دانشگاه صنعتی خواجه نصیرالدین طوسی

دانشکده علوم — گروه ریاضی

پایان نامه جهت دریافت درجه کارشناسی ارشد

ریاضی محض — گرایش جبر

موضوع:

کدهای شبه دوری به عنوان کدهایی روی حلقه‌های ماتریسی

نگارش:

سید نیما صالحی

استاد راهنما:

دکتر علیرضا مقدم فر

استاد مشاور:

دکتر امیر رهنمای برقی

تهران —بهمن ماه ۱۳۹۰

تقدیم به پیشگاه فرشتگانی که بودن هر لحظه‌شان جایگاه امروز من شد

پدر، مادر، برادر، خواهران و همسر عزیزم

اظهار نامه دانشجو

موضوع پایان نامه: کدهای شبه دوری به عنوان کدهایی روی حلقه‌های ماتریسی.

استاد راهنما: دکتر علیرضا مقدم فر.

نام دانشجو: سید نیما صالحی.

شماره دانشجویی: ۸۸۲۰۳۰۴.

اینجانب سید نیما صالحی دانشجوی کارشناسی ارشد ریاضی محض گرایش جبر دانشکده علوم دانشگاه صنعتی خواجه نصیرالدین طوسی گواهی می‌نمایم که تحقیقات ارائه شده در این پایان‌نامه توسط شخص اینجانب انجام شده و صحت و اصالت مطالب نگارش شده مورد تأیید می‌باشد و در مورد استفاده از کار دیگر محققان به مرجع مورد استفاده اشاره شده است. همچنین گواهی می‌نمایم که مطالب مندرج در پایان‌نامه تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگری در هیچ جا ارائه نشده است و در تدوین متن پایان‌نامه آئین‌نامه مصوب دانشگاه را به طور کامل رعایت کرده‌ام.

امضاء دانشجو: سید نیما صالحی.

تاریخ: ۱۳۹۰/۱۱/۳۰

فرم حق طبع و نشر و مالکیت نتایج

تشکر و قدردانی

آغاز می‌کنم با نامِ زیبای او که هرچه هستم از اوست. سپاسم از آنِ اوست که هر لحظه زیستنم نشان از لطف و عنایتِ بی‌پایانش دارد، که از اوست دانشِ من، اندیشهٔ من و تمامِ من، که هر چه نگاشتم قطره‌ای از دریای بی‌کرانِ معرفتش بود، که من قلمم و اوست نگارنده.

از صمیم قلب، ایزد منان را شاکرم که در گذر پر پیچ و خم زندگی این توفیق را نصیب اینجانب نموده است که در راه کسب علم و دانش توانستم از محضر و مکتب استادان بزرگ و عالیقدر بهره‌مند شوم. لذا لازم می‌دانم از همهٔ کسانی که مرا در مطالعه، تحقیق و نگارش این پایان‌نامه یاری دادند تشکر و قدردانی نمایم.

در این راستا از استاد عالیقدر جناب آقای دکتر **علیرضا مقدم‌فر** به دلیل زحمات بی‌دریغ و دلسوزانه و راهنمایی‌های ارزشمندشان، که نه تنها در تمام مراحل انجام این پایان‌نامه بلکه در تمامی سنوات دورهٔ کارشناسی و دورهٔ کارشناسی ارشد، به بنده ارزانی داشته‌اند، نهایت تشکر و قدردانی را ابراز نمایم. همچنین از جناب آقای دکتر **امیر رهنمای برقی** استاد مشاوره‌ام صمیمانه تشکر می‌کنم و از ممتحن خارجی جناب آقای دکتر **مهدی علائیان** (از دانشگاه علم و صنعت ایران) و ممتحن داخلی جناب آقای دکتر **علی ذاکری** که قبول زحمت فرمودند، سپاسگزارم. همچنین از سرکار خانم دکتر **فرشته ملک** معاونت محترم آموزشی و جناب آقای دکتر **محمدرضا پیغامی** معاونت محترم تحصیلات تکمیلی دانشکدهٔ علوم کمال تشکر را دارم.

در پایان بر خود لازم می‌دانم که از همراهان خوبِ زندگیم، پدر، مادر، برادر و همسر عزیزم، که هر لحظه بی‌تابیم را تاب آوردند و صبورانه در این راه یاریم دادند، صمیمانه تشکر و قدردانی نمایم.

