



جلسه دفاع از پایان نامه کارشناسی ارشد

کدگشایی در بچه کدهای کانولوشن LDPC روی کانال‌های پاک‌کننده دودویی

سخنران: ندا اسلامی‌زاده

زمان: شنبه ۲۴/۱۰/۹۲ ساعت ۳۰: ۱۳ صبح

مکان: سالن خوارزمی دانشکده علوم ریاضی

هیئت داوران

۱- پروفیسور مرتضی اسماعیلی

۲- دکتر محمدحسام تدین

۳- دکتر حمیدرضا مرزبان

۴- دکتر علی زاغیان

چکیده

در این پایان‌نامه، کلاس جدیدی از کدهای LDPC به نام کدگراف اصلی معرفی می‌شود و یک گراف اصلی به عنوان طرحی برای ساختن کدهای LDPC با اندازه دلخواه به کار می‌رود، سپس با معرفی کدهای کانولوشن LDPC، مدل‌هایی از کدهای LDPC و کدهای کانولوشن LDPC که می‌توانند با بسط یک گراف اصلی به دست آیند، ارائه می‌شوند. در ادامه الگوریتم‌های کدگشایی از جمله الگوریتم نشر اطمینان برای کدگشایی کدهای متناهی LDPC روی کانال پاک‌کننده دودویی بررسی می‌شود و این الگوریتم به الگوریتمی برای کدگشایی کدهای نامتناهی کانولوشن LDPC توسعه داده می‌شود که الگوریتم کدگشایی در بچه نامیده می‌شود. الگوریتم کدگشایی در بچه به دلیل پیچیدگی کم کدگشایی و تأخیر زمانی کوتاه نسبت به الگوریتم نشر اطمینان دارای اهمیت است. همچنین برخی از روش‌های ساخت کدهای (γ, ρ) -منظم LDPC با کارایی خوب تحت کدگشای در بچه بیان می‌شود که از این ویژگی‌ها برای کران‌یابی کوچکترین گستره مجموعه‌های متوقف‌کننده ($span_{min}$) و بیشترین پاک‌شده‌های پشت سر هم و قابل تصحیح (Δ_{max}) استفاده می‌شود. هدف از یافتن کران $span_{min}$ ، طراحی گراف‌های اصلی است که گستره مینیمالی نزدیک به این کران دارند. همچنین با استفاده از کران‌های Δ_{max} نشان داده می‌شود که می‌توان کدهایی ساخت که بیشترین طول پاک‌شده‌های پشت سر هم و قابل تصحیح در آن، متناسب با حافظه کد است.

کلمات کلیدی: کدهای LDPC، کدگشایی تکراری، الگوریتم نشر اطمینان، کدهای کانولوشن، کدهای کانولوشن LDPC، آستانه کدگشایی، کانال‌های پاک‌کننده، مجموعه‌های متوقف‌کننده، کدگشایی در بچه.



دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

کدگشایی در یچه کدهای کانولوشن LDPC روی کانال‌های پاک‌کننده دودویی

پایان نامه کارشناسی ارشد ریاضی کاربردی
ندا اسلامی زاده

استاد راهنما
پروفیسور مرضی اسماعیلی

دی ۱۳۹۲



دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد ریاضی کاربردی خانم ندا اسلامی زاده
تحت عنوان

کدگشایی در یچه کدهای کانولوشن LDPC روی کانال‌های پاک‌کننده دودویی

در تاریخ ۲۴ / ۱۰ / ۹۲ توسط کمیته تخصصی زیر مورد بررسی و تأیید نهایی قرار گرفت.

پروفسور مرتضی اسماعیلی

۱- استاد راهنما

دکتر محمدحسام تدین

۲- استاد مشاور

دکتر حمیدرضا مرزبان

۳- استاد داور ۱

دکتر علی زاغیان

۴- استاد داور ۲

دکتر فرید بهرامی

سرپرست تحصیلات تکمیلی دانشکده

شکرشایان نثار ایندمنان که توفیق را رفیق را بهم ساخت تا این پایان نامه را به پایان برسانم.
بسی سایه است

از استاد فریخته و فرزانه جناب آقای دکتر مرتضی اسماعیلی که بانگته‌های دلاویز و گفته‌های بلند، صحیفه سخن
را علم پرور نمود و همواره راه‌سما و راه‌کشای من در تمام و اکمال این پایان نامه بوده اند؛
از خانواده با محبتم به ویژه پدر و مادر عزیزم، این دو معلم بزرگوار که همواره بر کوتاهی و درستی من قلم عضو
کشیده و گریانه از کنار غفلت‌هایم گذشته اند و در تمام عرصه‌های زندگی ام یار و یاور می‌بی چشم داشت
برای من بوده اند؛

از همسر مهربانم که آرامش روحی و آسایش فکری مرا فراهم نمودند و از خانواده‌ی محترم ایشان؛

از جناب آقای دکتر محمد حسام‌تدین که زحمت مشاوره این پایان نامه را بر عهده گرفتند؛

از جناب آقایان دکتر علی زاغیان و دکتر حمید رضا مزربان، که زحمت داوری این پایان نامه را
متقبل شدند؛

و از تمامی دوستان دوران تحصیل که یاد و خاطره‌ی آن‌ها را فراموش نخواهم کرد؛

صمیمانه شکر و قدردانی نمایم. باشد که این خردترین، بخشی از زحمات آنان را پاس گوید.

