دانشکده‌ی علوم پایه
گروه ریاضی
پایان‌نامه‌ی دوره‌ی کارشناسی ارشد ریاضی محض

نمایش جبر لی $sl(n,\mathbb{C})$ و نظریه‌ی کدگذاری

نگارش: کبری علی‌محمدی

استاد راهنما: دکتر حسام‌الدین شریفی
استاد مشاور: دکتر محمدرضا درفشه

بهمن ۱۳۹۰


بسم الله الرحمن الرحيم

تشکر و قدردانی

حمد و سپاس خدای را، آن نخستین بی‌پیشین را و آن آخرین بی‌پسین را، خداوندی را که آفریدگان را به قدرت خود ابداع کرد و به مقتضای مشیت خویش جامه‌ی هستی پوشید و به همان راه که ارادت او بود روان داشت و رهسپار طریق محبت خویش گردانید.

اکنون که به فضل خدا، نگارش این پایان‌نامه به پایان رسیده بر خود لازم می‌دانم که از زحمات استاد راهنمای صبور، خوش‌خلق و ارزش‌مندم، جناب آقای دکتر «حسام‌الدین شریفی» و هم‌چنین راهنمایی‌های استاد مشاور ارجمند، دانشمند گران‌قدر، جناب آقای دکتر «محمدرضا درفشه» سپاس‌گزاری کنم، و نهایت سعادت‌مندی و بهروزی را برای ایشان از درگاه حق‌تعالی مسألت دارم. هم‌چنین بر خود فرض می‌دانم، مراتب قدردانی و سپاس خود را از اساتید بزرگوار آقای دکتر «بهزاد نجفی» و آقای دکتر «رضا عرفی» به خاطر قبول زحمت داوری این رساله ابراز دارم.

آخرین، اما نه کمترین؛ از خانواده‌ی عزیزم، به خصوص پدر و مادر نازنینم، که همواره از همراهی و سعه‌ی صدرشان بهره‌مند بوده‌ام، بسیار سپاس‌گزارم.

چکیده

کدهای خطی با مینیمم فاصله‌ی بزرگ از کدهای مهم تصحیح کننده‌ی خطا در نظریه‌ی اطلاعات هستند. کدهای متعامد کاربردهای زیادی در دیگر شاخه‌های ریاضیات دارند. در این پایان‌نامه کدهای متعامد دوتایی تولید شده توسط ماتریس‌های وزن مدول‌های متناهی‌البعد جبر لی ساده‌ی $sl(n,\mathbb{C})$ را مطالعه می‌کنیم. در تعیین مینیمم فاصله‌ها، از گروه‌های وایل و شاخه‌ای از قوانین نمایش‌های تحویل‌ناپذیر جبر لی ساده‌ی $sl(n,\mathbb{C})$ استفاده کرده‌ایم.

فهرست مطالب

مقدمه

در اواسط جنگ دوم جهانی چند ریاضیدان بزرگ و در رأس آن‌ها کلود شانون[1]، بررسی اصول ارتباطات در جامعه را آغاز کردند. حاصل این بررسی در سال ۱۹۴۸ طی چند مقاله منتشر شد، شاخص‌ترین آن‌ها مقاله‌ی شانون با عنوان «نظریه‌ی ریاضی ارتباط[2]» بود. یکی از جنبه‌های کار شانون را می‌توان در این جمله‌ی او خلاصه کرد: «مسأله‌ی اصلی ارتباطات، بازسازی دقیق یا تقریبی پیامی است که در نقطه‌ای دیگر انتخاب شده است». از آن زمان به بعد بخش عظیمی از تحقیقات به پیدا کردن روش‌های مناسبی اختصاص یافت که به وسیله‌ی آن‌ها اطلاعات دیجیتالی بتوانند برای یک انتقال قابل اعتماد از یک کانال پارازیت‌دار، کد شوند. نظریه‌ی کدگذاری گرایشی از ریاضیات است که اکثراً متکی به ایده‌های ریاضیات محض می‌باشد و به‌ویژه، بیانگر قدرت و زیبایی جبر است. نظریه‌ی کدگذاری، با استفاده از مدل‌هایی که از مفاهیم اصلی جبر ساخته می‌شود، به تشخیص اصل داده‌های دریافتی می‌پردازد.

کدهایی مفید هستند که قادر به تصحیح خطاها و تشخیص اصل داده‌های دریافتی باشند، به چنین کدهایی، کدهای تصحیح کننده‌ی خطا می‌گوییم. امروزه کدهای تصحیح کننده‌ی خطا در کاربرد، استفاده‌ی وسیعی دارند مثل گرفتن عکس از یک مکان عمیق، ذخیره‌ی اطلاعات روی نوارهای مغناطیسی و ...