چکیده

در این پایان‌نامه، کدهای شبه دوری روی یک میدان متناهی به عنوان کدهای دوری روی یک حلقهٔ ناجابجایی متشکل از ماتریس‌های روی یک میدان متناهی مورد مطالعه قرار گرفته‌اند. چنین دیدگاهی به ما این امکان را می‌دهد که برخی نتایج شناخته شده پیرامون دنباله‌های بازگشتی خطی را تعمیم دهیم و یک ساختمان جدید برای برخی کدهای شبه دوری و کدهای خوددوگان ارائه کنیم.

کلمات کلیدی: کد خطی، کد دوری، کد شبه دوری، دنبالهٔ بازگشتی خطی، کد خوددوگان اقلیدسی، کد خوددوگان هرمیتی.

مقدمه

در دورهٔ مُدرن، اطلاعات دیجیتال از اهمیت ویژه‌ای برخوردارند. به عنوان مثال رسانه‌های خبری، دولت‌ها، مؤسسات و دانشگاه‌ها، روزانه حجم بالایی از اطلاعات دیجیتال را رد و بدل می‌کنند. با این وجود، خطوطی که از آن‌ها برای انتقال اطلاعات استفاده می‌کنیم و همین طور دستگاه‌هایی که اطلاعات را در آن‌ها ذخیره می‌کنیم، به طور کامل قابل اعتماد نیستند و ممکن است اطلاعات، تحت تأثیر نویز[۱] یا به دلیل خطای دستگاه‌های مورد استفاده، دچار تغییر شوند.

یکی از مسائلی که دانشمندان و پژوهشگران حوزهٔ نظریهٔ کدگذاری[۲] با آن روبرو هستند، یافتن و ارتقای روش‌هایی است که در درجهٔ اول، خطای به وجود آمده را شناسایی کنند و در درجهٔ دوم، آن را تصحیح نمایند. این نظریه در سال ۱۹۴۸ و با مقالهٔ معروف کلود شنون[۳]، با عنوان «نظریهٔ ریاضی ارتباطات[۴]» متولد شد و تاکنون بسیاری از موضوعات مختلف ریاضیات، از جمله جبر و ترکیبیات را در هم آمیخته است.

به عملِ تبدیل منبعِ پیام[۵] به یک کد مناسب، جهتِ انتقال از طریق یک کانال، کدگذاری منبع[۶] گویند. به عنوان مثالی از کدگذاری منبع می‌توان به کد ASCII اشاره کرد که در آن، به هر کارکتر، یک بایت، تشکیل شده از ۸ بیت، نسبت داده می‌شود.

برای روشن شدن موضوع، مثال زیر را در نظر می‌گیریم:

فرض کنیم کدگذاری منبع برای چهار رنگِ قرمز، آبی، سفید و سبز، به ترتیب، به صورت ۰۰،

---

[۱] noise

[۲] coding theory

[۳] Claude Shannon

[۴] a mathematical theory of communication

[۵] message source

[۶] source encoding

۰۱، ۱۰ و ۱۱ انجام شده است. به علاوه فرض کنیم پیامِ «قرمز» که به صورت ۰۰ کدگذاری شده است، از طریق یک کانال نویزدار ارسال می‌شود. در این صورت اگر پیامِ ارسال شده، در طول مسیر تحریف شود و به صورت ۰۱ دریافت شود، آنگاه دریافت کنندهٔ پیام، متوجه معیوب بودن آن نمی‌شود و تصور می‌کند که پیامِ «آبی» ارسال شده است. بنابراین ارتباط، با مشکل روبرو خواهد شد.

مفهوم کدگذاری کانال[۷] به کدگذاری مجدد پیام، بعد از کدگذاری منبع گفته می‌شود، به این ترتیب که طول پیام کدگذاری شده به گونه‌ای افزایش داده می‌شود که بتوان خطاها را شناسایی و در صورت امکان آن‌ها را برطرف نمود.

در مثال قبل، می‌خواهیم کدگذاری کانال را با اضافه کردن یک بیت به پیامِ کدگذاریِ منبع شده، انجام دهیم. فرض کنیم کدگذاری کانال را برای چهار رنگ قرمز، آبی، سفید و سبز، به ترتیب، به صورت ۰۰۰، ۰۱۱، ۱۰۱ و ۱۱۰ انجام داده‌ایم و پیام «قرمز» را از طریق یک کانال نویزدار انتقال داده‌ایم و تنها یک خطا رخ داده است. در این صورت واژهٔ دریافت شده، می‌بایست یکی از واژه‌های ۱۰۰، ۰۱۰ یا ۰۰۱ باشد. از آنجا که هیچ یک از این واژه‌ها در میان پیام‌های کدگذاری شده نیستند، بر خلاف مثال قبل، می‌توان به صراحت گفت که خطایی رخ داده است.