تقدیم بہ:

پدر مہربان، مادر فداکارو، مہمسر عزیزم

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

فهرست مطالب

د	فهرست تصاویر
۱	۱ مقدمه
۱	۱.۱ نظریه کدگذاری
۲	۲.۱ تعاریف اولیه
۲	۱.۲.۱ گروه
۳	۲.۲.۱ میدان متناهی و فضای برداری
۵	۳.۲.۱ کدهای بلوکی خطی
۵	۴.۲.۱ ماتریس مولد و ماتریس بررسی-توازن
۸	۵.۲.۱ کمترین فاصله همینگ
۸	۶.۲.۱ کدهای دوری
۹	۷.۲.۱ کدهای <i>MDS</i>
۱۰	۳.۱ سیستم‌ها و کانال‌های مخابراتی
۱۰	۱.۳.۱ کانال متقارن دودویی
۱۱	۲.۳.۱ کانال پاک‌کننده دودویی
۱۲	۳.۳.۱ کانال گیلبرت-الیوت
۱۳	۴.۱ فرآیندهای تصادفی
۱۵	۲ کدهای کانولوشن <i>LDPC</i>
۱۵	۱.۲ کدهای <i>LDPC</i>
۱۷	۲.۲ نمایش گرافی کدهای <i>LDPC</i>

۱۹ کدهای کانولوشن	۳.۲
۲۰ کدگذاری کدهای کانولوشن	۱.۳.۲
۲۵ کد سیستماتیک	۲.۳.۲
۲۸ <i>LDPC</i> کدهای کانولوشن	۴.۲
۳۳ کدگذاری کدهای متناوب <i>LDPC</i> وابسته به زمان	۱.۴.۲
۳۷ کدهای <i>LDPC</i> بر مبنای گراف اصلی	۵.۲
۴۳ ساختار کلاسیک	۱.۵.۲
۴۹ ساختار اصلاح شده	۲.۵.۲
۵۰ نمایش چند جمله‌ای کدهای <i>LDPC</i>	۶.۲
۵۶ کدگشایی حداکثر درست‌نمایی	۷.۲
۵۷ الگوریتم‌های کدگشایی تکراری و تحلیل کارایی آن‌ها	۸.۲
۵۷ الگوریتم تعویض بیت	۱.۸.۲
۶۱ الگوریتم نشر اطمینان	۲.۸.۲
۶۶ مجموعه‌های متوقف‌کننده	۹.۲
۷۰ محورهای مجموعه‌های متوقف‌کننده	۱.۹.۲
۷۳ کدگشایی دریچه	۳
۷۳ کدگشای دریچه	۱.۳
۷۶ پیچیدگی الگوریتم‌های کدگشایی	۲.۳
۷۶ کدگشای نشر اطمینان	۱.۲.۳
۷۷ کدگشای دریچه	۲.۲.۳
۷۸ پیچیدگی تأخیر زمانی	۳.۲.۳
۹۳ کارایی کد	۳.۳
۹۳ آستانه‌های کدگشایی	۴.۳
۱۰۲ ویژگی‌های یک گراف اصلی برای ساخت کدهای (γ, ρ) -منظم <i>LDPC</i>	۵.۳
۱۱۱ کران‌یابی $span_{min}$ برای گراف اصلی B در کدهای <i>LDPC</i>	۶.۳
۱۱۱ استفاده از الگوریتم کدگشایی <i>BP</i>	۱.۶.۳
۱۲۳ استفاده از الگوریتم کدگشایی <i>WD</i>	۲.۶.۳
۱۲۶ کران‌یابی Δ_{max} در کدهای متناهی <i>LDPC</i>	۷.۳