معمولاً کدها شامل کلمات به طول مساوی n هستند. فرض کنید در کدی از الفبای Q استفاده شود اگر $|Q| = q$، یعنی q حرف داشته باشیم، می‌گوییم کد یک q-تایی است. کد، زیرمجموعه‌ای ناتهی از مجموعه‌ی تمام کلمات n حرفی در یک زبان q حرفی است. برای دو کلمه‌ی $x = x_1x_2\cdots x_n$ و $y = y_1y_2\cdots y_n$ در کد C، فاصله‌ی بین x و y را با نماد $d(x,y)$ نمایش می‌دهیم و تعریف می‌کنیم $d(x,y) = |\{i|x_i \neq y_i\}|$. فاصله‌ی بین هر دو کلمه در کد C را محاسبه می‌کنیم و کمترین مقدار بین این مقادیر را مینیمم فاصله‌ی کد می‌گوییم. مینیمم فاصله‌ی کد اهمیت زیادی دارد؛ هرچه این مقدار بیشتر باشد، قدرت تصحیح خطای کد بالاتر می‌رود. بنابراین، کدهایی اهمیت بیشتری دارند که مینیمم فاصله‌ی بزرگ دارند. کد خطی، کدی است که الفبای آن یک میدان جبری، مانند F_q، است و در نتیجه کد خطی C با طول n، زیر فضایی از F_q^n است. اگر پایه‌ای از این زیرفضا را در نظر بگیریم و عناصر آن را به عنوان سطرهای یک ماتریس قرار دهیم، کد C را کد خطی تولید شده توسط این ماتریس روی F_q

[1] Claude Shannon

[2] Mathematical Theory of Communication

می‌گوییم. کار کردن با کدهای خطی به دلیل ساختار جبری آن‌ها راحت‌تر است. کدهای خطی با مینیمم فاصله‌ی بزرگ از مهمترین کدهای تصحیح کننده‌ی خطا در نظریه‌ی اطلاعات هستند. در صورتی که C یک کد خطی باشد، یعنی C زیرفضایی از F_q^n باشد، می‌دانیم $C^\perp = \{a \in F_q^n | a \cdot b = 0, b \in C\}$ نیز زیرفضایی از F_q^n می‌باشد. $C^\perp$ را کد دوگان C می‌نامیم. در صورتی که $C \subseteq C^\perp$ باشد، کد C را متعامد می‌گوییم. وزن یک کدواژه در یک کد خطی، تعداد مؤلفه‌های ناصفر آن است. در مورد کدهای خطی، مینیمم فاصله‌ی C، دقیقاً مینیمم وزن کدواژه‌های ناصفر آن است. کد خطی را یک کد زوج (زوج-مضاعف) گویند، هرگاه وزن تمام کدواژه‌ها مضربی از ۲ (از ۴) باشد. مثال‌هایی از خانواده‌های نامتناهی شناخته شده از کدها کدهای دوری[۳]، کدهای باقیمانده‌ی مربعی[۴]، کدهای گپا[۵]، کدهای هندسه‌ی جبری[۶]، کدهای هادامارد[۷] و غیره هستند. اسامی این خانواده‌ها همچنین روش‌های ساختن کدها را مشخص می‌کند. خانواده‌ی نامتناهی جدیدی از کدها، برخاسته از نمایش‌های متناهی‌البعد جبرهای لی ساده وجود دارد که این خانواده از کدها را می‌توان کدهای نظری لی[۸] نامید. از خصوصیات مهم این کدها، این است که گروه وایل متناظر، روی آن‌ها به طور ایزومتری عمل می‌کند.

رده‌بندی زیبایی از جبرهای لی ساده روی میدان $\mathbb{C}$، آن‌ها را به سه خانواده‌ی نامتناهی از جبرهای لی ساده‌ی sl_n، so_n، sp_{2n} و جبرهای لی ساده‌ی نمایی g_2، f_4، e_6، e_7، و e_8 تقسیم می‌کند. در این پایان‌نامه، کدهای مربوط به نمایش $sl(n, \mathbb{C})$ بررسی شده است.

فرض کنید L جبر لی ساده‌ی متناهی‌البعد روی میدان اعداد مختلط، $\mathbb{C}$، باشد. زیرجبر کارتان، $\hbar$، و ریشه‌های ساده‌ی مثبت، $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$، را در نظر بگیرید. پایه‌ای برای $\hbar$ را به صورت مجموعه‌ی $\{H_1, H_2, \cdots, H_n\}$ نمایش می‌دهیم. برای L-مدول متناهی‌البعد V، می‌دانیم V تجزیه‌ای به زیرفضاهای وزن به صورت زیر دارد:

$$V = \oplus_{\mu \in \hbar^*} V_\mu, \quad V_\mu = \{v \in V | H \cdot v = \mu(H)v, \ H \in \hbar \text{ برای هر}\}.$$

[۳] cyclic codes

[۴] quadratic residue codes

[۵] Goppa codes

[۶] algebraic geometry codes

[۷] Hadamard codes

[۸] Lie theoretic codes

فرض کنید $\{u_۱, u_۲, \cdots, u_k\}$ بزرگترین مجموعه‌ی مستقل خطی از بردارهای وزن با وزن‌های ناصفر باشد. قرار دهید:

$$H_i \cdot u_j = c_{ij} u_j, \quad C(V) = (c_{ij})_{n \times k} \qquad (۱.۰)$$

در فصل ۳، نشان می‌دهیم که c_{ij}ها اعداد صحیح‌اند. $C(V)$ را ماتریس وزن L روی V می‌نامیم. اگر ابهامی به وجود نیاید، می‌توان این اعداد صحیح را با تصویر آن‌ها در $\mathbb{Z}_m$ نمایش داد. در این‌صورت، کد خطی mتایی تولید شده توسط $C(V)$ را با نماد $C_m(V)$ نمایش می‌دهیم.