در مثال فوق، از آنجا که می‌بایست ۳ بیت، به جای ۲ بیت ارسال شود، این شکلِ کدگذاری، به ما این اجازه را می‌دهد که به قیمت پایین آمدن سرعت انتقال اطلاعات، متوجه بروز خطا شویم. با این وجود، این شکل کدگذاری، امکان تصحیح خطا را به ما نمی‌دهد. مثلاً فرض کنیم واژهٔ ۱۰۰ دریافت شده باشد، در این صورت نمی‌توان گفت که این واژه، از کدام یک از واژه‌های ۰۰۰، ۱۱۰ یا ۱۰۱ آمده است. اگر طولِ پیامِ کدگذاری شده را باز هم افزایش دهیم، آنگاه قادر به تصحیح خطا نیز خواهیم بود، اما سرعت انتقال اطلاعات باز هم پایین‌تر می‌آید. برای نمونه، مثال زیر را در نظر می‌گیریم:

اگر کدگذاری کانال را برای چهار رنگ قرمز، آبی، سفید و سبز، به ترتیب، به صورت ۰۰۰۰۰، ۰۱۱۱۱، ۱۰۱۱۰ و ۱۱۰۰۱ انجام دهیم و پیام «قرمز» را از طریق یک کانال نویزدار انتقال دهیم و فقط یک خطا رخ دهد، آنگاه واژهٔ دریافت شده یکی از پنج واژهٔ ۱۰۰۰۰، ۰۱۰۰۰، ۰۰۱۰۰، ۰۰۰۱۰ یا ۰۰۰۰۱ خواهد بود. فرض کنیم مثلاً واژهٔ ۱۰۰۰۰ دریافت شده باشد، در این صورت می‌توان با قاطعیت گفت که واژهٔ ۱۰۰۰۰ از واژهٔ ۰۰۰۰۰ آمده است، چرا که حداقل ۲ خطا بین واژهٔ ۱۰۰۰۰ و هر یک از سه پیامِ کدگذاری شدهٔ ۰۱۱۱۱، ۱۰۱۱۰ و ۱۱۰۰۱ وجود دارد.

---

[۷] channel coding

در ادامه، یک روش کلی و ساده برای کدگذاری کانال، به منظورِ شناسایی و تصحیح خطا معرفی می‌شود. فرض کنیم کدگذاری منبع قبلاً انجام شده است و اطلاعات، شامل رشته‌هایی به طول ثابت k باشند. در این صورت، به منظور کدگذاری کانال، هر رشته را به اندازهٔ $2r + 1$ بار تکرار می‌کنیم، که در آن r یک عدد طبیعی می‌باشد. به عنوان مثال، اگر $k = r = 2$، آنگاه برای رشتهٔ ۰۱ کدگذاری کانال به صورت زیر انجام می‌شود:

$$01 \longrightarrow 0101010101.$$

کدگشایی[۸] نیز، مثلاً برای همین حالتِ خاص، به این صورت انجام می‌گیرد:

بیت اول، عددی است که بیشترین تکرار را در مکان‌های ۱، ۳، ۵، ۷ و ۹ در رشتهٔ دریافت شده داشته باشد و بیت دوم، عددی است که بیشترین تکرار را در مکان‌های ۲، ۴، ۶، ۸ و ۱۰ در رشتهٔ دریافت شده دارد. برای نمونه، اگر واژهٔ ۱۱۰۰۱۰۰۰۱۰ دریافت شده باشد، آنگاه آن را به ۱۰ کدگشایی می‌کنیم.

در این مثالِ خاص، اگر حداکثر دو خطا رخ دهد، آنگاه می‌توان واژهٔ دریافت شده را به درستی کدگشایی نمود. در حالتِ کلی، اگر حداکثر r خطا رخ دهد، آنگاه می‌توان واژهٔ دریافت شده را به درستی کدگشایی نمود. این شکلِ کدگذاری را کدِ تکرار[۹] می‌نامند.

مشکلِ کدگذاری کانال به روش کدِ تکرار، از دست دادن جدی سرعت انتقال اطلاعات است. بنابراین در کدگذاری کانال به دنبال روش‌های کارآمدتری می‌باشند. در حقیقت، هدف از کدگذاری کانال، ساختن کدگذارها[۱۰] و کدگشاهایی[۱۱] است که شرایط زیر را مهیا سازند:

(i) سریع بودن در کدگذاری پیام‌ها،

(ii) سادگی انتقال پیام کدگذاری شده،

(iii) سریع بودن کدگشایی پیام‌های دریافت شده،

(iv) ماکزیمم کردن انتقال اطلاعات در واحد زمان،

(v) به حداکثر رساندن قابلیت شناسایی و تصحیح خطاهای احتمالی.

