دانشکده‌ی علوم

پایان نامه‌ی کارشناسی ارشد در رشته‌ی ریاضی محض (جبر)

تعمیمی از کدهای بلوکی خطی

به کوشش:

سمیرا روئین تن اصفهانی

اساتید راهنما:

دکتر حبیب شریف

دکتر شهره نمازی

شهریور ۱۳۹۰


بسم الله الرحمن الرحيم

به نام خدا

اظهار نامه

اینجانب سمیرا روئین تن اصفهانی دانشجوی رشته ریاضی محض گرایش جبر دانشکده علوم اظهار می‌کنم که این پایان نامه حاصل پژوهش خودم بوده و در جاهایی که از منابع دیگران استفاده کرده‌ام،نشانی دقیق و مشخصات کامل آن‌را نوشته‌ام. همچنین اظهار می‌کنم که تحقیق و موضوع پایان نامه‌ام تکراری نیست و تعهد می نمایم که بدون مجوز دانشگاه دستاوردهای آن‌را منتشر ننموده و یا در اختیار غیر قرار ندهم. کلیه حقوق این اثر مطابق با آیین نامه مالکیت فکری و معنوی متعلق به دانشگاه شیراز است.

نام و نام خانوادگی: سمیرا روئین تن اصفهانی

تاریخ و امضا: ۱۳۹۰/۱۲/۲۴

به نام خدا

تعمیمی از کدهای بلوکی خطی

به وسیله‌ی:

سمیرا روئین تن اصفهانی

پایان نامه
ارائه شده به تحصیلات تکمیلی دانشگاه شیراز به عنوان بخشی
از فعالیت های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته‌ی:

ریاضی محض

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی کمیته پایان نامه، با درجه‌ی: عالی

دکتر حبیب شریف استاد بخش ریاضی (رئیس کمیته).....

دکترشهره نمازی استادیار بخش ریاضی (رئیس کمیته).....

دکتر منصور دوست فاطمه استادیار بخش ریاضی.....

دکتر محمد حسن شیردره حقیقی استادیار بخش ریاضی.....

شهریور ۱۳۹۰

تقدیم به:

پدر و مادر عزیزم که مرا در این راه یاری نمودند.

سپاسگزاری

با سپاس فراوان از خداوند منان به خاطر لطف و رحمت بی کرانش و سپاس از همه عزیزانی که در طول مدت تحصیل مرا یاری نمودند، بویژه جناب آقای دکتر شریف و سرکار خانم دکتر نمازی که به عنوان اساتید راهنما در طول این مدت زحمات و راهنمایی‌های بی‌دریغشان هموار کننده مسیر بنده بوده است و سپاس فراوان خدمت اساتید محترم مشاور جناب آقای دکتر دوست فاطمه و جناب آقای دکتر شیردره و همچنین نماینده تحصیلات تکمیلی جناب آقای دکتر افشین امینی را دارم. شاید این مجموعه یادگار و نمایانگر سپاس بی‌پایان من نسبت به کمک های بی‌دریغ آنان به شمار آید.

چکیده:

تعمیمی از کدهای بلوکی خطی

توسط:

سمیرا روئین تن اصفهانی

هدف از انجام این پایان نامه بررسی تعمیمی از کدهای خطی می با شد. در این تعمیم هر کدواژه را به جای این‌که به صورت برداری که مؤلفه‌های آن متعلق به میدان متناهی F باشد در نظر بگیریم، به طور کلی به صورت برداری تعریف می کنیم که مؤلفه‌های آن خود، برداری روی میدان F هستند (مؤلفه‌ها لزوما از یک طول نیستند). سپس تعاریف و قضایای اولیه‌ای را که برای کدهای معمولی داشتیم برای این کدها تعمیم می دهیم. همچنین رابطه بین کدهای روی میدان‌های $F_{q'}$ و F_q را بدست می آوریم که $F_{q'}$ و F_q به ترتیب میدان‌های متناهی از مرتبه q' و q (q' توانی از q است) می باشند. در ادامه به بررسی یک دیدگاه جبری کدهای شبه دوری که تعمیمی از کدهای دوری‌اند می پردازیم. ایده اصلی این است که حلقه‌ای را معرفی می‌کنیم که می‌توان یک کد شبه دوری روی یک میدان متناهی را به صورت کدی خطی روی آن حلقه در نظر گرفت. این حلقه به حاصلجمع مستقیمی از میدان‌های متناهی تجزیه می‌شود. از این ویژگی برای ساختن کدهای جدید از روی کدهایی با طول کمتر استفاده می کنیم، که در بعضی حالات همان ساختارهای آشنای $(u+v|u-v)$ ، تورین یا واندرموند را بدست می دهد. بعلاوه ساختار کدهای خوددوگان شبه دوری را بررسی می کنیم و تعداد آن‌ها را برای بعضی حالات خاص بدست می آوریم.

