دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

تحلیل کدهای حاصل‌ضرب برای کانال پاک‌شدگی دودویی

رساله دکتری ریاضی کاربردی، گرایش نظریه اطلاعات و کدگذاری

مرتضی هیودی

استاد راهنما

دکتر مرتضی اسماعیلی

۱۳۸۸

کلیه حقوق مادی مترتب بر نتایج مطالعات، ابتکارات و نوآوری‌های ناشی از تحقیق موضوع این پایان‌نامه متعلق به دانشگاه صنعتی اصفهان است.

فهرست مطالب

چکیده:

کارایی یک کد خطی تحت کدگشایی تکراری روی یک کانال پاک‌شدگی دودویی توسط مجموعه‌های متوقف‌کننده مشخص می‌شود. ارتباط بین مجموعه‌های متوقف‌کننده ماتریس‌های بررسی توازن برای کدهای حاصل‌ضرب با مجموعه‌های متوقف‌کننده ماتریس‌های بررسی توازن کدهای مؤلفه بررسی می‌شوند. کران‌های بالایی برای افزونگی متوقف‌کننده کدهای حاصل‌ضرب براساس افزونگی متوقف‌کننده کدهای مؤلفه ارائه می‌شود. سپس کران‌های بهتری برای افزونگی متوقف‌کننده کدهای حاصل‌ضرب معرفی می‌شود. نشان داده می‌شود که کران‌های به‌دست آمده، در برخی حالات، بهترین کران ممکن هستند. یک مفهوم جدید تحت عنوان افزونگی متوقف‌کننده بهینه معرفی شده و نشان داده شده است که کد حاصل‌ضرب یک بررسی—توازن r—بعدی، یک کد افزونگی متوقف‌کننده بهینه است. با استفاده از تحلیل مجموعه‌های متوقف‌کننده و فاصله متوقف‌کننده کدهای حاصل‌ضرب، کدهای حاصل‌ضرب خوبی بر اساس کدهای مؤلفه مناسب طراحی می‌شوند. از نقاط قوت کدهای ساخته شده، ساختار قوی ریاضی به‌همراه کدگذاری و کدگشایی بسیار ساده آن‌ها است. کدهای حاصل‌ضرب $LDPC$ ساخته شده نرخ و مینیمم فاصله خوبی دارند. همچنین فاصله متوقف‌کننده کدهای طراحی شده نسبت به کدهای $LDPC$ شناخته شده که فاصله متوقف‌کننده آن‌ها مشخص است، بهتر است. در بین کدهای ساخته شده، کدهای $LDPC$ با پارامترهای [۵۱۱,۱۸۰,۳۰]، [۹۴۵,۴۰۷,۲۷]، [۲۲۶۳,۱۱۷۰,۳۰] و [۴۰۹۵,۲۱۰۱,۵۴] به‌ترتیب دارای فاصله متوقف‌کننده ۳۰، ۲۷، ۳۰ و ۵۴ وجود دارند.

برای احتمال پاک‌شدگی کم کانال، احتمال خطای کدگشایی تکراری با استفاده از چندگانگی فاصله متوقف‌کننده مشخص می‌شود. احتمال خطای کدگشایی تکراری برای کدهای حاصل‌ضرب همینگ برای احتمال پاک‌شدگی کم کانال بررسی می‌شود. کدگشایی‌های بیشینه درست‌نمایی، تکراری (تکثیر اطمینان) و تکراری سطری—ستونی [۴۰] برای کدهای حاصل‌ضرب روی کانال پاک‌شدگی دودویی بیان شده‌اند. نشان داده می‌شود که برای احتمال پاک‌شدگی کم کانال، احتمال خطای کدگشایی تکراری برای کد حاصل‌ضرب همینگ بسیار نزدیک به احتمال خطای کدگشایی بیشینه درست‌نمایی و تکراری سطری—ستونی است.

کلمات کلیدی: فاصله متوقف‌کننده، افزونگی متوقف‌کننده، کدهای $LDPC$، کد حاصل‌ضرب.

فصل ۱

مقدمه

۱—۱ انگیزه و مقدمه تاریخی

نظریه کدگذاری دانشی برای انتقال صحیح داده‌ها با کم‌ترین هزینه ممکن از مکانی به مکان دیگر یا به زمان آینده است. واسطه فیزیکی انتقال داده‌ها کانال نامیده می‌شود. مکالمات تلفنی، ارسال اطلاعات به زمین توسط ایستگاه‌های فضایی و نگهداری داده‌ها روی یک CD نمونه‌هایی از انتقال داده‌ها از طریق یک کانال است. نظریه احتمال، جبر، جبر خطی، هندسه جبری، ترکیبیات و گراف ابزارهای ریاضی استفاده شده در عمر حدود شصت ساله این نظریه هستند. این نظریه در سال ۱۹۴۸ توسط کلود شانون پایه‌گذاری شده است. وی در مقاله‌ای با عنوان، نظریه ریاضی مخابرات، نشان داد که با افزودن بیت‌های اضافی می‌توان خطای رخ داده در انتقال داده‌ها را از یک کانال را بهتر تشخیص داد.[۴۳]. وی همچنین ثابت کرد که در یک کانال مخابراتی، پارامتری به‌نام ظرفیت کانال وجود دارد که انتقال داده‌ها با هر نرخ دلخواه و نزدیک به ظرفیت کانال و نه بیشتر از آن امکان پذیر است به گونه‌ای که احتمال خطای کدگشایی، با افزایش طول کد، به سمت صفر میل می‌کند.

