و $h_{x_۲}$ از مجموعه‌ی ستون‌های مستقل‌خطی $\{h_۱, h_۲, \ldots, h_m\}$ می‌باشند.
به طور فرض اگر $x_۱$ در نقاط غیرصفر (λ_r) و $x_۲$ در نقاط غیرصفر (λ_s) باشند، پس $x_۱$ در ترکیب خطی (λ_r) و $x_۲$ در ترکیب خطی (λ_s) قرار می‌گیرند. در واقع دو ستون $h_{x_۱}$ و $h_{x_۲}$ در ساختار h_{i_r} و h_{i_s} می‌باشند. فرض کنید $h_{y_۱}$ در بین ستون‌های $\{h_۱, h_۲, \ldots, h_m\}$ آن ستونی باشد که در ساختار h_{i_r} می‌باشد، در حالی که ستون $h_{y_۲}$ در بین ستون‌های $\{h_۱, h_۲, \ldots, h_m\}$ تنها ستونی باشد که در ساختار h_{i_s} می‌باشد، به طوری‌که

$$supp(\lambda_r) \setminus supp(\lambda_s) = \{y_۱\}, \quad supp(\lambda_s) \setminus supp(\lambda_r) = \{y_۲\}, \qquad (۴.۳)$$

بنابراین همه ستون‌های $h_{x_۱}$ ، $h_{x_۲}$ ، $h_{y_۱}$ و $h_{y_۲}$ مجزا هستند و مستقل‌خطی‌اند.
فرض کنید $x \in \{x_۱, x_۲\}$ می‌باشد. چون u_s و u_r از λ ساخته شده‌اند، بنابراین زمانی که $u_r - u_s$ را بنویسیم، روی λها بحث می‌کند و از آن‌جایی که وزن λ_r و λ_s هر دو برابر با ۳ و فاصله بین بردارها ۴ می‌باشد، مجموعه نقاط $\{x_۱, x_۲\}$ متعلق به نقاط غیرصفر $u_r - u_s$ می‌شوند، بنابراین λ_r و λ_s صفر نیستند. بنابر دو رابطه (۳.۳) و (۴.۳) دیدیم که دو نقطه‌ی $x_۱$ و $x_۲$ هر دو در اشتراک بودند و بنابراین x هر کدام از دو نقطه‌ی $x_۱$ و $x_۲$ می‌تواند باشد و همچنین همه ستون‌های $h_{x_۱}$، $h_{x_۲}$، $h_{y_۱}$ و $h_{y_۲}$ مجزا و مستقل‌خطی بودند. بنابراین اگر h_{i_r} و h_{i_s} را در نظر بگیریم نقطه x هیچ وقت روی خط راست $l_{i_ri_s}$ قرار نمی‌گیرد و ستون‌های h_x، $h_{y_۱}$ و $h_{y_۲}$ مستقل‌خطی‌اند. نهایتاً بنابر دو رابطه (۳.۳) و (۴.۳) هیچ ترکیب خطی از ستون‌های h_x، h_{i_r} و h_{i_s} متعلق به $\{h_۱, h_۲, \ldots, h_m\} \setminus \{h_x\}$ وجود ندارد.

حالت ۲.۲ . چون وزن λ_r و λ_s برابر با ۳ است، یعنی ۳ مؤلفه‌ی غیرصفر دارد، بنابراین نقاط غیرصفر λ_r حداکثر ۳ عنصر و نقاط غیرصفر λ_s حداکثر ۳ عنصر می‌باشد و اگر اشتراک

این دو ۳ گردد، در این صورت برابر می‌شوند، که این اتفاق نمی‌افتد. در نتیجه یا در ۲ نقطه اشتراک دارند یا در یک نقطه اشتراک خواهند داشت. اشتراک نقاط غیرصفر λ_r و λ_s فقط شامل یک نقطه می‌باشد که با در نظر گرفتن حالت قبل چون λ_s و λ_r به ترتیب از u_s و u_r می‌آیند، لذا نقاط غیرصفر متعلق به $\{۱,۲,\dots,m\}\cup\{i_r\}\cup i_s$ می‌گردند، پس x متعلق به تفاضل متقارن

$$supp(\lambda_r)\triangle supp(\lambda_s),$$

می‌باشد، بنابراین برای هر $s\in\{۱,۲,\dots,t\}$ ، $r\neq s$ و $u_r-u_s\notin R_{i_r}+R_{i_s}$. لذا اثبات کامل است. □