فهرست مطالب

عنوان **صفحه**

فصل اول: مقدمه

۱-۱ مقدمه ۲

۱-۲ تعاریف و قضایای مقدماتی ۵

فصل دوم: تعمیمی از کدهای بلوکی خطی

۲-۲ کدهای بلوکی خطی و کران‌های همینگ و سینگلتون ۱۶

۲-۲ روابط میان کدهای روی میدان های F_q و $F_{q'}$ ۲۹

۲-۳ تعمیم مفهوم کد دوگان و شمارنده وزن ۳۴

فصل سوم: بررسی ساختار جبری کدهای شبه دوری

۳-۱ ناظر بین کدهای شبه دوری و کدهای روی حلقه R ۴۴

۳-۲ تجزیه حلقه $R := R(F, m)$ به حاصلضرب میدان های متناهی..... ۴۸

۳-۳ حالت های خاصی از کدهای شبه دوری ۷۱

۳-۴ کدهای دودویی $l-$شبه دوری از نوع دوم..... ۹۳

۳-۵ ساختار واندرموند..... ۹۶

فهرست منابع ۱۰۰

فصل اول

مقدمه

۱-۱ مقدمه

یکی از کاربردهای عمده میدان های متناهی، نظریه کدگذاری است. ابداع این نظریه به قضیه معروفی از شانون[1] باز می‌گردد که وجود کدهایی را تضمین می‌کند که می‌توانند اطلاعات را به میزان نزدیک به حداکثر ظرفیت کانال ارتباطی و با احتمال خطایی به اندازه کوچک انتقال دهند. یکی از هدف‌های نظریه جبری کدگذاری، یعنی نظریه کدهای تشخیص دهنده و تصحیح کننده خطا، ابداع روش‌هایی برای ساخت چنین کدهایی است.

در خلال دو دهه اخیر ابزارهای جبری بیشتر و بیشتری مانند نظریه میدان‌های متناهی و نظریه چند جمله‌ای‌ها روی میدان‌های متناهی، در کدگذاری اثر گذاشته‌اند. بررسی هرچه بیشتر خواص جبری کدها و بدست آوردن کدهایی با خاصیت جبری مناسب که فرآیند کدگذاری و کدگشایی برای آنها را ساده‌تر کند، بسیار مورد توجه است.

یکی از دسته کدها با خاصیت جبری مناسب کد دوری است. هدف اصلی ما در این پایان-نامه،بررسی کدهای شبه دوری که درواقع تعمیمی از کدهای دوری هستند می باشد.

این پایان نامه برگرفته از مراجع [۶] و [۱۲] می باشد.

در فصل دوم این پایان‌نامه کدهای بلوکی خطی را تعمیم می‌دهیم به طوری که هر واژه به طول n متعلق به F_q^n را به بلوکهایی به طول $n_1, n_2, \ldots, n_s$ که $(1 \le i \le s)\, n_i \in N$ و $n = n_1 + n_2 + \cdots + n_s$ تجزیه می‌کنیم یا به عبارتی واژه را متعلق به فضای برداری $F_q^{n_1} \oplus F_q^{n_2} \oplus \cdots \oplus F_q^{n_s}$ روی F_q در نظر می‌گیریم که اگر تمام n_iها را برابر با ۱ بگیریم

1. Shannon

همان تعریف اولیه واژه را داریم. این تعمیم از کدهای بلوکی خطی در رمزنگاری، انتگرال‌گیری عددی از بعدهای بالا و طراحی‌های آزمایشگاهی کاربرد دارد.