۱۲۹..... نتیجه‌گیری ۸۰۳

۱۳۰ مراجع

۱۳۲ واژه‌نامه فارسی به انگلیسی و نمایه

۱۳۷ واژه‌نامه انگلیسی به فارسی

فهرست تصاویر

۱۱ کانال متقارن دودویی	۱۰.۱
۱۱ کانال پاک‌کننده دودویی	۲۰.۱
۱۱ کانال پاک‌کننده دودویی	۳۰.۱
۱۲ نمودار یک کانال گیلبرت-الیوت دو حالت با یک کانال متقارن دودویی در هر حالت	۴۰.۱
۱۸ (۱۰.۲) \mathbf{H} توازن رابطه	۱۰.۲
۲۰ $\mu = 3$ حافظه $\frac{1}{3}$ و نرخ	۲۰.۲
۲۰ یک سیستم کدگذاری دودویی برای یک (۳, ۳, ۴)-کد کانولوشن	۳۰.۲
۲۵ یک سیستم کدگذاری سیستماتیک	۴۰.۲
۲۷ یک سیستم کدگذاری سیستماتیک دودویی برای یک (۳, ۱, ۲)-کد کانولوشن	۵۰.۲
۳۰ ماتریس بررسی توازن یک کد $LDPC$ با دوره تناوب t'	۶۰.۲
	شکل سمت راست، ماتریس بررسی-توازن یک کد $LDPC$ را نشان می‌دهد که از یک کد بلوکی	۷۰.۲
۳۲ $LDPC$ (شکل سمت چپ) ساخته شده است.	۳۲
۳۴ نمایش یک کدگذار سیستماتیک برای کدهای متناوب $LDPC$ وابسته به زمان	۸۰.۲
۳۶ سیستم کدگذاری برای $t = 0$	۹۰.۲
۳۶ سیستم کدگذاری برای $t = 1$	۱۰۰.۲
۳۶ سیستم کدگذاری برای $t = 2$	۱۱۰.۲
۳۷ یک گراف اصلی ساده	۱۲۰.۲
۳۸ یک گراف اصلی که ۳ بار از گراف اصلی ساده نسخه‌برداری شده است.	۱۳۰.۲
۳۹ یک گراف مشتق از گراف اصلی	۱۴۰.۲
۴۱ ۳ بار نسخه‌برداری از یال	۱۵۰.۲
۴۱ جایگشت یال‌های شکل ۱۵۰.۲ در گراف مشتق	۱۶۰.۲
۴۲ ۳ بار نسخه‌برداری از یال	۱۷۰.۲

۴۲	جایگشت یال‌های شکل ۱۷.۲ در گراف مشتق شکل ۱۴.۲	۱۸.۲
۴۲	یک مثال از گراف اصلی	۱۹.۲
۴۵	گراف اصلی ماتریس رابطه (۴۰.۲)	۲۰.۲
۵۹	تکرار اول کدگشایی تکراری تعویض بیت برای مثال ۱۰.۲	۲۱.۲
۵۹	تکرار دوم کدگشایی تکراری تعویض بیت برای مثال ۱۰.۲	۲۲.۲
۵۹	تکرار سوم کدگشایی تکراری تعویض بیت برای مثال ۱۰.۲	۲۳.۲
۶۰	الگوریتم کدگشایی تکراری تعویض بیت برای مثال ۱۰.۲	۲۴.۲
۶۲	کدگشایی تکراری روی کانال پاک‌کننده دودویی-مرحله آغازین	۲۵.۲
۶۲	کدگشایی تکراری روی کانال پاک‌کننده دودویی-گام اول	۲۶.۲
۶۳	کدگشایی تکراری روی کانال پاک‌کننده دودویی-گام دوم	۲۷.۲
۶۳	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۲۸.۲
۶۳	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۲۹.۲
۶۴	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۳۰.۲
۶۴	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۳۱.۲
۶۴	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۳۲.۲
۶۵	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۳۳.۲
۶۵	انتقال پیام بین رأس‌های متغیر و رأس‌های بررسی در کدگشایی تکراری	۳۴.۲
۶۶	کدگشایی تکراری روی کانال پاک‌کننده دودویی-مرحله آغازین	۳۵.۲
۶۶	کدگشایی تکراری روی کانال پاک‌کننده دودویی-گام اول	۳۶.۲
۶۶	کدگشایی تکراری روی کانال پاک‌کننده دودویی-توقف در گام دوم	۳۷.۲
۶۷	نمایش یک مجموعه متوقف‌کننده	۳۸.۲
۷۰	یک زیرگراف تولیدشده توسط یک مجموعه متوقف‌کننده با اندازه ۶	۳۹.۲
۷۱	یک زیرگراف تولیدشده توسط یک مجموعه متوقف‌کننده با اندازه ۴	۴۰.۲
۷۵	کدگشایی WD برای کشویی با اندازه $w = 4$ برای کد $LDPCC$ با $L = 16$ در زمان $t' = 2$	۱.۳
	کدگشای دریچه برای یک کد $LDPCC$ ، $C_{mo}(\gamma, 2\gamma)$ با حافظه $\mu = 2$ و $L = 16$ با دریچه‌ای با اندازه $w = 4$ در چهارمین لحظه کدگشایی. یال‌های هاشورخورده مورب و عمودی، پیکربندی این دریچه را تشکیل می‌دهند.	۲.۳
۷۶		
۷۹	ماتریس بررسی-توازن متناظر با ماتریس پایه \mathbf{B}	۳.۳
۸۰	مرحله اول: کدگشایی همزمان دو دریچه مشخص شده	۴.۳

