بسمه تعالی

جلسه دفاع از پایان‌نامه کارشناسی ارشد

کدگشایی دریچه 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- پروفسور 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 کد گراف 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 به‌دست 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 $LDPC$ توسیع داده می‌شود که الگوریتم کدگشایی دریچه نامیده می‌شود. الگوریتم کدگشایی دریچه 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 $LDPCC$ با کارایی خوب تحت کدگشای دریچه 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 دریچه.

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

کدگشایی دریچه کدهای کانولوشن LDPC روی کانال‌های پاک‌کننده دودویی

پایان نامه کارشناسی ارشد ریاضی کاربردی

ندا اسلامی زاده

استاد راهنما

پروفسور مرتضی اسماعیلی

دی ۱۳۹۲

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد ریاضی کاربردی خانم ندا اسلامی‌زاده
تحت عنوان

کدگشایی دریچه کدهای کانولوشن LDPC روی کانال‌های پاک‌کننده دودویی

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

۱– استاد راهنما	پروفسور مرتضی اسماعیلی
۲– استاد مشاور	دکتر محمدحسام تدین
۳– استاد داور۱	دکتر حمیدرضا مرزبان
۴– استاد داور۲	دکتر علی زاغیان
سرپرست تحصیلات تکمیلی دانشکده	دکتر فرید بهرامی

سپاس شایان نثار ایزد منان که توفیق را رفیق راهم ساخت تا این پایان نامه را به پایان برسانم.

بسی شایسته است

از استاد فرهیخته و فرزانه جناب آقای دکتر مرتضی اسماعیلی که با نکته های دلاویز و گفته های بلند، صحیفه سخن را علم پرور نمود و همواره راهنما و راه گشای من در اتمام 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 درشتی من قلم عفو کشیده و کریمانه از کنار غفلت هایم گذشته اند و در تمام عرصه های زندگی ام یار و یاوری بی چشم داشت برای من بوده اند؛

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

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

از جناب آقایان دکتر علی زاغیان و دکتر حمیدرضا مرزبان، که زحمت داوری این پایان نامه را متقبل شدند؛

و از تمامی دوستان دوران تحصیل که یاد و خاطره ی آن ها را فراموش نخواهم کرد؛

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

تقدیم به:

پدر مهربان، مادر فداکار و همسر عزیزم

فهرست مطالب

فهرست تصاویر

چکیده

در این پایان‌نامه، کلاس جدیدی از کدهای $LDPC$ به نام کد گراف 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 به‌دست 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 $LDPC$ توسیع داده می‌شود که الگوریتم کدگشایی دریچه نامیده می‌شود. الگوریتم کدگشایی دریچه 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 $LDPCC$ با کارایی خوب تحت کدگشای دریچه 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 دریچه.

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 ازجمله 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 به‌ترتیب به منظور عمل کدگذاری و کدگشایی کانال آشنا می‌شویم. در آخر سیستم‌ها و کانال‌های مخابراتی، 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 مخابرات، 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 مخابراتی، پارامتری به‌نام 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 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 $(Low-density\ Parity-check(LDPC))$، 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، منحصربه‌فرد 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 '$H\leqslant G$' 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

$$<a>=\{a^n|n\in\mathbb{Z}\}.$$

گروه G دوری است اگر عنصر $a \in G$ موجود باشد به‌قسمی که $G =< a >$.

تعریف ۳.۲.۱ فرض کنید G یک گروه بوده و $H \leqslant G$. H را در G نرمال گوییم 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 آبلی (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 آبلی باشد. عنصر همانی نسبت به عمل ضرب را عنصر یکه $\mathbb{F}$ 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 درنظر 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

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

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 توسیع 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 آبلی V با یک عمل + روی آن را درنظر 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 $\mathbf{v} = \mathbf{v}$. ۱.

یک دنباله مرتب شده با n مؤلفه $a_۰$، $a_۱$، $\cdots$ و $a_{n-۱}$ که هر مؤلفه آن عنصری از $\mathbb{F}_q$ است را درنظر 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 $\mathbf{v} = (v_۰, v_۱, \cdots, v_{n-۱})$ و $\mathbf{u} = (u_۰, u_۱, \cdots, u_{n-۱})$ در $(\mathbb{F}_q)^n$، بردار $\mathbf{u}+\mathbf{v}$ به فرم زیر است

$$\mathbf{u}+\mathbf{v} = (u_۰ + v_۰, u_۱ + v_۱, \cdots, u_{n-۱} + v_{n-۱}).$$

- حاصل‌ضرب یک بردار در یک اسکالر: اگر $\mathbf{v} = (v_۰, v_۱, \cdots, v_{n-۱}) \in \mathbb{F}_q^n$ و $a \in \mathbb{F}_q$ داریم