قابل ذکر است که شانون در [۴۳] روشی برای ساخت کدهای خوب مطرح نکرد. روش‌های ساخت کدهای خوب و الگوریتم‌های کارا برای پیاده‌سازی آن‌ها به‌عنوان مسئله اصلی نظریه کدگذاری و از زمینه‌های کار محققان در چند دهه اخیر بوده است. در این راستا، اخیراً محققان به روش کدگشایی

تکراری، به‌ویژه روی کدهای با ماتریس بررسی—توازن خلوت $LDPC$، توجه فراوانی نموده‌اند. در ادامه این بخش به بیان تاریخچه کدهای $LDPC$ و کدگشایی تکراری پرداخته می‌شود.

کدهای $LDPC$ نخستین بار توسط گالاگر در سال ۱۹۶۲ مطرح شدند[۱۲]. وی در سال ۱۹۶۳ از رساله دکترای خود، با عنوان کدهای $LDPC$، در دانشگاه MIT دفاع نمود[۱۳]. گالاگر یک روش ساختاری برای کدهای $LDPC$ ارائه نمود و نشان داد که کارایی کدهای $LDPC$ تحت کدگشایی تکراری بسیار نزدیک به حد ارائه شده توسط شانون است. پس از آن کدهای $LDPC$ نزدیک سی سال به فراموشی سپرده شدند. محاسبات با پیچیدگی بالا برای شبیه‌سازی و نبود ابزارها و روش‌های کافی برای تجزیه و تحلیل این کدها دلیل اصلی این واقعیت هستند. چند سال بعد از ابداع کدهای توربو [۴ ،۳]، کدهای $LDPC$ دوباره مطرح شدند[۲۶ ،۶ ،۳۸ ،۳۷ ،۲۱ ،۲۸ ،۲۷].

در سال ۱۹۸۱ یک مدل گرافی برای توصیف کدهای $LDPC$ توسط تنر مطرح شد[۴۷] که به گراف تنر معروف است. این کدها توسط مک‌کی [۲۸]، ریچاردسون و همکارانش [۳۸ ،۳۷] و سایر محققان[۲۶ ،۶ ،۲۱] احیا، تجزیه، تحلیل و تعمیم داده شد و برای کدگشایی تکراری این کدها، الگوریتم‌های ساده‌ای مطرح شده است که پیچیدگی آن‌ها خطی است یعنی با افزایش طول کد $LDPC$، پیچیدگی محاسباتی کدگشایی به‌صورت خطی افزایش می‌یابد.

تجزیه و تحلیل کارایی کدگشایی تکراری روی کانال‌های مخابراتی یک موضوع مهم تحقیقاتی است. بهبود کدگشایی تکراری و ساخت کدهای بهتر نتایجی از این تجزیه و تحلیل است. محققان به روش کدگشایی تکراری(تکثیر اطمینان)، به‌ویژه روی کدهای با ماتریس بررسی—توازن خلوت $LDPC$، توجه فراوانی دارند. کارایی کدگشایی تکراری روی کانال پاک‌شدگی دودویی بررسی شده است[۷]. کانال پاک‌شدگی دودویی توسط الیاس [۸] در ۱۹۵۵ مطرح شد. اخیراً کانال پاک‌شدگی دودویی برای مدل‌بندی انتقال اطلاعات در اینترنت استفاده شده است[۴۴].

دی، پرویتی، تیلتر، ریچاردسون و اوربانکی در [۷] نشان داده‌اند که کارایی یک کد با ماتریس بررسی—توازن خلوت تحت کدگشایی تکراری روی کانال پاک‌شدگی دودویی توسط یک ساختار ترکیبیاتی که مجموعه متوقف‌کننده نامیده می‌شود، مشخص می‌شود. یک زیرمجموعه رئوس متغییر S در گراف تنر متناظر با یک ماتریس بررسی—توازن H برای کد $\mathcal{C}$ یک مجموعه متوقف‌کننده نامیده می‌شود هرگاه همه همسایه‌های S حداقل دو بار به S وصل شوند. در تعدادی از مقالات، از جمله در [۱۷ ،۳۳]، اندازه

کوچکترین مجموعه متوقف‌کننده را فاصله متوقف‌کننده نامیده‌اند. اندازه کوچکترین مجموعه متوقف‌کننده در یک گراف تنر برای یک کد $\mathcal{C}$ نقش مهمی در کارایی کد $\mathcal{C}$ تحت کدگشایی تکراری روی کانال پاک‌شدگی دودویی (یکسان با نقش می‌نیمم فاصله d برای کدگشایی بیشینه درست‌نمایی) دارد. یک تفاوت مهم بین می‌نیمم فاصله همینگ و فاصله متوقف‌کننده وجود دارد. می‌نیمم فاصله همینگ یک خاصیت کد $\mathcal{C}$ است ولی فاصله متوقف‌کننده به گراف تنر کد $\mathcal{C}$ (یا معادل آن به ماتریس بررسی—توازن H برای کد $\mathcal{C}$) وابسته است. فاصله متوقف‌کننده یک ماتریس بررسی—توازن H برای یک کد خطی $\mathcal{C}$ با $s(H)$ نشان داده می‌شود. کران‌های بالا و پایینی برای فاصله متوقف‌کننده کدهای $LDPC$ ساخته شده از ۲—طرح‌ها در [۱۷] وجود دارند. در [۳۳] فاصله متوقف‌کننده کدهای $LDPC$ منظم و نامنظم بررسی شده است. در [۵۰] یک کران پایین برای فاصله متوقف‌کننده کدهای هندسه متناهی $LDPC$ بیان شده است. ارتباط بین فاصله متوقف‌کننده و کمر گراف‌های تنر در [۳۲] بررسی شده است.

