دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

یک روش جبری برای ساخت کدهای LDPC شبه‌دوری براساس مربع‌های لاتین

پایان‌نامه کارشناسی ارشد ریاضی کاربردی (نظریه کدگذاری)

تقی عباسی

استاد راهنما

پروفسور مرتضی اسماعیلی

۱۳۹۰

دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

پایان‌نامه کارشناسی ارشد ریاضی کاربردی (نظریه کدگذاری) آقای تقی عباسی

تحت عنوان

یک روش جبری برای ساخت کدهای LDPC شبه‌دوری براساس مربع‌های لاتین

در تاریخ ۱۳۹۰/۶/۲۶ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهائی قرار گرفت.

۱ـ استاد راهنمای پایان‌نامه   پروفسور مرتضی اسماعیلی

۲ـ استاد مشاور پایان‌نامه   دکتر محمدحسام تدین

۳ـ استاد داور ۱   دکتر علی زاغیان
(دانشگاه صنعتی مالک اشتر)

۴ـ استاد داور ۲   دکتر حمیدرضا مرزبان

سرپرست تحصیلات تکمیلی دانشکده   دکتر اعظم اعتماد

فهرست مطالب

چکیده:

در این پایان‌نامه چند روش جبری برای ساخت کدهای $LDPC$ شبه دوری دودویی و غیردودویی بر پایه میدان‌های متناهی ارائه می‌شود. کمر گراف تنر متناظر با این کدها حداقل ۶ است و این کدها عملکرد خوبی با الگوریتم کدگشایی تکراری دارند. این روش‌های ساخت بر پایه میدان‌های متناهی برای ساخت کدهایی با نرخ بالا است که ماتریس بررسی توازن آن‌ها دارای وزن ستونی کم می‌باشد. در انتها چند روش جبری برای ساخت مربع‌های لاتین ارائه می‌دهیم و سپس کدهای $LDPC$ شبه دوری حاصل از آن‌ها را معرفی می‌کنیم.
کلمات کلیدی: کدهای $LDPC$ — ماتریس بررسی توازن — مربع لاتین — حلقه Z_n — گروه p—وجهی

فصل ۱

مقدمه

کدهای تصحیح کننده خطا برای تصحیح خطای پیام‌هایی مورد استفاده قرار می‌گیرند که از یک کانال ارتباطی پارازیت‌دار ارسال می‌شوند. برای مثال شاید بخواهیم یک دنباله از ۰—ها و ۱—ها را از یک کانال پارازیت‌دار با سرعت بالا و با قابلیت اطمینان ممکن انتقال دهیم. ممکن است کانال یک خط تلفن، یک شبکه رادیویی یا یک شبکه ارتباطی ماهواره‌ای باشد. پارازیت ممکن است یک خطای انسانی، آذرخش، پارازیت گرمایی یا نقص در تجهیزات یا غیره باشد که در این‌صورت اطلاعات دریافتی با اطلاعات فرستاده شده متفاوت است[۱۲].

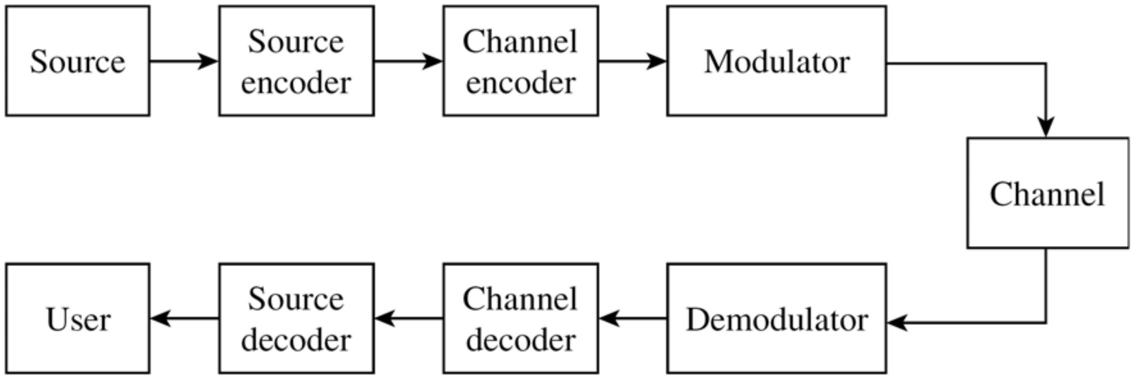
هدف یک کد تصحیح کننده خطا این است که اطلاعات را با اضافه کردن یک مقدار افزونگی مطمئن کدگذاری کند به‌طوری که اگر خطایی (نه به مقدار زیاد) در آن رخ دهد، پیام اصلی بتواند دوباره توسط گیرنده بازیابی شود. نمایی کلی از یک سیستم ارتباطی در شکل ۱—۱ نشان داده شده است[۱۸].