در ادامه کران‌های همینگ[۱] و سینگلتون[۲] و تعریف کد کامل و MDS[۳] را برای این کدها تعمیم می‌دهیم. در بخش دوم این فصل واژه‌ها را با بلوک‌هایی به طول مساوی $l \in N$ در نظر می‌گیریم و مهم‌ترین قضیه‌ی این فصل که رابطه‌ی بین کدهای روی F_{q^l} و کدهای روی F_q است را بیان می- کنیم.

در بخش سوم فصل ۲، مفهوم کدهای دوگان و شمارش‌گر وزن را تعمیم می‌دهیم.

در فصل سوم، تعمیمی از کدهای دوری به نام کدهای شبه‌دوری را معرفی می‌کنیم. کدهای شبه‌دوری بیش از چهل سال است که مورد مطالعه و بررسی قرار گرفته‌اند. در ابتدا این کدها به خاطر تنوع زیادی که داشتند مورد توجه قرار گرفتند [۱۰] و [۱۸] . سپس به عنوان کدهای باطول کم رکوردهای زیادی را بدست آوردند [۷] و [۸] . در [۵] و [۱۸] رابطه نزدیک آنها با کدهای کانولوشنال[۴] مورد بررسی قرار گرفتند. با اینکه مدت زیادی از شروع مطالعه این کدها می گذرد اما ساختار جبری آنها کمتر مورد توجه واقع شده است. در [۳]برای بررسی خواص جبری این کدها از ساختار مدول روی حلقه های متناهی استفاده کرده و در [۱۱] پایه‌های گرابنر را برای این منظور به کار برده است. ما در فصل سوم این پایان نامه که برگرفته از [۱۲] می باشد از تجزیه حلقه $R = \frac{F[Y]}{< Y^m - 1 >}$ به حاصل‌جمع مستقیمی از میدان‌های متناهی استفاده می کنیم. مزیت این شیوه این است که می توانیم کدهای شبه دوری را به گونه ای سیستماتیک بررسی کنیم و همچنین آنها را به کدهایی از طول کمتر تجزیه کنیم.

همان‌طور که می‌دانیم کدهای دوری به طول m را می‌توان به عنوان ایده‌الی از حلقه $R = \frac{F[Y]}{< Y^m - 1 >}$ در نظر گرفت. کدهای شبه دوری از اندیس l و طول ml که تعمیمی از کدهای دوری اند را می توان به عنوان زیرمدولی ازحلقه R^l در نظر گرفت. در واقع وقتی $l = ۱$

---

۱. Hamming
۲. Singletone
۳. Maximum distance Separable
۴. Convolutional

کد شبه دوری از اندیس ۱، همان کد دوری است. در بخش اول این فصل به همین بحث می‌پردازیم و مفهوم کد روی حلقه را بیان کرده و تناظر بین کدهای l–شبه دوری روی میدان F و کدهای خطی به طول l روی حلقه R را به دست می آوریم. در بخش دوم، حلقه R را به حاصل جمع مستقیم میدان‌های متناهی تجزیه کرده و هر کد شبه دوری را به حاصل‌جمع مستقیم کدهایی به طول l روی این میدان‌های متناهی نظیر می کنیم و سپس دوگان آن را بدست می‌آوریم.

همچنین ساختاری برای بدست آوردن کدهای شبه دوری روی F_q با استفاده از کدهای روی حلقه R ارائه می‌دهیم. در بخش سوم، حالت‌های خاص کدهای شبه دوری را بررسی کرده و تعداد کدهای خوددوگان شبه دوری را در این حالات بدست می‌آوریم. در بخش چهارم به مطالعه کدهای دودویی[۱] شبه دوری از نوع دوم می پردازیم و در بخش پنجم ساختار واندرموند[۲] را برای دسته ای از کدهای شبه دوری بدست می آوریم.

۱. Binary
۲. Vanderrmonde construction

۱-۲ تعاریف و قضایای مقدماتی

در کلیه فصل های این پایان نامه p یک عدد اول و q توانی از یک عدد اول و F_{q^i}، $(i \in N)$ میدانی متناهی از مرتبه q^i می باشند.