یک ماتریس بررسی—توازن H برای یک کد خطی $\mathcal{C}$، $n - dim(\mathcal{C})$ سطر مستقل خطی دارد. افزونگی $r(\mathcal{C})$ برای یک کد خطی $\mathcal{C}$ برابر حداقل تعداد سطرهای یک ماتریس بررسی—توازن برای $\mathcal{C}$ تعریف می‌شود. افزایش سطرهای وابسته در H، فاصله متوقف‌کننده $s(H)$ را بزرگتر می‌کند. شوارتز و واردی در [۴۲]، افزونگی متوقف‌کننده $\rho(\mathcal{C})$ را برای یک کد خطی $\mathcal{C}$ برابر حداقل تعداد سطرهای یک ماتریس بررسی—توازن H برای $\mathcal{C}$ تعریف کرده‌اند که $s(H) = d$ و d مینیمم فاصله کد $\mathcal{C}$ است. آن‌ها نشان داده‌اند که افزونگی متوقف‌کننده $\rho(C)$ خوش‌تعریف است و برای هر کد خطی دودویی $\rho(C) \leq ۲^{r(C)} - ۱$. همچنین یک کران بالا و یک کران پایین برای افزونگی متوقف‌کننده کدهای خطی دودویی و کران‌هایی برای افزونگی متوقف‌کننده برخی کدهای خطی از جمله کد گلی [۲۴, ۱۲, ۸]، کدهای رید—مولر و کدهای MDS معرفی شده است. هان و سیگل [۱۴] کران‌های بالای بهتری برای افزونگی متوقف‌کننده کدهای خطی مطرح کرده‌اند. همچنین آن‌ها کران‌های بالای قوی‌تری برای افزونگی متوقف‌کننده کدهای MDS ارائه داده‌اند. در [۱۱] افزونگی متوقف‌کننده کدهای رید—مولر دودویی، به ویژه کد رید—مولر مرتبه اول، بررسی شده است.

در [۴۲] کران‌های بالایی برای افزونگی متوقف‌کننده کدهای ساخته شده از کدهای دیگر (ساختارهای (u,v) و (u,u)) ارائه شده است و بر اساس ساختار ترکیبی آن‌ها تحلیلی برای کدگشایی آن‌ها بیان شده است. سؤال باز این است که برای افزونگی متوقف‌کننده ساختارهای دیگر چه چیزی می‌توان

بیان کرد؟ یک روش برای ساختن کدهای قوی‌تر از کدهای دیگر ضرب کدها است. کد حاصل‌ضرب توسط الیاس [۹] در ۱۹۵۴ مطرح شده است. فرض کنید کدهای خطی دودویی $\mathcal{R}$ و $\mathcal{C}$ به‌ترتیب دارای پارامترهای $[n,k,d]$ و $[n',k',d']$ باشند. در این‌صورت کد حاصل‌ضرب با کدهای مؤلفه $\mathcal{R}$ و $\mathcal{C}$، $\mathcal{P}=\mathcal{R}\otimes\mathcal{C}$، شامل همه ماتریس‌های $n'\times n$ است که هر سطر آن یک کدکلمه $\mathcal{R}$ و هر ستون آن یک کدکلمه $\mathcal{C}$ است. کد حاصل‌ضرب ساخته‌شده از کدهای همینگ با طول‌های یکسان، کد حاصل‌ضرب همینگ نامیده می‌شود[۱۵]. فرض کنید کدهای خطی دودویی $\mathcal{C}_1$،$\mathcal{C}_2$،...،$\mathcal{C}_r$ به‌ترتیب دارای پارامترهای $[n_1,k_1,d_1]$، $[n_2,k_2,d_2]$، ... و $[n_r,k_r,d_r]$ باشند. دراین‌صورت کد حاصل‌ضرب r–بعدی آن‌ها دارای طول $n=\prod_{i=1}^{r}n_i$، مینیمم فاصله $d=\prod_{i=1}^{r}d_i$ و نرخ $R=\prod_{i=1}^{r}R_i$ است که R_i نرخ کد $\mathcal{C}_i$ است [۳۵]. اگر کدهای مؤلفه $\mathcal{C}_i$، $1\leq i\leq r$، کدهای یک بررسی–توازن به‌طول یکسان n باشند آنگاه مینیمم فاصله و نرخ کد حاصل‌ضرب به‌ترتیب برابر 2^r و $(\frac{n-1}{n})^r$ است. این کد، کد حاصل‌ضرب یک بررسی–توازن r–بعدی نامیده می‌شود. کدهای حاصل‌ضرب بر اساس کدهای یک بررسی–توازن ابتدا در[۲] مورد توجه قرار گرفته است.