این پایان‌نامه، شامل ۴ فصل می‌باشد. در فصل اول، با تعاریف و مفاهیمی در نظریه‌ی کدگذاری آشنا می‌شویم. در فصل دوم، اصطلاحات و قضایایی از جبر لی گنجانده شده است. فصل سوم، بررسی نمایش جبر لی ساده‌ی $sl(n, \mathbb{C})$، متشکل از ماتریس‌های $n \times n$ با اثر صفر، می‌باشد؛ در این فصل گروه وایل و عمل آن روی فضاهای وزن مطرح می‌شود که نتایجی از این مطالب در تعیین مینیمم فاصله‌های کدها، که به طور کلی کار راحتی نیست، نقش مؤثری دارند و در نهایت در فصل چهارم، کد ساخته شده توسط جبر لی ساده‌ی $sl(n, \mathbb{C})$ معرفی می‌شود و در این فصل نشان می‌دهیم:

(۱) کد وزن دودویی $C_۲(V)$ از $sl(۲m, \mathbb{C})$، برای $m \geq ۲$ یک $[m(۲m-۱), ۲(m-۱), ۴(m-۱)]$–کد متعامد دودویی زوج–مضاعف است.

(۲) کد وزن دودویی $C_۲(V)$ از $sl(n, \mathbb{C})$ در صورتی که $n > ۹$ و (به پیمانه‌ی ۴) $n \equiv ۲, ۳$، یک $[\binom{n}{۳}, n-۱, (n-۲)(n-۳)]$–کد متعامد دودویی زوج–مضاعف است.

مطالبی که در این فصل بیان شده، از مرجع [۵] استنباط شده است. در ادامه، نویسنده‌ی [۵] به بررسی کدهای سه‌تایی پرداخته است. چنین به نظر می‌آید، ماتریسی که احتمالاً نویسنده برای محاسبات خود به کار برده است با ماتریسی که با توجه به روابط موجود به دست می‌آید در برخی درایه‌ها اختلاف دارند. در ادامه‌ی مطالب فصل، ماتریس‌های $C_۳(A_۲)$ و $C_۳(A_۳)$ ارائه شده و درایه‌هایی که با محاسبات به دست آمده از روابط موجود اختلاف دارند مشخص شده‌اند ولی جهت بررسی محاسبات نویسنده، این درایه‌ها در ماتریس‌های بیان شده، بر اساس ماتریسی می‌باشند که احتمالاً مورد نظر ایشان بوده است. البته، متذکر می‌شویم که در این مرجع، این ماتریس‌ها و محاسبات مربوطه صراحتاً بیان نشده‌اند و این ادعا بر اساس استنباط از روابط بیان شده است.

در این پایان‌نامه، فقط کدهای مربوط به نمایش $sl(n,\mathbb{C})$ بررسی شده است. سایر جبرهای لی ساده نیز به همین ترتیب، کدهایی با مینیمم فاصله‌های بزرگ تولید می‌کنند. مشاهده‌ی این پدیده‌ی نظریه‌ی کدگذاری، زمانی صورت گرفت که نمایش‌های چندجمله‌ای این جبرها در حال بررسی بود. به خوانندگان علاقه‌مند، مطالعه‌ی کدهای مربوط به دیگر جبرهای لی ساده نیز پیشنهاد می‌شود.

فصل ۱

مقدماتی از نظریه‌ی کدگذاری

در این فصل با مفاهیم اولیه‌ی کدگذاری آشنا می‌شویم. تمامی مطالبی که در این فصل گنجانده شده است، به استناد مرجع [۴] می‌باشد.

۱.۱ کد

تعریف ۱.۱. فرض کنید $A = \{a_1, a_2, ..., a_q\}$، مجموعه‌ای با اندازه‌ی q باشد که به عنوان *الفبای* کد به آن مراجعه می‌کنیم و اعضای آن را *علائم کد* می‌نامیم.

(۱) یک *کلمه‌ی* $q-$*آرایه‌ای* از طول n روی الفبای A دنباله‌ای به صورت $\mathbf{w} = w_1 w_2 ... w_n$ می‌باشد که برای هر i، $w_i \in A$. معادلاً، $\mathbf{w}$ را می‌توان به شکل بردار $(w_1, ..., w_n)$ در نظر گرفت.

(۲) یک کد *بلوکی* $q-$*آرایه‌ای* از طول n روی الفبای A مجموعه‌ی ناتهی C از کلمات $q-$آرایه‌ای است که دارای طول یکسان n می‌باشند.