۵.۳	گام اول کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه‌ای w_1	۸۱
۶.۳	گام دوم کدگذاری نشر اطمینان	۸۱
۷.۳	انتقال پیام در کدگذاری نشر اطمینان و کدگذاری سمبل‌های هدف (۶ سمبل اول) دریچه w_1	۸۱
۸.۳	گام اول کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه w_4 در تکرار اول	۸۲
۹.۳	گام دوم کدگذاری نشر اطمینان در تکرار اول	۸۳
۱۰.۳	انتقال پیام در کدگذاری نشر اطمینان و کدگذاری تعدادی از سمبل‌های هدف برای دریچه w_4 در تکرار اول	۸۳
۱۱.۳	گام دوم کدگذاری نشر اطمینان در تکرار دوم	۸۳
۱۲.۳	انتقال پیام در کدگذاری نشر اطمینان	۸۴
۱۳.۳	گام دوم کدگذاری نشر اطمینان در تکرار سوم	۸۴
۱۴.۳	انتقال پیام در کدگذاری نشر اطمینان و کدگذاری تمامی سمبل‌های هدف برای دریچه w_4 در تکرار سوم	۸۴
۱۵.۳	مرحله دوم: انتقال دریچه‌های مرحله اول (۶ ستون به سمت راست و ۳ سطر به سمت پایین) و کدگذاری همزمان دریچه‌های حاصل	۸۵
۱۶.۳	گام اول کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه w_2 در تکرار اول	۸۶
۱۷.۳	گام دوم کدگذاری نشر اطمینان در تکرار اول	۸۶
۱۸.۳	انتقال پیام در کدگذاری نشر اطمینان و کدگذاری سمبل‌های هدف برای دریچه w_2 در تکرار اول	۸۶
۱۹.۳	گام اول کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه w_5 در تکرار اول	۸۷
۲۰.۳	گام دوم کدگذاری نشر اطمینان در تکرار اول	۸۸
۲۱.۳	انتقال پیام در کدگذاری نشر اطمینان	۸۸
۲۲.۳	توقف در کدگذاری	۸۸
۲۳.۳	مرحله سوم: انتقال دریچه‌های مرحله دوم (۶ ستون به سمت راست و ۳ سطر به سمت پایین) و کدگذاری همزمان دریچه‌های حاصل	۸۹
۲۴.۳	گام اول کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه w_3 در تکرار اول	۹۰
۲۵.۳	گام دوم کدگذاری نشر اطمینان در تکرار اول	۹۰
۲۶.۳	انتقال پیام در کدگذاری نشر اطمینان و کدگذاری تمامی سمبل‌های هدف برای دریچه w_3	۹۰
۲۷.۳	گام اول کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه w_6 در تکرار اول	۹۱
۲۸.۳	گام دوم کدگذاری نشر اطمینان	۹۱
۲۹.۳	انتقال پیام در کدگذاری نشر اطمینان و کدگذاری تمامی سمبل‌های هدف	۹۲
۳۰.۳	گام دوم کدگذاری نشر اطمینان یک کد $LDPCC$ برای دریچه w_6 در تکرار دوم	۹۲

۹۳	انتقال پیام در کدگشایی تکراری و کدگشایی تمامی سمبل‌های دريچه w_6
۹۶	درخت جستجو برای يال $a \rightarrow 1$ در گراف اصلی
۹۷	درخت جستجو برای يال $a \rightarrow 1$ در گراف اصلی
۹۹	i -امین پیکربندی دريچه برای اندازه‌های w و $w + 1$
۱۰۰	نمایش دو دريچه با اندازه‌های متفاوت و يال‌های بين آنها
۱۲۷	دريچه‌هایی با اندازه w و $w - (i - 1)$ و نمایش ستون‌های متناظر با سمبل‌های هدف در این دريچه‌ها

چکیده

در این پایان نامه، کلاس جدیدی از کدهای $LDPC$ به نام کد گراف اصلی معرفی می شود و یک گراف اصلی به عنوان طرحی برای ساختن کدهای $LDPC$ با اندازه دلخواه به کار می رود، سپس با معرفی کدهای کانولوشن $LDPC$ ، مدل هایی از کدهای $LDPC$ و کدهای کانولوشن $LDPC$ که می توانند با بسط یک گراف اصلی به دست آیند، ارائه می شوند. در ادامه الگوریتم های کدگشایی از جمله الگوریتم نشر اطمینان برای کدگشایی کدهای متناهی $LDPC$ روی کانال پاک کننده دودویی بررسی می شود و این الگوریتم به الگوریتمی برای کدگشایی کدهای نامتناهی کانولوشن $LDPC$ توسعه داده می شود که الگوریتم کدگشایی درجه نامیده می شود. الگوریتم کدگشایی درجه به دلیل پیچیدگی کم کدگشایی و تأخیر زمانی کوتاه نسبت به الگوریتم نشر اطمینان دارای اهمیت است. همچنین برخی از روش های ساخت کدهای (γ, ρ) -منظم $LDPC$ با کارایی خوب تحت کدگشای درجه بیان می شود که از این ویژگی ها برای کران یابی کوچکترین گستره مجموعه های متوقف کننده ($span_{min}$) و بیشترین پاک شده های پشت سر هم و قابل تصحیح (Δ_{max}) استفاده می شود. هدف از یافتن کران $span_{min}$ ، طراحی گراف های اصلی است که گستره مینیمالی نزدیک به این کران دارند. همچنین با استفاده از کران های Δ_{max} نشان داده می شود که می توان کدهایی ساخت که بیشترین طول پاک شده های پشت سر هم و قابل تصحیح در آن، متناسب با حافظه کد است.

کلمات کلیدی: کدهای $LDPC$ ، کدگشایی تکراری، الگوریتم نشر اطمینان، کدهای کانولوشن، کدهای کانولوشن $LDPC$ ، آستانه کدگشایی، کانال های پاک کننده، مجموعه های متوقف کننده، کدگشایی درجه.