از نقطه نظر ریاضیات، اهداف اصلی، (iv) و (v) می‌باشند.

---

[۸] decoding
[۹] repetition code
[۱۰] encoder
[۱۱] decoder

در این راستا کدهای بسیاری، از جمله کدهای خطی و در حالتِ خاصِ آن کدهای دوری، معرفی و مورد مطالعه قرار گرفته‌اند. یکی دیگر از انواعِ کدهای شناخته شده، کدهای شبه دوری می‌باشند که از دههٔ ٦٠ میلادی مورد مطالعه و بررسی قرار گرفته‌اند. در مرجع [٦]، مقدمه‌ای بر کاربردها و تاریخچهٔ آن‌ها آورده شده است. از سال ۱۹۹۳، که کونان[۱۲] و سِگوِیین[۱۳] مقالهٔ خود را با عنوان «خواصِ ساختاری و شمارشِ کدهای شبه دوری[۱۴]» به چاپ رساندند (مرجع [۲] را ببینید)، دانشمندان بسیاری، دیدگاه‌های گوناگونی را برای توصیفِ ساختارهای مختلفِ این نوع از کدها ارائه کرده‌اند.

به عنوان مثال، در مرجعِ [۳]، کدهای شبه دوری با شاخص ℓ روی $\mathbb{F}_q$ به عنوان یک زیر مدولِ حلقهٔ خارج قسمتی $\mathbb{F}_{q^\ell}[X]/(X^m - ۱)$ در نظر گرفته شده‌اند، که در آن $(X^m - ۱)$، ایده‌الِ تولید شده توسط چندجمله‌ای $X^m - ۱$ می‌باشد؛ این رویکرد، رده‌بندی کامل کدهای خوددوگان با شاخص ۲ را به دست می‌دهد. در مراجعِ [٦] و [۷]، نویسندگان، کدهای شبه دوری را به عنوان کدهایی خطی روی یک حلقهٔ جابجایی در نظر گرفته‌اند.

در این پایان‌نامه، کدهای شبه دوری، به عنوان کدهایی دوری روی یک حلقه از ماتریس‌های روی $\mathbb{F}_q$ در نظر گرفته شده اند. فصل اول به تعاریف و نمادگذاری نظریهٔ کدگذاری اختصاص یافته است. در فصل دوم به معرفی و بیان برخی خواص کدهای خطی و کدهای دوری می‌پردازیم. در فصل آخر این پایان‌نامه با دنباله‌های بازگشتی خطی با ضرایب ماتریسی مواجه خواهیم شد و به معرفی و ساخت برخی کدهای شبه دوری خواهیم پرداخت. به خصوص در این فصل، به مطالعهٔ کدِ دوگانِ یک $\Omega(P)$–کد می‌پردازیم و نشان می‌دهیم که کدِ دوگانِ یک $\Omega(P)$–کد (چه در حالت اقلیدسی[۱۵] و چه در حالت هرمیتی[۱٦])، یک $\Omega(P')$–کد می‌باشد. مراجع اصلی در نگارش این پایان‌نامه، مراجع [۱]، [۴] و [۸] می‌باشند.

[۱۲] J. Conan

[۱۳] G. Seguin

[۱۴] structural properties and enumeration of quasi-cyclic codes

[۱۵] Euclidean

[۱٦] Hermitian

فهرست مندرجات

فصل ۱

تعاریف و نمادگذاری نظریه کدگذاری

در این فصل، ابتدا به تعریف کد می‌پردازیم و سپس فاصلهٔ همینگ را معرفی نموده و با استفاده از آن، الگوی کدگشایی نزدیک‌ترین همسایگی را برای یک کد ارائه می‌دهیم. در ادامه، فاصلهٔ کد را معرفی خواهیم کرد که یکی از مشخصه‌های مهم یک کد می‌باشد. در پایانِ این فصل، کدهای دوگان اقلیدسی و هرمیتی را مورد بررسی قرار می‌دهیم.

۱.۱ کد

در زیر به برخی تعاریف بنیادین در ارتباط با نظریهٔ کدگذاری می‌پردازیم:

تعریف ۱.۱.۱ فرض کنیم $A = \{a_۱, a_۲, \dots, a_q\}$ یک مجموعهٔ q عضوی باشد، در این صورت A را الفبای کد[۱] و هر عضو آن را نمادِ کد[۲] می‌نامند.