(۳) هر عضو مجموعه‌ی C یک *کدواژه* در C نامیده می‌شود.

(۴) تعداد کدواژه‌ها در C، که با $|C|$ نمایش داده می‌شود، *اندازه‌ی* C نامیده می‌شود.

(۵) یک کد از طول n و اندازه‌ی M یک $(n, M)-$کد نامیده می‌شود.

تذکر ۲.۱. الفبای کد معمولاً میدان متناهی $\mathbf{F}_q$ از مرتبه‌ی q در نظر گرفته می‌شود.

تعریف ۳.۱. یک کد روی الفبای $\mathbf{F}_۲ = \{۰, ۱\}$ *کد دودویی(دوتایی)* نامیده می‌شود؛ به عبارت دیگر، علائم کد دودویی ۰ و ۱ هستند. همین‌طور یک کد روی الفبای $\mathbf{F}_۳ = \{۰, ۱, ۲\}$ *کد سه‌تایی* نامیده می‌شود.

روش کدگشایی. در یک کانال ارتباطی کد شده، فقط کدواژه‌ها ارسال می‌شوند. فرض کنید کلمه‌ی $\mathbf{w}$ دریافت شده است. اگر $\mathbf{w}$ یک کدواژه‌ی معتبر باشد، می‌توان نتیجه گرفت که خطایی در انتقال وجود ندارد. اما اگر بدانیم چند خطا اتفاق افتاده است، به روشی برای پیدا کردن محتمل‌ترین کدواژه‌ی ارسال شده نیاز داریم. چنین روشی به *روش کدگشایی* معروف است.

۲.۱ فاصله‌ی همینگ

تعریف ۴.۱. فرض کنید $\mathbf{x}$ و $\mathbf{y}$ کلماتی از طول n روی الفبای A باشند. *فاصله‌ی(همینگ)* از $\mathbf{x}$ تا $\mathbf{y}$ که با $d(\mathbf{x}, \mathbf{y})$ نمایش داده می‌شود، تعداد مکان‌هایی است که $\mathbf{x}$ و $\mathbf{y}$ متفاوت از هم‌اند. اگر $\mathbf{x} = x_۱...x_n$ و $\mathbf{y} = y_۱...y_n$، در این‌صورت:

$$d(\mathbf{x}, \mathbf{y}) = d(x_۱, y_۱) + ... + d(x_n, y_n), \qquad (۱.۱)$$

که در آن x_i و y_i به شکل کلماتی از طول ۱ در نظر گرفته می‌شوند، و

$$d(x_i, y_i) = \begin{cases} ۱ & x_i \neq y_i \text{ اگر} \\ ۰ & x_i = y_i \text{ اگر} \end{cases}$$

مثال ۵.۱. فرض کنید $A = \{۰, ۱\}$، $\mathbf{x} = ۰۱۰۱۰$ و $\mathbf{y} = ۰۱۱۰۱$. در این‌صورت:

$$d(\mathbf{x}, \mathbf{y}) = ۳.$$

گزاره ۶.۱. فرض کنید $\mathbf{x}$، $\mathbf{y}$ و $\mathbf{z}$ کلماتی از طول n روی الفبای A باشند. در این‌صورت داریم:

(۱) $۰ \leq d(\mathbf{x}, \mathbf{y}) \leq n$،

(۲) $d(\mathbf{x},\mathbf{y})=0$ اگر و فقط‌اگر $\mathbf{x}=\mathbf{y}$،

(۳) $d(\mathbf{x},\mathbf{y})=d(\mathbf{y},\mathbf{x})$،

(۴) (نامساوی مثلثی.) $d(\mathbf{x},\mathbf{z})\leq d(\mathbf{x},\mathbf{y})+d(\mathbf{y},\mathbf{z})$.

اثبات. (۱)، (۲) و (۳) با توجه به تعریف فاصله‌ی همینگ واضح‌اند. با توجه به (۱.۱) کافی است (۴) را برای حالت $n=1$ ثابت کنیم، پس فرض می‌کنیم $n=1$.

اگر $\mathbf{z}=\mathbf{x}$، در این‌صورت (۴) به وضوح درست است زیرا $d(\mathbf{x},\mathbf{z})=0$.

اگر $\mathbf{z}\neq\mathbf{x}$، در این‌صورت $\mathbf{y}\neq\mathbf{x}$ یا $\mathbf{y}\neq\mathbf{z}$ پس در این حالت نیز (۴) صحیح می‌باشد. □

۳.۱ کدگشایی مینیمم فاصله

فرض کنید کدواژه‌هایی از کد C، روی یک کانال ارتباطی ارسال می‌شوند. اگر کلمه‌ی $\mathbf{x}$ دریافت شود، در صورتی که $d(\mathbf{x},\mathbf{c_x})$ در میان تمام کدواژه‌های C کمترین باشد، به عبارت دیگر

$$d(\mathbf{x},\mathbf{c_x})=\min_{\mathbf{c}\in C} d(\mathbf{x},\mathbf{c}), \qquad (۲.۱)$$