در شکل ۱—۱:

منبع و کاربر: منبع به‌عنوان تولیدکننده سمبل‌هایی که از یک مدل احتمالی خاص پیروی می‌کنند درنظر گرفته می‌شود. کاربر ممکن است یک شخص یا یک کامپیوتر باشد.

کدگذار و کدگشای منبع: کدگذار دنباله سمبل‌های پیام را به یک دنباله از بیت‌های صفر و یک تبدیل می‌کند و کدگشا عکس عمل کدگذاری را انجام می‌دهد.

کدگذار و کدگشای کانال: نقش کدگذار کانال محافظت از بیت‌های ارسالی در مقابل پارازیت است. وظیفه کدگشای کانال نیز تبدیل یک کلمه دریافتی به نزدیک‌ترین کدکلمه آن می‌باشد.



شکل ۱—۱: نمودار بلوکی یک سیستم انتقال اطلاعات

مدولاتور و دمدولاتور: وظیفه مدولاتور تبدیل دنباله صفر و یک به شکل سازگار با کانال برای ارسال است. وظیفه دمدولاتور بازیابی دنباله ورودی به مدولاتور از روی خروجی کانال می‌باشد.

کانال: یک محیط فیزیکی است که خروجی مدولاتور از آن عبور می‌کند. کانال می‌تواند یک خط تلفن، یک شبکه رادیویی یا یک شبکه ارتباطی ماهواره‌ای باشد.

یک مسئله مهم دیگر چگونگی کشف و اصلاح خطا در اطلاعات است. نظریه اطلاعات که بخش عمده آن ریشه در مقاله مهم سال ۱۹۴۸ شانون [۱] دارد، از توزیع احتمال برای اندازه‌گیری اطلاعات (از طریق تابع آنتروپی) و ارتباط دادن آن با میانگین طول کلمه در کدگذاری‌های آن اطلاعات استفاده می‌کند. قضیه اساسی شانون وجود کدهای خوب تصحیح کننده خطا را تضمین می‌کند و هدف نظریه کدگذاری استفاده از روش‌های ریاضی برای ساخت یک چنین کدهایی به همراه الگوریتم‌های کارا برای استفاده از آن‌ها می‌باشد. ایده اساسی قضیه شانون این است که می‌توان اطلاعات را با صحت بالا و با نرخ نزدیک به ظرفیت کانال ارسال کرد.

کدهای $LDPC$ [۲] بلوکی، کلاسی از کدهای بلوکی خطی هستند که اولین‌بار توسط گالاگر [۳] در سال ۱۹۶۲ مطرح شد[۱۱]، ولی بعد از آن حدود سه دهه به فراموشی سپرده شد. در واقع پیچیدگی کاربری این کدها در آن زمان، آن را از توانایی رقابت با سایر کدها باز داشته و باعث شده بود این دسته از کدها مورد توجه قرار نگیرند، تا اینکه تنر[۴] در سال ۱۹۸۱ کدهای $LDPC$ را تعمیم داد و نمایش گرافی از کدهای $LDPC$ که تنر گراف نامیده می‌شود را معرفی کرد[۳۲]. در سال ۱۹۹۰ موضوع کدهای $LDPC$ توسط مک‌کی [۵]، لوبی[۶] و نیل[۷] دوباره

[۱] Shannon
[۲] Low-density parity-check
[۳] Gallager
[۴] Tanner
[۵] MacKay
[۶] Luby
[۷] Nil

احیا شد. در سال ۱۹۹۸ نیز کدهای $LDPC$ غیر دودویی اولین‌بار توسط دیوی[۸] و مک‌کی مطرح شد[۲۳]، [۲۴]، [۲۵]. در سال ۲۰۰۰ هندسه‌های متناهی برای ساخت کدهای $LDPC$ شبه‌دوری دوتایی مورد استفاده قرار گرفت. همچنین در سال ۲۰۰۰ نشان داده شده است که با استفاده از میدان‌های متناهی نیز می‌توان کدهای $LDPC$ شبه‌دوری ساخت[۲۷].

