

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد رمز و کد

ساختن کدهای کم‌چگال توسط گراف‌های متقارن مکعبی

نگارنده: یاسمن محمدنیا

استاد راهنما

دکتر عبدالله آل‌هوز

بهمن‌ماه ۱۴۰۰

تقدیم...

این پایان نامه را تقدیم می کنم به تمام کسانی که با حضورشان موجبات دلگرمی را
برای من فراهم نموده اند.

سپاس گزاری...

با سپاس و تقدیر ویژه از استاد گرانقدر جناب آقای دکتر آل هوز که در مراحل مختلف این پژوهش، راهنمایی‌های ارزنده و سازنده خود را بر من ارزانی داشته و از هیچ کوششی در این زمینه دریغ ننمودند.
پدر و مادر عزیز و مهربانم، از اینکه در تمام مراحل زندگی یار و پشتیبانم بوده‌اید بی‌نهایت سپاسگزارم.

یاسمن محمدنیا

بهمن‌ماه ۱۴۰۰

تعهد نامه

اینجانب یاسمن محمدنیا دانشجوی کارشناسی ارشد رشته ریاضی کاربردی علوم ریاضی دانشگاه شاهرود، نویسنده پایان نامه با عنوان ساختن کدهای کم چگال توسط گراف های متقارن مکعبی، تحت راهنمایی دکتر عبدالله آل هوز متعهد می شوم:

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش های دیگر پژوهش گران، به مرجع مورد استفاده استناد شده است.
- مطالب این پایان نامه، تا کنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود تعلق دارد، و مقالات مستخرج با نام “دانشگاه صنعتی شاهرود” یا “Shahrood University of Technology” به چاپ خواهد رسید.
- قوق معنوی تمام افرادی که در به دست آوردن نتایج اصلی پایان نامه تاثیرگذار بوده اند، در مقالات مستخرج از پایان نامه رعایت می گردد.
- در تمام مراحل انجام این پایان نامه، در مواردی که از موجود زنده (یا بافت های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده شده است)، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

یاسمن محمدنیا

بهمن ماه ۱۴۰۰

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه های رایانه ای، نرم افزارها و تجهیزات ساخته شده) متعلق به دانشگاه صنعتی شاهرود می باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان نامه بدون ذکر منبع مجاز نمی باشد.

چکیده

کدهای (با ماتریس کنترل توازن) کم چگال (LDPC) به این دلیل که در نزدیکی حد شانون رفتار می کنند مورد توجه بسیاری قرار گرفتند. در این پایان نامه، نحوه ی ساختن کدهای LDPC با استفاده از گراف های (نیم) متقارن مکعبی ارائه خواهد شد. کدهای ساخته شده (۳،۳) - منظم هستند و اکثریت قریب به اتفاق گراف های تنر متناظر آنها، کمر بزرگ تر از ۴ دارند. خصوصیات کدهای به دست آمده را تجزیه و تحلیل کرده و برای پارامترهای کد، علی الخصوص برای بعد و مینیمم فاصله کد، کران هایی ارائه خواهد شد. اطلاعات کدهای LDPC ساخته شده از گراف های متقارن مکعبی دوبخشی با مرتبه کمتر از ۲۰۰ را نیز ارائه می دهیم. مشاهده خواهیم کرد که برخی از کدهای ساخته شده بهینه هستند و همچنین دارای ویژگی های دیگری مانند خود- متعامد بودن یا خاصیت دوگان- مکمل (کدهای LCD) می باشند.

کلمات کلیدی: کد کم چگال (LDPC)، گراف مکعبی، گراف کمان- انتقالی، گراف دوبخشی

فهرست مطالب

م	فهرست تصاویر
س	فهرست جداول
۱	۱ تعاریف مقدماتی
۱	۱.۱ مقدمه
۱	۲.۱ تعاریف مرتبط به نظریه کدگذاری
۵	۳.۱ تعاریف مرتبط به ماتریس و جبر خطی
۸	۴.۱ تعاریف مرتبط به نظریه گراف
۱۵	۲ کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی
۱۵	۱.۲ مقدمه
۱۶	۲.۲ کدهای کم چگال ساخته شده توسط گراف‌های متقارن مکعبی
۲۱	۳.۲ واریانس وزن سندروم
۲۳	۳ کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی
۲۳	۱.۳ مقدمه
۲۴	۲.۳ کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی
۲۸	۳.۳ واریانس وزن سندروم
۲۸	۴.۳ مجموعه جاذب
۳۱	۴ شبیه‌سازی و نتایج محاسباتی
۳۱	۱.۴ مقدمه
	۲.۴ نتایج محاسباتی کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی
۳۱	۳.۴ نتایج شبیه‌سازی کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی
۳۴	مکعبی

۴.۴	نتایج محاسباتی کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن
۳۶	مکعبی
۵.۴	نتایج شبیه‌سازی کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن
۳۸	مکعبی
۴۱	واژه‌نامه انگلیسی به فارسی
۴۵	واژه‌نامه فارسی به انگلیسی
۴۹	مراجع

فهرست تصاویر

۱.۳	تنها ساختار ممکن از مجموعه جاذب از اندازه ۳ در گراف تنر کدهای کم
۲۹	چگال $C_H(G)$ و $C_{HT}(G)$
۲.۳	تنها ساختار ممکن از مجموعه جاذب از اندازه چهار در گراف تنر کدهای
۳۰	کم چگال $C_H(G)$ و $C_{HT}(G)$
۱.۴	پارامترهای کدهای LDPC ساخته شده توسط گراف متقارن مکعبی با
۳۲	کمتر از ۲۰۰ رأس به دست آمده است.
۲.۴	$(d(n,k), N(n,k, d(n,k)))$
۳۳	عملکرد BER کد LDPC [۲۶، ۶، ۱۰] برگرفته از گراف ۴۸A
۳۵	عملکرد BER کد LDPC [۹۶، ۱۸، ۱۶] برگرفته از گراف ۱۹۲A
۳۵	پارامترهای کدهای LDPC ساخته شده توسط گرافهای نیم متقارن مکعبی
۵.۴	با کمتر از ۱۰۰۰ رأس (با استفاده از روش ارائه شده در مرجع [۱۹])
۳۶	عملکرد BER کد LDPC [۵۶، ۱۲، ۱۶] به دست آمده از گراف Ljubljana
۳۸	عملکرد BER کد LDPC [۱۴۷، ۲۶، ۲۶] به دست آمده از گراف نیم متقارن
۷.۴	مکعبی با ۲۹۴ رأس.
۳۹	عملکرد BER کد LDPC [۲۸۸، ۳۲، ۵۶] به دست آمده از گراف نیم متقارن
۸.۴	مکعبی با ۵۷۶ رأس.
۳۹	عملکرد BER کد LDPC [۴۴۸، ۴۸، ۱۰۰] به دست آمده از گراف نیم متقارن
۹.۴	مکعبی با ۸۹۶ رأس.
۴۰	

فهرست جداول

۱.۴	نرخ کدهای LDPC ساخته شده از گراف‌های متقارن و نیم متقارن مکعبی
۳۷	با طول یکسان

پیشگفتار

کدهای کم‌چگال^۱ (LDPC) برای اولین بار توسط گالاگر^۲ در اوایل دهه ۱۹۶۰ معرفی شدند و توسط میکی^۳ و نیل^۴ مورد بررسی بیشتر و دقیق‌تر قرار گرفتند. این کدها به دلیل این که می‌توانند در نزدیکی حد شانون عمل کنند، مورد توجه بسیاری از پژوهشگران می‌باشند. طی سال‌های گذشته، محققان کدهای LDPC که فاقد دورهایی با طول ۴ هستند را با استفاده از ساختارهای مختلف از جمله گراف‌ها، ساخته‌اند.

گراف‌های متقارن مکعبی^۵ (CSG) برای اولین بار توسط فاستر^۶ مورد مطالعه قرار گرفتند و پس از آن مورد توجه پژوهشگران زیادی قرار دارند. کاندلر^۷ و ندلا^۸ ثابت کردند برحسب عملیات کمان-انتقالی که برای گراف‌های متقارن مکعبی داریم، می‌توانیم این گراف‌ها را به ۱۷ خانواده رده‌بندی کنیم.

گراف‌های نیم‌متقارن مکعبی^۹ (CSSG) اولین بار توسط فلکمن^{۱۰} مورد مطالعه قرار گرفت. او ساختار گراف‌های نیم‌متقارن را پیشنهاد داد و کوچک‌ترین گراف نیم‌متقارن مکعبی با ۲۰ رأس و ۴۰ یال را ساخت (گراف فلکمن). علاوه بر این، او ثابت کرد که هیچ گراف نیم‌متقارن با $2p$ یا $2p^2$ رأس، جایی که p عدد اول باشد، وجود ندارد.

در این پایان‌نامه، برخی رده‌هایی از کدهای LDPC، با استفاده از گراف‌های متقارن مکعبی دوبخشی به عنوان گراف‌های تنر کدهای LDPC، ساخته شده‌اند.

هدف این پایان‌نامه ساختن کدهای LDPC فاقد دورهای کوتاه، به ویژه فاقد دورهایی با طول ۴، با استفاده از گراف‌های متقارن مکعبی (CSG) دوبخشی و گراف‌های نیم‌متقارن مکعبی (CSSG) همبند دوبخشی به عنوان گراف‌های تنر^{۱۱} کدهای LDPC می‌باشد.

پایان‌نامه به شرح زیر سازماندهی شده است:

¹Low-density parity-check

²Gallager

³Meaky

⁴Neal

⁵Cubic Symmetric Graph

⁶Foster

⁷Cander

⁸Nedela

⁹Semisymmetric

¹⁰Folkman

¹¹Tanner

در فصل اول، تعاریف و مفاهیم مقدماتی لازم از نظریه گراف‌ها، نظریه ماتریس و جبر خطی و همچنین نظریه کدگذاری آورده شده و به بیان مفاهیم مقدماتی لازم مرتبط با کدهای LDPC پرداخته‌ایم.

در فصل دوم، نحوه ساختن کدهای LDPC با استفاده از گراف‌های متقارن مکعبی بیان شده و نتایج مربوط به پارامترهای کد ارائه شده است. همچنین واریانس وزن سندروم کدهای LDPC مورد مطالعه و بررسی قرار گرفته است.

در فصل سوم، نحوه ساختن کدهای LDPC با استفاده از گراف نیم‌متقارن مکعبی و نتایج مربوط به پارامترهای کد ارائه شده است. همچنین واریانس وزن سندروم کدهای LDPC مورد مطالعه و بررسی قرار گرفته و در مورد مجموعه جاذب و مجموعه تله‌ای مربوط به این کدها نتایجی ارائه شده است.

در فصل چهارم، نتایج محاسباتی مربوط به کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی و همچنین گراف‌های نیم‌متقارن مکعبی آورده شده است. همچنین مثال‌هایی را که عملکرد (BER) کدهای ساخته شده در هر کدام از وضعیت‌های دوگانه فوق را نشان می‌دهند، ارائه می‌دهیم.

فصل ۱

تعاریف مقدماتی

۱.۱ مقدمه

در این فصل تعاریف و مفاهیم مقدماتی مدنظر که در سرتاسر این پایان نامه مورد استفاده قرار خواهند گرفت، بیان شده است. ابتدا مفاهیم لازم از نظریه کدگذاری، سپس مفاهیم لازم از نظریه ماتریس و جبر خطی و پس از آن مفاهیمی از نظریه گرافها آورده شده است.

۲.۱ تعاریف مرتبط به نظریه کدگذاری

تعریف ۱.۲.۱. یک $[n, k]$ - کد خطی^۱ دودویی C ، زیرفضای k -بعدی از فضای برداری $\mathbb{F}_2^n$ می باشد.

تعریف ۲.۲.۱. برای $x, y \in \mathbb{F}_2^n$ ، $d(x, y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|$ فاصله همینگ^۲ نامیده می شود.

تعریف ۳.۲.۱. مینیمم فاصله کد به صورت $d = \min\{d(x, y) : x \neq y \in C\}$ تعریف می شود. سرتاسر این پایان نامه، یک $[n, k]$ - کد خطی دودویی با مینیمم فاصله d یک $[n, k, d]$ - کد نامیده می شود.

^۱Linear Code

^۲Hamming Distance

مثال ۱.۲.۱. فرض کنید کد C به صورت $C = \{01201, 12200, 21011\}$ روی الفبای $A = \mathbb{F}_3$ داده شده باشد، در این صورت فاصله کد به صورت زیر می باشد:

$$d_H(c_1, c_2) = 3, \quad d_H(c_1, c_3) = 3 \quad \text{و} \quad d_H(c_2, c_3) = 5$$

بنابراین داریم:

$$d(C) = \min\{d(x, y) : x \neq y \in C\} = 3.$$

تعریف ۴.۲.۱. نرخ ارسال اطلاعات^۱ (نرخ) کد C ، به صورت نسبت $r = \frac{k}{n}$ می باشد، جایی که k تعداد بیت های اطلاعات مفید ما می باشد که قرار است ارسال شود و n تعداد بیت هایی است که کدگذار صرف کدگذاری اطلاعات و داده ها می کند، یعنی $n \geq k$ و به تعداد $n - k$ تا بیت در فرایند کدگذاری به پیام اصلی اضافه شده است.

تعریف ۵.۲.۱. کد بهینه^۲ کدی است که کران بالای نظری را برای مینیمم فاصله به دست می آورد.

تعریف ۶.۲.۱. زیرمجموعه S از $\mathbb{F}_q^n$ دوری^۳ می باشد اگر برای هر $(a_0, a_1, \dots, a_{n-1}) \in S$ داشته باشیم:

$$(a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in S$$

کد خطی C یک کد دوری نامیده می شود اگر C یک مجموعه دوری باشد.

مثال ۲.۲.۱. مجموعه $\mathbb{F}_3^4$ $\{(0, 1, 1, 2), (2, 0, 1, 1), (1, 2, 0, 1), (1, 1, 2, 0)\} \subset \mathbb{F}_3^4$ مجموعه دوری می باشد اما کد دوری نیست، زیرا یک کد خطی نمی باشد.