روش کدگشایی مینیمم فاصله، $\mathbf{x}$ را به $\mathbf{c_x}$ کدگشایی خواهد کرد. در روش کدگشایی مینیمم فاصله، کدگشایی به دو صورت انجام می‌شود. برای کلمه‌ی دریافت شده‌ی $\mathbf{x}$، اگر برای دو یا بیش از دو کدواژه‌ی $\mathbf{c_x}$ رابطه‌ی (۲.۱) برقرار باشد، در این‌صورت *روش کدگشایی کامل* یکی از آن‌ها را به دلخواه به عنوان محتمل‌ترین واژه‌ی ارسال شده انتخاب می‌کند، در حالی که *روش کدگشایی ناکامل* ارسال دوباره‌ای را درخواست می‌کند.

۴.۱ فاصله‌ی کد

غیر از طول و اندازه‌ی کد، ویژگی مهم و مفید دیگر آن *فاصله‌ی کد* می‌باشد.

تعریف ۷.۱. برای کد C شامل حداقل ۲ کلمه، *(مینیمم) فاصله‌ی* C که با $d(C)$ نمایش داده می‌شود

به صورت زیر است:

$$d(C) = min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}$$

تعریف ۸.۱. یک کد از طول n، اندازه‌ی M و فاصله‌ی d، (n, M, d)–*کد* نامیده می‌شود. اعداد n، M و d را *پارامترهای کد* می‌نامند.

مثال ۹.۱. فرض کنید $C = \{۰۰۰۰۰, ۰۰۱۱۱, ۱۱۱۱۱\}$، یک کد دودویی باشد. در این‌صورت $d(C) = ۲$، زیرا:

$$d(۰۰۰۰۰, ۰۰۱۱۱) = ۳,$$
$$d(۰۰۰۰۰, ۱۱۱۱۱) = ۵,$$
$$d(۰۰۱۱۱, ۱۱۱۱۱) = ۲.$$

از این‌رو، C یک $(۵, ۳, ۲)$–کد دودویی است.

فاصله‌ی کد، ارتباط نزدیکی با توانایی تشخیص و تصحیح خطای کد دارد.

تعریف ۱۰.۱. فرض کنید u عدد صحیح مثبتی باشد. یک کد، u–*تشخیص‌دهنده‌ی خطا* است در صورتی که اگر در کدواژه‌ای حداقل یک خطا و حداکثر u خطا اتفاق افتاد کلمه‌ی نتیجه شده یک کدواژه نباشد. کد C، *دقیقاً* u–*تشخیص‌دهنده‌ی خطا* است هرگاه u–تشخیص‌دهنده‌ی خطا باشد ولی $(u + ۱)$–تشخیص‌دهنده‌ی خطا نباشد.

مثال ۱۱.۱. کد دودویی $C = \{۰۰۰۰۰, ۰۰۱۱۱, ۱۱۱۱۱\}$، ۱–تشخیص‌دهنده‌ی خطا است زیرا تغییر هر کدواژه در یک مکان کدواژه‌ی دیگری را نتیجه نمی‌دهد. به عبارت دیگر،

۰۰۱۱۱ $\rightarrow$ ۰۰۰۰۰ به سه بیت تغییر نیاز دارد،
۱۱۱۱۱ $\rightarrow$ ۰۰۰۰۰ به پنج بیت تغییر نیاز دارد،
۱۱۱۱۱ $\rightarrow$ ۰۰۱۱۱ به دو بیت تغییر نیاز دارد.

در واقع C، دقیقاً ۱−تشخیص‌دهنده‌ی خطا می‌باشد زیرا با تغییر دو مکان نخست ۰۰۱۱۱ کدواژه‌ی دیگر ۱۱۱۱۱ نتیجه خواهد شد (بنابراین C، کد ۲−تشخیص‌دهنده‌ی خطا نیست).

قضیه ۱۲.۱. کد C، u−تشخیص‌دهنده‌ی خطا است اگر و فقط‌اگر $d(C) \geqslant u + ۱$؛ یعنی کدی با فاصله‌ی d، کد دقیقاً $(d - ۱)$−تشخیص‌دهنده‌ی خطا است.

اثبات. فرض کنید $d(C) \geqslant u + ۱$. اگر $\mathbf{c} \in C$ و $\mathbf{x}$ به گونه‌ای باشد که $۱ \leqslant d(\mathbf{c}, \mathbf{x}) \leqslant u < d(C)$، در این‌صورت $\mathbf{x} \notin C$؛ بنابراین C، u−تشخیص‌دهنده‌ی خطا است. از طرف دیگر اگر $d(C) < u + ۱$ یعنی $d(C) \leq u$، در این‌صورت $\mathbf{c}_۱, \mathbf{c}_۲ \in C$ وجود دارند که $۱ \leq d(\mathbf{c}_۱, \mathbf{c}_۲) = d(C) \leq u$. بنابراین امکان‌پذیر است که با $\mathbf{c}_۱$ شروع کنیم و $d(C)$ خطا (که $۱ \leq d(C) \leq u$) طوری اتفاق بیافتد که کلمه‌ی نتیجه شده، $\mathbf{c}_۲$، کدواژه‌ی دیگری در C باشد. از این‌رو، C یک کد u−تشخیص‌دهنده‌ی خطا نیست. □

تذکر ۱۳.۱. مثال‌های ۹.۱ و ۱۱.۱ نیز قضیه‌ی فوق را تأیید می‌کنند.