کدهای $LDPC$ دارای ماتریس بررسی توازن خلوت می‌باشند و روش خوبی برای رسیدن به ظرفیت شانون برای کانال‌هایی با برد عریض هستند. الگوریتم کدگشایی آن‌ها، نظیرالگوریتم جمع — ضرب[۹]، از یک روش تکراری بهره می‌گیرند که در آن‌ها پیچیدگی محاسباتی به‌طور خطی با طول کد افزایش می‌یابد[۴]. ساخت کدهای $LDPC$ به دو روش تصادفی و ساختاری صورت می‌گیرد. کدهای ساختاری نسبت به کدهای تصادفی ساخته شده توسط مک‌کی از پیچیدگی ذخیره‌سازی و کدگذاری کمتری برخوردار هستند.

این پایان‌نامه از پنج فصل تشکیل شده است: در فصل اول تعاریف و مفاهیم لازم را بیان می‌کنیم. در فصل دوم یک روش ساخت کدهای $LDPC$ شبه‌دوری روی میدان متناهی را با استفاده از ماتریس‌های جایگشتی دوری معرفی می‌کنیم. در فصل سوم چند روش ساخت کدهای $LDPC$ مورد مطالعه قرار می‌گیرد. در فصل چهارم نیز چند روش برای ساخت مربع‌های لاتین ارائه شده و در فصل پنج روش‌های دیگری برای ساخت کد براساس مربع‌های لاتین ساخته شده ارائه می‌شود.

۱—۱ گروه

تعریف ۱.۱ مجموعه ناتهی G را با عمل دودویی $(*)$ روی آن یک گروه گویند، اگر شرایط زیر برقرار باشد.

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

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

۳) 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.

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

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

---
۸ Davey
۹ Sum-Product

عنصر a' را وارون عنصر a گویند.

اگر G شامل تعداد متناهی عنصر باشد، G را یک گروه متناهی گویند. در یک گروه عنصر همانی و وارون هر عنصر منحصربه‌فرد هستند.

تعریف ۲.۱ زیرمجموعه ناتهی H از یک گروه G را تحت عمل $*$ یک زیرگروه G می‌گویند اگر H با عمل $*$ خود یک گروه باشد، یا در شرایط زیر صدق کند که با نماد $H \leq G$ نمایش می‌دهند.

۱) برای هر دو عنصر $a, b \in H$ داشته باشیم: $a * b \in H$.

۲) اگر $a \in H$ آن‌گاه $a^{-1} \in H$.

گروه G آبلی 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 $< a >= \{a^n | n \in Z\}$. گروه G دوری است اگر عنصر $a \in G$ موجود باشد به‌قسمی که $G =< a >$.

تعریف ۳.۱ فرض کنید G یک گروه بوده و $H \leq G$. H را در G نرمال می‌گوییم و می‌نویسیم $H \trianglelefteq G$، هرگاه برای هر $g \in G$، $gHg^{-1} \in H$.

۱—۲ حلقه

تعریف ۴.۱ حلقه R یک مجموعه ناتهی با دو عمل $+$ و $\cdot$ است به‌طوری که شرایط زیر برقرار باشد.

۱) R تحت عمل جمع یک گروه آبلی است.

۲) R تحت عمل $\cdot$ شرکت‌پذیر است، یعنی $a.(b.c) = (a.b).c$.

۳) ضرب نسبت به جمع توزیع‌پذیر است، یعنی $a.(b + c) = a.b + ac$.

تعریف ۵.۱ زیرمجموعه ناتهی S از حلقه R را یک زیرحلقه از R می‌گویند اگر S با عمل‌های تعریف شده روی R خود یک حلقه باشد.