تعریف ۱-۲-۱: عناصر $\alpha, \beta \in F_{q^i}$ روی F_q مزدوج نامیده می شوند هرگاه هردو ریشه یک چندجمله ای تحویل ناپذیر تکین روی F_q باشند. یا به عبارت دیگر چندجمله ای مینیمال آن‌ها روی F_q یکی باشد.

قضیه ۱-۲-۲: مزدوج های متمایز $\alpha \in F_{q^m}$ روی F_q برابر است با $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ جایی که d کوچکترین عدد صحیح مثبتی است که $\alpha^{q^d} = \alpha$. در واقع d درجه چندجمله ای مینیمال α روی F_q می باشد.

تابع اثر

تعریف۱-۲-۳: فرض کنید $F = F_{q^m}$ و $K = F_q$. برای $\alpha \in F$، اثر یا رد α (روی K) را با $Tr_{\frac{F}{K}}(\alpha)$ نشان می دهند و به صورت $Tr_{\frac{F}{K}}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$ تعریف می کنند.

اگر K زیرمیدان اول F باشد، آنگاه $Tr_{\frac{F}{K}}(\alpha)$ را اثر مطلق α می نامند و آن را به صورت ساده $Tr_F(\alpha)$ نشان می دهند.

قضیه۱ -۲-۴: اگر $\alpha \in F_{q^m} = F$ و $K = F_q$، آنگاه $Tr_{\frac{F}{K}}(\alpha) \in K$.

اثبات. فرض کنید چندجمله‌ای $f \in K[Y]$ چندجمله ای مینیمال α روی K باشد. اگر $deg(f) = d$، آنگاه $F_{q^d} = F_q[\alpha]$ میدان شکافنده f روی F_q است. از طرفی از آنجا که $\alpha \in F_{q^m}$، بنابرین $F_{q^d} \prec F_{q^m}$ و طبق خواص توسیع میدان های متناهی، $d|m$. حال عناصر $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ را در نظر می گیریم. از آ نجا که $\alpha^{q^d} = \alpha$، درواقع این عناصر همان

$\alpha,\alpha^q,\ldots,\alpha^{q^{d-1}}$ می باشند که هرکدام $\frac{m}{d}$ بار تکرار شده اند. بنابر این در اصل عناصر فوق ریشه های چندجمله ای $g = f^{\frac{m}{d}}$ می باشند. چون ضرایب f متعلق به K است، ضرایب g نیز متعلق به K است. از طرفی طبق آنچه گفته شد $g=(Y-\alpha)+(Y-\alpha^q)+\cdots+(Y-\alpha^{q^{m-1}})$. واضح است که $Tr_{\frac{F}{K}}(\alpha)$، قرینه ضریب Y^{m-1} در چندجمله ای g می باشد. بنابراین $Tr_{\frac{F}{K}}(\alpha)\in K$.

قضیه۱-۲-۵: فرض کنید $F=F_{q^m}$ و $K=F_q$. در این صورت تابع اثر $Tr_{\frac{F}{K}}(\alpha)$ یک تبدیل خطی از F به روی K (تابعکی خطی و پوشا روی F) می باشد که خواص زیر را داراست:

الف) به ازای هر $\alpha\in K$، $Tr_{\frac{F}{K}}(\alpha)=m\alpha$.

ب) به ازای هر $\alpha\in F$، $Tr_{\frac{F}{K}}(\alpha^q)=Tr_{\frac{F}{K}}(\alpha)$.

اثبات. باتوجه به اینکه به ازای هر $\alpha\in F$، $Tr_{\frac{F}{K}}(\alpha)\in K$، $Tr_{\frac{F}{K}}$ نگاشتی از F به K است.

به ازای α و $\beta\in F$ داریم:

$$Tr_{\frac{F}{K}}(\alpha+\beta)=(\alpha+\beta)+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{m-1}}$$

$$=\alpha+\beta+\alpha^q+\beta^q+\cdots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \qquad \text{(زیرا } F \text{ از مشخصه } p \text{ است)}$$

$$=(\alpha+\alpha^q+\cdots+\alpha^{q^{m-1}})+(\beta+\beta^q+\cdots+\beta^{q^{m-1}})$$

$$=Tr_{\frac{F}{K}}(\alpha)+Tr_{\frac{F}{K}}(\beta)\ .$$

فرض کنید $c\in K$ بنابراین $c^q=c$ و در نتیجه برای هر i که $1\le i\le m$، $c^{q^i}=c$. پس