(i) یک واژهٔ q تایی[۳] به طول n روی A، رشته‌ای به شکلِ $w = w_۱w_۲\dots w_n$ می‌باشد، که در آن، به ازای هر $۱ \leq i \leq n$، $w_i \in A$. به طور هم ارز می‌توان w را به صورت بردار $(w_۱, \dots, w_n)$ نیز در نظر گرفت.

---

[۱] code alphabet

[۲] code symbol

[۳] q-ary word

(ii) به مجموعهٔ ناتهی C، متشکل از واژه‌های q تایی به طول n روی A، یک کد بلوکیِ q تایی [۴] به طول n روی A می‌گویند. در نتیجه $C \subseteq A^n$. گاهی اوقات، کد بلوکیِ q تایی C را کد q تایی یا به طور خلاصه‌تر کد می‌نامند.

(iii) A^n را فضای کد[۵] و اعضای کدِ C را کدواژه[۶] می‌نامند.

(iv) منظور از $|C|$، اندازهٔ کد C می‌باشد که عبارت است از تعداد اعضای کد C.

(v) کدِ به طول n و با اندازهٔ M را (n, M)—کد می‌نامند.

معمولاً میدانِ متناهی $\mathbb{F}_q$ را به عنوان الفبای کد در نظر می‌گیرند. یک کد، با الفبای کد $\mathbb{F}_۲ = \{۰, ۱\}$ را کد دودویی[۷] می‌نامند؛ به عبارت دیگر، نمادهای یک کد دودویی ۰ و ۱ می‌باشند. به دلیل پر کاربرد بودنِ کدهای دودویی، مناسب به نظر می‌رسد که مثال‌هایی از آن‌ها را ارائه کنیم.

مثال ۱.۱.۱ نمونه‌هایی از کدهای دودویی عبارتند از:

(i) $C_۱ = \{۰۰, ۰۱, ۱۰, ۱۱\}$ یک $(۲, ۴)$—کد است؛

(ii) $C_۲ = \{۰۰۰, ۰۱۱, ۱۰۱, ۱۱۰\}$ یک $(۳, ۴)$—کد می‌باشد؛

(iii) $C_۳ = \{۰۰۱۱, ۰۱۰۱, ۱۰۱۰, ۱۱۰۰, ۱۰۰۱, ۰۱۱۰\}$ یک $(۴, ٦)$—کد است.

۲.۱ فاصلهٔ همینگ

ابتدا تعریف زیر را در نظر می‌گیریم:

تعریف ۱.۲.۱ فرض کنیم x و y دو واژه به طول n روی الفبای A باشند، در این صورت فاصلهٔ همینگ[۸] از x تا y را با $d(x, y)$ نمایش می‌دهیم که عبارت است از تعداد جایگاه‌هایی که x و y با هم تفاوت دارند. به عبارت دیگر، اگر $x = x_۱ \cdots x_n$ و $y = y_۱ \cdots y_n$، آنگاه

$$d(x, y) = d(x_۱, y_۱) + \cdots + d(x_n, y_n), \qquad (۱)$$

[۴] q-ary block code
[۵] codespace
[۶] codeword
[۷] binary code
[۸] Hamming distance

که در آن x_i و y_i واژه‌های به طول ۱ هستند و

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

اکنون مثال زیر را در نظر می‌گیریم:

مثال ۱.۲.۱ (i) اگر $x = ۰۱۰۱۰$، $y = ۰۱۱۰۱$ و $z = ۱۱۱۰۱$ واژه‌هایی روی الفبای کد $A = \{۰, ۱\}$ باشند، آنگاه

$$\begin{aligned} d(x,y) &= ۳, \\ d(y,z) &= ۱, \\ d(z,x) &= ۴. \end{aligned}$$

(ii) فرض کنیم $A = \{۰, ۱, ۲, ۳, ۴\}$، $x = ۱۲۳۴$، $y = ۱۴۲۳$ و $z = ۳۲۱۴$. در این صورت داریم:

$$\begin{aligned} d(x,y) &= ۳, \\ d(y,z) &= ۴, \\ d(z,x) &= ۲. \end{aligned}$$

در گزارهٔ زیر یک خاصیت مهم فاصلهٔ همینگ آورده شده است:

گزاره ۱.۲.۱ فاصلهٔ همینگ، یک متر روی فضای کد A^n تعریف می‌کند. به عبارت دیگر اگر x، y و z واژه‌هایی به طول n روی A باشند، آنگاه

(i) $۰ \leq d(x,y) \leq n$،

(ii) $d(x,y) = ۰ \Longleftrightarrow x = y$،

(iii) $d(x,y) = d(y,x)$،

(iv) (نامساوی مثلثی) $d(x,z) \leq d(x,y) + d(y,z)$.