تعریف ۶.۱ یک زیرمجموعه I از یک حلقه R یک ایده‌آل نامیده می‌شود اگر شرایط زیر برقرار باشد.

۱) اگر $a, b \in I$ آن‌گاه $a - b \in I$.

۲) برای هر $a \in R$ و $i \in I$، عناصر ia و ai در I هستند.

۱ــ۳ میدان متناهی و فضای برداری

۱ــ۳ــ۱ میدان

تعریف **۷.۱** فرض کنید F یک مجموعه از عناصر با دو عمل دودویی جمع $+$ و ضرب $\cdot$ باشد. F نسبت به دو عمل جمع $+$ و ضرب $\cdot$ یک میدان است اگر در شرایط زیر صدق کند.

۱) F نسبت به عمل جمع یک گروه آبلی است. عنصر همانی نسبت به عمل جمع را عنصر صفر F نامیده و با 0 نمایش می‌دهیم.

۲) مجموعه عناصر ناصفر F تحت عمل ضرب یک گروه آبلی است. عنصر همانی نسبت به عمل ضرب را عنصر یکه F نامیده و با 1 نمایش می‌دهیم.

۳) عمل ضرب نسبت به عمل جمع توزیع‌پذیر است، یعنی

$$a \cdot (b+c) = a \cdot b + a \cdot c, \quad a, b, c \in F.$$

طبق تعریف، هر میدان دارای حداقل دو عنصر 0 و 1 است. یک میدان با تعداد متناهی عنصر را یک میدان متناهی می‌گویند و تعداد عناصر آن را مرتبه میدان می‌نامند. میدان F_q با q عنصر را درنظر بگیرید. فرض کنید α یک عنصر ناصفر در F_q باشد. چون مجموعه عناصر ناصفر F_q تحت عمل ضرب بسته است، بنابراین توان‌های α

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

عناصری ناصفر در F_q هستند.

کوچکترین عدد صحیح مثبت n با خاصیت $\alpha^n = 1$ را مرتبه عنصر α می‌نامیم. در یک میدان عنصر ناصفر α را اولیه گویند اگر $q-1$ مرتبه α باشد. بنابراین توان‌های یک عنصر اولیه همه عناصر ناصفر میدان 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 F یک میدان باشد. زیرمجموعه K از F را یک زیرمیدان F می‌گویند اگر K نیز تحت عمل‌های F یک میدان باشد. F را نیز توسیع میدان K می‌نامیم. اگر $F \neq K$ باشد، K را یک زیرمیدان سره F گویند.

۱—۳—۲ نمایش برداری عناصر F_{q^m}

تعریف ۸.۱ به ازاء $0 \leq i < q^m - 1$ برای هر عنصر ناصفر $\alpha^i \in F_{q^m}$، برداری به‌طول $q^m - 1$ روی F_2 به‌صورت

$$C_b(\alpha^i) = (c_0, c_1, \cdots, c_{q^m-2})$$

متناظر کنید به‌طوری که مولفه i—ام آن برابر یک و دیگر مولفه‌های آن صفر باشد. این بردار را بردار مکان عنصر α^i می‌گویند. بردار مکان عنصر صفر برابر $C_b(\mathbf{0}) = (0, 0, \cdots, 0)$ است[۱۵].

فرض کنید δ یک عنصر ناصفر F_{q^m} باشد. آن‌گاه بردار مکان $C_b(\alpha\delta)$ برابر با انتقال دوری (یک واحد به سمت راست) بردار مکان $C_b(\delta)$ است. ماتریس مربعی $B(\delta)$ از مرتبه $q^m - 1$ را روی F_2 درنظر بگیرید به‌طوری که بردارهای مکان نقاط δ، $\alpha\delta$، $\cdots$ و $\alpha^{q^m-2}\delta$ سطرهای متوالی آن باشند. برای مثال اگر $\delta = \alpha^i$ آن‌گاه ماتریس $B(\alpha^i)$ به فرم زیر است.