مثال ۳.۲.۱. کدهای زیر دوری می باشند:

۱. کدهای بدیهی $\{0\}$ ، $\{\lambda \cdot 1 : \lambda \in \mathbb{F}_q\}$ و $\mathbb{F}_q^n$.

۲. $[3, 2, 2]$ - کد خطی دودویی $\{000, 110, 101, 011\}$.

تعریف ۷.۲.۱. چندجمله ای منفرد^۴ به چندجمله ای گفته می شود که ضریب کمترین درجه اش ۱ باشد.

تعریف ۸.۲.۱. چندجمله ای منفرد منحصر به فرد از کمترین درجه ایده آل ناصفر $I = \frac{\mathbb{F}_q[x]}{(x^n - 1)}$ ، چندجمله ای مولد^۵ I نامیده می شود. برای کد دوری C ، چندجمله ای مولد $\Pi(C)$ که

$$\Pi: \mathbb{F}_q^n \rightarrow \frac{\mathbb{F}_q[x]}{(x^n - 1)}$$

می باشد، چندجمله ای مولد از کد C نامیده می شود.

¹Information Rate or Code Rate

²Optimal Code

³Cyclic Code

⁴Singular Polynomial

⁵Generator Polynomial

مثال ۴.۲.۱. چندجمله‌ای مولد کد دوری $\{000, 110, 011, 101\}$ ، برابر با $x + 1$ می‌باشد.

تعریف ۹.۲.۱. فرض کنید $h(x) = \sum_{i=0}^k a_i x^i$ چندجمله‌ای از درجه k روی میدان $\mathbb{F}_q$ باشد. چندجمله‌ای متقابل^۱ $h_R(x)$ از $h(x)$ به صورت زیر تعریف می‌شود:

$$h_R(x) = x^k h\left(\frac{1}{x}\right) = \sum_{i=0}^k a_{k-i} x^i.$$

مثال ۵.۲.۱. برای چندجمله‌ای $h(x) = 1 + 2x + 3x^5 + x^7 \in \mathbb{F}_5[x]$ ، چندجمله‌ای متقابل $h(x)$ به صورت زیر است:

$$\begin{aligned} h_R(x) &= x^7 h\left(\frac{1}{x}\right) \\ &= x^7 \left(1 + 2\left(\frac{1}{x}\right) + 3\left(\frac{1}{x}\right)^5 + \left(\frac{1}{x}\right)^7\right) \\ &= 1 + 3x^2 + 2x^6 + x^7. \end{aligned}$$

تعریف ۱۰.۲.۱. فرض کنید C کد دوری q -تایی از طول n باشد. قرار دهید

$$h(x) = \frac{(x^n - 1)}{g(x)}$$

آن‌گاه $h_o^{-1} h_R(x)$ چندجمله‌ای کنترل توازن^۲ C نامیده می‌شود، که در آن h_o جمله ثابت $h(x)$ است.

تعریف ۱۱.۲.۱. فرض کنید C یک $[n, k]$ -کد دوری q -تایی با چندجمله‌ای مولد $g(x)$ باشد. قرار دهید $h(x) = \frac{(x^n - 1)}{g(x)}$. فرض کنید $h(x) = h_o + h_1 x + \dots + h_k x^k$ ، آن‌گاه ماتریس

$$H = \begin{bmatrix} h_R(x) \\ x h_R(x) \\ \vdots \\ x^{n-k-1} h_R(x) \end{bmatrix} = \begin{bmatrix} h_k & h_{(k-1)} & \dots & h_o & \circ & \circ & \circ & \dots & \circ \\ \circ & h_k & \dots & \circ & h_o & \circ & \circ & \dots & \circ \\ \vdots & & & & & & & & \\ \circ & \dots & \dots & h_k & h_{(k-1)} & \dots & \dots & \dots & h_o \end{bmatrix}$$

ماتریس کنترل توازن کد C می‌باشد.

تعریف ۱۲.۲.۱. کدهای (با ماتریس کنترل توازن) کم‌چگال LDPC دودویی، یک کد خطی دودویی است که توسط ماتریس کنترل توازن کم‌چگال^۳ H تعریف شده است، به این معنا که H دارای تعداد بسیار کمی درایه ناصفر می‌باشد.

کدواژه‌های یک $[n, k, d]$ -کد در شرط $m \geq n - k$ معادله کنترل توازن صدق می‌کند. اگر بیت کدواژه متناظر در معادله کنترل توازن گنجانده شود، هر معادله کنترل توازن را می‌توان

^۱Reciprocal

^۲Parity Check

^۳Sparse

توسط یک بردار دودویی از طول n که در جایگاه j -ام برابر با ۱ است، نشان داد. مجموعه‌ای از m معادله کنترل توازن را می‌توان با ماتریس کنترل توازن $H = [h_{i,j}]$ نشان داد. اگر $h_{i,j} = 1$ ، آن‌گاه معادله کنترل توازن i -ام شامل بیت کدواژه j -ام می‌باشد. سطرهای ماتریس کنترل توازن، فضای پوچی^۱ (یا دوگان^۲) $C^\perp$ از C را شامل می‌شوند.

تعریف ۱۳.۲.۱. کد LDPC، (W_c, W_r) - منظم نامیده می‌شود اگر ماتریس کنترل توازن H دارای جمع سطری ثابت W_r و جمع ستونی ثابت W_c باشد. اگر کد LDPC، (W_c, W_r) - منظم باشد، آن‌گاه هر رأس بیت^۳ دارای درجه یکسان W_c و هر رأس کنترل^۴ دارای درجه یکسان W_r می‌باشد.

ملاحظه ۱.۲.۱. عملکرد کدگشایی یک کد LDPC به ساختار گراف تر متناظر آن بستگی دارد. هرچه دورها کوتاه‌تر باشند، تأثیر منفی آن‌ها در عملکرد کدگشایی قابل توجه‌تر است. به همین دلیل، پژوهشگران دنبال ساختن کدهای LDPC فاقد دورهای کوتاه به ویژه کدهای فاقد دورهایی با طول ۴ می‌باشند.

تعریف ۱۴.۲.۱. فرض کنیم C یک کد خطی در $\mathbb{F}_q^n$ باشد، آن‌گاه کد دوگان C که با $C^\perp$ نمایش داده می‌شود، برابر با مکمل متعامد کد C در $\mathbb{F}_q^n$ می‌باشد، یعنی:

$$C^\perp = \{v \in \mathbb{F}_q^n | v \cdot c = 0, \forall c \in C\}.$$

تعریف ۱۵.۲.۱. کد LCD^۵ (کد خطی دوگان-مکمل) یک کد خطی C است که در شرط $C \cap C^\perp = \{0\}$ صدق می‌کند.

قضیه ۱.۲.۱. یک $[n, 1, d(n, 1)]$ - کد LCD منحصر به فرد در حد هم‌ارزی وجود دارد.

قضیه ۲.۲.۱. ۱. فرض کنید n یک عدد فرد باشد. در این صورت یک $[n, n-1, 2]$ - کد LCD منحصر به فرد در حد هم‌ارزی وجود دارد.

۲. فرض کنید n یک عدد زوج باشد. در این صورت $\frac{n}{2}$ $[n, n-1, 1]$ - کد LCD غیر هم‌ارز وجود دارد.

قضیه ۳.۲.۱. ۱. برای $t \geq 1$ ، یک $[6t, 2, 4t-1]$ - کد LCD منحصر به فرد در حد هم‌ارزی وجود دارد.

۲. برای $t \geq 1$ ، یک $[6t+1, 2, 4t]$ - کد LCD منحصر به فرد در حد هم‌ارزی وجود دارد.

¹Null Space

²Dual

³Bit node

⁴Check node

⁵Linear Complementary Dual

۳. برای $t \geq 1$ ، یک $[6t + 2, 2, 4t + 1]$ -کد LCD منحصر به فرد در حد هم‌ارزی وجود دارد.

۴. برای $t \geq 1$ ، یک $[6t + 3, 2, 4t + 2]$ -کد LCD منحصر به فرد در حد هم‌ارزی وجود دارد.

تعریف ۱۶.۲.۱. فرض کنید C یک کد خطی و $C^\perp$ دوگان آن باشد. در این صورت اگر کد C در شرط $C \subseteq C^\perp$ صدق کند، آن‌گاه به آن کد خود-متعامد^۱ می‌گویند.

۳.۱ تعاریف مرتبط به ماتریس و جبر خطی

تعریف ۱.۳.۱. فرض کنید مجموعه G یک مجموعه ناتهی باشد و عمل دوتایی $\cdot$ روی مجموعه G را در نظر بگیریم. در این صورت G به همراه عمل دوتایی $\cdot$ یک گروه^۲ نامیده می‌شود هرگاه دارای شرایط زیر باشد:

۱. G نسبت به عمل دوتایی $\cdot$ بسته باشد، یعنی:

$$\forall (a, b) \in G \times G, a \cdot b \in G.$$

۲. G نسبت به عمل دوتایی $\cdot$ شرکت‌پذیر باشد، یعنی:

$$a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

۳. G نسبت به عمل دوتایی $\cdot$ دارای عنصر خنثی یا همانی باشد، یعنی عضو منحصر به فردی چون e موجود باشد به طوری که به ازای هر $a \in G$ داشته باشیم:

$$a \cdot e = e \cdot a = a.$$

۴. G نسبت به عمل دوتایی $\cdot$ دارای عنصر وارون باشد، یعنی به ازای هر عنصر $a \in G$ ، عضو منحصر به فردی چون $b \in G$ موجود باشد به طوری که:

$$a \cdot b = b \cdot a = e.$$

تعریف ۲.۳.۱. فرض کنید R یک مجموعه ناتهی باشد که به دو عمل دوتایی $+$ و $\cdot$ مجهز شده باشد. در این صورت $(R, +, \cdot)$ یک حلقه^۳ می‌باشد هرگاه دارای ویژگی‌های زیر باشد:

• $(R, +)$ یک گروه آبدی باشد. یعنی:

^۱Self-Orthogonal

^۲Group

^۳Ring

۱. نسبت به عمل جمع بسته باشد.
 ۲. نسبت به عمل جمع شرکت پذیر باشد.
 ۳. نسبت به عمل جمع عنصر خنثی داشته باشد.
 ۴. نسبت به عمل جمع عنصر وارون داشته باشد.
 ۵. نسبت به عمل جمع دارای خاصیت جابجایی باشد.
- $(R, \cdot)$ یک نیم گروه باشد، یعنی R نسبت به عمل ضرب بسته و شرکت پذیر باشد.
 - عمل ضرب روی جمع دارای خاصیت توزیع پذیری باشد، یعنی:

$$\forall a, b, c \in R$$

$$a \cdot (a + c) = a \cdot b + a \cdot c \quad \text{و} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

تعریف ۳.۳.۱. فرض کنید R یک حلقه باشد. زیرمجموعه ناتهی I از حلقه R یک ایده آل است اگر:

۱. برای هر $a, b \in I$ داشته باشیم:

$$a + b \in I \quad \text{و} \quad a - b \in I.$$

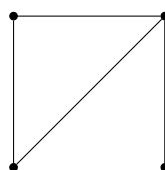
۲. برای هر $a \in I$ و $r \in R$ داشته باشیم:

$$r \cdot a \in I.$$

تعریف ۴.۳.۱. فرض کنید $G = (V, E)$ یک گراف ساده، بدون جهت و بدون وزن باشد به طوری که $V = \{v_1, v_2, \dots, v_n\}$ مجموعه رئوس گراف باشند. ماتریس مجاورت^۱ یک ماتریس $n \times n$ به صورت $A = [a_{ij}]$ با مقادیر تعیین شده در رابطه زیر است:

$$[a_{ij}] = \begin{cases} 1 & v_i v_j \in E, \\ 0 & v_i v_j \notin E. \end{cases}$$

مثال ۱.۳.۱. گراف G با چهار رأس و چهار یال را به صورت زیر در نظر بگیرید:



¹Adjacency Matrix

در این صورت ماتریس مجاورت آن به صورت زیر می‌باشد:

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

تعریف ۵.۳.۱. فرض کنید V یک فضای برداری روی میدان $\mathbb{F}$ باشد و همچنین T یک تبدیل خطی^۱ روی فضای برداری V و A ماتریس متناظر با این تبدیل خطی باشد. در این صورت گوییم بردار ناصفر v یک بردار ویژه^۲ از T است هرگاه $T(v)$ ضرب اسکالری از v باشد، یعنی: $Av = \lambda v$ یا $T(v) = \lambda v$ که در آن λ یک اسکالر در میدان $\mathbb{F}$ است که به آن مقدار ویژه یا مقدار مشخصه متناظر با بردار ویژه v نیز می‌گویند. به بیان دیگر، برای ماتریس A ، ریشه‌های چندجمله‌ای مشخصه آن، مقادیر ویژه ماتریس هستند.

مثال ۲.۳.۱. فرض کنید

$$A = \begin{bmatrix} 1 & 2 \\ 8 & 1 \end{bmatrix}$$

یک ماتریس 2×2 و

$$v = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

بردار ویژه باشد. در این صورت داریم:

$$Av = \lambda v \quad \rightarrow \quad (A - \lambda I)v = 0 \quad \rightarrow \quad \det(A - \lambda I) = 0$$

چندجمله‌ای مشخصه به صورت زیر به دست می‌آید:

$$\det(A - \lambda I) = \lambda^2 - 2\lambda - 15 = (\lambda - 5)(\lambda + 3) = 0$$

$$\rightarrow \quad \lambda = 5 \quad \text{و} \quad \lambda = -3$$

یعنی -3 و 5 مقادیر ویژه می‌باشند.

تعریف ۶.۳.۱. برای یک ماتریس مربعی M مجموعه‌ی مقادیر ویژه همراه با مرتبه تکرار آن را طیف^۳ ماتریس M می‌نامند که با نماد $\text{Spec}(M)$ نمایش داده می‌شود.

مثال ۳.۳.۱. در مثال قبل، طیف ماتریس

$$A = \begin{bmatrix} 1 & 2 \\ 8 & 1 \end{bmatrix}$$

برابر با $\text{Spec}(A) = \{-3, 5\}$ می‌باشد.