حال قضیه نشاندن را اثبات می‌کنیم. توجه داشته باشید که e_i برداری یکه از طول n است که مؤلفه‌ی iام آن ۱ است و بقیه‌ی مؤلفه‌ها صفر هستند.
فرض کنیم؛

$$\mathcal{T}_{q,m}=\left(H_{q,m}\setminus\bigcup_{s=۱}^{t}(R_{i_s}+u_s)\right)\bigcup\left(\bigcup_{s=۱}^{t}(R_{i_s}+u_s+\mu_s.e_{i_s})\right). \qquad (۵.۳)$$

بنابر قضیه‌ی (۲.۳.۳) یک خانواده از مؤلفه‌های $R_{i_۱}+u_۱,R_{i_۲}+u_۲,\dots,R_{i_t}+u_t$ از کد همینگ $H_{q,m}$ قابل قبول است اگر $(R_{i_r}+u_r)\cap(R_{i_s}+u_s)=\varnothing$ باشد. در این صورت همسایگی‌های مجزا دارند. در نتیجه مجموعه‌ی $\mathcal{T}_{q,m}$ یک کد ۱ـ کامل qـ تایی با طول n می‌باشد (در مرجع‌های [۵،۱۱] ببینید). بنابر قضیه‌ی (۱.۳.۳)، $\mathcal{T}_{q,m}$ شامل بردار صفر است.

قضیه ۳.۳.۳. هر کد qـ تایی با وزن ثابت ۳ و با مینیمم فاصله ۴ و با طول m در برخی کدهای ۱ـ کامل qـ تایی با طول $n=\frac{q^m-۱}{q-۱}$ نشانده می‌شود.

برهان. توجه می‌کنیم که برای هر $۰\neq x\in F^n$، یک h_i یکتا چنان وجود دارد که $x\in\langle h_i\rangle$ باشد، به عبارت دیگر $x=\gamma h_i$. لذا هر xای در n انتخاب کنیم داریم؛

$$\forall\, h_i\neq h_j,\langle h_i\rangle\cap\langle h_j\rangle=\{۰\}\Rightarrow\Big|\bigcup_{i=۱}^{n}\langle h_i\rangle\Big|=۱+(q-۱)\times n\leq|F^m|=q^m\Rightarrow n\leq\frac{q^m-۱}{q-۱}.$$

ولی با توجه به این‌که در کد همینگ $n=\frac{q^m-۱}{q-۱}$ می‌باشد، بنابراین $\bigcup_{i=۱}^{n}\langle h_i\rangle=F^m$. لذا هر بردار $x\in F^n$ که در نظر بگیریم، x متعلق به مجموعه ستون‌های $\{h_۱,h_۲,\dots,h_m\}$ نمی‌باشد. در اینجا هر دو ستون مستقل‌خطی می‌باشند و اگر اشتراک داشته باشند وابسته‌ی‌خطی می‌شوند. بنابراین می‌توانیم از بردارهایی به طول m در کد Λ خانواده‌ای از مؤلفه‌ها از کد همینگ $H_{q,m}$ با طول $n=\frac{q^m-۱}{q-۱}$ بسازیم که برای هر $r\neq s$ و $r,s\in\{۱,۲,\dots,t\}$، تساوی

$$(R_{i_r}+u_r)\cap(R_{i_s}+u_s)=\varnothing,$$

برقرار می‌باشد و در این صورت همسایگی‌های مجزا دارند. در نتیجه مجموعه‌ی $\mathcal{T}_{q,m}$ یک کد ۱ـ کامل qـ تایی با طول n می‌باشد. طبق ساختاری که در بالا شرح داده شد، یک کد qـ تایی با وزن ثابت ۳ با مینیمم فاصله ۴ و طول m در نظر بگیرید.
فرض کنید Λ حاوی t بردار $(\lambda_1, \lambda_2, \ldots, \lambda_t)$ است، به طوری‌که وزن هر کدام برابر با ۳ می‌باشد. فاصله بین دو بردار متفاوت در $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_t\}$ حداقل ۴ است. برای هر بردار $\lambda_s = (\lambda_{s_1}, \lambda_{s_2}, \ldots, \lambda_{s_m})$ از طول m، یک بردار u_s از طول n نظیر می‌کنیم، جایی‌که $s \in \{1, \ldots, t\}$ می‌باشد. قرار می‌دهیم

$$\mu_s h i_s = \lambda_{s_1} h_1 + \lambda_{s_2} h_2 + \cdots + \lambda_{s_m} h_m,$$

جایی‌که $\mu_s \in F_q$ و $i_s \in \{m+1, m+2, \ldots, n\}$ می‌باشد.
آنگاه داریم؛

$$u_s = (\lambda_{s_1}, \lambda_{s_2}, \ldots, \lambda_{s_m}, 0, \ldots, 0, -\mu_s, 0, \ldots, 0),$$

نقاط غیرصفر u_s متعلق به $\{1, 2, \ldots, m\} \cup \{i_s\}$ است.
یک خانواده قابل قبول از مؤلفه‌های کد همینگ qـ تایی $H_{q,m}$ می‌سازیم و فرمول (۵.۳) نیز دلالت بر این دارد که هر کد qـ تایی Λ با وزن ثابت ۳، طول m و با مینیمم فاصله ۴ در کد ۱ـ کامل qـ تایی $\mathcal{T}_{q,m}$ از طول $n = \frac{q^m - 1}{q-1}$ نشانده می‌شود.