$$B(\delta) = \begin{pmatrix} C_b(\delta) \\ C_b(\alpha\delta) \\ \vdots \\ C_b(\alpha^{q^m-2}\delta) \end{pmatrix} = \left(\begin{array}{c|c} (O)_{q^m-i-1\times i} & \begin{matrix} 1 & & O \\ & \ddots & \\ O & & 1 \end{matrix} \\ \hline \begin{matrix} 1 & & O \\ & \ddots & \\ O & & 1 \end{matrix} & (O)_{i\times q^m-i-1} \end{array}\right)_{q^m-1\times q^m-1} \qquad (1)$$

ماتریس $B(\delta)$ یک ماتریس جایگشتی دوری از مرتبه $(q^m - 1) \times (q^m - 1)$ روی F_2 است. چون $B(\delta)$ به‌وسیله پراکندگی توسط δ به‌دست می آید، به آن یک ماتریس پراکندگی نسبت به δ می‌گویند. به‌وضوح ماتریس پراکندگی برای عنصر صفر F_{q^m} یک ماتریس تمام صفر از مرتبه $(q^m - 1) \times (q^m - 1)$ است.

مثال ۹.۱ میدان F_8 را با عناصر $\{0, \alpha^0, \alpha^1, \cdots, \alpha^6\}$ درنظر بگیرید. فرض کنید $\delta = \alpha^2$. ماتریس $B(\alpha^2)$ روی F_2 با استفاده از (۱) به فرم زیر است.

$$B(\alpha^2) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

تعریف ۱۰.۱ به ازاء $\circ \leq i < q^m - ۱$ برای هر عنصر ناصفر $\alpha^i \in F_{q^m}$، برداری به طول $q^m - ۱$ روی F_{q^m} به شکل

$$C_{q^m}(\alpha^i) = (f_\circ, f_۱, \cdots, f_{q^m - ۲})$$

متناظر کنید به‌طوری که مولفه i–ام آن برابر $f_i = \alpha^i$ و دیگر مولفه‌های آن صفر باشد. این بردار را بردار مکان عنصر α^i روی F_{q^m} می‌گویند. به عنصر $\mathbf{0} \in F_{q^m}$ یک بردار تمام‌صفر به‌طول $q^m - ۱$ به‌صورت $C_{q^m}(\mathbf{0}) = (\circ, \circ, \cdots \circ)$ متناظر کنید.

فرض کنید δ یک عنصر ناصفر F_{q^m} باشد. بردار مکان $C_{q^m}(\alpha\delta)$ برای عنصر $\alpha\delta$ برابر با بردار مکان $C_{q^m}(\delta)$ مضرب α است، یعنی اگر بردار مکان $C_{q^m}(\delta)$ را یک واحد به سمت راست انتقال داده و سپس در α ضرب کنید، بردار مکان $C_{q^m}(\alpha\delta)$ به‌دست می آید. ماتریس مربعی $Q(\delta)$ از مرتبه $q^m - ۱$ را روی F_{q^m} درنظر بگیرید به‌طوری که بردارهای مکان نقاط δ، $\alpha\delta$، $\cdots$ و $\alpha^{q^m-۲}\delta$ سطرهای متوالی آن باشند. برای مثال اگر $\delta = \alpha^i$ باشد ماتریس $Q(\delta)$ به فرم زیر است.

$$\begin{pmatrix} C_{q^m}(\delta) \\ C_{q^m}(\alpha\delta) \\ \vdots \\ C_{q^m}(\alpha^{q^m-۲}\delta) \end{pmatrix} = \left(\begin{array}{c|c} (O)_{q^m-i-۱\times i} & \begin{matrix} \alpha^i & & & \\ & \alpha^{i+۱} & & O \\ O & & \ddots & \\ & & & \alpha^{q^m-۲} \end{matrix} \\ \hline \begin{matrix} ۱ & & & \\ & \alpha & & O \\ O & & \ddots & \\ & & & \alpha^{i-۱} \end{matrix} & (O)_{i\times q^m-i-۱} \end{array}\right)_{q^m-۱\times q^m-۱} \qquad (۲)$$

ماتریس $Q(\delta)$ یک نوع ویژه از ماتریس‌های جایگشتی دوری است، زیرا هر سطر آن یک انتقال دوری مضرب α سطر بالای آن و سطر اول آن یک انتقال دوری مضرب α سطر آخر آن است. $Q(\delta)$ را یک ماتریس پراکندگی نسبت به δ می‌گویند. ماتریس پراکندگی عنصر صفر F_{q^m} یک ماتریس تمام صفر از مرتبه $(q^m - ۱) \times (q^m - ۱)$ است.