^۱Linear Transformation

^۲Eigenvector

^۳Spectrum

قضیه ۱.۳.۱. فرض کنید G یک گراف k -منظم باشد، در این صورت برای مقدار ویژه λ از ماتریس مجاورت گراف G داریم:

$$|\lambda| \leq k.$$

ملاحظه ۱.۳.۱. فرض کنید G یک گراف، A ماتریس مجاورت آن و λ یک مقدار ویژه از ماتریس مجاورت A باشد. در این صورت λ^2 یک مقدار ویژه از ماتریس مجاورت A^2 می باشد.

تعریف ۷.۳.۱. فرض کنید V و W دو فضای برداری روی میدان $\mathbb{F}$ و T یک تبدیل خطی از V به W باشد. فضای پوچ^۱ T عبارت است از مجموعه همه بردارهای α از V با شرط $T\alpha = 0$. هرگاه بعد V متناهی باشد، رتبه T بعد برد T است و پوچی^۲ T بعد فضای پوچ T .

قضیه ۲.۳.۱. فرض کنید V و W دو فضای برداری روی میدان $\mathbb{F}$ و T یک تبدیل خطی از V به W باشد. اگر بعد V متناهی باشد، آن گاه:

$$\text{رتبه}(T) + \text{پوچی}(T) = \text{بعد}(T).$$

۴.۱ تعاریف مرتبط به نظریه گراف

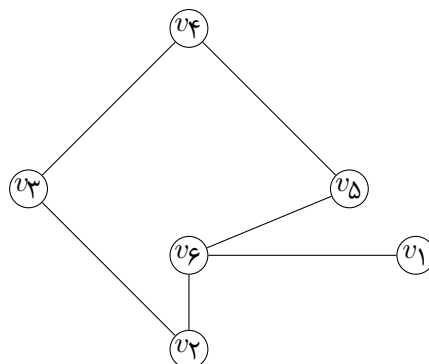
تعریف ۱.۴.۱. فرض کنید G گرافی با مجموعه رئوس $V(G) = \{v_1, v_2, \dots, v_n\}$ و مجموعه یالی $E(G)$ باشد که با $G = (V(G), E(G))$ نشان داده می شود.

تعداد رئوس گراف G ، یعنی $|V(G)|$ ، را مرتبه گراف G نامیده و با n نمایش می دهیم.

تعداد یال های گراف G ، یعنی $|E(G)|$ ، را اندازه گراف G نامیده و با m نمایش می دهیم.

تعریف ۲.۴.۱. فرض کنید v یک رأس از گراف G باشد. همسایگی باز v که با نماد $N_G(v)$ نشان داده می شود برابر با مجموعه همه رأس هایی می باشد که با رأس v مجاور است و درجه رأس v برابر با اندازه $N_G(v)$ است و با $\deg_G(v)$ نشان داده می شود.

مثال ۱.۴.۱. گراف زیر را در نظر بگیرید:



^۱ این فضا را هسته T نیز می نامند.
^۲ پوچی را بعد هسته هم می نامند.

مرتبه این گراف برابر ۶ و اندازه گراف نیز ۶ می باشد.
رأس v_6 را در نظر بگیرید. همسایگی باز این رأس به صورت زیر می باشد:

$$N_G(v_6) = \{v_5, v_1, v_2\}.$$

همچنین همسایگی بسته این رأس به صورت زیر می باشد:

$$\{v_6\} \cup N_G(v_6) = N_G[v_6] = \{v_6, v_5, v_1, v_2\}.$$

تعریف ۳.۴.۱. زیرگراف یک گراف G ، گرافی است که مجموعه رأس هایش زیرمجموعه رأس های گراف G باشد و مجموعه یال هایش نیز زیرمجموعه یال های گراف G باشد.

تعریف ۴.۴.۱. گراف کامل گرافی است که بین هر دو رأس مجزای آن، یال وجود داشته باشد. به بیان دیگر، گراف کامل K_n ، گرافی متشکل از n رأس می باشد که درجه هر رأس آن $n - 1$ می باشد.

تعریف ۵.۴.۱. گراف همبند^۱ گرافی است که هر دو رأس دلخواه از آن حداقل از طریق یک مسیر به هم متصل باشند.

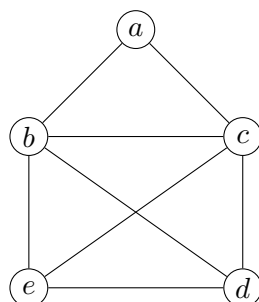
تعریف ۶.۴.۱. فرض کنیم G یک گراف همبند با مجموعه رئوس $V(G)$ باشد. فاصله بین دو رأس $u, v \in V(G)$ با نماد $d_G(u, v)$ یا d_{uv} نشان داده می شود که برابر با طول کوتاه ترین مسیر بین دو رأس u و v در گراف G می باشد.

تعریف ۷.۴.۱. قطر^۲ گراف برابر با ماکزیمم فاصله بین رئوس گراف می باشد.

تعریف ۸.۴.۱. خوشه^۳ یک زیرمجموعه از رأس های یک گراف (با یال های بی جهت) است که هر دو رأس مجزا در آن به یکدیگر متصل باشند (بین آن ها یال وجود داشته باشد). به عبارت دیگر، یک خوشه از گراف یک زیرگراف کامل از آن گراف است.

تعریف ۹.۴.۱. عدد خوشه ای^۴ که با نماد $\omega(G)$ نشان داده می شود، تعداد رأس های بزرگترین خوشه از گراف می باشد.

مثال ۲.۴.۱. گراف زیر را در نظر بگیرید:



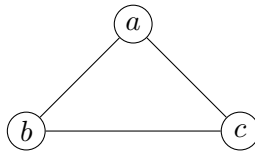
¹Connected Graph

²Diagonal

³Clique

⁴Clique number

در این صورت



یک خوشه از گراف متناظر می‌باشد و عدد خوشه‌ای گراف برابر $\omega(G) = 4$ می‌باشد.

تعریف ۱۰.۴.۱. اگر در گراف G تمام رئوس گراف از درجه برابر r باشند، آن‌گاه گراف G را یک گراف r -منظم می‌نامند. به بیان دیگر، گراف منظم به گرافی گفته می‌شود که تمام رئوس آن درجه یکسانی دارند.

تعریف ۱۱.۴.۱. دو گراف ساده G و H را در نظر بگیرید. گراف‌های G و H یکرخت^۱ هستند اگر و تنها اگر تابع دوسویی $\phi: v(G) \rightarrow v(H)$ موجود باشد به گونه‌ای که $e = uv$ یک یال از گراف G باشد اگر و تنها اگر $\phi(e) = \phi(u)\phi(v)$ یک یال از ماتریس H باشد. در این حال ϕ را یک یکرختی از G روی H می‌نامیم.

تعریف ۱۲.۴.۱. گراف ساده G را در نظر بگیرید. یک خودریختی^۲ از گراف G ، یک یکرختی از گراف G به روی خودش می‌باشد.

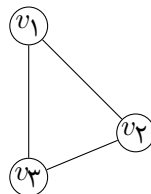
حال فرض کنیم که گراف ساده G داده شده باشد، آن‌گاه تمام خودریختی‌های گراف G را در یک مجموعه قرار دهیم و آن را $T(G)$ نام گذاری نماییم، یعنی داریم:

$$T(G) = \{\phi: G \rightarrow G \mid \phi \text{ گراف } G \text{ باشد}\}.$$

قضیه ۱.۴.۱. مجموعه $T(G)$ متشکل از تمام خودریختی‌های گراف ساده‌ی G به همراه عمل ترکیب توابع $\circ$ ، یک گروه را تشکیل می‌دهد. $(T(G), \circ)$ یک گروه است.

ملاحظه ۱.۴.۱. گروه خودریختی‌های گراف ساده‌ی G را با نماد $\text{Aut}(G)$ نمایش می‌دهیم.

مثال ۳.۴.۱. گروه خودریختی گراف $G = K_3$ (گراف کامل از مرتبه‌ی ۳) به صورت زیر می‌باشد:



$$\phi_0 = id = (1)(2)(3), \phi_1 = (12)(3), \phi_2 = (13)(2), \phi_3 = (23)(1), \phi_4 = (123), \phi_5 = (132)$$

در این صورت داریم:

$$\text{Aut}(G) = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5\}.$$

¹Isomorphism

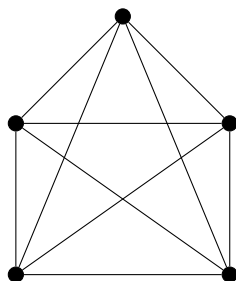
²Automorphism

تعریف ۱۳.۴.۱. فرض کنید G یک گراف باشد، در این صورت گراف G را متقارن^۱ (کمان-انتقالی^۲) نامیم هرگاه برای هر دو زوج از رأس‌های مجاور گراف به مانند $u_1 - v_1$ و $u_2 - v_2$ یک خودریختی از گراف G مانند $f: v(G) \rightarrow v(G)$ موجود باشد به گونه‌ای که $f(u_1) = u_2$ و $f(v_1) = v_2$. به بیان دیگر، گراف G گرافی متقارن است هرگاه گروه اتومورفیسم‌های گراف G به صورت متعدی (انتقالی) روی مجموعه کمان‌های G (زوج‌های مرتب از رأس‌های مجاور) عمل کند.

گراف رأس-انتقالی گرافی است که هیچ رأس تنهایی نداشته باشد.

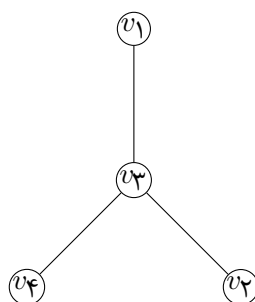
ملاحظه ۲.۴.۱. یک گراف متقارن است اگر رأس-انتقالی و یال-انتقالی باشد. هر گراف متقارن، یال-انتقالی است اما هر گراف یال-انتقالی، لزوماً متقارن نیست.

مثال ۴.۴.۱. گراف کامل K_5 را در نظر بگیرید، این گراف متقارن است.



تعریف ۱۴.۴.۱. گراف منظم G را در نظر بگیرید. این گراف نیم متقارن است اگر یال-انتقالی باشد اما رأس-انتقالی نباشد.

مثال ۵.۴.۱. گراف ستاره $K_{1,3}$ زیر را در نظر بگیرید:



این گراف، یال-انتقالی هست اما رأس-انتقالی نیست. زیرا:

$$f: v(G) \rightarrow v(G)$$

$$v_3 \rightarrow v_3$$

بنابراین گراف ستاره $K_{1,3}$ ، یک گراف نیم متقارن است.

¹Symmetric

²Arc-transitive Graph

تعریف ۱۵.۴.۱. گراف دوبخشی^۱ گرافی است که رأس‌هایش را می‌توان به دو مجموعه مجزا مثل U و V تقسیم کرد، طوری که هر یال از آن گراف یک رأس از V را به یک رأس از U متصل می‌کند. بنابراین گراف دوبخشی گرافی است که دور فرد ندارد. گراف دوبخشی را معمولاً به صورت $G = (U, V, E)$ نشان می‌دهیم که U و V دو بخش گراف و E مجموعه یال‌های گراف می‌باشد.

ملاحظه ۳.۴.۱. هر گراف نیم متقارن، یک گراف دوبخشی با بخش‌های برابر می‌باشد.

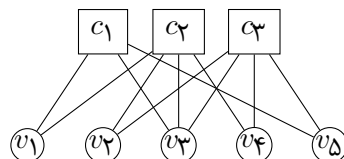
تعریف ۱۶.۴.۱. گراف تنر یک گراف دوبخشی است که شامل دو مجموعه از رؤوس می‌باشد: رؤوس بیتی که مطابق با بیت‌های کدواژه است و معادل با ستون‌های ماتریس کنترل توازن می‌باشد و رؤوس کنترل که مطابق با معادله‌های کنترل توازن است و معادل با سطرهای ماتریس کنترل توازن می‌باشد.

رؤوس درون هر دسته به یکدیگر متصل نیستند اما رؤوس هر دسته با توجه به عناصر صفر و یک ماتریس کنترل توازن به رؤوس دسته دیگر متصل می‌شوند. رأس j -ام از دسته اول به رأس i -ام از دسته دوم متصل است اگر و تنها اگر $H(i, j) = 1$. در واقع ماتریس H ماتریس مجاورت گراف دوبخشی نیز محسوب می‌شود. به بیان دیگر، یک یال از رأس بیت به رأس کنترل متصل می‌شود اگر آن بیت در معادله کنترل توازن متناظر گنجانده شود.

مثال ۶.۴.۱. ماتریس کنترل توازن H زیر را در نظر بگیرید:

$$H = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 & v_5 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} & \begin{matrix} c_1 \\ c_2 \\ c_3 \end{matrix} \end{matrix}$$

در این صورت گراف تنر متناظر با ماتریس کنترل توازن H به صورت زیر می‌باشد:



تعریف ۱۷.۴.۱. دور^۲ در گراف یک دنباله از یال‌هاست که مسیری را در گراف تشکیل می‌دهد، به گونه‌ای که اولین رأس با آخرین رأس برابر می‌باشد.

تعریف ۱۸.۴.۱. طول یک دور تعداد یال‌های موجود در آن است و کمر^۳ گراف طول کوتاه‌ترین دور می‌باشد.

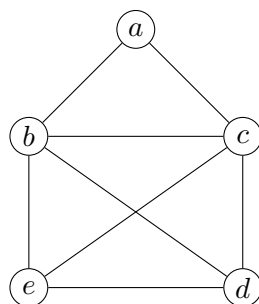
از آنجا که گراف تنر دوبخشی است، طول یک دور باید زوج و حداقل ۴ باشد.

¹Bipartite Graph

²Cycle

³Girth

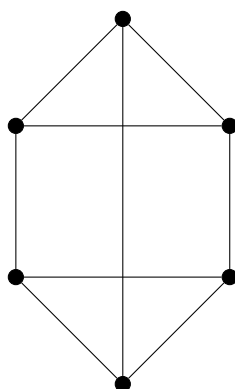
مثال ۷.۴.۱. گراف G زیر را در نظر بگیرید:



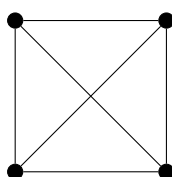
کمر گراف ۳ می باشد.