در فصل دوم این رساله مجموعه‌های متوقف‌کننده کدهای حاصل‌ضرب بررسی می‌شوند. همچنین فاصله متوقف‌کننده کدهای حاصل‌ضرب محاسبه می‌شود. در فصل سوم افزونگی متوقف‌کننده کدهای حاصل‌ضرب بررسی می‌شود. کران‌های بالایی برای کدهای حاصل‌ضرب ارائه می‌شود. سپس کران‌های بهتری برای افزونگی متوقف‌کننده کدهای حاصل‌ضرب بیان می‌شود. نشان داده می‌شود که کران‌های به‌دست آمده در برخی حالات، بهترین کران ممکن است. یک مفهوم جدید تحت عنوان افزونگی متوقف‌کننده بهینه معرفی شده و نشان داده می‌شود که کد حاصل‌ضرب یک بررسی–توازن r–بعدی، یک کد افزونگی متوقف‌کننده بهینه است. از این‌رو یک مثال خوب برای این مفهوم ارائه شده است. از نظر کاربردی، کدگشایی تکراری برای کدهای افزونگی متوقف‌کننده بهینه دارای پیچیدگی کم با کارایی نزدیک به کارایی کدگشایی بیشینه درست‌نمایی ML است.

در فصل چهارم با استفاده از تحلیل مجموعه‌های متوقف‌کننده و فاصله متوقف‌کننده کدهای حاصل‌ضرب، کدهای حاصل‌ضرب خوبی بر اساس کدهای مؤلفه مناسب طراحی می‌شوند. فاصله متوقف‌کننده کدهای حاصل‌ضرب ساخته شده بزرگ و قابل مقایسه با فاصله متوقف‌کننده بهترین کدهای بررسی–توازن خلوت شناخته شده است. از نقاط قوت این کدها، کارایی بالا به‌همراه کدگذاری و

کدگشایی ساده آن‌ها است.

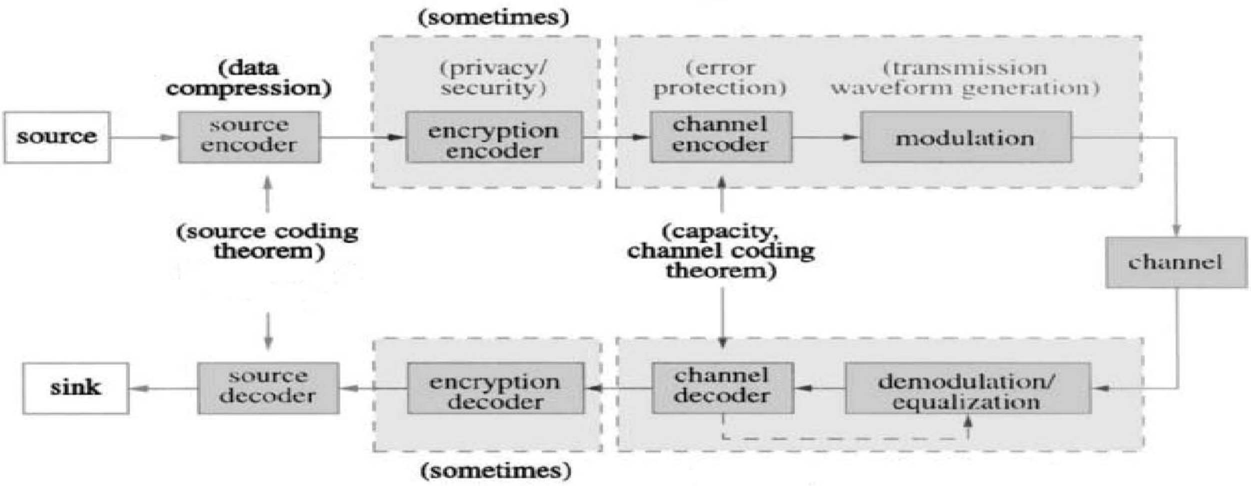
چندگانگی فاصله متوقف‌کننده(تعداد مجموعه‌های متوقف‌کننده با کمترین اندازه) نقشی اساسی در کارایی کد C تحت کدگشایی تکراری روی کانال پاک‌شدگی دودویی دارد. این نقش، یکسان با نقش چندگانگی می‌نیمم فاصله d برای کدگشایی بیشینه درست‌نمایی است. برای احتمال پاک‌شدگی کم کانال، احتمال خطای کدگشایی تکراری توسط چندگانگی فاصله متوقف‌کننده محاسبه می‌شود[۴۹]. در فصل پنجم چندگانگی فاصله متوقف‌کننده کدهای حاصل‌ضرب بررسی می‌شود. کدگشایی‌های بیشینه درست‌نمایی، تکراری (تکثیر اطمینان) و تکراری سطری—ستونی[۴۰] برای کدهای حاصل‌ضرب روی کانال پاک‌شدگی دودویی بیان شده‌اند. در کدگشایی تکراری سطری—ستونی، هر سطر از کلمه دریافتی با کدگشایی بیشینه درست‌نمایی کد سطری R و سپس هر ستون با کدگشایی بیشینه درست‌نمایی کد ستونی C کدگشایی می‌شود. این روند تا رسیدن به یک کدکلمه یا متوقف شدن کدگشایی در مرحله‌ای معین تکرار می‌شود. کدگشایی تکراری (تکثیر اطمینان) با استفاده از یک روش تکراری روی گراف تنر متناظر با یک ماتریس بررسی—توازن کد انجام می‌شود. در این رساله منظور از کدگشایی تکراری، کدگشایی تکراری تکثیر اطمینان می‌باشد. در فصل پنجم برای احتمال پاک‌شدگی کم کانال، احتمال خطای کدگشایی‌های مختلف برای کد حاصل‌ضرب با هم مقایسه می‌شوند. در ادامه این فصل مقدمات مورد نیاز بیان می‌گردد.

۱—۲ سیستم‌ها و کانال های مخابراتی

در شکل ۱—۱ دیاگرام یک سیستم مخابراتی نشان داده شده است.