مثال ۱۱.۱ F_{16} را با عناصر $\{0, \alpha^0, \alpha^1, \cdots, \alpha^{14}\}$ درنظر بگیرید. فرض کنید $\delta = \alpha^8$. ماتریس $Q(\alpha^8)$ با استفاده از (۲) به شکل زیر است.

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^8 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^9 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{10} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{11} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{12} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{13} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^{14} \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \alpha^1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \alpha^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \alpha^4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \alpha^5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \alpha^6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^7 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

ماتریس‌های جایگشتی دوری $B(\delta)$ و $Q(\delta)$ از مرتبه $(q^m - 1) \times (q^m - 1)$ دو نمایش ماتریسی متفاوت از یک عنصر ناصفر δ در میدان F_{q^m} به‌ترتیب روی F_2 و F_{q^m} هستند.

۱–۳–۳ فضای برداری

تعریف ۱۲.۱ یک گروه آبلی V با یک عمل دودویی جمع + روی آن را درنظر بگیرید. فرض کنید F یک میدان بوده و یک عمل ضرب اسکالر $\cdot$ از $F \times V$ به V تعریف شده باشد. مجموعه V را یک فضای برداری روی F نامند اگر در شرایط زیر صدق کند[۱۲].

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

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

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

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

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

۳) برای هر $\mathbf{v} \in V$ داریم $1 \cdot \mathbf{v} = \mathbf{v}$.

یک دنباله مرتب شده با n مولفه a_0، a_1، $\cdots$ و a_{n-1} که هر مولفه آن عنصری از F_q است را درنظر بگیرید. این دنباله را یک n—تایی روی F_q می‌نامیم. q روش برای انتخاب هر a_i وجود دارد، بنابراین q^n، n—تایی متفاوت موجود است. مجموعه $(F_q)^n$ همه n—تایی‌های مرتب روی F_q است که آن را با F_q^n نشان می‌دهیم. عناصر F_q^n را بردار می‌نامیم.

دو عمل روی F_q^n تعریف می‌کنیم.

الف) جمع دو بردار: برای هر $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ و $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ در F_q^n، بردار $\mathbf{u} + \mathbf{v}$ به فرم زیر است.

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

ب) حاصل‌ضرب یک بردار در یک اسکالر: اگر $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in F_q^n$ و $a \in F_q$ داریم:

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

جمع برداری و ضرب اسکالر تعریف شده در (الف) و (ب) به‌ترتیب در قوانین توزیع‌پذیری و شرکت‌پذیری صدق می‌کنند. بنابراین مجموعه F_q^n یک فضای برداری روی F_q است.

یک زیرمجموعه از F_q^n یک زیرفضای F_q^n است هرگاه تحت عمل جمع و ضرب تعریف شده روی F_q^n یک فضای برداری باشد. هر زیرفضا از 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.

۱—۴ کدهای بلوکی خطی

فرض کنید خروجی یک منبع دنباله‌ای از سمبل‌های دوتایی روی F_2 باشد. سمبل‌های صفر و یک 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[18].

در کدگذاری کانال، هر پیام k بیتی $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ 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 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 $R = \frac{k}{n}$ را نرخ کد می‌نامند. نرخ کد را می‌توان متوسط تعداد بیت اطلاعات در هر بیت‌کد تعبیر کرد.

تعریف **۱۳.۱** یک کد دودویی با طول n و 2^k کدکلمه، یک $[n,k]$—کد بلوکی خطی نامیده می‌شود اگر و تنها اگر 2^k کدکلمه آن یک زیرفضای k بعدی از فضای برداری تمام مولفه‌های n—تایی روی F_2 باشد.