فصل ۱

مقدمه

در این فصل، مفاهیم لازم برای درک مباحث این پایان‌نامه را به شکل مختصر بیان می‌کنیم. ابتدا نظریه کدگذاری و برخی مفاهیم جبری از جمله گروه، زیرگروه، میدان و فضای برداری را معرفی می‌کنیم. سپس با دو بخش نظریه کدگذاری، یعنی کدگذاری منبع و کدگذاری کانال آشنا شده و کدهای بلوکی و زیرکلاس‌های آن را معرفی می‌کنیم. در ادامه، با ماتریس مولد و ماتریس بررسی-توازن به ترتیب به منظور عمل کدگذاری و کدگشایی کانال آشنا می‌شویم. در آخر سیستم‌ها و کانال‌های مخبراتی، یعنی کانال بدون حافظه و کانال باحافظه را معرفی کرده و فرآیندهای تصادفی را شرح خواهیم داد.

۱.۱ نظریه کدگذاری

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، جبرخطی، هندسه جبری، ترکیبیات و گراف، ابزارهای ریاضی استفاده شده در عمر حدود شصت ساله این نظریه هستند. این نظریه در سال ۱۹۴۸ توسط شانون [۲۴] پایه‌گذاری شده است. وی در مقاله‌ای با عنوان نظریه ریاضی مخبرات، نشان داد که با افزودن بیت‌های اضافی می‌توان خطای داده در انتقال داده‌ها از یک کانال را بهتر تشخیص داد. وی همچنین ثابت کرد که در یک کانال مخبراتی، پارامتری به نام ظرفیت کانال وجود دارد که انتقال داده‌ها با هر نرخ دلخواه و نزدیک به ظرفیت کانال و نه بیشتر از آن امکان‌پذیر است به گونه‌ای که احتمال خطای کدگشایی، با افزایش طول کد، به سمت صفر میل می‌کند.

شانون این مطلب را تنها در قالب یک قضیه و بر پایه نظریه احتمال بیان کرد و هیچ روش خاصی برای ساخت یک کد مطلوب ارائه نکرد. روش‌های ساخت کدهای خوب و الگوریتم‌های کارا برای پیاده‌سازی آن‌ها به عنوان 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 ($Low - density Parity - check(LDPC)$)، توجه فراوانی نموده‌اند.

۲.۱ تعاریف اولیه

۱.۲.۱ گروه

تعریف ۱.۲.۱ یک مجموعه ناتهی G را با عمل دوتایی $*$ روی آن یک گروه گویند، اگر شرایط زیر برقرار باشد:

• G تحت عمل $*$ بسته باشد، یعنی برای هر $a, b \in G$ ، عنصر $a * b$ در G است.

• عمل $*$ شرکت‌پذیر است، یعنی همواره $a * (b * c) = (a * b) * c$.

• G شامل یک عنصر e است به‌طوری که برای هر عنصر $a \in G$ داریم

$$a * e = e * a = a.$$

e را عنصر همانی G نسبت به عمل $*$ گویند.

• برای هر عنصر $a \in G$ ، عنصر a' موجود است به‌طوری که

$$a * a' = a' * a = e.$$

عنصر a' را وارون عنصر a گویند.

اگر G شامل تعداد متناهی عنصر باشد، G یک گروه متناهی نامیده می‌شود. در یک گروه عنصر همانی و وارون هر عنصر، منحصر به فرد هستند.

تعریف ۲.۲.۱ یک زیرمجموعه ناتهی H از یک گروه G را تحت عمل $*$ یک زیرگروه G گویند اگر با عمل $*$ خود یک گروه باشد. برای این منظور از نماد $H \leq G$ استفاده می‌شود. ثابت می‌شود که H یک زیرگروه G است اگر و فقط اگر دو شرط زیر برقرار باشد:

• برای هر دو عنصر $a, b \in H$ داشته باشیم $a * b \in H$.

• اگر $a \in H$ آنگاه $a^{-1} \in H$.

گروه G جابجایی است اگر برای هر $a, b \in G$ داشته باشیم $a * b = b * a$. اگر G یک گروه و $a \in G$ ، آنگاه مجموعه همه توان‌های a یک زیرگروه از G است که زیرگروه تولید شده توسط a نامیده می‌شود و

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}.$$

گروه G دوری است اگر عنصر $a \in G$ موجود باشد به قسمی که $\langle a \rangle = G$.

تعریف ۳.۲.۱ فرض کنید G یک گروه بوده و $H \leq G$. H را در G نرمال گوئیم و می‌نویسیم ' $H \trianglelefteq G$ '، هرگاه برای هر $g \in G$ داشته باشیم

$$gHg^{-1} \in H.$$

۲.۲.۱ میدان متناهی و فضای برداری

میدان

تعریف ۴.۲.۱ فرض کنید \mathbb{F} یک مجموعه از عناصر با دو عمل دودویی جمع '+' و ضرب '.' باشد. \mathbb{F} نسبت به دو عمل + و . یک میدان است اگر دارای شرایط زیر باشد.