$$a(v_۰, v_۱, \cdots, v_{n-۱}) := (av_۰, av_۱, \cdots, av_{n-۱}).$$

جمع برداری و ضرب اسکالر تعریف شده در بالا به‌ترتیب 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 $A = \{a_۱, a_۲, \cdots, a_r\}$ 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 به‌صورت $\mathbf{a} = a_{i_۱}a_{i_۲}\cdots a_{i_n}$ نشان می‌دهند. همچنین طول یک رشته را برابر تعداد سمبل‌های آن تعریف کرده و با نماد $\mathbf{len}(\mathbf{a}) = n$ نشان داده می‌شود. مجموعه تمام رشته‌ها روی A را با A^* نمایش می‌دهند. اگر الفبای کد $\{۰, ۱\}$ باشد، آن‌گاه کد را دودویی و در غیر این‌صورت آن را یک کد غیردودویی می‌نامند.

تعریف ۷.۲.۱ (کدگشایی)

فرض کنید $A = \{a_۱, a_۲, \cdots, a_q\}$ الفبای کد باشد. برای کدهای به طول n، A^n کل فضا را می‌سازد. از این‌رو هر کدکلمه که ارسال شود یک کلمه از A^n دریافت می‌شود. باید تابعی چون $f : A^n \longrightarrow C$ 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 به‌صورت $R = \frac{log_q^M}{n}$ 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 نظریهٔ 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 $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ با قوانین معینی به یک دنباله n بیتی $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ $(n > k)$ 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 $\mathbf{g}_0$ ، $\mathbf{g}_1$، $\cdots$ و $\mathbf{g}_{k-1}$ وجود دارند به‌طوری که می‌توان هر کدکلمه $\mathbf{c} \in C$ را به‌صورت یک

ترکیب خطی از آن‌ها بیان کرد. این k کدکلمه یک پایه برای کد C است. فرض کنید $\mathbf{u} = (u_۰, u_۱, \cdots, u_{k-۱})$ یک پیام است تا کدگذاری شود، کدکلمه متناظر با $\mathbf{u}$ از ترکیب خطی $\{\mathbf{g}_۰, \mathbf{g}_۱, \cdots, \mathbf{g}_{k-۱}\}$ و k بیت $\mathbf{u}$ به‌دست می‌آید

$$\mathbf{v} = u_۰\mathbf{g}_۰ + u_۱\mathbf{g}_۱ + \cdots + u_{k-۱}\mathbf{g}_{k-۱}.$$

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

$$\mathbf{G} = \begin{pmatrix} \mathbf{g}_۰ \\ \mathbf{g}_۱ \\ \vdots \\ \mathbf{g}_{k-۱} \end{pmatrix} = \begin{pmatrix} g_{۰,۰} & g_{۰,۱} & \cdots & g_{۰,n-۱} \\ g_{۱,۰} & g_{۱,۱} & \cdots & g_{۱,n-۱} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-۱,۰} & g_{k-۱,۱} & \cdots & g_{k-۱,n-۱} \end{pmatrix}.$$

کدکلمه $\mathbf{v}$ متناظر با پیام $\mathbf{u}$ به‌صورت ضرب ماتریسی $\mathbf{v} = \mathbf{u}.\mathbf{G}$ به‌دست 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. درحالت 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 $\mathbb{F}_۲^n$ است، پس C یک زیرفضای $n-k$ بعدی از فضای برداری تمام مؤلفه‌های n-تایی می‌باشد و با $C^\perp$ نمایش داده می‌شود

$$C^\perp = \{\mathbf{w} \in V : < \mathbf{w}, \mathbf{v} >= ۰, \forall \mathbf{v} \in C\}$$

که در آن

$$< \mathbf{w}, \mathbf{v} >= \Sigma_{i=۱}^{n} w_i v_i$$

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 $\mathbf{h}_۰$، $\mathbf{h}_۱$، $\cdots$ و $\mathbf{h}_{n-k-۱}$ تشکیل شود، می‌توان هر کدکلمه در آن را به‌صورت یک ترکیب خطی از $n-k$ عنصر پایه بیان کرد. مشابه ماتریس مولد، ماتریس $(n-k) \times n$ زیر را درنظر بگیرید

$$\mathbf{H} = \begin{pmatrix} \mathbf{h}_۰ \\ \mathbf{h}_۱ \\ \vdots \\ \mathbf{h}_{n-k-۱} \end{pmatrix} = \begin{pmatrix} h_{۰,۰} & h_{۰,۱} & \cdots & h_{۰,n-۱} \\ h_{۱,۰} & h_{۱,۱} & \cdots & h_{۱,n-۱} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-۱,۰} & h_{n-k-۱,۱} & \cdots & h_{n-k-۱,n-۱} \end{pmatrix}.$$

ماتریس $\mathbf{H}$ یک ماتریس مولد برای کد دوگان C است. همچنین $\mathbf{G} \times \mathbf{H}^T = \mathbf{o}$، به‌طوری که "$\mathbf{o}$" 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