برهان. (i)، (ii) و (iii) به وضوح از تعریف فاصلهٔ همینگ (تعریف ۱.۲.۱) نتیجه می‌شوند. برای اثبات (iv)، با توجه به رابطهٔ (۱)، کافی است اثبات را تنها در حالت $n = ۱$ ارائه دهیم.در این صورت:

اگر $x = z$، آنگاه $d(x,z) = ۰$ و بنابراین (iv) به وضوح درست است.

اگر $x \neq z$، آنگاه $x \neq y$ یا $z \neq y$، و در نتیجه (iv) مجدداً درست می‌باشد. ■

۳.۱ کدگشایی نزدیکترین همسایگی یا کدگشایی کمترین فاصله

فرض کنیم کدواژه‌های کدِ C از طریق یک کانال ارتباطی ارسال می‌شوند. در این صورت، اگر واژهٔ x دریافت شود، آنگاه قانون کدگشایی نزدیکترین همسایگی[۹] (یا قانون کدگشایی کمترین فاصله[۱۰]) x را به c_x کدگشایی می‌کند، به طوری که c_x کمترین فاصله را تا x داشته باشد، یعنی:

$$d(x, c_x) = \min_{c \in C} d(x, c).$$

(i) کدگشایی کامل نزدیکترین همسایگی: اگر x دریافت شد، آنگاه نزدیکترین همسایه‌اش را پیدا کن. اگر بیش از یک چنین کدواژه‌ای پیدا شد، آنگاه یکی را به دلخواه انتخاب کن.

(ii) کدگشایی غیرکامل نزدیکترین همسایگی: اگر x دریافت شد، آنگاه نزدیکترین همسایه‌اش را پیدا کن. اگر بیش از یک چنین کدواژه‌ای پیدا شد، آنگاه درخواست کن که انتقال، مجدداً صورت گیرد.

مثال ۱.۳.۱ فرض کنیم کدواژه‌های کد دودویی

$$C = \{۰۰۰۰, ۰۰۱۱, ۱۰۰۰, ۱۱۰۰, ۰۰۰۱, ۱۰۰۱\},$$

از طریق یک کانال ارسال می‌شوند. در این صورت، اگر $x = ۰۱۱۱$ دریافت شود، آنگاه

$$\begin{aligned} d(۰۱۱۱, ۰۰۰۰) &= ۳, \\ d(۰۱۱۱, ۰۰۱۱) &= ۱, \\ d(۰۱۱۱, ۱۰۰۰) &= ۴, \\ d(۰۱۱۱, ۱۱۰۰) &= ۳, \\ d(۰۱۱۱, ۰۰۰۱) &= ۲, \\ d(۰۱۱۱, ۱۰۰۱) &= ۳, \end{aligned}$$

و با استفاده از کدگشایی نزدیکترین همسایگی، x را به ۰۰۱۱ کدگشایی می‌کنیم.

مثال ۲.۳.۱ کد دودویی $C = \{۰۰۰, ۰۱۱\}$ را در نظر می‌گیریم. جدول کدگشایی غیرکامل نزدیکترین همسایگی، برای C در جدول ۱ آورده شده است، که در آن "−" یعنی درخواست شده است که انتقال مجدداً صورت گیرد.

---

[۹] nearest neighbour decoding

[۱۰] minimum distance decoding

جدول ۱ . کدگشایی غیرکامل نزدیکترین همسایگی برای C.

کدگشایی به	$d(x, ۰۱۱)$	$d(x, ۰۰۰)$	x دریافت شده
۰۰۰	۲	۰	۰۰۰
۰۰۰	۳	۱	۱۰۰
–	۱	۱	۰۱۰
–	۱	۱	۰۰۱
–	۲	۲	۱۱۰
–	۲	۲	۱۰۱
۰۱۱	۰	۲	۰۱۱
۰۱۱	۱	۳	۱۱۱

۱.۴ فاصلهٔ کد

هر کد، علاوه بر اندازه و طول، مشخصهٔ مهم دیگری نیز دارد که فاصلهٔ کد می‌باشد.