- \mathbb{F} نسبت به عمل جمع یک گروه آبدلی (جابجایی) باشد. عنصر همانی نسبت به عمل جمع را عنصر صفر \mathbb{F} نامیده و با '۰' نشان داده می‌شود.
- مجموعه عناصر ناصفر \mathbb{F} تحت عمل ضرب یک گروه آبدلی باشد. عنصر همانی نسبت به عمل ضرب را عنصر یک \mathbb{F} نامیده و با '۱' نمایش می‌دهند.

طبق تعریف، هر میدان دارای حداقل دو عنصر ۰ و ۱ است. یک میدان با تعداد متناهی عنصر را یک میدان متناهی می‌گویند و تعداد عناصر آن را مرتبه میدان می‌نامند. میدان \mathbb{F}_q با q عنصر را در نظر بگیرید. فرض کنید α یک عنصر ناصفر در \mathbb{F}_q باشد. چون مجموعه عناصر ناصفر \mathbb{F}_q تحت عمل ضرب بسته است، بنابراین توان‌های α

$$\alpha^1 = \alpha, \alpha^2 = \alpha \cdot \alpha, \alpha^3 = \alpha \cdot \alpha \cdot \alpha$$

عناصری ناصفر در \mathbb{F}_q هستند. کوچکترین عدد صحیح مثبت n با خاصیت $\alpha^n = 1$ ، مرتبه عنصر α نامیده می‌شود. در یک میدان \mathbb{F}_q عنصر ناصفر α را عنصر اولیه میدان گویند اگر $q-1$ مرتبه α باشد. بنابراین توان‌های یک عنصر اولیه همه عناصر ناصفر میدان \mathbb{F}_q را تولید می‌کنند. هر میدان متناهی دارای عنصر اولیه است. برای هر توانی از یک عدد اول p (مثل p^m) یک میدان با $q = p^m$ عنصر وجود دارد.

فرض کنید \mathbb{F} یک میدان باشد. زیر مجموعه K از \mathbb{F} را یک زیرمیدان \mathbb{F} گویند اگر K نیز تحت عمل‌های \mathbb{F} یک میدان باشد. \mathbb{F} نیز توسعه میدان K نامیده می‌شود. اگر $\mathbb{F} \neq K$ باشد، K را یک زیرمیدان سره \mathbb{F} گویند.

فضای برداری

تعریف ۵.۲.۱ یک گروه آبدلی V با یک عمل + روی آن را در نظر بگیرید. فرض کنید \mathbb{F} یک میدان بوده و یک عمل . از $\mathbb{F} \times V$ به V تعریف شده باشد. مجموعه V را یک روی \mathbb{F} نامند اگر دارای شرایط زیر باشد.

- قانون توزیع‌پذیری بین \mathbb{F} و V برقرار باشد، یعنی اگر $a, b \in \mathbb{F}$ و $\mathbf{u}, \mathbf{v} \in V$ آن‌گاه

$$a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v},$$

$$(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}.$$

• قانون شرکت‌پذیری بین \mathbb{F} و V برقرار باشد، یعنی اگر $a, b \in \mathbb{F}$ و $\mathbf{v} \in V$ آن‌گاه

$$(ab)\mathbf{v} = a(b\mathbf{v}).$$

• برای هر $\mathbf{v} \in V$ داشته باشیم $\mathbf{v} = 1 \cdot \mathbf{v}$.

یک دنباله مرتب شده با n مؤلفه a_0, a_1, \dots, a_{n-1} که هر مؤلفه آن عنصری از \mathbb{F}_q است را در نظر بگیرید. این دنباله را یک n -تایی روی \mathbb{F}_q می‌نامیم. q انتخاب برای هر a_i وجود دارد، بنابراین q^n ، n -تایی متفاوت موجود است. مجموعه $(\mathbb{F}_q)^n$ همه n -تایی‌های مرتب روی \mathbb{F}_q است که آن را با \mathbb{F}_q^n نشان می‌دهیم. عناصر \mathbb{F}_q^n بردار نامیده می‌شوند. دو عمل روی \mathbb{F}_q^n تعریف می‌شود.

• جمع دو بردار: برای هر $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ و $\mathbf{u} = (u_0, u_1, \dots, u_{n-1})$ در $(\mathbb{F}_q)^n$ ، بردار $\mathbf{u} + \mathbf{v}$ به فرم زیر است

$$\mathbf{u} + \mathbf{v} = (u_0 + v_0, u_1 + v_1, \dots, u_{n-1} + v_{n-1}).$$

• حاصل ضرب یک بردار در یک اسکالر: اگر $\mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_q^n$ و $a \in \mathbb{F}_q$ داریم

$$a(v_0, v_1, \dots, v_{n-1}) := (av_0, av_1, \dots, av_{n-1}).$$

جمع برداری و ضرب اسکالر تعریف شده در بالا به ترتیب از قوانین توزیع‌پذیری و شرکت‌پذیری پیروی می‌کنند. بنابراین مجموعه \mathbb{F}_q^n یک فضای برداری روی \mathbb{F}_q است. یک زیرمجموعه از \mathbb{F}_q^n یک زیرفضای \mathbb{F}_q^n است هرگاه تحت عمل جمع و ضرب تعریف شده روی \mathbb{F}_q^n یک فضای برداری باشد. هر زیرفضا از \mathbb{F}_q^n شامل یک مجموعه مولد متناهی است. این مجموعه را پایه فضای برداری و تعداد بردارهای یک پایه فضای برداری را بعد فضای برداری نامیده و با $\dim()$ نمایش می‌دهند.