تعریف ۱۹.۴.۱. گراف‌های مکعبی^۱، گراف‌های ۳-منظم می باشند، یعنی تمام رئوس آن دارای درجه یکسان ۳ می باشد. همچنین، گراف متقارن مکعبی را که با نماد CSG نشان می دهند، گراف متقارن ۳-منظم می باشد.

مثال ۸.۴.۱. گراف زیر یک گراف ۳-منظم می باشد:



مثال ۹.۴.۱. گراف کامل K_4 گراف CSG می باشد.



تعریف ۲۰.۴.۱. یک مجموعه مستقل رأسی از گراف G ، زیرمجموعه‌ای از رئوس آن است به طوری که هیچ دو عضو از آن یالی از گراف G نباشد. عدد استقلال رأسی و یا به طور خلاصه، عدد استقلال، اندازه مجموعه مستقل رأسی ماکزیمم در یک گراف است. این عدد را با $\alpha(G)$ نمایش می دهیم.

به طور مشابه، یک مجموعه مستقل یالی در گراف G ، زیرمجموعه‌ای از یال‌های آن است به طوری که هیچ دو یال از آن رأس مشترک نداشته باشند. این عدد را با $\beta(G)$ نمایش می دهیم. در این پایان نامه، فقط گراف‌های همبند متناهی غیر بدیهی بدون طوقه و یال چندگانه مورد بررسی قرار می گیرد.

¹Cubical Graphs

فصل ۲

کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی

۱.۲ مقدمه

در این فصل درمورد کدهای کم چگال ساخته شده توسط گراف‌های متقارن مکعبی صحبت خواهد شد.

ابتدا اطلاعاتی در مورد کدهای کم چگال^۱ ساخته شده توسط گراف‌های متقارن مکعبی آورده شده است که شامل قضایای مرتبط و اثبات آن‌ها می‌باشد. سپس، واریانس وزن سندروم^۲ کدهای کم چگال ساخته شده توسط گراف‌های متقارن مکعبی دوبخشی بیان شده است.

^۱Low-Density Code

^۲Variance of a syndrom weight

۲.۲ کدهای کم‌چگال ساخته شده توسط گراف‌های متقارن مکعبی

طبق تعریف ۱۹.۴.۱ می‌دانیم گراف‌های مکعبی، گراف‌های ۳-منظم هستند. همچنین می‌دانیم که گراف‌های متقارن مکعبی گراف‌های کمان-انتقالی ۳-منظم هستند. اکثر گراف‌های متقارن مکعبی دوبخشی هستند و واضح است که دقیقاً ۵ گراف متقارن مکعبی همبند با کمر کمتر از ۶ وجود دارد (گراف K_4 ، گراف دوبخشی $K_{3,3}$ ، مکعب، گراف پترسن و دوازده‌وجهی). فرض کنید G یک گراف متقارن مکعبی همبند با $2n$ رأس باشد و توسط A که ماتریس مجاورت آن است، مشخص شده باشد. اگر G یک گراف دوبخشی باشد، ماتریس مجاورت آن به شرح زیر نوشته می‌شود:

$$A = \begin{bmatrix} \circ & H \\ H^T & \circ \end{bmatrix} \quad (۱.۲)$$

که H یک ماتریس $n \times n$ می‌باشد.

با در نظر گرفتن H به عنوان ماتریس کنترل توازن کد، می‌توان یک کد LDPC $C(G)$ ساخت. چگالی^۱ ماتریس کنترل توازن برابر $\frac{2}{n}$ می‌باشد و کد به‌دست آمده یک کد LDPC (۳و۳)-منظم از طول n و بعد $n - \text{rank}_2(H)$ می‌باشد که در آن $\frac{1}{2}\text{rank}_2(A) = \text{rank}_2(H)$. طبق تعریف ۱۳.۴.۱ میدانیم که هر گراف کمان-انتقالی بدون رأس‌های جدا، گراف رأس-انتقالی^۲ می‌باشد. بنابراین به‌دست آوردن ماتریس H از طریق ماتریس H^T با عوض کردن سطر و ستون‌های آن آسان است. از این‌رو، کدهای LDPC به‌دست آمده از H و H^T برابر هستند و توجه داشته باشید که دو کد دودویی برابر هستند اگر و تنها اگر هم‌ریخت باشند.

اگر G یک گراف غیر دوبخشی باشد، ماتریس مجاورت آن که M می‌باشد، ماتریس کنترل توازن کد LDPC (۳و۳)-منظم را تعیین می‌کند که گراف تنر آن یک گراف متقارن مکعبی دارای ماتریس مجاورت به شکل ۱.۲ با $H = M$ است. از این‌رو، طبق طبقه‌بندی گراف‌های متقارن مکعبی، کد LDPC ساخته شده از گراف متقارن مکعبی غیر دوبخشی (گرفتن ماتریس مجاورت آن به عنوان ماتریس کنترل توازن کد) با کد LDPC به‌دست آمده از برخی گراف‌های متقارن مکعبی دوبخشی (که همان گراف تنر است) با دو برابر تعداد رؤس نسبت به گراف اولیه هم‌ریخت است. بنابراین فقط کدهای LDPC ساخته شده از گراف‌های متقارن مکعبی دوبخشی در نظر گرفته می‌شود.

در ادامه، هنگامی که یک گراف متقارن مکعبی G را در نظر می‌گیریم، به یک گراف متقارن مکعبی دوبخشی همبند G با $2n$ رأس اشاره می‌کنیم. کد LDPC از طول n که گراف G گراف

¹Density

²Vertex-transitive

تنر آن می‌باشد را با $C(G)$ نشان می‌دهیم.

فرض کنید H ماتریس کنترل توازن کد $C(G)$ باشد. گراف رأس بیتی Γ به صورت زیر تعریف می‌شود: این گراف دارای n رأس است که با بیت‌های کدواژه مطابقت دارد و دو رأس مجاور هستند اگر و تنها اگر رأس‌های بیتی متناظر با گراف تنر G از کد $C(G)$ ، همسایه مشترک داشته باشند.

قضیه ۱.۲.۲. فرض کنید گراف G یک گراف متقارن مکعبی دوبخشی همبند با $2n$ ، $n \geq 7$ ، رأس باشد و فرض کنید H ماتریس کنترل توازن کد $C(G)$ باشد. آن‌گاه گراف رأس بیتی متناظر Γ ۶-منظم می‌باشد.

برهان. هر گراف متقارن مکعبی دوبخشی G با $2n$ ، $n \geq 7$ ، رأس دارای کمر حداقل ۶ است. یک رأس بیتی v از گراف تنر G از کد $C(G)$ دارای درجه ۳ است و هر کدام از همسایه‌های آن با دو رأس بیتی دیگر آن مجاور هستند. از آنجایی که G هیچ دوری از طول ۴ ندارد، رأس v یک همسایه مشترک با دقیقاً ۶ رأس بیتی دیگر دارد. به بیان دیگر، رأس v از گراف Γ دارای درجه ۶ می‌باشد. از این‌رو گراف Γ ۶-منظم است. $\square$

قضیه ۲.۲.۲. فرض کنید گراف G یک گراف متقارن مکعبی همبند با $2n$ ، $n \geq 7$ ، رأس باشد. فرض کنید H ماتریس کنترل توازن کد $C(G)$ باشد و فرض کنید Γ گراف رأس بیتی متناظر باشد. آن‌گاه یک $(1 \circ)$ -ماتریس T از مرتبه n ماتریس مجاورت گراف Γ است اگر و تنها اگر $H^T H = 3I + T$.

برهان. عناصر قطری^۱ ماتریس $H^T H = 3I + T$ مشابه درجه رأس‌های بیتی گراف تنر کد $C(G)$ که برابر با ۳ است، می‌باشد. از آنجا که G دارای هیچ دوری به طول ۴ نیست، عناصر دیگر ماتریس که ۰ یا ۱ هستند وابسته به این است که رأس‌های بیتی متناظر همسایه مشترک دارند یا خیر. به این معنی که عناصر غیر قطری^۲ ماتریس $H^T H$ ۱ یا ۰ هستند وابسته به این است که رأس‌های متناظر گراف Γ مجاور هستند یا خیر. از این‌رو $H^T H = 3I + T$ ، که T ماتریس مجاورت گراف Γ می‌باشد.

برعکس: فرض کنید T یک $(1 \circ)$ -ماتریس از مرتبه n می‌باشد به طوری که $H^T H = 3I + T$. یک ماتریس متقارن است، بنابراین T یک ماتریس متقارن است. بدیهی است که ماتریس T روی قطر خود دارای صفر می‌باشد. یک عنصر قطری از T مطابق با تعداد همسایه‌های مشترک رأس‌های بیتی متناظر با گراف تنر G از کد $C(G)$ می‌باشد. از آنجا که کمر گراف تنر G حداقل ۶ است، تعداد همسایه‌های مشترک ۰ یا ۱ است. بنابراین T ماتریس مجاورت گراف Γ می‌باشد. $\square$

^۱Diagonal

^۲Non-diagonal

قضیه ۳.۲.۲. فرض کنید C یک کد خطی دودویی با ماتریس کنترل توازن H باشد. آن‌گاه یک کدواژه در کد C با وزن W وجود دارد اگر و تنها اگر W تا ستون در H وجود داشته باشد که جمع برداری^۱ آن یک بردار صفر شود.

اثبات این قضیه در مرجع [۳۴] آورده شده است.

قضیه ۴.۲.۲. فرض کنید C یک کد خطی دودویی با ماتریس کنترل توازن H باشد. آن‌گاه مینیمم فاصله کد C برابر تعداد کوچک‌ترین ستون‌های واقع در H است که جمع برداری آن‌ها یک بردار صفر می‌شود.

اثبات این قضیه در مرجع [۳۴] آورده شده است.

با توجه به این‌که وزن ستونی ماتریس کنترل توازن H کد $C(G)$ برابر با ۳ است، قضیه ۳.۲.۲ اشاره می‌کند که کد $C(G)$ زوج است. علاوه بر این، مینیمم فاصله کد $C(G)$ یک عدد زوج است.

از قضیه ۴.۲.۲ برای اثبات قضیه ۵.۲.۲ استفاده می‌کنیم:

قضیه ۵.۲.۲. فرض کنید گراف G یک گراف متقارن مکعبی همبند با $2n$ ، $n \geq 2$ ، رأس باشد و فرض کنید Γ گراف رأس بیتی متناظر با آن باشد. مینیمم فاصله کد $C(G)$ حداقل ۶ است اگر و تنها اگر عدد خوشه‌ای گراف Γ حداکثر ۳ باشد.

برهان. کمر گراف G کد $C(G)$ بزرگتر از ۴ است، از این‌رو مینیمم فاصله کد حداقل ۴ می‌باشد. اگر مجموعه S در گراف G چنان وجود داشته باشد که از ۴ رأس بیتی با این خاصیت که هر جفت از رؤس دارای همسایگی مشترک هستند، تشکیل شده باشد، آن‌گاه مجموعه ستون‌های متناظر ماتریس کنترل توازن برابر صفر می‌باشد. از این‌رو، مینیمم فاصله کد برابر ۴ است. به عبارت دیگر، اگر گراف کامل K_4 زیرگراف Γ باشد، آن‌گاه مینیمم فاصله کد برابر ۴ می‌باشد. در نتیجه، اگر مینیمم فاصله کد حداقل ۶ باشد، آن‌گاه عدد خوشه‌ای گراف Γ حداکثر ۳ می‌باشد.

برعکس: فرض کنید عدد خوشه‌ای گراف Γ حداقل ۳ است. بر این اساس نمی‌توان ۴ ستون از ماتریس کنترل توازن پیدا کرد که جمع آن‌ها برابر صفر باشد. از قضیه ۴.۲.۲ نتیجه می‌شود که مینیمم فاصله کد حداقل ۶ است. $\square$

قضیه ۶.۲.۲. اگر گراف G کد LDPC (W_c, W_r) - منظم همبند باشد و n رأس بیتی داشته باشد، آن‌گاه مینیمم فاصله کد در $d \geq \max\{d_1, d_2\}$ صدق می‌کند، که در آن

$$d_1 = \frac{n(2W_c - \mu_2)}{W_c W_r - \mu_2}$$

$$d_2 = \frac{2n(2W_c + W_r - 2 - \mu_2)}{W_r(W_c W_r - \mu_2)}.$$

اثبات این قضیه در مرجع [۳۵] آورده شده است.