تعریف ۱۴.۱. فرض کنید روش کدگشایی ناکامل استفاده شود و v عدد صحیح مثبتی باشد. کد C، v−*تصحیح‌کننده‌ی خطا* است اگر کدگشایی مینیمم فاصله قادر به تصحیح v یا تعداد کمتری خطا باشد. کد C، *دقیقاً* v−*تصحیح‌کننده‌ی خطا* است اگر v−تصحیح‌کننده‌ی خطا باشد ولی $(v + ۱)$−تصحیح‌کننده‌ی خطا نباشد.

مثال ۱۵.۱. کد دودویی $C = \{۰۰۰, ۱۱۱\}$ را در نظر بگیرید. با استفاده از روش کدگشایی مینیمم فاصله، مشاهده می‌شود:

- اگر ۰۰۰ ارسال شود و یک خطا در انتقال اتفاق بیافتد، در این‌صورت کلمه‌ی دریافتی (۱۰۰، ۰۱۰ یا ۰۰۱) به ۰۰۰ کدگشایی خواهد شد؛
- اگر ۱۱۱ ارسال شود و یک خطا در انتقال اتفاق بیافتد، در این‌صورت کلمه‌ی دریافتی (۱۱۰، ۱۰۱ یا ۰۱۱) به ۱۱۱ کدگشایی خواهد شد.

در تمام حالت‌ها یک خطا، تصحیح شده است. از این‌رو C، ۱−تصحیح‌کننده‌ی خطا است.

اگر حداقل دو خطا اتفاق بیافتد، روش کدگشایی ممکن است کدواژه‌ی نادرستی را نتیجه دهد. برای مثال اگر ۰۰۰ ارسال شود و ۰۱۱ دریافت شود، در این‌صورت ۰۱۱ با استفاده از روش کدگشایی مینیمم فاصله به ۱۱۱ کدگشایی خواهد شد. از این‌رو C، دقیقاً ۱−تصحیح‌کننده‌ی خطا است.

قضیه ۱۶.۱. کد C، $v-$تصحیح‌کننده‌ی خطا است اگر و فقط‌اگر $d(C) \geqslant 2v+1$؛ یعنی کدی با فاصله‌ی d، کد دقیقاً $\lfloor \frac{(d-1)}{2} \rfloor-$تصحیح‌کننده‌ی خطا است. در این‌جا، $\lfloor x \rfloor$ بزرگترین عدد صحیح کمتر یا مساوی x می‌باشد.

اثبات. '$\Rightarrow$' فرض کنید $d(C) \geqslant 2v+1$، $\mathbf{c}$ کدواژه‌ی ارسالی و $\mathbf{x}$ کدواژه‌ی دریافتی باشد. اگر v خطا یا کمتر در انتقال اتفاق افتاده باشد، در این‌صورت $d(\mathbf{x},\mathbf{c}) \leq v$. از این‌رو، برای هر کدواژه‌ی $\mathbf{c}' \in C$ که $\mathbf{c} \neq \mathbf{c}'$، داریم:

$$\begin{aligned} d(\mathbf{x},\mathbf{c}') &\geqslant d(\mathbf{c},\mathbf{c}') - d(\mathbf{x},\mathbf{c}) \\ &\geqslant 2v+1-v \\ &= v+1 \\ &> d(\mathbf{x},\mathbf{c}). \end{aligned}$$

بنابراین اگر روش کدگشایی مینیمم فاصله استفاده شود، $\mathbf{x}$ (به طور صحیح) به $\mathbf{c}$ کدگشایی می‌شود. این نشان می‌دهد که C، $v-$تصحیح‌کننده‌ی خطا است.

'$\Leftarrow$' فرض کنید کد C، $v-$تصحیح‌کننده‌ی خطا باشد. اگر $d(C) < 2v+1$ باشد، در این‌صورت کدواژه‌های مجزای $\mathbf{c},\mathbf{c}' \in C$ وجود دارند که $d(\mathbf{c},\mathbf{c}') = d(C) \leq 2v$. نشان می‌دهیم در صورت ارسال $\mathbf{c}$ و رخداد حداکثر v خطا، کدگشایی مینیمم فاصله می‌تواند یا کلمه‌ی دریافتی را به شکل ناصحیح به صورت $\mathbf{c}'$ کدگشایی کند و یا یک نتیجه‌ی مساوی گزارش دهد (و در نتیجه اگر روش کدگشایی ناکامل استفاده شود، این خطاها نمی‌توانند تصحیح شوند). این نتیجه با فرض $v-$تصحیح‌کننده بودن C تناقض خواهد داشت، از این‌رو نشان می‌دهد $d(C) \geqslant 2v+1$.