تعریف ۶.۲.۱ فرض کنیم $A = \{a_1, a_2, \dots, a_r\}$ یک مجموعه متناهی باشد که آن را مجموعه الفبا می‌نامیم. یک مجموعه $C \subset A^n$ یک کدکلمه یا یک رشته r -تایی به طول n روی A نامیده می‌شود که معمولاً آن را به صورت $\mathbf{a} = a_{i_1} a_{i_2} \dots a_{i_n}$ نشان می‌دهند. همچنین طول یک رشته را برابر تعداد سمبل‌های آن تعریف کرده و با نماد $\text{len}(\mathbf{a}) = n$ نشان داده می‌شود. مجموعه تمام رشته‌ها روی A را با A^* نمایش می‌دهند. اگر الفبای کد $\{0, 1\}$ باشد، آن‌گاه کد را دودویی و در غیر این صورت آن را یک کد غیردودویی می‌نامند.

تعریف ۷.۲.۱ (کدگشایی)

فرض کنید $A = \{a_1, a_2, \dots, a_q\}$ الفبای کد باشد. برای کدهای به طول n ، A^n کل فضا را می‌سازد. از این رو هر کدکلمه که ارسال شود یک کلمه از A^n دریافت می‌شود. باید تابعی چون $f: A^n \rightarrow C$ تعریف کنیم که یک کلمه دریافت شده را به یک کدکلمه کدگشایی کند. تابع f را تابع تصمیم (تابع کدگشایی) می‌نامند و تبدیل کلمه دریافتی به طول n به یک کدکلمه را عمل کدگشایی می‌نامند.

تعریف ۸.۲.۱ اگر اندازه C برابر M باشد، یعنی $|C| = M$ ، نرخ C به صورت $R = \frac{\log_q M}{n}$ تعریف می‌شود.

۳.۲.۱ کدهای بلوکی خطی

معمولاً نظریه کدگذاری را در دو بخش، کدگذاری منبع و کدگذاری کانال مورد مطالعه و بررسی قرار می‌دهند که در اینجا یک توضیح مختصری از آن‌ها ارائه می‌شود. در این پایان‌نامه کدگذاری روی کانال مورد نظر است. در بحث کدگذاری منبع (کدگذاری بدون نویز)، هیچ خطایی روی داده‌ها صورت نمی‌گیرد. مسأله مهم در کدگذاری کانال و در ارسال پیام، یافتن خطاها و اصلاح آن‌ها در پیام‌های دریافتی می‌باشد. با توجه به نویز کانال، پیام‌های ارسالی معمولاً دچار خطا می‌شوند. در نظریه کدگذاری کانال امکان کشف و تصحیح خطاهای ایجاد شده روی پیام‌های ارسالی در اثر نویز کانال، در مبحث کدهای تصحیح کننده خطا بررسی می‌شود. بنابراین در کدگذاری کانال کشف خطا از یک طرف و از طرف دیگر تصحیح خطا از اهمیت بالایی برخوردار است. فرض کنید خروجی یک منبع دنباله‌ای از سمبل‌های دوتایی روی \mathbb{F}_2 باشد. سمبل‌های ۰ و ۱ دنباله اطلاعات را بیت‌های اطلاعات می‌نامند. در کدگذاری بلوکی دنباله اطلاعات به پیام‌هایی با طول مشخص k بیت تقسیم می‌شود. بنابراین 2^k پیام متمایز وجود دارد. در کدگذاری کانال، هر پیام k بیت $\mathbf{u} = (u_0, u_1, \dots, u_{k-1})$ با قوانین معینی به یک دنباله n بیتی $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$ ($n > k$) نگاشت می‌شود. بیت‌های یک کدکلمه بیت‌کد نامیده می‌شوند. چون 2^k پیام متمایز وجود دارد، پس 2^k کدکلمه خواهیم داشت. مجموعه 2^k کدکلمه یک $[n, k]$ -کد بلوکی نامیده می‌شود اگر تشکیل یک زیرفضای k -بعدی از \mathbb{F}_2^n بدهند. تعداد $n - k$ بیت اضافه شده به هر پیام را بیت‌های افزونگی می‌گویند. بیت‌های افزونگی اطلاعات جدیدی با خود حمل نمی‌کنند و تنها استفاده آن‌ها در تشخیص خطای رخ داده توسط کانال و تصحیح آن است. نسبت $R = \frac{k}{n}$ نیز نرخ کد می‌باشد. نرخ کد را می‌توان متوسط تعداد بیت اطلاعات در هر بیت‌کد تعبیر کرد.