تعریف ۱.۴.۱ فرض کنیم C کدی با اندازهٔ حداقل ۲ باشد، در این صورت فاصلهٔ کد C که با $d(C)$ نشان داده می‌شود عبارت است از:

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

کدِ به طول n و با اندازهٔ M و فاصلهٔ d را (n, M, d)—کد می‌نامند. به علاوه، اعداد n، M و d را پارامترهای کد می‌نامند.

مثال ۱.۴.۱ (i) اگر $C = \{۰۰۰۰۰, ۰۰۱۱۱, ۱۱۱۱۱\}$، آنگاه $d(C) = ۲$، چرا که

$$\begin{aligned} d(۰۰۰۰۰, ۰۰۱۱۱) &= ۳, \\ d(۰۰۰۰۰, ۱۱۱۱۱) &= ۵, \\ d(۰۰۱۱۱, ۱۱۱۱۱) &= ۲. \end{aligned}$$

در نتیجه C یک $(۵, ۳, ۲)$—کد است.

(ii) فرض کنیم $C=\{۰۰۰۰۰۰,۰۰۰۱۱۱,۱۱۱۲۲۲\}$ یک کد سه‌سه‌ای[۱۱] باشد (یعنی الفبای کد آن $\{۰,۱,۲\}$ است). در این صورت از آنجا که

$$\begin{aligned} d(۰۰۰۰۰۰,۰۰۰۱۱۱) &= ۳,\\ d(۰۰۰۰۰۰,۱۱۱۲۲۲) &= ۶,\\ d(۰۰۰۱۱۱,۱۱۱۲۲۲) &= ۶, \end{aligned}$$

پس $d(C)=۳$ و در نتیجه C یک $(۶,۳,۳)$—کد سه‌سه‌ای می‌باشد.

حال قضیهٔ زیر را داریم:

قضیه ۱.۴.۱ فرض کنیم C، کدی با اندازهٔ $d=d(C)$ باشد. در این صورت، اگر از الگوی کدگشایی نزدیکترین همسایگی استفاده کنیم، آنگاه قادر به شناسایی حداکثر $d-۱$ خطا هستیم و به علاوه، حداکثر تا $\lfloor\frac{d-۱}{۲}\rfloor$ خطا را می‌توانیم تصحیح نماییم.

برهان. در مرجعِ [۸] قضایای ۶.۵.۲ و ۱۰.۵.۲ را ببینید. ■

۵.۱ کدِ دوگان اقلیدسی و هرمیتی

در این قسمت به معرفی کدِ دوگان اقلیدسی و هرمیتی برای یک کد می‌پردازیم که از اهمیت ویژه‌ای در این پایان‌نامه برخوردارند. در این راستا ابتدا تعریف زیر را در نظر می‌گیریم:

تعریف ۱.۵.۱ اگر $\mathcal{R}$ یک حلقهٔ جابجایی باشد و $n\in\mathbb{N}$، آنگاه ضرب داخلی اقلیدسی[۱۲] به صورت زیر تعریف می‌شود:

$$\forall a=(a_۱,\dots,a_n)\in\mathcal{R}^n,\quad \forall b=(b_۱,\dots,b_n)\in\mathcal{R}^n,\qquad \langle a,b\rangle_e=\sum_{i=۱}^{n}a_ib_i.$$

حال می‌توانیم کدِ دوگان اقلیدسیِ یک کد را به صورت زیر تعریف نماییم:

[۱۱] ternary code

[۱۲] Euclidean inner product

تعریف ۱.۵.۲ فرض کنیم $\mathcal{R}$ یک حلقهٔ جابجایی باشد و $n \in \mathbb{N}$. به علاوه فرض کنیم C یک کد به طول n روی $\mathcal{R}$ باشد. در این صورت، مجموعهٔ زیر را کدِ دوگان اقلیدسی [۱۳] کدِ C می‌نامند:

$$\{d \in \mathcal{R}^n :\ \forall c \in C, \quad \langle c, d\rangle_e = 0\}.$$

کدِ دوگان اقلیدسی کد C را با $C^{\perp_e}$ نمایش می‌دهند.