□

مراجع

[۱] پروانه مسیحا، سیدهاشم، احتمال، نظریه اطلاع و کدگذاری، انتشارات دانشگاه خواجه نصیرالدین طوسی، سال ۱۳۹۲.

[2] S. V. Avgustinovich and D. S. Krotov, Embedding in a perfect code, *J. Comb. Des.*, 17(5) (2009), 419–423.

[3] T. M. Cover and J. A. Thomas, *Elements of information theory*, John Wiley, New York (2006).

[4] T. Etzion, Nonequivalent q- ary perfect codes, *SIAM J. Discrete Math.*, 9(3) (1996), 413–423.

[5] T. Etzion and A. Vardy, Perfect binary codes: constructions, properties and enumeration, *IEEE Trans. Inform. Theory*, 40(3) (1994), 754–763.

[6] B. Ganter, Finite partial quadruple systems can be finitely embedded, *Discrete Math.*, 10(2) (1974), 397–400.

[7] G. A. Jones and J. M. Jones, *Information and coding theory*, Springer- Verlag , London (1946).

[8] D. S. Krotov and E. V. Sotnikova, Embedding in q- ary 1-perfect codes and partitions, *Discrete Math.*, 338(11) (2015), 1856–1859.

[9] B. Lindström, On group and nongroup perfect codes in q symbols, *Math. Scand.*, 25 (1969), 149–158.

[10] S. Ling and C. P. Xing, *Coding theory, A first course*, Cambridge University Press, New York (2004).

[11] K. T. Phelps and M. Villanueva, Ranks of q- ary 1-perfect codes, *Des. Codes. Cryptography*, 27(1-2) (2002), 139–144.

[12] A. M. Romanov, On the embedding of constant-weight codes into perfect codes, *J. Appl. Ind. Math.*, 10(4) (2016), 556–559.

[13] A. M. Romanov, On the admissible families of components of Hamming codes, *Diskretn. Anal. Issled. Oper.*, 19(2) (2012), 84–91.

[14] A. M. Romanov, A survey of methods for constructing nonlinear perfect binary codes, *Diskretn. Anal. Issled. Oper. Ser.*, 13(4) (2006), 68–88.

[15] J. Schönheim, On linear and nonlinear single-error-correcting q-ary perfect codes, *Inform. Control.*, 12 (1968), 23–26.

[16] C. Treash, The completion of finite incomplete steiner triple systems with applications to loop theory, *J. Comb. Theory, Ser. A.*, 10(3) (1971), 259–265.

[17] J. H. Vanlint, *An introduction to coding theory*, Third edition, *Springer* (1999).

[18] Yu. L. Vasilev, On nongroup close-packed codes, in *Problems of Cybernetics*, 8, Edited by A. A. Lya-Punov (Fizmatgiz, Moscow), (1962), 375–378.

واژه‌نامه فارسی به انگلیسی

۱-کد 1-code
الفبای کد . . . . . Code alphabet
اندازه کد . . . . . Code cardinality
افراز . . . . . Partition
بعد . . . . . Dimension
پایه . . . . . Basis
ترکیب خطی . . . . . Linear combination
زیرفضا . . . . . Subspace
فاصله . . . . . Distance
فاصله همینگ . . . . . Hamming distance
فضای برداری . . . . . Vector space
کانال پارازیت‌دار . . . . . Noisy channel
کد ۱-کامل . . . . . 1-Perfect code
کد با وزن ثابت . . . . . Constant-weight code
کد بلوکی . . . . . Block code
کد بهینه . . . . . Optimal code
کد تکرار . . . . . Repeat code
کد خطی . . . . . Linear code
کد دودویی . . . . . Binary code
کد دوگان . . . . . Dual code
کد کامل . . . . . Perfect code
کد کامل غیرخطی . . . . . Nonlinear perfect code
کدگذاری . . . . . Encoding
کدگشایی . . . . . Decoding
کدگشایی ماکزیمم احتمال . . . . . Maximum likelihood decoding
کدگشایی مینیمم فاصله . . . . . Minimum distance decoding