تعریف ۹.۲.۱ یک کد دودویی با طول n و 2^k کدکلمه، یک $[n, k]$ -کد بلوکی نامیده می‌شود اگر 2^k کدکلمه آن یک زیرفضای k بعدی از فضای برداری \mathbb{F}_2^n باشد.

در تعریف ۷.۲.۱ اگر $A = \mathbb{F}_q$ ، آن‌گاه $A^n = \mathbb{F}_q^n$ ، و همچنین \mathbb{F}_q^n یک فضای برداری روی \mathbb{F}_q می‌باشد. پس اگر C یک زیرفضای دلخواه از \mathbb{F}_q^n روی \mathbb{F}_q باشد، آن‌گاه C یک کد بلوکی خطی با طول n روی \mathbb{F}_q نامیده می‌شود. اگر بعد C به‌عنوان یک زیرفضای برداری از \mathbb{F}_q^n روی \mathbb{F}_q برابر k باشد، آن‌گاه C را یک $[n, k]$ -کد بلوکی خطی می‌نامیم. اگر $d_{\min}(C) = d$ ، آن‌گاه گوییم C یک $[n, k, d]$ -کد خطی است. در این حالت چون C یک $[n, k]$ -کد خطی روی \mathbb{F}_q است، بنابراین $|C| = q^k$ و طبق تعریف نرخ کد داریم

$$R = \frac{\log_q |C|}{n} = \frac{\log_q q^k}{n} = \frac{k}{n}.$$

۴.۲.۱ ماتریس مولد و ماتریس بررسی-توازن

چون یک $[n, k]$ -کد خطی C یک زیرفضای k بعدی از فضای برداری تمام مؤلفه‌های n -تایی روی \mathbb{F}_2 است، پس k کدکلمه مستقل خطی $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{k-1}$ وجود دارند به طوری که می‌توان هر کدکلمه $\mathbf{c} \in C$ را به صورت یک

ترکیب خطی از آن‌ها بیان کرد. این کدکلمه یک پایه برای کد C است. فرض کنید $\mathbf{u} = (u_0, u_1, \dots, u_{k-1})$ یک پیام است تا کدگذاری شود، کدکلمه متناظر با \mathbf{u} از ترکیب خطی $\{\mathbf{g}_0, \mathbf{g}_1, \dots, \mathbf{g}_{k-1}\}$ و k بیت \mathbf{u} به دست می‌آید

$$\mathbf{v} = u_0 \mathbf{g}_0 + u_1 \mathbf{g}_1 + \dots + u_{k-1} \mathbf{g}_{k-1}.$$

در این صورت می‌توان k کدکلمه مستقل را در سطرهای یک ماتریس قرار داد و یک ماتریس $k \times n$ به شکل زیر به دست آورد

$$\mathbf{G} = \begin{pmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \dots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \dots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \dots & g_{k-1,n-1} \end{pmatrix}.$$

کدکلمه \mathbf{v} متناظر با پیام \mathbf{u} به صورت ضرب ماتریسی $\mathbf{v} = \mathbf{u} \cdot \mathbf{G}$ به دست می‌آید. واضح است که کدکلمه \mathbf{v} یک ترکیب خطی از سطرهای \mathbf{G} است. ماتریس \mathbf{G} را ماتریس مولد $[n, k]$ -کد خطی می‌نامند. در حالت کلی یک $[n, k]$ -کد خطی C بیشتر از یک پایه دارد، بنابراین بیش از یک ماتریس مولد برای کد موجود است. چون یک $[n, k]$ -کد خطی C یک زیرفضای k بعدی از فضای \mathbb{F}_q^n است، پس C یک زیرفضای $n - k$ بعدی از فضای برداری تمام مؤلفه‌های n -تایی می‌باشد و با C^\perp نمایش داده می‌شود

$$C^\perp = \{\mathbf{w} \in V : \langle \mathbf{w}, \mathbf{v} \rangle = 0, \forall \mathbf{v} \in C\}$$

که در آن

$$\langle \mathbf{w}, \mathbf{v} \rangle = \sum_{i=1}^n w_i v_i$$

و C^\perp یک $[n, n - k]$ -کد خطی است که کد دوگان C نامیده می‌شود.

مشابه بحثی که برای ماتریس مولد مطرح شد، اگر فضای دوگان کد C از $n - k$ پایه مستقل خطی $\mathbf{h}_0, \mathbf{h}_1, \dots, \mathbf{h}_{n-k-1}$ تشکیل شود، می‌توان هر کدکلمه در آن را به صورت یک ترکیب خطی از $n - k$ عنصر پایه بیان کرد. مشابه ماتریس مولد، ماتریس $(n - k) \times n$ زیر را در نظر بگیرید

$$\mathbf{H} = \begin{pmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \dots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \dots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \dots & h_{n-k-1,n-1} \end{pmatrix}.$$

ماتریس \mathbf{H} یک ماتریس مولد برای کد دوگان C است. همچنین $\mathbf{G} \times \mathbf{H}^T = \mathbf{0}$ ، به طوری که "0" یک ماتریس تمام صفر از مرتبه $k \times (n - k)$ است. چون ماتریس \mathbf{H} دارای $n - k$ سطر مستقل خطی است، پس می‌توان کد C