مثال ۱.۵.۱ می‌خواهیم کدِ دوگان اقلیدسیِ کد دودویی $C = \{0100, 0101\}$ را بیابیم. برای این منظور فرض کنیم $v = (v_1, v_2, v_3, v_4)$ واژه‌ای از $C^{\perp_e}$ باشد، در این صورت داریم:

$$\langle (0,1,0,0), v\rangle_e = 0 \implies v_2 = 0,$$
$$\langle (0,1,0,1), v\rangle_e = 0 \implies v_2 + v_4 = 0.$$

در نتیجه $v_2 = v_4 = 0$. از آنجا که v_1 و v_3 می‌توانند ۰ یا ۱ باشند، پس داریم:

$$C^{\perp_e} = \{0000, 0010, 1000, 1010\}.$$

برای معرفی کدِ دوگان هرمیتیِ یک کد، لازم به نظر می‌رسد که ابتدا تعریف زیر را ارائه نماییم:

تعریف ۱.۵.۳ فرض کنیم $\mathcal{R}$ یک حلقهٔ جابجایی، $n \in \mathbb{N}$ و θ یک خودریختی $\mathcal{R}$ از مرتبهٔ ۲ باشد. در این صورت، ضرب داخلی هرمیتی [۱۴] در $\mathcal{R}^n$ به صورت زیر تعریف می‌شود:

$$\forall a = (a_1, \dots, a_n) \in \mathcal{R}^n, \forall b = (b_1, \dots, b_n) \in \mathcal{R}^n, \qquad \langle a, b\rangle_h = \sum_{i=1}^{n} a_i \theta(b_i).$$

حال به تعریف کدِ دوگان هرمیتی می‌پردازیم.

تعریف ۱.۵.۴ اگر $\mathcal{R}$ یک حلقهٔ جابجایی، $n \in \mathbb{N}$ و C کدی به طول n روی $\mathcal{R}$ باشد، آنگاه مجموعهٔ زیر را کدِ دوگان هرمیتی [۱۵] کدِ C می‌نامند:

$$\{d \in \mathcal{R}^n :\ \forall c \in C, \quad \langle c, d\rangle_h = 0\}.$$

کدِ دوگان هرمیتی کدِ C را با $C^{\perp_h}$ نمایش می‌دهند.

[۱۳] Euclidean dual code
[۱۴] Hermitian inner product
[۱۵] Hermitian dual code

مثال ۲.۵.۱ فرض کنیم $\mathbb{F}_4 = \mathbb{F}_2[w]$ $(w^2 + w + 1 = 0)$ و نگاشت θ به این شکل تعریف شده باشد:

$$\begin{aligned} \theta : \mathbb{F}_4 &\longrightarrow \mathbb{F}_4 \\ x &\mapsto x^2, \end{aligned}$$

در این صورت می‌خواهیم کدِ دوگان هرمیتیِ کد $C = \{0101\}$ روی $\mathbb{F}_4$ را بیابیم. برای این منظور فرض کنیم $v = (v_1, v_2, v_3, v_4)$ واژه‌ای از $C^{\perp_h}$ باشد، در این صورت داریم:

$$\langle (0, 1, 0, 1), v \rangle_h = 0 \implies {v_2}^2 + {v_4}^2 = 0.$$

اگر v_2 یا v_4 برابر با صفر باشند، آنگاه دیگری نیز برابر با صفر می‌شود. حال فرض می‌کنیم v_2 و v_4 غیر صفر باشند. در این صورت با ضربِ $v_2 v_4$ در طرفین تساوی $0 = {v_2}^2 + {v_4}^2$، داریم:

$$v_4 {v_2}^3 + v_2 {v_4}^3 = 0.$$

از آنجا که در یک میدانِ متناهی، هر عضو به توانِ «مرتبهٔ میدان منهای ۱» برابر با ۱ است، پس داریم:

$$v_4 + v_2 = 0,$$

و چون مشخصهٔ میدان $\mathbb{F}_4$ برابر با ۲ می‌باشد، نتیجه می‌گیریم که $v_2 = v_4$. برعکس، از آنجا که مشخصهٔ میدان $\mathbb{F}_4$ برابر با ۲ است، پس به ازای هر $v_2 = v_4 \in \mathbb{F}_4$ داریم:

$${v_2}^2 + {v_4}^2 = 0.$$

پس در کل می‌توان نوشت:

$$C^{\perp_h} = \{(\alpha, \beta, \gamma, \beta) \ : \ \alpha, \beta, \gamma \in \mathbb{F}_4\}.$$

در تعریف زیر به معرفی دو ردهٔ مهم از کدها می‌پردازیم.

تعریف ۵.۵.۱ برای کدِ C داریم:

(i) C را کدِ خوددوگان اقلیدسی[۱۶] نامیم هر گاه $C = C^{\perp_e}$،

(ii) C کدِ خوددوگان هرمیتی[۱۷] می‌باشد هر گاه $C = C^{\perp_h}$.

[۱۶] Euclidean self-dual code

[۱۷] Hermitian self-dual code