$$Tr_{\frac{F}{K}}(c\alpha)=c\alpha+c\alpha^q+\cdots+c\alpha^{q^{m-1}}$$

بنابراین $Tr_{\frac{F}{K}}$ یک تابعک خطی است. برای اثبات پوشا بودن این نگاشت کافی است نشان دهیم عضوی مانند α از F وجود دارد به گونه ای که $Tr_{\frac{F}{K}}(\alpha)\neq 0$. می دانیم $Tr_{\frac{F}{K}}(\alpha)=0$ اگر وتنها اگر α ریشه چندجمله ای $Y+Y^q+\ldots Y^{q^{m-1}}\in K[Y]$ در F باشد. ولی چون این چندجمله ای می تواند حداکثر q^{m-1} ریشه در F داشته باشد و F به تعداد q^m عضو دارد، نتیجه مطلوب حاصل می شود.

اگر $\alpha\in K$، آنگاه $\alpha^q=\alpha$. پس برای هر $1\leq i\leq m$، $\alpha^{q^i}=\alpha$. بنابر این

$$Tr_{\frac{F}{K}}(\alpha)=\alpha+\alpha^q+\ldots+\alpha^{q^{m-1}}=m\alpha$$

بدین ترتیب خاصیت (الف) برقرار است.

چون $\alpha\in F$، $\alpha^{q^m}=\alpha$. درنتیجه

$$Tr_{\frac{F}{K}}(\alpha^q)=\alpha^q+\alpha^{q^2}+\ldots+\alpha^{q^m}=Tr_{\frac{F}{K}}(\alpha)$$

بدین ترتیب خاصیت (ب) نیز اثبات می شود.

قضیه ۱-۲-۶: (قضیه تعدی اثر) فرض کنید K میدانی متناهی، F توسیعی متناهی از K و E توسیعی متناهی از F باشد. در این صورت به ازای هر $\alpha\in E$،

$$Tr_{\frac{E}{K}}(\alpha)=Tr_{\frac{F}{K}}\left(Tr_{\frac{E}{F}}(\alpha)\right).$$

اثبات. فرض کنید $K=F_q$، $[F:K]=m$ و $[E:F]=n$. دراین صورت بنابر قضیه برج در مبحث توسیع میدانها، $[E:K]=mn$. بنابراین به ازای $\alpha\in E$،

$$Tr_{\frac{F}{K}}\left(Tr_{\frac{E}{F}}(\alpha)\right)=\sum_{i=0}^{m-1}Tr_{\frac{E}{F}}(\alpha)^{q^i}=\sum_{i=0}^{m-1}\left(\sum_{j=0}^{n-1}\alpha^{q^{jm}}\right)^{q^i}=\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\alpha^{q^{jm+i}}=\sum_{k=0}^{mn-1}\alpha^{q^k}=Tr_{\frac{E}{K}}(\alpha)$$

کلیه تعاریف و قضایای مربوط به تابع اثر از مرجع [۲۰] آورده شده اند.

R–زیر مدول‌های حلقه R^l:

لم ۱-۲-۷: فرض کنید R_1 و R_2 دوحلقه باشند و $R = R_1 \oplus R_2$.

آنگاه $R_1^l \oplus R_2^l$، یک R–مدول می‌باشد و با $(R_1 \oplus R_2)^l$ به عنوان R–مدول یکریخت است.

اثبات. فرض کنید $a \in R_1^l$ و $b \in R_2^l$ و $r = (r_1, r_2) \in R$، تعریف می‌کنیم $r(a,b) = (r_1 a, r_2 b)$.

از آنجا که r به صورت منحصر به فردی به شکل (r_1, r_2) می‌باشد، پس عمل فوق خوش تعریف است. بقیه خواص مدول بودن به راحتی قابل بررسی است. پس $R_1^l \oplus R_2^l$ یک R–مدول می‌باشد. می‌دانیم که تابع $\varphi : R^l \to R_1^l \oplus R_2^l$ با ضابطه $\phi\left(\{r_i\}_{i=1}^l\right) = \{r_{i1}\}_{i=1}^l \oplus \{r_{i2}\}_{i=1}^l$، جایی که $r_i = (r_{i1}, r_{i2}) \in R_1 \oplus R_2$، $1 \le i \le l$ یکریختی حلقه‌ای است. به سادگی دیده می‌شود که این یک ریختی، یک ریختی R–مدولی نیز می‌باشد.