قضیه ۷.۲.۲. فرض کنید G یک گراف متقارن مکعبی دوبخشی همبند با $2n$ ، $n \geq 7$ ، باشد و فرض کنید λ_2 دومین بزرگترین مقدار ویژه ماتریس مجاورت A باشد. مینیمم فاصله کد $C(G)$ در شرط زیر صدق می‌کند:

$$d \geq \begin{cases} \frac{2}{5}n, & \lambda_2 \leq 2, \\ \frac{2}{3}n, & 2 < \lambda_2 \leq \sqrt{6}, \\ 4 & \sqrt{6} < \lambda_2 < 3. \end{cases}$$

برهان. از آنجا که G یک گراف دوبخشی است، طیف G نسبت به صفر متقارن است. علاوه بر این، از آنجا که گراف G ۳-منظم است، برای هر مقدار ویژه λ از ماتریس مجاورت A ، نامساوی $|\lambda| \leq 3$ طبق قضیه ۱.۳.۱ برقرار است. علاوه بر این، اگر λ یک مقدار ویژه از ماتریس A باشد آن‌گاه λ^2 طبق ملاحظه ۱.۳.۱ یک مقدار ویژه از ماتریس A^2 می‌باشد. فرض کنید μ_2 دومین بزرگترین مقدار ویژه ماتریس $H^T H$ باشد که در آن H ماتریس کنترل توازن کد $C(G)$ می‌باشد. با استفاده از این اصل که ماتریس‌های $H^T H$ و HH^T دارای مقادیر ویژه ناصفر یکسان هستند و این اصل که $\lambda_2 \geq 1$ ، نتیجه می‌شود $\mu_2 = \lambda_2^2$. طبق قضیه ۶.۲.۲، مینیمم فاصله کد $C(G)$ در $d \geq \max\{d_1, d_2\}$ صدق می‌کند، که در آن

$$d_1 = \frac{n(6 - \mu_2)}{9 - \mu_2}$$

و

$$d_2 = \frac{2n(7 - \mu_2)}{3(9 - \mu_2)}.$$

از این تساوی‌ها به راحتی می‌توان به دست آورد:

$$\mu_2 = \frac{6n - 9d_1}{9 - \mu_2} \quad (2.2)$$

و

$$\mu_2 = \frac{14n - 27d_2}{2n - 3d_2}. \quad (3.2)$$

نامساوی $d_1 \geq d_2$ برای $\mu_2 \leq 4$ و $d_2 \geq d_1$ برای $\mu_2 > 4$ برقرار است. حال سه حالت زیر را در نظر می‌گیریم:

در حالت اول، اگر $\mu_2 \leq 4$ ، آن‌گاه با استفاده از تساوی (۲.۲) داریم: $d \geq d_2 \geq \frac{2}{5}n$.
در حالت دوم، اگر $4 < \mu_2 \leq 6$ ، آن‌گاه مینیمم فاصله در نامساوی $d \geq d_2 \geq \frac{2}{3}n$ صدق می‌کند، که می‌توان با استفاده از (۳.۲) آن را به دست آورد.
در حالت سوم، اگر $\mu_2 \geq 6$ ، آن‌گاه مینیمم فاصله کد حداقل ۴ است، که در اثبات قضیه ۵.۲.۲ در مورد آن بحث شد. $\square$

قضیه ۸.۲.۲. فرض کنید گراف G یک گراف متقارن مکعبی دوبخشی همبند با $2n$ ، $n \geq 7$ ، رأس باشد. آن گاه بعد کد $C(G)$ حداکثر $\frac{5n}{6}$ است.

برهان. برای به دست آوردن بعد کد $C(G)$ ماتریس کنترل توازن مرتبه $12 \times H$ آن را مشاهده می‌کنیم. ماتریس مرتبه $2 \times H$ بزرگ‌تر یا مساوی از اندازه مجموعه مستقل ماکسیمال^۲ گراف رأس بیتی Γ می‌باشد. از این رو، بعد کد حداکثر $n - \alpha(\Gamma)$ است که n طول کد یعنی تعداد رئوس گراف Γ می‌باشد و $\alpha(\Gamma)$ عدد استقلال^۳ گراف Γ می‌باشد.

هر گراف همبند ۶-منظم با n رأس، غیر از K_7 ، دارای مجموعه مستقل است که شامل حداقل $\frac{n}{6}$ رأس می‌باشد. بنابراین از قضیه ۱.۲.۲ داریم که نامساوی $\alpha(\Gamma) \geq \frac{n}{6}$ برقرار است. از این رو، کران بالا برای بعد کد $\frac{5n}{6}$ می‌باشد. $\square$

اگر A ماتریس مجاورت گراف متقارن مکعبی دوبخشی G ، دارای مرتبه کامل باشد، آن گاه ماتریس کنترل توازن H کد LDPC نیز دارای مرتبه کامل می‌باشد. از این رو، کد LDPC ساخته شده دارای بعد صفر می‌باشد، یعنی کد ساخته شده بدیهی است.

قضیه ۹.۲.۲. بعد فضای پوچ ماتریس مجاورت گراف ۳-کمان-انتقالی که برای $S \geq 2$ S -منظم است، ناصفر می‌باشد.

اثبات این قضیه در مرجع [۳۵] آورده شده است.

قضیه ۱۰.۲.۲. فرض کنید p یک عدد اول باشد و فرض کنید G گراف چندگانه^۴ S -منظم رأس-انتقالی با n رأس باشد. فرض کنید $\mathbb{F}$ میدانی از مشخصه^۵ P باشد، اگر $\gcd(p, s) = 1$ و n توانی از P باشد، آن گاه ماتریس مجاورت گراف G روی میدان $\mathbb{F}$ معکوس پذیر است.

اثبات این قضیه در مرجع [۳۵] آورده شده است.

قضیه ۱۱.۲.۲. یک شرط برای کد LDPC ساخته شده از گراف متقارن مکعبی با 2^t $v = 2^t$ رأس بدیهی به ما می‌دهد.

قضیه ۱۱.۲.۲. فرض کنید گراف G یک گراف متقارن مکعبی دوبخشی همبند با 2^t $v = 2^t$ رأس باشد و فرض کنید $C(G)$ کد LDPC ساخته شده از گراف G باشد. آن گاه پارامترهای کد $C(G)$ ، $[2^{t-1}, 0, 2^{t-1}]$ می‌باشد.

برهان. طول کد $2^{t-1} = v$ می‌باشد. هر گراف کمان-انتقالی بدون رأس جدا شده، گراف رأس-انتقالی است، بنابراین G یک گراف رأس-انتقالی می‌باشد. از آنجا که G یک گراف ۳-منظم با 2^t $v = 2^t$ رأس می‌باشد، با استفاده از قضیه ۱۰.۲.۲ نتیجه می‌شود که ماتریس مجاورت

¹2-rank

²Maximal independent set

³Independence of number

⁴Multigraph

⁵Characteristic

G دارای مرتبه کامل روی $\mathbb{F}_2$ می باشد. از این رو، ماتریس کنترل توازن کد $C(G)$ یک ماتریس مرتبه کامل است. بنابراین بعد کد $C(G)$ صفر می باشد. $\square$

در حالتی که گراف G یک گراف متقارن مکعبی ۳-کمان-انتقالی دوبخشی همبند باشد، بعد کد $C(G)$ بزرگتر از صفر است. این بیانیه دقیقاً از قضیه ۹.۲.۲ پیروی می کند.

قضیه ۱۲.۲.۲. یک گراف ۳-وزن-ستون با گراف تنر از کمر $G \geq 10$ می تواند $1 - \frac{g}{q}$ خطا را در $\frac{g}{q}$ تکرار الگوریتم Gallar A تصحیح کند.

اثبات این قضیه در مرجع [۱۷] آورده شده است.

نتیجه ۱.۲.۲. فرض کنید G یک گراف متقارن مکعبی دوبخشی با کمر $G \geq 10$ باشد و فرض کنید $C(G)$ یک کد LDPC ساخته شده از گراف متقارن مکعبی G باشد. آن گاه $C(G)$ می تواند $1 - \frac{g}{q}$ خطا را در $\frac{g}{q}$ تکرار الگوریتم Gallar A تصحیح کند.

۳.۲ واریانس وزن سندروم

اطلاعت وضعیت کانال^۱ (CSI)، به عنوان مثال احتمال متقاطع^۲، برای سیستم های اطلاعاتی بسیار مهم است و از آن می توان برای پیش بینی کارایی کدگذاری استفاده کرد. برای محاسبه سندروم، کانال مشاهده شده به کانال متقارن دودویی^۳ (BSC) تبدیل می شود و اطلاعات وضعیت کانال اصلی از احتمال متقاطع پیش بینی شده به دست می آید.

فرض کنید C یک کد خطی دودویی باشد و H یک ماتریس $m \times n$ ، ماتریس کنترل توازن آن با وزن سطر r_i ، $i \in 1, 2, \dots, m$ باشد. علاوه بر این، فرض کنید $HH^T = [\lambda_{i,j}]$ ماتریس تقارن^۴ H باشد. فرض کنید کدواژه $c \in C$ از طریق کانال متقارن دودویی با احتمال متقاطع ρ ارسال شده باشد و بردار y دریافت شده باشد. بردار $S = y \cdot H^T$ ، $S = (s-1, s-2, \dots, s-m)$ ، سندروم y است. وزن سندروم که با w نشان داده می شود، به صورت $w = \sum_{i=1}^m s_i$ به دست می آید.

فرض کنید f_t تابعی است که توسط $f_t = \frac{1-(1-2\rho)^t}{2}$ تعریف می شود.

برای کد LDPC که گراف تنر آن فاقد دور از طول ۴ است، در مواردی که رأس های کنترل آن دارای درجه یکسان r باشد، واریانس وزن سندروم W به شرح زیر محاسبه می شود:

$$Var(w) = \frac{m}{2} f_{2r}(\rho) + \frac{g_1}{2} (f_{2r}(\rho) - f_{2r-2}(\rho)) \quad (1.2)$$

که در آن $g_1 = \sum_{i \neq j} \lambda_{i,j}$

¹Channel State Information

²Crossover probability

³Binary Symmetric Channel

⁴concurrence matrix

ورودی‌های $\lambda_{i,j}$ ، $i \neq j$ ، از ماتریس متقارن کنترل توازن H کد کم چگال $C(G)$ ، عناصر مجموعه $\{0, 1\}$ هستند. مقدار $\lambda_{i,j}$ تعداد همسایه‌های مشترک برای رأس‌های کنترل i –ام و j –ام گراف تنر را نشان می‌دهد. از این‌رو، اگر رأس‌های کنترل متناظر دارای همسایه مشترک باشند، آن‌گاه $\lambda_{i,j} = 1$ ، در غیر این‌صورت $\lambda_{i,j} = 0$. با استفاده از شمارش ساده می‌توان دریافت که هر رأس کنترل دارای همسایه مشترک با دقیقاً ۶ رأس کنترل است. بر این اساس، $g_1 = 6n$. با استفاده از تساوی (۱.۲) واریانس وزن سندروم را می‌توان مانند زیر محاسبه کرد:

$$Var(w) = \frac{n}{4} (Vf_6(\rho) - 6f_4(\rho)).$$

فصل ۳

کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی

۱.۳ مقدمه

در این فصل در مورد کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی^۱ (CSSG) صحبت شده است. ابتدا اطلاعاتی در مورد کدهای کم چگال ساخته شده توسط گراف‌های نیم متقارن مکعبی آورده شده است که شامل قضایای مرتبط و اثبات آن‌ها نیز می‌شود. سپس، ساختار کوچکترین مجموعه‌های جاذب این کدهای LDPC مورد بحث قرار داده شده‌اند. پس از آن، واریانس وزن سندروم کدهای ساخته شده توسط گراف‌های نیم متقارن مکعبی را بیان شده است.

^۱Cubic SemiSymmetric Graph

۲.۳ کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی

گراف نیم متقارن مکعبی^۱، گراف ۳-منظم نیم متقارن است. ساختار گراف‌های نیم متقارن مکعبی و (عدم) وجود گراف‌ها با مقدار معین تعداد رئوس موضوع مطالعات بسیاری از پژوهشگران بوده است.

فرض کنید G یک گراف نیم متقارن مکعبی همبند با $2n$ رأس باشد و توسط A که ماتریس مجاورت آن است، مشخص شود. چون هر گراف نیم متقارن، گراف دوبخشی با دو بخش مساوی است، ماتریس مجاورت آن به شرح زیر نوشته می‌شود:

$$A = \begin{bmatrix} \circ & H \\ H^T & \circ \end{bmatrix}$$

که H یک ماتریس $n \times n$ می‌باشد.

با در نظر گرفتن ماتریس H به عنوان ماتریس کنترل توازن کد، می‌توان یک کد LDPC $(3,3)$ -منظم $C_H(G)$ از طول n ساخت. بعد کد $n - \text{rank}_\mathbb{F}(H)$ است، که در آن $\text{rank}_\mathbb{F}(H) = \text{rank}_\mathbb{F}(A)$. علاوه بر این، چگالی ماتریس کنترل توازن برابر $\frac{2}{n}$ می‌باشد. برای کد ساخته شده $C_H(G)$ ، گراف نیم متقارن مکعبی G ، گراف تر آن می‌باشد.

از این واقعیت که گراف‌های نیم متقارن، یال-انتقالی هستند اما رأس-انتقالی نیستند، نتیجه می‌شود که ماتریس H^T کد LDPC $C_{H^T}(G)$ دیگری را تعیین می‌کند. کد $C_{H^T}(G)$ کد LDPC $(3,3)$ -منظم از طول n می‌باشد، همچنین بعد آن برابر $n - \text{rank}_\mathbb{F}(H)$ است.

فرض کنید H و H^T به ترتیب ماتریس‌های کنترل توازن $n \times n$ کد $C_H(G)$ و $C_{H^T}(G)$ باشد. برای هر کد $C_H(G)$ گراف رأس بیتی Γ_b به صورت زیر تعریف می‌شود:

رأس‌های گراف رأس بیتی Γ_b با بیت‌های کدواژه متناظر هستند و دو رأس مجاور هستند اگر و تنها اگر بیت‌ها در معادله کنترل توازن یکسان گنجانده شوند. به بیان دیگر، دو رأس از گراف Γ_b مجاور هستند اگر و تنها اگر رأس‌های بیتی متناظر با گراف تر G از کد $C_H(G)$ ، همسایه مشترک داشته باشند.

مشابهاً، رأس‌های گراف رأس کنترل Γ_c با معادله‌های کنترل توازن کد متناظر می‌باشند و دو رأس مجاور هستند اگر و تنها اگر معادله‌های کنترل توازن متناظر دارای بیت‌های مشترک باشند. به بیان دیگر، دو رأس از گراف Γ_c مجاور هستند اگر و تنها اگر رأس‌های کنترل متناظر با گراف تر G از کد $C_H(G)$ ، همسایه مشترک داشته باشند. توجه داشته باشید که گراف رأس کنترل Γ_c از کد $C_H(G)$ ، همان گراف رأس بیتی از کد $C_{H^T}(G)$ می‌باشد.

¹Semisymmetric

قضیه ۱.۲.۳. فرض کنید گراف G یک گراف نیم متقارن مکعبی همبند با کمر حداقل ۶ باشد و فرض کنید H ماتریس کنترل توازن کد $C_H(G)$ باشد. آن‌گاه گراف رأس بیتی متناظر Γ_b و گراف رأس کنترل متناظر Γ_c ۶-منظم می‌باشند.