اگر $d(\mathbf{c},\mathbf{c}') < v+1$ بود، در این‌صورت $\mathbf{c}$ می‌توانست با متحمل شدن حداکثر v خطا به $\mathbf{c}'$ تبدیل شود و این خطاها غیر قابل تصحیح می‌شدند (درواقع، غیر قابل تشخیص) زیرا $\mathbf{c}'$ دوباره در C قرار

می‌گیرد. که در هر حال، با فرض $v-$تصحیح‌کننده بودن C تناقض دارد. بنابراین، $d(\mathbf{c},\mathbf{c}') \geqslant v+۱$. بدون از دست دادن کلیت می‌توان فرض کرد $\mathbf{c}$ و $\mathbf{c}'$ در دقیقاً $d = d(C)$ مکان اول متفاوت‌اند، که $v+۱ \leqslant d \leqslant ۲v$. اگر کلمه‌ی

$$x = \underbrace{x_۱, ..., x_v}_{\text{موافق با } \mathbf{c}'} \underbrace{x_{v+۱}, ..., x_d}_{\text{موافق با } \mathbf{c}} \underbrace{x_{d+۱}, ..., x_n}_{\text{موافق با هر دو}}$$

دریافت شود، در این‌صورت داریم

$$d(\mathbf{x},\mathbf{c}') = d - v \leq v = d(\mathbf{x},\mathbf{c}).$$

بنابراین هریک از نتایج $d(\mathbf{x},\mathbf{c}') < d(\mathbf{x},\mathbf{c})$ که در این حالت $\mathbf{x}$ به طور ناصحیح به $\mathbf{c}'$ کدگشایی می‌شود، یا $d(\mathbf{x},\mathbf{c}) = d(\mathbf{x},\mathbf{c}')$ که در این حالت نتیجه‌ی مساوی گزارش می‌شود، به دست می‌آید. □

۵.۱ کدهای خطی

در ادامه، کدهای خطی را معرفی می‌کنیم و برخی خصوصیات مقدماتی آن‌ها را بیان می‌کنیم.

تعریف ۱۷.۱. *کد خطی* C از طول n روی F_q، یك زیرفضا از F_q^n است.

مثال ۱۸.۱. $C = \{(\lambda, \lambda, ..., \lambda) : \lambda \in F_q\}$ یک کد خطی است. این کد، اغلب *کد تکرار* نامیده می‌شود.

تعریف ۱۹.۱. فرض کنید C یك کد خطی در F_q^n باشد.

(۱) *دوگان کد* C، $C^\perp$ مکمل متعامد زیرفضای C از F_q^n است.

(۲) *بعد کد خطی* C، بعد C به عنوان یك فضای برداری روی F_q یعنی $dim(C)$ می‌باشد.

قضیه ۲۰.۱. فرض کنید C یك کد خطی از طول n روی F_q باشد. در این‌صورت:

(۱) $|C| = q^{dim(C)}$، به عبارت دیگر $dim(C) = log_q|C|$؛

(۲) $C^\perp$ یك کد خطی است و $dim(C) + dim(C^\perp) = n$؛

(۳) $(C^{\perp})^{\perp} = C$.

مثال ۲۱.۱. (۱) $(q = ۲)$ فرض کنید $C = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱۱\}$، پس داریم $log_۲|C| = log_۲۴ = ۲$. می‌توان دید $C = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱۱\} = C^{\perp}$، و $dim(C^{\perp}) = ۲$.

(۲) $(q = ۳)$ فرض کنید $C = \{۰۰۰, ۰۰۱, ۰۰۲, ۰۱۰, ۰۲۰, ۰۱۱, ۰۱۲, ۰۲۱, ۰۲۲\}$، پس $dim(C) = log_۳|C| = log_۳۹ = ۲$. داریم $C^{\perp} = \{۰۰۰, ۱۰۰, ۲۰۰\}$، بنابراین $dim(C^{\perp}) = ۱$.

تذکر ۲۲.۱. یک کد خطی از طول n و بعد k روی F_q یک $[n, k]$–کد q–*آرایه‌ای*، یا اگر q با استفاده از متن مشخص باشد یک $[n, k]$–کد نامیده می‌شود. این کد همچنین یک (n, q^k)–کد خطی است. اگر فاصله‌ی کد C نیز مشخص باشد، این کد همچنین گاهی اوقات یک $[n, k, d]$–*کد خطی* ذکر می‌شود.

تعریف ۲۳.۱. فرض کنید C یک کد خطی باشد.

(۱) C *خودمتعامد* است اگر $C \subseteq C^{\perp}$.

(۲) C *خوددوگان* است اگر $C = C^{\perp}$.

گزاره ۲۴.۱. بعد یک کد خودمتعامد از طول n باید کمتر یا مساوی $n/۲$ باشد و بعد یک کد خوددوگان از طول n برابر $n/۲$ است.