لم ۱-۲-۸: فرض کنید R_1 و R_2 دو حلقه یکدار باشند و $R = R_1 \oplus R_2$. آنگاه هر R–زیر مدول R^l، $(l \in N)$ به فرم $M_1 \oplus M_2$ است که M_1 یک R_1–مدول و M_2 یک R_2–مدول می‌باشند.

اثبات. اگر $R = R_1 \oplus R_2$، پس $R^l = (R_1 \oplus R_2)^l$ و طبق لم ۱-۲-۷ با $R_1^l \oplus R_2^l$ یک ریخت است. پس با تقریب یک ریختی R^l را با $R_1^l \oplus R_2^l$ یکی می‌گیریم.

فرض کنید M یک زیرمدول R^l باشد، اگر $M_1 = \pi_1(M)$ و $M_2 = \pi_2(M)$ که π_1 و π_2 تابع تصویر به ترتیب روی مؤلفه اول و دوم باشند، آنگاه نشان می‌دهیم $M = M_1 \oplus M_2$. از آنجا که M یک مدول است، پس یک گروه آبلی است بنابراین M_1 نیز گروه آبلی می‌باشد.

همچنین فرض کنید $r_1 \in R_1$ و $m_1 \in M$ دلخواه باشند. از آنجا که $M_1 = \pi_1(M) \le R_1^l$، پس $m_2 \in R_2^l$ وجود دارد به نحوی که $(m_1, m_2) \in M$. از آنجا که M زیرمدول R^l است، پس $(r_1, 0)(m_1, m_2) = (r_1 m_1, 0) \in M$، بنابراین $r_1 m_1 \in M_1$. لذا M_1 یک R_1–مدول است.

به طریق مشابه ثابت می شود که M_2 نیز یک R_2–مدول می‌باشد.

واضح است که $M \le M_1 \oplus M_2$. برعکس فرض کنید $(m_1, m_2) \in M_1 \oplus M_2$. از آنجا که $m_1 \in M_1 = \pi_1(M)$، $m_2' \in M_2$ وجود دارد به نحوی که $(m_1, m_2') \in M$. از طرفی از آنجا که R_1 حلقه‌ای یکدار است، پس $(1,0) \in R$. اما M یک R – مدول است. بنابراین $(1,0)(m_1, m_2') = (m_1, 0) \in M$.

به طریق مشابه داریم $(0, m_2) \in M$. پس $(m_1, 0) + (0, m_2) \in M$ و بنابراین $(m_1, m_2) \in M$. در نتیجه $M_1 \oplus M_2 = M$.

نتیجه۱-۲-۹: اگر R_i $(1 \le i \le n)$ حلقه‌های یکدار باشند و $R = \bigoplus_{i=1}^{n} R_i$، آنگاه هر R–زیر مدول R^l به شکل $\bigoplus_{i=1}^{n} M_i$ می‌باشد که هر M_i یک R_i – مدول است.

هم مجموعه‌های دایره بر:

تعریف ۱-۲-۱۰: فرض کنید $F = F_q$ و $(m,q) = 1$ و $i \in Z$. مجموعه $C_i = \{i, iq, ..., iq^{d-1}\}$ را امین هم مجموعه دایره بر برای q به سنج m، گویند، هرگاه d کوچک ترین عدد صحیح مثبت باشد به طوری که $iq^d \equiv i \pmod m$.

یک تناظر یک به یک بین تمام هم مجموعه‌های دایره بر برای q به سنج m و تمام شمارنده‌های تحویل‌ناپذیر $Y^m - 1$ در $F_q[Y]$ وجود دارد. زیرا می‌دانیم که اگر ξ یک ریشه mام اولیه واحد روی F_q باشد، آنگاه تمام ریشه‌های $Y^m - 1$ به صورت ξ^i برای یک $1 \le i \le m$ می‌باشند. فرض کنید C_i ، iامین هم مجموعه دایره بر باشد. پس $C_i = \{i, iq, ..., iq^{d_i - 1}\}$ که $d_i \in Z$ کوچکترین عددی است که $iq^{d_i} \equiv i \pmod m$. فرض کنید f شمارنده تحویل‌ناپذیر $Y^m - 1$ باشد به گونه‌ای که ξ^i یکی از ریشه‌های آن باشد. بنا بر قضیه ۱-۲-۲، تمام ریشه‌های f عبارتنداز $S_{C_i} = \{\xi^i, \xi^{iq}, ..., \xi^{iq^{d_i-1}}\}$ و واضح است که درجه f ، d_i می‌باشد.