تعریف ۱.۱ :

یک کانال گسسته، یک سیستم شامل الفبای ورودی X و الفبای خروجی Y و ماتریس احتمال انتقال $p(y|x)$ است که $p(y|x)$ احتمال مشاهده خروجی y به شرط ارسال ورودی x است. یک کانال بدون حافظه نامیده می‌شود هرگاه توزیع احتمال خروجی تنها به ورودی در آن زمان بستگی داشته باشد و به‌طور شرطی مستقل از ورودی‌ها و خروجی‌های قبلی کانال باشد. در ادامه برخی کانال‌های مخابراتی مهم معرفی می‌شوند.



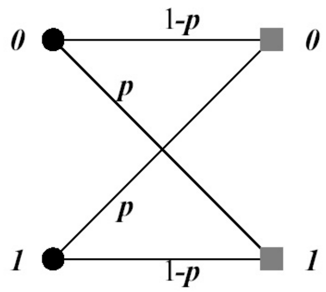
شکل ۱—۱: یک سیستم مخابراتی

کانال متقارن دودویی BSC

الفبای ورودی و خروجی این کانال دودویی است یعنی $X = Y = \{۰, ۱\}$. در این کانال هر بیت با احتمال $۱ - p$ به‌درستی و با احتمال p به غلط دریافت می‌شود. مقدار p را احتمال خطای کانال می‌نامند. بنابراین

$$Pr(۱|۰) = Pr(۰|۱) = p, \quad Pr(۰|۰) = Pr(۱|۱) = ۱ - p.$$

نمودار این کانال در شکل ۱—۲ نشان داده شده است.



شکل ۱—۲: نمودار یک کانال متقارن دودویی

ظرفیت این کانال برابر $C = 1 - H(p)$ است که در آن تابع آنتروپی $H(p)$ به‌صورت زیر تعریف می‌شود:

$$H(p) = p\log(1/p) + (1-p)\log(1/(1-p)).$$

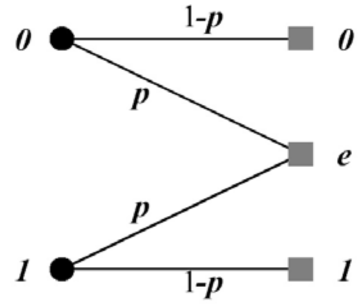
کانال پاک‌کننده دودویی BEC

کانال BEC مشابه کانال متقارن دودویی است که در آن هر بیت ورودی با احتمال p خراب می‌شود. در شکل ۱—۳ نشان داده شده است که این کانال دو ورودی و سه خروجی دارد. ظرفیت این کانال برابر $C = 1 - p$ است.

تعریف ۲.۱ مجموعه متناهی $A = \{a_1, a_2, \ldots, a_q\}$ را به‌عنوان الفبا درنظر بگیرید. هر زیرمجموعه غیرتهی $\mathbf{C}$ از A^n را یک کد qتایی به‌طول n روی A می‌نامند.

تعریف ۳.۱ (کدگذاری و کدگشایی)

فرض کنید $A = \{a_1, a_2, \ldots, a_q\}$ الفبای کد باشد. برای کدهای به‌طول n، A^n کل فضا را می‌سازد. از این‌رو هر کدکلمه که ارسال شود یک کلمه از A^n دریافت می‌شود. باید تابعی چون $f : A^n \longrightarrow \mathbf{C}$ تعریف کنیم که یک کلمه دریافت شده را به یک کدکلمه کدگشایی کند. تابع f را تابع تصمیم (تابع کدگشایی) می‌نامند. در حقیقت تبدیل یک پیام به‌طول k به یک کدکلمه به‌طول $k < n$ را عمل کدگذاری و تبدیل کلمه دریافتی به‌طول n به یک کدکلمه را عمل کدگشایی می‌نامند.



شکل ۱—۳: نمودار یک کانال پاک‌شدگی دودویی

تعریف ۴.۱ اگر اندازه $\mathbf{C}$ برابر M باشد، یعنی $|\mathbf{C}| = M$، نرخ $\mathbf{C}$ به‌صورت $R = \frac{\log_q M}{n}$ تعریف می‌شود.

قضیه ۱.۱ (قضیه اساسی شانون یا قضیه کدگذاری کانال)
فرض کنید Γ یک کانال بدون حافظه گسسته دودویی با ظرفیت $C > 0$ باشد. در این‌صورت هر نرخ کمتر از ظرفیت C دست‌یافتنی است، یعنی برای هر نرخ $R < C$، یک دنباله $(2^{nR}, n)$ کد با بیشترین احتمال خطای $\lambda^{(n)}$ وجود دارد که $\lambda^{(n)} \longrightarrow 0$.
به‌عکس، برای هر دنباله $(2^{nR}, n)$ کد با خاصیت $\lambda^{(n)} \longrightarrow 0$ داریم $R < C$.

۱–۳ کدهای خطی

در این بخش ابتدا به ارائه مفاهیم جبری مورد نیاز و سپس کدهای خطی پرداخته می‌شود. برای توضیحات بیشتر و همچنین اثبات قضایای مطرح شده می‌توان به[۲۲، ۳۹، ۲۹] مراجعه کرد.

۱–۳–۱ میدان‌های متناهی

یک میدان متناهی میدانی است که شامل تعداد متناهی عضو باشد. تعداد اعضای یک میدان متناهی را مرتبه آن میدان می‌نامند. در این قسمت بعضی از خواص میدان‌های متناهی را بدون اثبات بیان می‌کنیم.