اثبات. این گزاره نتیجه‌ی مستقیم قضیه‌ی ۲۰.۱ (۲) و تعاریف کدهای خودمتعامد و خوددوگان است. □

مثال ۲۵.۱. کد مثال ۲۱.۱ (۱)، خوددوگان است.

۶.۱ وزن همینگ

فاصله‌ی همینگ بین دو کلمه‌ی $x, y \in F_q^n$، $d(x, y)$، را تعریف کردیم.

تعریف ۲۶.۱. فرض کنید x یک کلمه در F_q^n باشد. *وزن(همینگ)* x که با $wt(x)$ نمایش داده می‌شود، تعداد مؤلفه‌های ناصفر x تعریف می‌شود؛ به عبارت دیگر، $wt(x) = d(x, ۰)$ که ۰ کلمه‌ی صفر است.

تعریف ۲۷.۱. کد خطی را یک *کد زوج* (*کد زوج-مضاعف*) گویند، هرگاه وزن تمام کدواژه‌ها مضربی از ۲ (از ۴) باشد.

تذکر ۲۸.۱. برای هر عضو $x \in F_q$، وزن همینگ را می‌توانیم به صورت زیر تعریف کنیم:

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

در این‌صورت با نوشتن $x \in F_q^n$ به شکل $x = (x_۱, x_۲, ..., x_n)$، وزن همینگ x می‌تواند معادلاً به صورت زیر تعریف شود:

$$wt(x) = wt(x_۱) + wt(x_۲) + ... + wt(x_n) \qquad (۳.۱)$$

لم ۲۹.۱. اگر $x, y \in F_q^n$، آنگاه $d(x, y) = wt(x - y)$.

اثبات. برای $x, y \in F_q$، $d(x, y) = ۰$ اگر و فقط‌اگر $x = y$ که این نیز برقرار است اگر و فقط‌اگر $x - y = ۰$ یا معادلاً $wt(x - y) = ۰$. حال لم ۲۹.۱ از (۱.۱) و (۳.۱) نتیجه می‌شود. □

از آن‌جا که برای هر $a \in F_q$ در مورد qهای زوج داریم $a = -a$، نتیجه‌ی زیر پیامد مستقیم لم ۲۹.۱ می‌باشد.

نتیجه ۳۰.۱. فرض کنید q زوج باشد. اگر $x, y \in F_q^n$، آنگاه $d(x, y) = wt(x + y)$.

برای $x = (x_۱, x_۲, ..., x_n)$ و $y = (y_۱, y_۲, ..., y_n)$ در F_q^n، قرار دهید:

$$x \star y = (x_۱y_۱, x_۲y_۲, ..., x_ny_n).$$

گزاره ۳۱.۱. اگر $x, y \in F_۲^n$، آنگاه:

$$wt(x + y) = wt(x) + wt(y) - ۲wt(x \star y) \qquad (۴.۱)$$

x	y	$x \star y$	$wt(x)+wt(y)-۲wt(x\star y)$	$wt(x+y)$
۰	۰	۰	۰	۰
۰	۱	۰	۱	۱
۱	۰	۰	۱	۱
۱	۱	۱	۰	۰

جدول ۱.۱:

اثبات. با استفاده از (۳.۱)، کافی است نشان دهیم (۴.۱) برای $x, y \in F_۲$ برقرار است. که این نیز به شکل بیان شده در جدول ۱.۱ به راحتی قابل دست‌یابی است. □

تعریف ۳۲.۱. فرض کنید C یك کد باشد (نه لزوماً خطی). *مینیمم وزن (همینگ)* C، که با $wt(C)$ نمایش داده می‌شود، کمترین وزن کدواژه‌های ناصفر C می‌باشد.

قضیه ۳۳.۱. فرض کنید C یك کدخطی روی F_q باشد. در این‌صورت $d(C) = wt(C)$.

اثبات. یادآور می‌شویم که برای هر دو کلمه‌ی x, y داریم $d(x, y) = wt(x - y)$. با توجه به تعریف، $x', y' \in C$ وجود دارند که $d(x', y') = d(C)$ بنابراین

$$d(C) = d(x', y') = wt(x' - y') \geq wt(C),$$

زیرا $x' - y' \in C$. برعکس، $z \in C \setminus \{۰\}$ وجود دارد که $wt(C) = wt(z)$ بنابراین

$$wt(C) = wt(z) = d(z, ۰) \geq d(C).$$

□

تذکر ۳۴.۱. **(برخی مزایای کدهای خطی.)** موارد زیر دلایلی هستند که چرا ممکن است استفاده از کدهای خطی نسبت به کدهای غیرخطی مورد ترجیح باشد.

(۱) از آن‌جا که یك کد خطی یك فضای برداری است، می‌تواند با استفاده از پایه کاملاً توصیف شود.

(۲) فاصله‌ی یك کد خطی با کمترین وزن کدواژه‌های ناصفر آن برابر است.

(۳) روش‌های کدگذاری و کدگشایی برای یك کد خطی نسبت به کدهای غیرخطی دلخواه، سریع‌تر و آسان‌تر است (در ادامه با یکی از این روش‌ها آشنا می‌شویم).