از طرفی از آنجا که شمارنده‌های تحویل ناپذیر $Y^m - 1$ متمایزند، پس مجموعه ریشه‌های آن‌ها نیز متمایزند. پس نظیر هر مجموعه مانند S_{C_i}، تنها یک شمارنده تحویل‌ناپذیر $Y^m - 1$ وجود داردکه مجموعه ریشه‌هایش S_{C_i} می‌باشد و برعکس. از طرفی اگر $C_i = C_j$، آنگاه واضح

است که $S_{C_i} = S_{C_j}$ و برعکس. بنابراین نظیر هر چند جمله‌ای تحویل‌ناپذیر که شمارنده $Y^m - 1$ است، تنها یک هم مجموعه دایره بر وجود دارد و برعکس.

توجه کنید ممکن است که $i \neq j$ ولی $C_i = C_j$. بنابراین منظور از C_i تمام مجموعه‌های مساوی C_i می‌باشد. C_i $(1 \leq i \leq m)$ را به عنوان نماینده‌ای از کلاس این مجموعه‌ها در نظر می‌گیریم.

نکته ۱-۲-۱۱: اگر C_i $(1 \leq i \leq m)$ یک هم مجموعه دایره بر برای q به سنج m باشد و f شمارنده تحویل ناپذیر $Y^m - 1$ نظیر C_i باشد، آنگاه بنا بر آنچه گفته شد $|C_i| = \deg f$.

تعاریف و قضایای اولیه کد

تعریف ۱-۲-۱۱: فرض کنید $A = \{a_1, a_2, \ldots, a_q\}$ یک مجموعه متناهی باشد که به آن مجموعه الفبای کد می گوییم. هر عضو A^n یک واژه به طول n نامیده می شود. به هر زیرمجموعه غیر تهی C از A^n یک کد به طول n و به هر عضو C یک کدواژه گفته می شود.

تعریف ۱-۲-۱۲: فرض کنید A یک مجموعه الفبا و $x = (x_1, x_2, \ldots, x_n)$، $y = (y_1, y_2, \ldots, y_n)$ واژه هایی به طول n باشند. فاصله همینگ $\boldsymbol{x}$ و $\boldsymbol{y}$ را به صورت زیر تعریف کرده و با نماد $d(\boldsymbol{x}, \boldsymbol{y})$ نشان می دهیم.

$$d(x,y) = \left|\left\{1 \leq i \leq n \,\middle|\, x_i \neq y_i\right\}\right|$$

تعریف ۱-۲-۱۳: اگر C یک کد باشد، فاصله مینیمم کد C را به صورت زیر تعریف کرده وبا نماد $d_{\min}(C)$ نشان می دهیم.

$$d_{\min}(C) = \min\left\{d(x,y) \,\middle|\, x, y \in C \text{ و } x \neq y\right\}$$

تعریف ۱-۲-۱۴: فرض کنید F_q مجموعه الفبای کد و C یک زیرفضای برداری F_q^n باشد. دراین صورت به کد C یک کد خطی به طول n می گویند. اگر C از بعد k و مینیمم وزن d باشد به آن یک $[n,k,d]$-کد می‌گوییم.

تعریف ۱-۲-۱۵: فرض کنید C یک کد خطی روی F_q به طول n باشد و $x=(x_1,x_2,\ldots,x_n)\in C$ کدواژه ای متعلق به C باشد، در این صورت وزن x به صورت زیر تعریف می شود.

$$w(x)=\left|\{1\le i\le n \mid x_i\neq 0\}\right|$$

تعریف ۱-۲-۱۶: اگر C یک کد باشد، وزن مینیمم C را به صورت زیر تعریف می کنیم:

$$\min\{w(x)\mid x\in C \text{ و } x\neq 0\}$$

توجه کنید به راحتی دیده می شود که وقتی C یک کد خطی باشد مینیمم وزن و مینیمم فاصله کد C با هم برابرند.