تعریف ۵.۱ فرض کنید F یک میدان متناهی و عدد صحیح مثبت m وجود داشته باشد به‌قسمی که برای هر $\beta \in F$ داشته باشیم $m\beta = 0$. کوچکترین عدد m با این خاصیت را مشخصه میدان F می‌نامیم. در غیر این‌صورت مشخصه میدان را صفر تعریف می‌کنیم.

قضیه ۲.۱ فرض کنید F یک میدان متناهی باشد. در این‌صورت مشخصه F یک عدد اول است. همچنین تعداد اعضای یک میدان متناهی توانی از یک عدد اول است. این عدد اول مشخصه میدان است. به‌علاوه برای هر عدد اول p و عدد طبیعی m یک میدان منحصر به‌فرد F_{p^m} با p^m عضو وجود دارد.

تعریف ۶.۱ فرض کنید $p(x) \in F_q[x]$ از درجه $t > 0$ باشد. $p(x)$ را تحویل‌ناپذیر می‌نامند هرگاه روی F_q قابل تجزیه به عوامل با درجه کمتر از t نباشد.

قضیه ۳.۱ اگر $f(x)$ یک چندجمله‌ای تحویل‌ناپذیر از درجه m در $F_q[x]$ باشد آنگاه $f(x)$ ریشه‌ای چون α در F_{q^m} دارد. به‌علاوه تمام ریشه‌های $f(x)$ ساده هستند و با m عضو مجزای α، α^q، $\cdots$ و $\alpha^{q^{m-1}}$ در F_{q^m} مشخص می‌شوند.

قضیه ۴.۱ در هر میدان متناهی F_q گروه ضربی F_q^* دوری است.

تعریف ۷.۱ هر مولد گروه دوری F_q^* را یک عضو اولیه میدان F_q می‌نامند.

۱—۳—۲ کدهای خطی

تعریف ۸.۱ F_q را یک میدان متناهی از مرتبه q درنظر بگیرید. هر زیرفضای F_q^n را یک کد خطی qتایی به‌طول n می‌نامند. اگر بعد کد خطی $\mathbf{C}$ برابر k باشد آنگاه $\mathbf{C}$ را یک $[n,k]$—کد می‌نامند. اعضای یک کد $\mathbf{C}$ را کدکلمه می‌نامند. اگر $\mathbf{C}$ یک $[n,k]$—کد باشد آن‌گاه نرخ $\mathbf{C}$ برابر $R=\frac{k}{n}$ است.

مثال ۱.۱ کد دودویی $\mathbf{C}=\{۱۱۰,۰۱۱,۱۰۱,۰۰۰\}$ یک $[۳,۲]$—کد با نرخ $\frac{۲}{۳}$ است.

تعریف ۹.۱ فرض کنید $\mathbf{x},\mathbf{y}\in F_q^n$. فاصله همینگ بین $\mathbf{x}$ و $\mathbf{y}$ تعداد مولفه‌های متفاوت بین $\mathbf{x}$ و $\mathbf{y}$ است و با $d(\mathbf{x},\mathbf{y})$ نمایش داده می‌شود. مثلاً $d(۱۱۰,۱۰۱)=۲$.
فاصله یک کد را برابر می‌نیمم فاصله همینگ بین کدکلمه‌های $\mathbf{C}$ تعریف می‌کنیم، یعنی:

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

اگر $\mathbf{C}$ یک $[n,k]$—کد بامی‌نیمم فاصله d باشد آنگاه $\mathbf{C}$ را یک $[n,k,d]$—کد می‌نامند.

تعریف ۱۰.۱ فرض کنید $\mathbf{C}$ یک کد خطی باشد. وزن هر بردار $\mathbf{c}=(c_۱,c_۲,\ldots,c_n)\in\mathbf{C}$ برابر فاصله آن با بردار $\mathbf{0}=(۰,۰,\ldots,۰)$ تعریف می‌شود:

$$wt(\mathbf{c})=d(\mathbf{c},\mathbf{0}).$$

به‌عبارت دیگر، وزن $\mathbf{c}$، $wt(\mathbf{c})$، برابر تعداد مولفه‌های ناصفر $\mathbf{c}$ تعریف می‌شود. کمترین وزن یک کد برابر کمترین وزن کدکلمه‌های ناصفر $\mathbf{C}$ تعریف می‌شود؛ یعنی

$$w(\mathbf{C}) = \min\{wt(\mathbf{c}) \ : \ \mathbf{c} \in \mathbf{C}, \mathbf{c} \neq \mathbf{0}\}.$$

لم ۱.۱ اگر $\mathbf{C}$ یک کد خطی باشد آنگاه $d(\mathbf{C}) = w(\mathbf{C})$.