برهان. فرض کنید v یک رأس بیتی از گراف تنر G باشد. درجه رأس v برابر ۳ است و هر کدام از همسایه‌های آن با دو رأس بیتی دیگر آن مجاور هستند. از آنجا که گراف G فاقد دوری از طول ۴ می‌باشد، رأس v یک همسایه مشترک با دقیقاً ۶ رأس بیتی دیگر دارد. به بیان دیگر، رأس v از گراف رأس بیتی Γ_b دارای درجه ۶ می‌باشد. از این‌رو گراف Γ_b ۶-منظم است. به بیان مشابه، می‌توان ثابت کرد که گراف رأس کنترل Γ_c نیز ۶-منظم می‌باشد. $\square$

قضیه ۲.۲.۳. فرض کنید گراف G یک گراف نیم متقارن مکعبی همبند با $2n$ رأس و کمر حداقل ۶ باشد. فرض کنید H ماتریس کنترل توازن کد $C_H(G)$ باشد و فرض کنید Γ_b و Γ_c به ترتیب، گراف رأس بیتی و گراف رأس کنترل متناظر باشند. ماتریس‌های T_c و T_b (10°) -ماتریس‌های مربعی از مرتبه n در $T_b = H^T H - 3I$ و $T_c = H H^T - 3I$ صدق می‌کنند اگر و تنها اگر T_c و T_b به ترتیب ماتریس‌های مجاورت گراف‌های Γ_b و Γ_c باشند.

برهان. فرض کنید $H^T H = [h_{i,j}]$ یک ماتریس $n \times n$ باشد. درجه رأس بیتی گراف تنر G از کد $C_H(G)$ برابر ۳ می‌باشد. از این‌رو، $h_{i,i} = 3$ ، $i = \{1, 2, \dots, n\}$. عنصر $h_{i,j}$ ، $i \neq j$ ، از ماتریس H برابر صفر یا یک می‌باشد که وابسته به این است که رأس‌های گراف Γ_b مجاور هستند یا خیر. بر این اساس، $T_b = H^T H - 3I$ ، که در آن ماتریس مجاورت گراف Γ_b می‌باشد.

برعکس، فرض کنید $T_b = [t_{i,j}]$ یک (10°) -ماتریس $n \times n$ با ویژگی $T_b = H^T H - 3I$ باشد. از آنجا که $H^T H$ یک ماتریس متقارن می‌باشد، نتیجه می‌شود که ماتریس T_b نیز ماتریس متقارن می‌باشد به طوری که $t_{i,i} = 0$ ، $i \in \{1, 2, \dots, n\}$. کمر گراف تنر G بزرگ‌تر از ۴ است، بنابراین $h_{i,j}$ ، $i \neq j$ ، که برابر صفر یا یک هستند، تعداد همسایه‌های مشترک رأس بیتی متناظر با گراف تنر G از کد $C_H(G)$ را نشان می‌دهند. بنابراین، نتیجه می‌شود که ماتریس T_b ماتریس مجاورت گراف Γ_b می‌باشد.

به‌طور مشابه، یک عبارت آنالوگ برای ماتریس T_c با مشاهده رئوس کنترل گراف تنر کد $C_H(G)$ را می‌توان تشکیل داد. $\square$

لم ۱.۲.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند باشد. فرض کنید $C_H(G)$ کد LDPC متناظر باشد و فرض کنید Γ_b و Γ_c به ترتیب گراف رأس بیتی و گراف رأس کنترل آن باشد. آن‌گاه، اعداد خوشه‌ای گراف‌های Γ_b و Γ_c حداقل ۳ می‌باشد.

برهان. هر رأس کنترل از گراف تنر G ، یک همسایه مشترک از هر جفت از سه رأس بیتی مجاورت آن می‌باشد. بنابراین، هر رأس کنترل، گراف کامل K_3 را به عنوان زیرگراف گراف رأس بیتی Γ_b تعیین می‌کند. به‌طور مشابه، هر رأس بیتی از گراف تنر گراف کامل K_3 را به عنوان زیرگراف گراف رأس کنترل Γ_c تعیین می‌کند. بنابراین: $\omega(\Gamma_b), \omega(\Gamma_c) \geq 3$. $\square$

لم ۲.۲.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با کمر بزرگ‌تر از ۶ باشد. از این‌رو، فرض کنید $C_H(G)$ کد LDPC متناظر باشد و فرض کنید Γ_b و Γ_c به ترتیب گراف رأس بیتی و گراف رأس کنترل آن باشد. آن‌گاه گراف کامل K_4 زیرگراف گراف‌های T_b یا T_c نمی‌باشد.

برهان. فرض کنید گراف K_4 زیرگراف گراف T_b باشد. فرض کنید رأس‌های بیتی u_1, u_2, u_3 و u_4 رأس‌های گراف K_4 باشند. در این‌صورت دو حالت زیر ممکن است:

۱. یکی از رأس‌های کنترل (مثلاً v_1) در زیرگراف متناظر از گراف تنر G دارای درجه ۳ باشد. فرض کنید u_1, u_2 و u_3 رأس‌های بیتی مجاور با رأس v_1 باشند. بنابراین، فرض کنید رأس کنترل v_2 همسایه مشترک u_1 و u_4 باشد. از آنجا که رأس‌های u_1 و u_4 در گراف Γ_b مجاور هستند، دارای همسایه مشترک v_3 در گراف G می‌باشند. آن‌گاه $u_1v_1u_2v_3u_4v_2u_1$ یک دور از طول ۶ است که این غیر ممکن است زیرا کمر گراف G بزرگ‌تر از ۶ می‌باشد.
 ۲. رأس‌های کنترل در زیرگراف متناظر از گراف تنر G دارای درجه‌های حداکثر ۲ می‌باشند. فرض کنید رأس کنترل v_i همسایه مشترک رأس‌های بیتی u_1 و u_{i+1} باشد. از آنجا که رؤس u_2 و u_4 در گراف Γ_b مجاور هستند، دارای همسایه مشترک u_4 در گراف G می‌باشند. آن‌گاه $u_1v_1u_2v_4u_4v_3u_1$ یک دور از طول ۶ می‌باشد که با این حقیقت که کمر گراف بزرگ‌تر از ۶ است متناقض است.
- به‌طور مشابه، ثابت کی‌شود که گراف K_4 زیرگراف گراف Γ_c نیز نمی‌باشد.

□

قضیه زیر مستقیماً از لم‌های ۱.۲.۳ و ۲.۲.۳ نتیجه می‌شود.

قضیه ۳.۲.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با کمر بزرگ‌تر از ۶ باشد. از این‌رو، فرض کنید $C_H(G)$ کد LDPC متناظر باشد و فرض کنید Γ_b و Γ_c به ترتیب گراف رأس بیتی و گراف رأس کنترل آن باشد. آن‌گاه $\omega(\Gamma_b) = \omega(\Gamma_c) = 3$.

وزن ستونی ماتریس‌های کنترل توازن H و H^T از کدهای $C_H(G)$ و $C_{HT}(G)$ برابر ۳ است، طبق قضیه ۳.۲.۲، این کدها زوج هستند. بنابراین مینیمم فاصله کدها عددی زوج می‌باشد.

قضیه ۴.۲.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با کمر بزرگ‌تر از ۶ باشد. فرض کنید $d(C_H(G))$ و $d(C_{HT}(G))$ به ترتیب مینیمم فاصله کدهای $C_H(G)$ و $C_{HT}(G)$ باشند. آن‌گاه $d(C_H(G)) \geq 6$ و $d(C_{HT}(G)) \geq 6$.

برهان. وزن ستونی ماتریس کنترل توازن H کد $C_H(G)$ برابر ۳ می‌باشد. از آنجا که گراف G هیچ دوری از طول ۴ ندارد، نتیجه می‌شود که مینیمم فاصله کد حداقل ۴ است. فرض کنید مینیمم فاصله کد برابر با ۴ باشد، از قضیه ۴.۲.۲ نتیجه می‌شود که ۴ ستون از ماتریس کنترل

توازن که جمع آن‌ها صفر می‌شود، وجود دارد. بنابراین یک مجموعه S در گراف G که شامل چهار رأس بیتی است، وجود دارد. به طوری که هر جفت از رئوس دارای همسایگی مشترک متفاوت در گراف G می‌باشند. علاوه بر این، مجموعه S گراف کامل K_4 را به عنوان زیرگراف گراف رأس بیتی Γ_b تعیین می‌کند. با استفاده از قضیه ۳.۲.۳ نتیجه می‌گیریم که مینیمم فاصله کد حداقل ۶ می‌باشد.

با مشاهده رأس‌های کنترل گراف تنر کد $C_H(G)$ و گراف رأس کنترل Γ_c ، می‌توان ثابت کرد که این واقعیت برای مینیمم فاصله کد $C_{HT}(G)$ نیز برقرار است. $\square$

قضیه ۵.۲.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با $2n$ رأس باشد و فرض کنید λ_2 دومین بزرگترین مقدار ویژه ماتریس مجاورت A باشد. فرض کنید $d(C_H(G))$ و $d(C_{HT}(G))$ به ترتیب مینیمم فاصله‌های کدهای $C_H(G)$ و $C_{HT}(G)$ باشد. آن‌گاه نامساوی زیر برقرار است:

$$d \geq \begin{cases} \frac{2}{5}n, & \lambda_2 \leq 2, \\ \frac{2}{3}n, & 2 < \lambda_2 \leq \sqrt{6}, \\ 6 & \sqrt{6} < \lambda_2 < 3, \end{cases}$$

که در آن $d \in \{d(C_H(G)), d(C_{HT}(G))\}$.

قضیه ۶.۲.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با $2n$ رأس باشد. آن‌گاه بعد کدهای $C_H(G)$ و $C_{HT}(G)$ حداکثر $1 + 2\alpha(\Gamma_b) - n$ می‌باشد، که در آن $\alpha(\Gamma_b)$ عدد استقلال گراف رأس بیتی Γ_b است.

برهان. ماتریس کنترل توازن مرتبه ۲ کد دودویی، بعد آن را تعیین می‌کند. ماتریس H مرتبه ۲ برابر ماتریس H^T مرتبه ۲ می‌باشد. از این‌رو، برای مشاهده، ماتریس H و کد $C_H(G)$ کافی است. یک مجموعه مستقل ماکسیمال Γ_b ستون‌های مستقل خطی $\alpha(\Gamma_b)$ از ماتریس کنترل توازن H را تعیین می‌کند. این ستون‌ها این ویژگی را دارند که هیچ دو ستونی دارای درایه برابر با یک در جایگاه مشابه نداشته باشند. با توجه به این‌که $\alpha(\Gamma_b)$ گراف ۶-منظم می‌باشد، یک $\alpha(\Gamma_b)$ در جایگاه‌های مختلف در ستون‌ها وجود دارد. بنابراین، با اضافه کردن هر یک از ستون‌های $\alpha(\Gamma_b) - 1$ از ماتریس، یک مجموعه از ستون‌های مستقل خطی $2\alpha(\Gamma_b) - 1$ از ماتریس کنترل توازن تعریف می‌شود. از این‌رو، ماتریس H مرتبه ۲ حداقل $2\alpha(\Gamma_b) - 1$ می‌باشد.

به عنوان یک نتیجه، بعد کد حداکثر $1 + 2\alpha(\Gamma_b) - n$ می‌باشد که در آن n طول کد می‌باشد، یعنی تعداد رئوس گراف Γ_b ، و $\alpha(\Gamma_b)$ عدد استقلال گراف Γ_b می‌باشد. $\square$

۳.۳ واریانس وزن سندروم

اطلاعت وضعیت کانال (CSI)، (به عنوان مثال احتمال متقاطع)، برای سیستم‌های اطلاعاتی بسیار مهم است و از آن می‌توان برای پیش‌بینی کارایی کدگذاری استفاده کرد. بیانی برای واریانس وزن سندروم کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی در بخش ۳.۲ آورده شده است. به روشی مشابه، می‌توان بیانی برای واریانس وزن سندروم کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی به دست آورد که به صورت زیر می‌باشد:

$$Var(w) = \frac{n}{\varphi} (\sum f_{\varphi}(\rho) - \varphi f_{\varphi}(\rho)),$$

که در آن تابع f_t به صورت $f_t(\rho) = \frac{1-(1-\varphi)^t}{\varphi}$ تعریف می‌شود.

۴.۳ مجموعه جاذب

فرض کنید $G = G(C)$ گراف تنر کد کم چگال C باشد که توسط ماتریس کنترل توازن $m \times n$ H تعیین شده است. مجموعه تله‌ای^۱ $A(\kappa, \tau)$ یک مجموعه T است که از κ رأس بیتی تشکیل شده است، به طوری که دارای این ویژگی است که زیرگراف القائی $G[T]$ دارای دقیقاً τ رأس کنترل از درجه فرد می‌باشد. مضرترین مجموعه‌های تله‌ای، مجموعه‌هایی با سایز کوچک و نسبت $\frac{\tau}{\kappa}$ کوچک هستند. اگر گراف تنر یک کد کم چگال، مجموعه‌های تله‌ای با سایز کوچک‌تر از مینیمم فاصله کد نداشته باشد، آن‌گاه خطای کد تحت سلطه مینیمم فاصله قرار می‌گیرد. فرض کنید T یک مجموعه تله‌ای باشد. اگر هر رأس بیتی در $G[T]$ با رأس‌های کنترل کمتری از درجه فرد از رأس‌های کنترل از درجه زوج، مجاور باشد، آن‌گاه T مجموعه جاذب^۲ نامیده می‌شود.

فرض کنید A یک (κ, τ) - مجموعه تله‌ای در گراف تنر $(\mathcal{C}, w_r)$ - کد کم چگال باشد. با محاسبه ساده می‌توان دید که τ یک عدد زوج است اگر κ زوج باشد و τ یک عدد فرد است اگر κ فرد باشد.

نتایج در ادامه به کدهای کم چگال گراف تنر متناظر آن که دارای کمر حداقل ۶ است، اشاره می‌کند. وجود کوچکترین مجموعه‌های جاذب در گراف تنر کدهای کم چگال ساخته شده توسط گراف‌های نیم متقارن مکعبی بررسی می‌شود.