کد گولای ..... Golay code
کد غیرخطی ..... Nonlinear code
کدواژه ..... Codeword
کدهای با ماتریس کنترل توازن کم- چگال ..... Low- density parity check codes
کدهای پیچشی ..... Wrap codes
کدهای کانولوشنال ..... Convolutional codes
کدهای کوانتومی ..... Quantum codes
کدهای فضا- زمان ..... Space- time codes
کدهای تصحیح‌گر خطا ..... Error correcting codes
کد همینگ ..... Hamming code
کران همینگ ..... Hamming bound
ماتریس کنترل توازن ..... Parity-check matrix
مستقل‌خطی ..... Linearly independent
مؤلفه ..... Component
مینیمم فاصله ..... Minimum distance
نرخ ارسال اطلاعات ..... Information rate
نشاندن ..... Embedding
نظریه کدگذاری ..... Coding theory
وزن همینگ ..... Hamming weight
همدسته ..... Coset
هندسه تصویری ..... Projective geometry

واژه‌نامه انگلیسی به فارسی

۱-کد 1-code
کد ۱-کامل ..... 1-Perfect code
پایه ..... Basis
کد بلوکی ..... Block code
کد دودویی ..... Binary code
الفبای کد ..... Code alphabet
اندازه کد ..... Code cardinality
کدواژه ..... Codeword
نظریه کدگذاری ..... Coding theory
مؤلفه ..... Component
کد با وزن ثابت ..... Constant-weight code
کدهای کانولوشنال ..... Convolutional codes
همدسته ..... Coset
کدگشایی ..... Decoding
بعد ..... Dimension
فاصله ..... Distance
کد دوگان ..... Dual code
نشاندن ..... Embedding
کدگذاری ..... Encoding
کدهای تصحیح‌گر خطا ..... Error correcting codes
کد گولای ..... Golay code
کران همینگ ..... Hamming bound
کد همینگ ..... Hamming code
فاصله همینگ ..... Hamming distance
وزن همینگ ..... Hamming weight
نرخ ارسال اطلاعات ..... Information rate

کد خطی ..... Linear code
ترکیب خطی ..... Linear combination
مستقل‌خطی ..... Linearly independent
کدهای با ماتریس کنترل توازن کم ـ چگال ..... Low- density parity check codes
کدگشایی ماکزیمم احتمال ..... Maximum likelihood decoding
مینیمم فاصله ..... Minimum distance
کدگشایی مینیمم فاصله ..... Minimum distance decoding
کانال پارازیت‌دار ..... Noisy channel
کد غیرخطی ..... Nonlinear code
کد کامل غیرخطی ..... Nonlinear perfect code
کد بهینه ..... Optimal code
افراز ..... Partition
ماتریس کنترل توازن ..... Parity-check matrix
کد کامل ..... Perfect code
هندسه تصویری ..... Projective geometry
کدهای کوانتومی ..... Quantum codes
کد تکرار ..... Repeat code
کدهای فضاـ زمان ..... Space- time codes
زیرفضا ..... Subspace
فضای برداری ..... Vector space
کدهای پیچشی ..... Wrap codes

Abstract

The study of the perfect codes is important because of their interesting structure and properties. These codes are also very applicable in other sciences like telecommunication. In this thesis, we are going to show embedding and partitioning of 1 -perfect codes and constant-weight codes in the perfect code. We investigate embedding and partitioning in q-ary perfect codes. We will also indicate that 1-error-correcting code over a finite field can be embedded in a 1-perfect code of some larger length. Embedding in this context means that the original code is a subcode of the resulting 1-perfect code and can be obtained from it by repeated shortening. Further, the result is generalized to partitions: every partition of the Hamming space into 1-error-correcting codes can be embedded in partition of a space of some larger dimension into 1-perfect codes. For the partitions, the embedding length is close to the theoretical bound for the general case and optimal for the binary case.

Moreover, we show that each q-ary constant-weight code of weight 3, minimum distance 4, and length m embeds in a q-ary 1-perfect code of length $n = \frac{(q^m-1)}{(q-1)}$.

Keywords: Hamming code, Perfect code, Partitioning, Embedding, 1-Perfect code, Nonlinear perfect code, Constant-weight code.

Shahrood University of Technology

Faculty Of Mathematical Sciences

MSc Thesis in: Cryptography and Coding

Embedding and partitioning in q-ary perfect codes

By: Mohanna Ghaffari Sabil

Supervisors

Dr. Abdollah Alhevaz
Dr. Meysam Alishahi

Advisor

Prof. Ebrahim Hashemi

October 2019