فرض کنید $A_q(n,d)$ معرف بیشترین اندازه در بین تمامی کدهای qتایی به‌طول n و کمترین فاصله d باشد که $d \leqslant n$. قضیه زیر به کران گیلبرت—ورشامو معروف است[۳۱]:

قضیه ۵.۱ اگر $q \geqslant ۲$ و $n \geqslant d \geqslant ۱$ آنگاه

$$A_q(n,d)(۱ + \binom{n}{۱}(q-۱) + \binom{n}{۲}(q-۱)^۲ + \cdots + \binom{n}{d-۱}(q-۱)^{d-۱}) \geqslant q^n.$$

تعریف ۱۱.۱ فرض کنید سطرهای یک ماتریس G تشکیل یک پایه برای کد خطی $\mathbf{C}$ بدهند. در این‌صورت ماتریس G را یک ماتریس مولد برای $\mathbf{C}$ می‌نامند. فرض کنید G یک ماتریس مولد برای یک $[n,k]$—کد $\mathbf{C}$ باشد. در این‌صورت هر کدکلمه در $\mathbf{C}$ یک ترکیب خطی از سطرهای G است. پس

$$\mathbf{C} = \{xG \ : \ x \in F_q^k\}.$$

مثال ۲.۱ ماتریس $G = \begin{bmatrix} ۱ & ۱ & ۰ \\ ۰ & ۱ & ۱ \end{bmatrix}$ یک ماتریس مولد برای کد $\mathbf{C} = \{۱۱۰, ۰۱۱, ۱۰۱, ۰۰۰\}$ است.

تعریف ۱۲.۱ ماتریس مولد $G = (I_k|A)$ که I_k ماتریس همانی از مرتبه k است، یک ماتریس مولد به فرم استاندرد نامیده می‌شود.

دلیل توجه فراوان به کدهای خطی، ساده بودن آن‌ها است به‌عنوان یک فضای برداری روی یک میدان، کد می‌تواند توسط یک مجموعه‌ای از کدکلمه‌های پایه مشخص شود و کار کردن با ماتریس مولد بسیار ساده‌تر از کار کردن با همه کدکلمه‌ها است.

تعریف ۱۳.۱ دو کد $\mathbf{C}$ و $\mathbf{C}'$ را معادل می‌نامند هرگاه $\mathbf{C}$ بتواند توسط ترکیبی خطی از اعمال زیر از روی $\mathbf{C}'$ به‌دست آید:

۱) یک جایگشت روی مختصات.

۲) ضرب یک مولفه ثابت در تمامی کدکلمات در یک اسکالر ناصفر.

تعریف ۱۴.۱ تبدیل دوری T برای یک کدکلمه $\mathbf{c} = (c_۰, c_۱, \ldots, c_{n-۱})$ به‌فرم زیر تعریف می‌شود:

$$T(\mathbf{c}) = (c_{n-۱}, c_۰, c_۱, \ldots, c_{n-۲}).$$

تعریف ۱۵.۱ یک کد $\mathbf{C}$ را دوری نامند هرگاه تحت T پایا باشد.

کدهای دوری ساختاری بسیار غنی در بین کدهای خطی دارند. اعمال کدگذاری این کدها بسیار ساده انجام می‌شود و از این‌رو کدهای دوری اهمیت زیادی در نظریه کدگذاری دارند.

تعریف ۱۶.۱ فرض کنید $\mathbf{C}$ یک کد روی F_q با یک ضرب داخلی $<,>$ باشد. در این‌صورت دوگان کد $\mathbf{C}$ به‌صورت زیر تعریف می‌شود:

$$\mathbf{C}^{\perp} = \{u \in {F_q}^n \mid \ < u, c >= ۰, \quad c \in \mathbf{C}\}.$$

به‌آسانی دیده می‌شود دوگان یک کد خطی دودویی یک کد خطی دودویی است. لم مقدماتی زیر بدون اثبات ارائه می‌گردد.

لم ۲.۱ اگر $\mathbf{C}$ یک $[n,k]$—کد روی F_q باشد آنگاه $(\mathbf{C}^{\perp})^{\perp} = \mathbf{C}$ و $\mathbf{C}^{\perp}$ یک $[n, n-k]$—کد روی F_q است.

در حالت کلی رابطه زیر برقرار است:

$$\mathbf{C} \ \subseteq \ (\mathbf{C}^{\perp})^{\perp}.$$

تعریف ۱۷.۱ اگر $\mathbf{C} \subseteq \mathbf{C}^{\perp}$ آنگاه $\mathbf{C}$ را یک کد خودمتعامد می‌نامند.

تعریف ۱۸.۱ اگر $\mathbf{C} = \mathbf{C}^{\perp}$ آنگاه $\mathbf{C}$ یک کد خوددوگان نامیده می‌شود.

تعریف ۱۹.۱ فرض کنید H یک ماتریس مولد برای کد دوگان $\mathbf{C}^{\perp}$ باشد. در این‌صورت ماتریس H را یک ماتریس بررسی—توازن برای کد $\mathbf{C}$ می‌نامند.

فرض کنید $\mathbf{C}$ یک $[n,k]$—کد خطی روی F_q با ماتریس بررسی توازن H باشد. در این‌صورت بردار $v \in F_q^n$ یک کدکلمه است اگروفقط اگر $vH^T = \mathbf{0}$، یعنی فضای پوچ H همان کد C است.
اگر $G = (I_k|A)$ یک ماتریس مولد به فرم استاندرد برای کد C باشد آنگاه $H = (-A^T|I_{n-k})$ یک ماتریس بررسی—توازن برای کد $\mathbf{C}$ است. در قضیه بعد ارتباط بین می‌نیمم فاصله کد و یک ماتریس بررسی—توازن بیان می‌شود.

قضیه ۶.۱ فرض کنید $\mathbf{C}$ یک $[n,k,d]$—کد با ماتریس بررسی—توازن H باشد. دراین‌صورت می‌نیمم فاصله d برابر می‌نیمم تعداد ستون‌های H است که وابسته خطی هستند، یعنی هر $d-۱$ ستون از ماتریس H مستقل خطی بوده و یک d ستون وابسته خطی در H وجود دارد.