تعریف ۱-۲-۱۷: ماتریس $k\times n$، G را یک ماتریس مولد برای کد خطی C گوییم هرگاه C از بعد k و فضای سطری G برابر C باشد.

تعریف ۱-۱-۱۸: اگر C یک $[n,k,d]$-کد خطی باشد تعریف می کنیم:

$$C^{\perp}=\{\beta\in F_q^n \mid \alpha.\beta=0,\forall\alpha\in C\}$$

و $C^{\perp}$ را دوگان کد C می نامیم.منظور از $\alpha.\beta$، ضرب اقلیدسی داخلی α و β می باشد.

قضیه ۱-۲-۱۹: اگر C یک $[n,k,d]$-کد خطی روی F_q باشد دراین صورت:

۱) $C^{\perp}$ یک $[n,n-k,d]$-کد خطی روی F_q است یعنی $\dim(C)+\dim(C^{\perp})=n$.

۲) $(C^{\perp})^{\perp}=C$

به هر ماتریس مولد $C^{\perp}$ که یک ماتریس $n-k\times n$ است یک ماتریس امتحان توازن کد C می‌گوییم و آن را با H نمایش می دهیم. واضح است که $GH^t=0$.

تعریف ۱-۲-۲۰: به $[n,k,d]$-کد C یک کد کامل گفته می شود هرگاه، $d=2t+1$ و $\sum_{i=0}^{t}\binom{n}{i}(q-1)^i=q^{n-k}$.

فرض کنید S_n گروه جایگشت ها روی مجموعه $\{1,2,\ldots,n\}$ باشد و $u=(u_1,u_2,\ldots,u_n)$ یک واژه به طول n روی F_q و $\sigma\in S_n$ یک جایگشت باشد، در این صورت منظور از $\sigma(u)$،

nتایی $\left(u_{\sigma(1)},u_{\sigma(2)},\ldots,u_{\sigma(n)}\right)$ می باشد. اگر C یک کد خطی به طول n روی F_q باشد، آنگاه منظور از $\sigma(C)$، $\sigma(C)=\left\{\sigma(u)\middle|\ u\in C\right\}$ می باشد.

تعریف ۱-۲-۲۱: دو کد خطی دودویی C و C' را معادل گویند هرگاه $C'=\sigma(C)$.

تعریف ۱-۲-۲۲: به هر $[n,k,d]$-کد خطی روی F_q به طوری که $n=\frac{q^r-1}{q-1}$، $k=n-r$ و $d=3$ یک کد همینگ می گوییم و آن را با $H_r(q)$ نمایش می دهیم.

اگر $q=2$ به آن کد همینگ دو دویی می گوییم. دسته کد همینگ به طور مستقل توسط گُلِی[1] در سال ۱۹۴۹ و ریچارد همینگ در سال ۱۹۵۰ کشف شد. کد همینگ، کدی کامل است و به راحتی کدگشایی می شود.

مثال ۱-۲-۲۳: کد دودویی با ماتریس مولد زیر یک $[7,4,3]$-کد است.

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

با توجه به مشخصات کد واضح است که این کد، کد همینگ $H_3(2)$ می باشد.

تعریف ۱-۲-۲۴: کد خطی C به طول n روی F_q را یک کد دوری گوییم هرگاه اگر $\left(c_1,c_2,\ldots,c_n\right)\in C$، آنگاه $\left(c_n,c_1,\ldots,c_{n-1}\right)\in C$.

فرض کنید کد خطی C یک کد دوری به طول n روی F_q باشد. به هر کدواژه $\left(c_1,c_2,\ldots,c_n\right)\in C$، چندجمله ای $c_0+c_1Y+\cdots+c_{m-1}Y^{m-1}$ را نظیر می کنیم. طبق این تناظر به سادگی ثابت می شود که هر کد دوری به طول m نظیر یک ایده آل از حلقه $R=\frac{F[Y]}{\langle Y^n-1\rangle}$ است.

---

[1]. Golay