قضیه ۱.۴.۳. فرض کنید گراف تنر کد کم چگال $C_H(G)$ ، گراف نیم متقارن مکعبی همبند G با کمر حداقل ۶ باشد. آن‌گاه هیچ مجموعه جاذب از اندازه کوچک‌تر از ۳ در گراف G وجود ندارد.

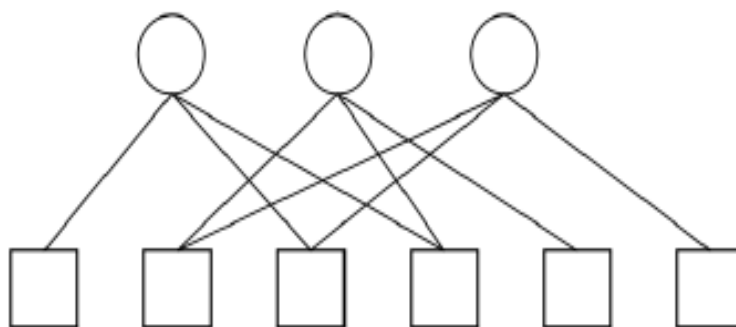
¹Trapping set

²Absorbing set

برهان. اثبات این قضیه مستقیماً از تعریف مجموعه جاذب و این حقیقت که گراف تنر کد فاقد دوری از طول ۴ می باشد، به دست می آید. □

قضیه ۲.۴.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با کمر بزرگتر از ۶ باشد که گراف تنر کدهای کم چگال $C_H(G)$ و $C_{HT}(G)$ می باشد. گراف تنر G هیچ مجموعه جاذبی از طول ۳ ندارد.

برهان. فرض کنید A یک $(3,3)$ - مجموعه جاذب باشد که تنها ساختار ممکن از مجموعه جاذب از سایز ۳ در گراف تنر کدها می باشد (شکل ۴.۳ را ببینید). اثبات قضیه مستقیماً از این حقیقت که مجموعه جاذب یک دور از طول ۶ در گراف تنر تعریف می کند، به دست می آید.

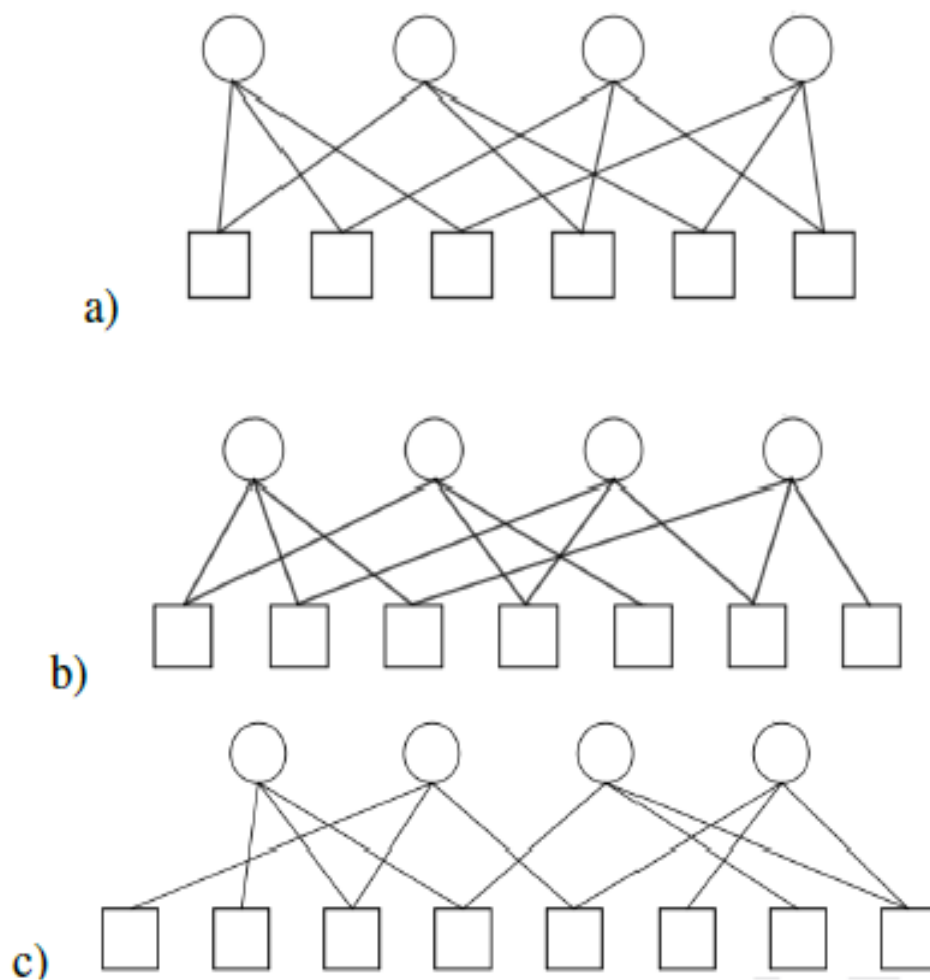


شکل ۱.۳: تنها ساختار ممکن از مجموعه جاذب از اندازه ۳ در گراف تنر کدهای کم چگال $C_H(G)$ و $C_{HT}(G)$.

□

قضیه ۳.۴.۳. فرض کنید G یک گراف نیم متقارن مکعبی همبند با کمر بزرگتر از ۶ باشد که گراف تنر کدهای کم چگال $C_H(G)$ و $C_{HT}(G)$ می باشد. تنها ساختار ممکن از مجموعه جاذب از اندازه چهار، $(4,4)$ - مجموعه جاذب می باشد.

برهان. از آنجایی که اندازه مجموعه جاذب عددی زوج است، و براساس مشاهدات قبلی، تنها ساختار ممکن از مجموعه جاذب از اندازه چهار در گراف تنر آن کدها، مجموعه های جاذب $(4,0)$ ، $(4,2)$ و $(4,4)$ هستند (شکل ۲.۳ را ببینید). اثبات قضیه مستقیماً از این حقیقت که مجموعه های جاذب $(4,0)$ و $(4,2)$ گراف کامل K_4 را به عنوان زیرگراف گراف Γ_b تعریف می کند، به دست می آید.



شکل ۲.۳: تنها ساختار ممکن از مجموعه جاذب از اندازه چهار در گراف تنر کدهای کم چگال $C_H(G)$ و $C_{HT}(G)$.

□

فصل ۴

شبیه‌سازی و نتایج محاسباتی

۱.۴ مقدمه

در این فصل، ابتدا اطلاعاتی در مورد کدهای LDPC ساخته شده از گراف‌های متقارن مکعبی دوبخشی با کمتر از ۲۰۰ رأس ارائه شده است. سپس، نتایج شبیه‌سازی کدهای LDPC آورده شده در بخش ۳.۴ برگرفته از گراف‌های متقارن مکعبی ۴۸A و ۱۹۲C بر کانال اختلال گاوسی سفید^۱ (AWGN) ارائه شده است. پس از آن، اطلاعاتی در مورد کدهای LDPC ساخته شده از گراف‌های نیم متقارن مکعبی دوبخشی با کمتر از ۱۰۰۰ رأس ارائه شده است. سپس نتایج شبیه‌سازی کدهای LDPC به‌دست آمده از گراف‌های نیم متقارن مکعبی روی کانال اختلال گاوسی افزودنی نشان داده شده است.

۲.۴ نتایج محاسباتی کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی

در این بخش از گراف‌های متقارن مکعبی موجود در [۶] استفاده شده است. پارامترهای کدهای LDPC ساخته شده در جدول ۱.۴ آورده شده است. کدهای به‌دست آمده دارای نرخ

^۱Additive White Gaussian Noise

پایین^۱ و مینیمم فاصله خوب هستند.

CSG	LDPC	Girth	CSG	LDPC	Girth	CSG	LDPC	Girth
6A	[3,2,2]*	4	74A	[37,0,37]	6	134A	[67,0,67]	6
8A	[4,0,4]	4	78A	[39,2,26]*	6	144A	[72,8,32]	8
14A	[7,3,4]	6	80A	[40,4,16]	10	144B	[72,6,30]	10
16A	[8,0,8]	6	86A	[43,0,43]	6	146A	[73,9,28]	6
18A	[9,2,6]*	6	90A	[45,11,10]	10	150A	[75,2,50]*	6
20B	[10,4,4]*	6	96A	[48,8,18]	6	152A	[76,0,76]	6
24A	[12,4,6]	6	96B	[48,12,8]	8	158A	[79,0,79]	6
26A	[13,0,13]	6	98A	[49,3,28]	6	162A	[81,2,54]*	6
30A	[15,5,6]	8	98B	[49,6,24]	6	162B	[81,2,54]*	12
32A	[16,0,16]	6	104A	[52,0,52]	6	162C	[81,14,18]	12
38A	[19,0,19]	6	110A	[55,10,10]*	10	168A	[84,10,30]	6
40A	[20,4,8]	8	112A	[56,8,14]	8	168E	[84,13,30]	12
42A	[21,5,10]	6	112B	[56,8,16]	8	168F	[84,8,38]*	12
48A	[24,6,10]	8	112C	[56,6,24]	10	182A	[91,3,52]	6
50A	[25,0,25]	6	114A	[57,2,38]*	6	182B	[91,3,52]	6
54A	[27,2,18]*	6	120A	[60,5,20]	8	182D	[91,14,26]*	12
56A	[28,6,12]	6	120B	[60,4,24]	10	186A	[93,2,62]*	6
56C	[28,8,8]*	8	122A	[61,0,61]	6	192A	[96,23,8]	8
62A	[31,0,31]	6	126A	[63,5,30]	6	192B	[96,16,22]	10
64A	[32,0,32]	8	128A	[64,0,64]	6	192C	[96,18,16]	12
72A	[36,4,18]	6	128B	[64,0,64]	10	194A	[97,0,97]	6

شکل ۱.۴: پارامترهای کدهای LDPC ساخته شده توسط گراف متقارن مکعبی با کمتر از ۲۰۰ رأس به‌دست آمده است.

کمر گراف‌های تنر کدهای ساخته شده به جز کدهای به‌دست آمده از گراف‌های ۶A (گراف دوبخشی کامل $K_{3,3}$) و گراف ۸A (مکعب) که کمر آن‌ها ۴ است، حداقل ۶ می‌باشد. کد LDPC به‌دست آمده از گراف ۱۴A با کد LDPC به‌دست آمده از صفحه تصویری از مرتبه ۲، یعنی طراحی ۲- $(7,3,1)$ متقارن با در نظر گرفتن ماتریس تلاقی صفحه تصویری به‌عنوان ماتریس کنترل توازن کد، هم‌ریخت است. کدهای به‌دست آمده از گراف‌های ۱۸۲A و ۱۸۲B نیز هم‌ریخت هستند. برخی از کدهای ساخته شده که به صورت پررنگ مشخص شده‌اند، کران بالا برای مینیمم فاصله به‌دست آورده‌اند، یعنی این کدها، کدهای بهینه هستند. علاوه بر این، برخی از این کدهای ساخته شده دارای ویژگی دیگری مانند خود-متعامد بودن یا کدهای خطی دوگان-مکمل (LCD) می‌باشند. برخی از کدهای به‌دست آمده خود-متعامد هستند. به عنوان مثال، کدهایی که با ویژگی‌های گراف‌های

¹Low rate

۱۴A، ۳۰A، ۴۰A، ۵۶A، ۸۰A، ۹۰A، ۹۸A، ۹۸B، ۱۱۲B، ۱۱۲C، ۱۲۰A، ۱۲۰B، ۱۴۴A، ۱۴۶A، ۱۸۲A و ۱۸۲B به‌دست آمده‌اند، خود-متعامد هستند.

کدهای ساخته شده از گراف‌های ۶A، ۱۸A، ۵۴A، ۷۸A، ۱۱۴A، ۱۵۰A، ۱۶۲A، ۱۶۲B و ۱۸۶A، کدهای LCD منحصر به‌فرد با پارامترهای در حد هم‌ارزی هستند (۱.۲.۱، ۲.۲.۱ و ۳.۲.۱). طبق طبقه‌بندی کدهای LCD داده شده در جدول ۲.۴ ([۵])، دقیقاً ۵ کد LCD با پارامترهای [۱۰، ۴، ۴] وجود دارد. در این پایان‌نامه، یک کد LCD [۱۰، ۴، ۴] با استفاده از ماتریس مجاورت گراف متقارن مکعبی ۲۰B به‌دست آمده است.

شکل ۲.۴: $(d(n,k), N(n,k, d(n,k)))$

CSG	LDPC	Girth	CSG	LDPC	Girth	CSG	LDPC	Girth
6A	[3,2,2]*	4	74A	[37,0,37]	6	134A	[67,0,67]	6
8A	[4,0,4]	4	78A	[39,2,26]*	6	144A	[72,8,32]	8
14A	[7,3,4]	6	80A	[40,4,16]	10	144B	[72,6,30]	10
16A	[8,0,8]	6	86A	[43,0,43]	6	146A	[73,9,28]	6
18A	[9,2,6]*	6	90A	[45,11,10]	10	150A	[75,2,50]*	6
20B	[10,4,4]*	6	96A	[48,8,18]	6	152A	[76,0,76]	6
24A	[12,4,6]	6	96B	[48,12,8]	8	158A	[79,0,79]	6
26A	[13,0,13]	6	98A	[49,3,28]	6	162A	[81,2,54]*	6
30A	[15,5,6]	8	98B	[49,6,24]	6	162B	[81,2,54]*	12
32A	[16,0,16]	6	104A	[52,0,52]	6	162C	[81,14,18]	12
38A	[19,0,19]	6	110A	[55,10,10]*	10	168A	[84,10,30]	6
40A	[20,4,8]	8	112A	[56,8,14]	8	168E	[84,13,30]	12
42A	[21,5,10]	6	112B	[56,8,16]	8	168F	[84,8,38]*	12
48A	[24,6,10]	8	112C	[56,6,24]	10	182A	[91,3,52]	6
50A	[25,0,25]	6	114A	[57,2,38]*	6	182B	[91,3,52]	6
54A	[27,2,18]*	6	120A	[60,5,20]	8	182D	[91,14,26]*	12
56A	[28,6,12]	6	120B	[60,4,24]	10	186A	[93,2,62]*	6
56C	[28,8,8]*	8	122A	[61,0,61]	6	192A	[96,23,8]	8
62A	[31,0,31]	6	126A	[63,5,30]	6	192B	[96,16,22]	10
64A	[32,0,32]	8	128A	[64,0,64]	6	192C	[96,18,16]	12
72A	[36,4,18]	6	128B	[64,0,64]	10	194A	[97,0,97]	6

از نتیجه ۱.۲.۲ نتیجه شده است که کدهای به‌دست آمده از گراف‌های متقارن مکعبی ۹۰A، ۱۱۰A، ۱۱۲C، ۱۲۰B، ۱۲۸B، ۱۴۴B و ۱۹۲B می‌توانند ۴ خطا را در ۵ تکرار الگوریتم Gallar A تصحیح کنند و کدهای به‌دست آمده از گراف‌های ۱۶۲B، ۱۶۲C، ۱۶۸E، ۱۶۸F و ۱۸۲D می‌توانند ۵ خطا را در ۶ تکرار از آن الگوریتم تصحیح کنند.