۱—۵ ماتریس مولد و ماتریس بررسی توازن

چون یک $[n,k]$—کد خطی $\mathcal{C}$ یک زیرفضای k بعدی از فضای برداری تمام مولفه‌های n—تایی روی 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 $\mathbf{c} \in \mathcal{C}$ را به‌صورت یک ترکیب خطی از آن‌ها بیان کرد. این k کدکلمه یک پایه برای کد $\mathcal{C}$ است. فرض کنید $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ یک پیام است تا کدگذاری شود. کدکلمه متناظر با $\mathbf{u}$ از ترکیب خطی $\{\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{k-1}\}$ و k بیت $\mathbf{u}$ به‌دست می آید.

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

در این‌صورت می‌توان k کدکلمه مستقل را در سطرهای یک ماتریس قرار داد و یک ماتریس از مرتبه $k \times n$ به شکل زیر به‌دست آورد[۱۸].

$$G = \begin{pmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{pmatrix} \qquad (۳)$$

کدکلمه $\mathbf{v}$ متناظر با پیام $\mathbf{u}$ به‌صورت ضرب ماتریسی $\mathbf{v} = \mathbf{u}.G$ به‌دست می آید. واضح است که کدکلمه $\mathbf{v}$ یک ترکیب خطی از سطرهای G است. ماتریس G را ماتریس مولد $[n,k]$—کد خطی $\mathcal{C}$ می‌نامند. کد $\mathcal{C}$ را نیز فضای سطری G می‌نامند. در حالت کلی یک $[n,k]$—کد خطی $\mathcal{C}$ بیشتر از یک پایه دارد، بنابراین بیش از یک ماتریس مولد برای $\mathcal{C}$ موجود است.

چون یک $[n,k]$—کد خطی $\mathcal{C}$ یک زیرفضای k بعدی از فضای برداری تمام مولفه‌های n—تایی روی F_2 است، پس فضای دوگان $\mathcal{C}$ یک زیرفضای $n-k$ بعدی از فضای برداری تمام مولفه‌های n—تایی می‌باشد که با $\mathcal{C}^{\perp}$ نمایش داده می‌شود که $< \mathbf{w}, \mathbf{v} >$ بیانگر ضرب داخلی $\mathbf{w}$ و $\mathbf{v}$ است.

$$\mathcal{C}^{\perp} = \{\mathbf{w} \in V :< \mathbf{w}, \mathbf{v} >= 0, \forall\ \mathbf{v} \in C\}.$$

$\mathcal{C}^{\perp}$ را می‌توان یک $[n, n-k]$—کد خطی درنظر گرفت که کد دوگان $\mathcal{C}$ نامیده می‌شود.

مشابه بحثی که برای ماتریس مولد مطرح شد، اگر فضای دوگان کد $\mathcal{C}$ از $n-k$ پایه مستقل خطی $\mathbf{h}_0$، $\mathbf{h}_1$، $\cdots$ و $\mathbf{h}_{n-k-1}$ 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.

$$H = \begin{pmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{pmatrix} \qquad (۴)$$

ماتریس H یک ماتریس مولد برای کد دوگان $\mathcal{C}$ است. همچنین $G \times H^T = \mathbf{0}$، به‌طوری که $\mathbf{0}$ یک ماتریس تمام صفر از مرتبه $(n-k) \times k$ است. چون ماتریس H دارای $n-k$ سطر مستقل خطی است، پس می‌توان کد $\mathcal{C}$ را با ماتریس H به‌صورت زیر معرفی کرد.

$$\mathcal{C} = \{\mathbf{v} \in F_2^n : \mathbf{v}.H^T = 0\}.$$

ماتریس H را ماتریس بررسی توازن کد $\mathcal{C}$ و $\mathcal{C}$ را فضای تهی H می‌نامند. یک کد خطی به‌طور منحصربه‌فرد با ماتریس‌های مولد و بررسی توازن معرفی می‌شود. عمل کدگذاری در کد خطی با ماتریس مولد و عمل کدگشایی با ماتریس بررسی توازن صورت می‌گیرد.