تعریف ۲۰.۱ اگر یک کد بتواند همه خطاهای به وزن t یا کمتر را تشخیص دهد ولی بعضی از خطاهای به وزن $t+۱$ قابل تشخیص نباشند این کد t خطا تشخیص دهنده است. بنابراین با توجه به تعریف، یک کد با کمترین فاصله d قابلیت تشخیص خطا $d-۱$ را دارد. اگر یک کد همه خطاهای به وزن t یا کمتر را تصحیح کند ولی این خاصیت برای $t+۱$ برقرار نباشد این کد را t خطا تصحیح کننده می‌نامند. برای یک کد با کمترین فاصله d داریم $t = [\frac{d-۱}{۲}]$.

۱—۴ کدهای $LDPC$ و گراف تنر

۱—۴—۱ کدهای $LDPC$ و نمایش ماتریسی آن‌ها

کدهای با ماتریس بررسی—توازن خلوت $LDPC$ توسط گالاگر در رساله دکترایش مطرح شد[۱۳]. چون تعداد یک‌ها در هر سطر و ستون یک ماتریس بررسی—توازن این کدها نسبت به طول کد بسیار کوچک است، این کدها را کدهای با ماتریس بررسی—توازن خلوت می‌نامند. در زیر تعریف دقیق کدهای $LDPC$ منظم مطرح می‌شود.

تعریف ۲۱.۱ فرض کنید C یک کد خطی با ماتریس بررسی—توازن H باشد. در این‌صورت کد C را یک کد با ماتریس بررسی—توازن خلوت (γ,ρ)— منظم می‌نامند هر گاه

۱) وزن هر سطر برابر ρ باشد.

۲) وزن هر ستون برابر γ باشد.

۳) مقادیر ρ و γ به ترتیب نسبت به طول کد و تعداد سطرهای H کوچک باشند.

فرض کنید C یک کد $LDPC$ (γ,ρ)—منظم با ماتریس بررسی—توازن $m \times n$ H باشد. در این‌صورت $\rho m = \gamma n$. بنابراین برای نرخ کد داریم

$$R = \frac{k}{n} \geq \frac{n-m}{n} = 1 - \frac{\gamma}{\rho}.$$

اگر سطرهای H مستقل خطی باشند آنگاه $R = 1 - \frac{\gamma}{\rho}$.

مثال ۳.۱ کد C با ماتریس بررسی—توازن H که در زیر بیان شده است را در نظر بگیرید.

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

در این ماتریس

۱) وزن هر سطر $\rho = 5$ است.

۲) وزن هر ستون $\gamma = 2$ است.

۳) مقادیر $\rho = 5$ و $\gamma = 2$ به ترتیب نسبت به ۲۵ و ۱۰ کوچک هستند.

بنابراین C یک کد $LDPC$ $(2,5)$— منظم است. بنابراین $R \geq 1 - \frac{\gamma}{\rho} = \frac{3}{5} = 0/6$. نرخ واقعی این کد برابر $\frac{16}{25} = 0/64$ است.

اگر در تعریف ۲۱.۱ تعداد درایه‌های یک در هر سطر و ستون ثابت نباشد. آنگاه کد $LDPC$ را نامنظم می‌نامند.

۱—۴—۲ نمایش گرافی کدهای $LDPC$

تنر یک نمایش کارا به‌فرم گراف‌های دوبخشی برای کدهای $LDPC$ مطرح کرد[۴۷]. این نمایش، گراف تنر نامیده می‌شود. گراف تنر در پیاده سازی الگوریتم کدگشایی تکراری نقش تسهیل کننده‌ای دارد.

تعریف ۲۲.۱ یک گراف دوبخشی نامیده می‌شود هر گاه بتوان رئوس آن را به دو بخش A و B افراز نمود که هر یال گراف، رأسی از A را به رأسی از B وصل کند.

تعریف ۲۳.۱ در یک گراف، دنباله‌ای از یال‌های متصل به هم که از یک رأس شروع و به همان رأس ختم می‌شود و هیچ رأسی به‌جز رأس ابتدایی بیش از یک‌بار ظاهر نشود را یک دور می‌نامند. طول یک دور برابر تعداد یالهای دور است. طول کوتاه‌ترین دور در یک گراف، کمر گراف نامیده می‌شود.

تعریف ۲۴.۱ (گراف تنر)

فرض کنید C یک کد خطی با ماتریس بررسی—توازن $H = (h_{ij})$ باشد. در این‌صورت گراف تنر متناظر با ماتریس بررسی—توازن H یک گراف دوبخشی است که رئوس آن به دو بخش رئوس متغیر و رئوس بررسی تقسیم می‌شوند. هر ستون از ماتریس H با یک رأس متغیر و هر سطر از H با یک رأس بررسی متناظر می‌شود. در این گراف، iاُمین رأس بررسی به jاُمین رأس متغیر متصل است اگر و تنها اگر $h_{ij} \neq 0$.

مثال ۴.۱ فرض کنید C یک کد خطی با ماتریس بررسی—توازن H که در زیر بیان شده است، باشد.

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

گراف تنر متناظر با H در شکل ۱—۴ آمده است که در آن v_iها معرف رئوس متغیر و c_jها معرف رئوس بررسی می‌باشند.

در سطر اول ماتریس بررسی—توازن H داریم $h_{11} = h_{12} = h_{13} = h_{14} = 1$ و مابقی درایه‌ها صفر است. بنابراین رأس بررسی c_1 به رئوس متغیر v_1, v_2, v_3, v_4 وصل شده است.