فرض کنید یک کدکلمه در یک کد به دو بخش پیام و افزونگی تقسیم شود که قسمت پیام متشکل از k بیت پیام اصلی و قسمت افزونگی متشکل از $n-k$ بیت بررسی توازن است. یک کد خطی با این ساختار، کد خطی استاندارد نامیده می‌شود. یک کد خطی استاندارد به‌طور کامل با یک ماتریس مولد $k \times n$ به شکل زیر مشخص می‌شود.

$$G = \begin{pmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{pmatrix} = \begin{pmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & \vdots & 1 \end{pmatrix} \qquad (۵)$$

ماتریس مولد G از دو زیرماتریس تشکیل شده است، یک زیرماتریس P از مرتبه $k \times (n-k)$ در سمت چپ با درایه‌هایی از F_2 و یک ماتریس همانی از مرتبه k در سمت راست. برای راحتی ماتریس G را با $G = [P|I_k]$ نمایش می‌دهیم.

k مولفه سمت راست حاصل از ضرب هر پیام در G، همان k بیت پیام است. به $n-k$ بیت که از حاصل‌جمع بیت‌های اطلاعات به‌دست می آیند، بیت‌های بررسی توازن می‌نامند. این بیت‌ها با زیر ماتریس P بطور

منحصربه‌فرد توسط معادلات زیر مشخص می‌شوند.

$$v_j = u_0 p_{0,j} + u_1 p_{1,j} + \cdots + u_{k-1} p_{k-1,j}\ ,\quad j = 0, 1, \cdots, n-k-1$$

معادلات بالا را معادلات بررسی توازن و زیرماتریس P را زیرماتریس توازن می‌نامند.

اگر ماتریس مولد کد $\mathcal{C}$ در حالت استاندارد نباشد، می‌توان آن را با عملیات سطری مقدماتی (و احتمالا جایگشت ستون‌ها) به یک ماتریس استاندارد تبدیل کرد. کد حاصل از این ماتریس با کد اولیه $\mathcal{C}$ در چیدمان بیت‌هایشان تفاوت دارند، به‌این معنا که کدکلمه‌های $\mathcal{C}$ از یک جایگشت مشخص در مکان کدبیت‌های جدید حاصل می‌شود.

اگر ماتریس مولد یک $[n,k]$—کد خطی در حالت استاندارد باشد، ماتریس بررسی توازن آن به فرم زیر است.

$$H = [I_{n-k}\ \ P^T] = \begin{pmatrix} 1 & 0 & \cdots & 0 & p_{0,0} & p_{1,0} & \cdots & p_{k-1,0} \\ 0 & 1 & \cdots & 0 & p_{0,1} & p_{1,1} & \cdots & p_{k-1,1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \vdots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{pmatrix} \qquad (6)$$

۱—۶ کمترین فاصله همینگ

فرض کنید $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ یک بردار n—تایی روی F_2 باشد. وزن همینگ بردار $\mathbf{v}$ برابر تعداد مولفه‌های ناصفر $\mathbf{v}$ می‌باشد و با $w(\mathbf{v})$ نمایش داده می‌شود. کمترین وزن کدکلمه‌های ناصفر $\mathcal{C}$ که با $w_{min}(\mathcal{C})$ نمایش داده می‌شود، کمترین وزن $\mathcal{C}$ نامیده می‌شود، یعنی

$$w_{min}(\mathcal{C}) := min\{w(\mathbf{v}) : \mathbf{v} \in \mathcal{C}, \mathbf{v} \neq 0\}.$$

تعریف ۱.۱۴ فاصله همینگ بین دو بردار $\mathbf{u}$ و $\mathbf{v}$ از F_q^n برابر است با تعداد مکان‌هایی که آن‌ها با هم متفاوت هستند و با $d(\mathbf{u},\mathbf{v})$ نمایش داده می‌شود.

فاصله همینگ یک تابع متریک می‌باشد. یکی از پارامترهای خیلی مهم یک کد $\mathcal{C}$ که یک اندازه خوب در تصحیح خطا ارائه می‌دهد مینیمم فاصله کد است[۱۸].

تعریف ۱.۱۵ مینیمم فاصله یک کد $\mathcal{C}$ برابر کمترین فاصله بین کدکلمه‌های $\mathcal{C}$ است، و با $d(\mathcal{C})$ نمایش داده می‌شود.

$$d(\mathcal{C}) := min\{d(\mathbf{u},\mathbf{v}) | \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}.$$