نتیجه ۱.۲.۴. کدهای LDPC به‌دست آمده دارای نرخ پایین هستند. برای به‌دست آوردن کدهایی با نرخ بالاتر می‌توان موارد زیر را انجام داد:

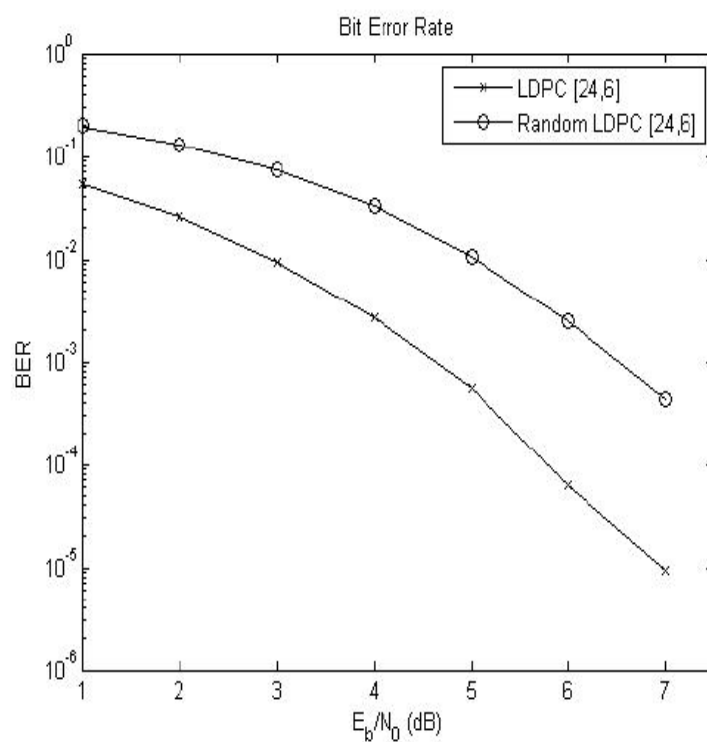
می‌توان از ماتریس $A' = [A|I_n]$ به‌عنوان ماتریس کنترل‌توازن کد LDPC c' استفاده کرد که در آن I_n ماتریس همانی از مرتبه n می‌باشد. کد c' یک کد LDPC نامنظم^۱ از طول $2n$ و بعد n است، یعنی با نرخ برابر با 0.5 . مینیمم فاصله کد ۴ است و کمر گراف تنر حفظ شده است، یعنی کمر گراف تنر کد به‌دست آمده مشابه کمر گراف کد اولیه می‌باشد. به جای ماتریس I_n می‌توان از ماتریس B $n \times 1$ که شامل l ستون از ماتریس I_n است، برای به‌دست آوردن کد LDPC با ماتریس کنترل‌توازن $[A|B]$ که دارای طول $n+1$ و بعد حداقل k می‌باشد، استفاده کرد. مینیمم فاصله کد برای $l \geq 3$ برابر ۴ می‌باشد.

۳.۴ نتایج شبیه‌سازی کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی

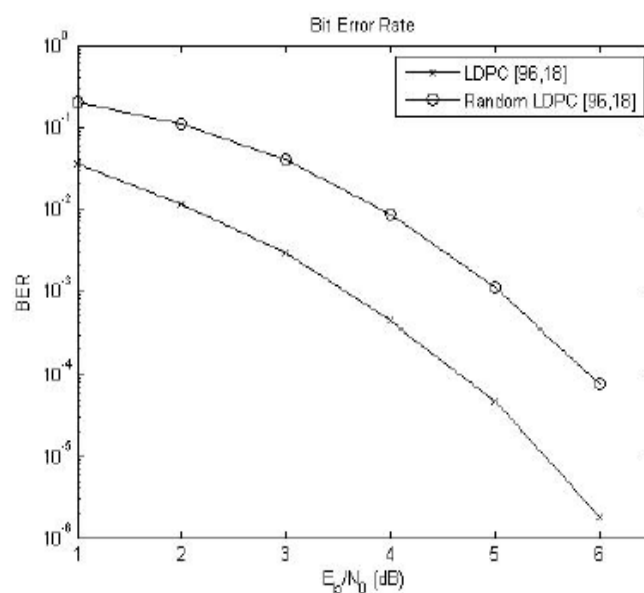
به عنوان مثال، نتایج شبیه‌سازی کدهای LDPC $[24, 6, 10]$ و $[96, 18, 16]$ برگرفته از گراف‌های متقارن مکعبی $48A$ و $192C$ بر کانال اختلال گاوسی افزودنی (AWGN) ارائه داده شده است. این کدها با کدهای LDPC که به طور تصادفی ساخته شده‌اند، از طول و بعد یکسان و ماتریس کنترل‌توازن با وزن ستونی برابر با ۳ مقایسه شده‌اند. برای کدهایی که به طور تصادفی ساخته شده‌اند، از نرم‌افزاری برای کدهای LDPC که در مرجع [۴] آورده شده است، استفاده شده است، به طوری که از ساختار آورده شده در مرجع [۳] استفاده شده است. کدها با الگوریتم جمع-حاصلضرب^۲ کدگشایی شده‌اند و حداکثر تعداد تکرار روی 50° تنظیم شده است. شکل‌های ۳.۴ و ۴.۴ عملکرد کدها را نشان می‌دهند.

¹Irregular

²Sum-Product Algorithm



شکل ۳.۴: عملکرد BER کد LDPC [۲۴،۶،۱۰] برگرفته از گراف ۴۸A



شکل ۴.۴: عملکرد BER کد LDPC [۹۶،۱۸،۱۶] برگرفته از گراف ۱۹۲A

از شکل‌های ۳.۴ و ۴.۴ می‌توان دریافت که کدهای LDPC که از گراف‌های متقارن مکعبی

ساخته شده‌اند در مقایسه با کدهای LDPC که به طور تصادفی ساخته شده‌اند، عملکرد BER بهتری دارند.

۴.۴ نتایج محاسباتی کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی

در این بخش، پارامترهای کدهای LDPC به دست آمده از گراف‌های نیم متقارن مکعبی ارائه شده است. برای ساخت گراف‌های نیم متقارن مکعبی، روشی که در مرجع [۱۹] ارائه شده است، به کار گرفته شده است. پارامتر v تعداد رئوس گراف نیم متقارن مکعبی متناظر را نشان می‌دهد.

v	LDPC ₁	LDPC ₂	v	LDPC ₁	LDPC ₂
54	[27, 8, 6]	[27, 8, 8]*	448	[224, 33, 32]	[224, 33, 32]
112	[56, 12, 14]	[56, 12, 16]	486	[243, 2, 162]*	[243, 2, 162]*
120	[60, 14, 8]	[60, 14, 12]	546	[273, 5, 130]	[273, 5, 130]
144	[72, 16, 12]*	[72, 16, 14]*	576	[288, 32, 48]	[288, 32, 56]
216	[108, 16, 24]	[108, 16, 32]	672	[336, 47, 14]	[336, 47, 42]
240	[120, 22, 16]	[120, 22, 24]	702	[351, 8, 78]	[351, 8, 104]*
294	[147, 26, 14]	[147, 26, 26]	720	[360, 10, 120]	[360, 10, 120]
336	[168, 24, 14]	[168, 24, 42]	784	[392, 12, 98]	[392, 12, 112]
378	[189, 11, 42]	[189, 11, 56]	798	[399, 5, 190]	[399, 5, 190]
384	[192, 35, 16]	[192, 35, 18]	864	[432, 32, 96]	[432, 32, 108]
400	[200, 24, 32]	[200, 24, 60]	882	[441, 44, 42]	[441, 44, 78]
432	[216, 24, 48]	[216, 24, 60]	896	[448, 48, 84]	[448, 48, 100]

شکل ۵.۴: پارامترهای کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی با کمتر از ۱۰۰۰ رأس (با استفاده از روش ارائه شده در مرجع [۱۹]).

گراف‌های تنر کدهای ساخته شده دارای کمر حداقل هشت هستند. کدهای $C_H(G)$ و $C_{HT}(G)$ در حالتی هم‌ریخت هستند که تعداد رئوس گراف نیم متقارن مکعبی G ، ۴۸۶، ۵۴۶، ۷۲۰ و ۷۹۸ باشد.

ملاحظه ۱.۴.۴. پژوهشگران اخیراً علاقه زیادی به کدهای LCD نشان داده‌اند، زیرا این کدها کاربرد مهمی در رمزنگاری در محافظت در برابر حملات کانال جانبی و خطا دارند (مرجع [۲۰]).

نتایج محاسباتی کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی ۳۷

را ببینید). کدهای خود-متعامد را می‌توان برای ساخت کدهای تصحیح‌گر کوانتوم^۱ استفاده کرد، که می‌تواند از اطلاعات کوانتومی در محاسبات کوانتومی و ارتباطات کوانتومی محافظت کند(مرجع [۲۱] را ببینید).

کدهای LDPC که در جدول ۵.۴ پررنگ نمایش داده شده‌اند، کدهای خود-متعامد و کدهایی که با * برچسب‌گذاری شده‌اند، کدهای LCD هستند.

ملاحظه ۲.۴.۴. کدهای $C_H(G)$ و $C_{HT}(G)$ ساخته شده توسط گراف‌های نیم متقارن مکعبی دارای طول و بعد یکسان و مینیمم فاصله متفاوت هستند. بنابراین، ساختار متنوعی برای همان گراف می‌دهد، که این حالت برای کدهای LDPC که در بخش ۲.۲ با استفاده از گراف‌های متقارن مکعبی ساخته می‌شود، صدق نمی‌کند.

برحسب طبقه‌بندی گراف‌های نیم متقارن مکعبی با حداکثر ۷۶۸ رأس (مرجع [۲۲] را ببینید)، همه گراف‌ها دارای کمر حداقل ۸ هستند، که بر حسب مرجع [۱۸] تعداد زیادی از گراف‌های متقارن مکعبی دارای کمر ۶ هستند. علاوه بر این، گراف‌های نیم متقارن خانواده وسیع‌تری را نسبت به گراف‌های متقارن مکعبی تشکیل می‌دهند.

علاوه بر این، پارامترهای کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی با پارامترهای کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی مقایسه شده است. نتیجه در جدول زیر آورده شده است:

n	Rate (CSSG)	Rate (CSG)
۲۷	۰.۲۹۶	۰.۰۷۴
۵۶	۰.۲۱۴	{۰.۰، ۱۴۳.۱۰۷}
۶۰	۰.۲۳۳	{۰.۰، ۸۳.۰۶۷}
۷۲	۰.۲۲۲	{۰.۰، ۱۱۱.۰۸۳}

جدول ۱.۴: نرخ کدهای LDPC ساخته شده از گراف‌های متقارن و نیم متقارن مکعبی با طول یکسان

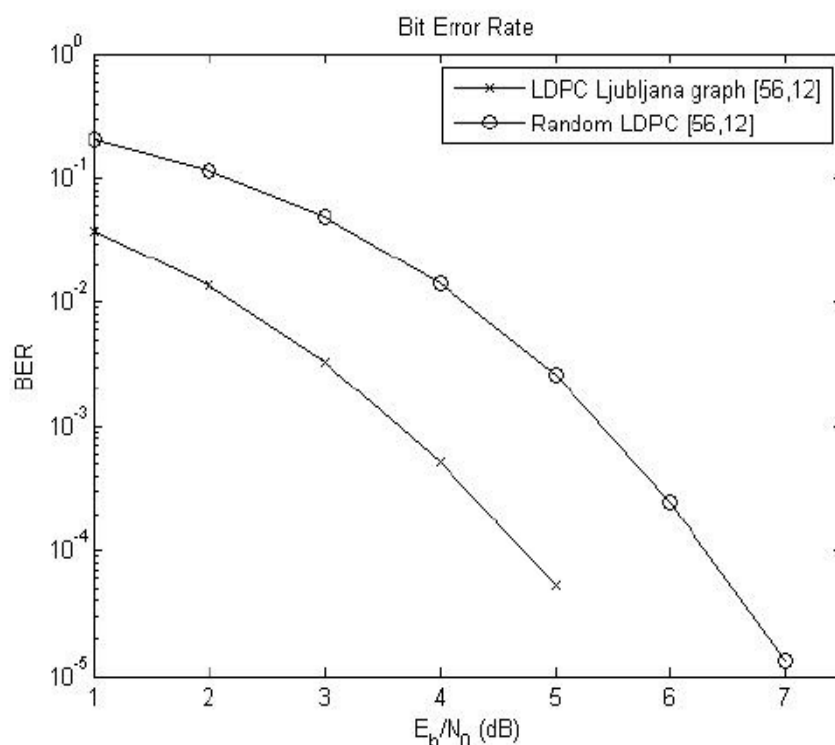
می‌توان نتیجه گرفت که برای طول کد یکسان، کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی، نرخ کد بالاتری از کدهای LDPC ساخته شده توسط گراف‌های متقارن مکعبی دارند. وقتی $n = ۲۷$ ، نرخ کد چهار برابر بیشتر می‌باشد.

^۱Quantum error-correcting

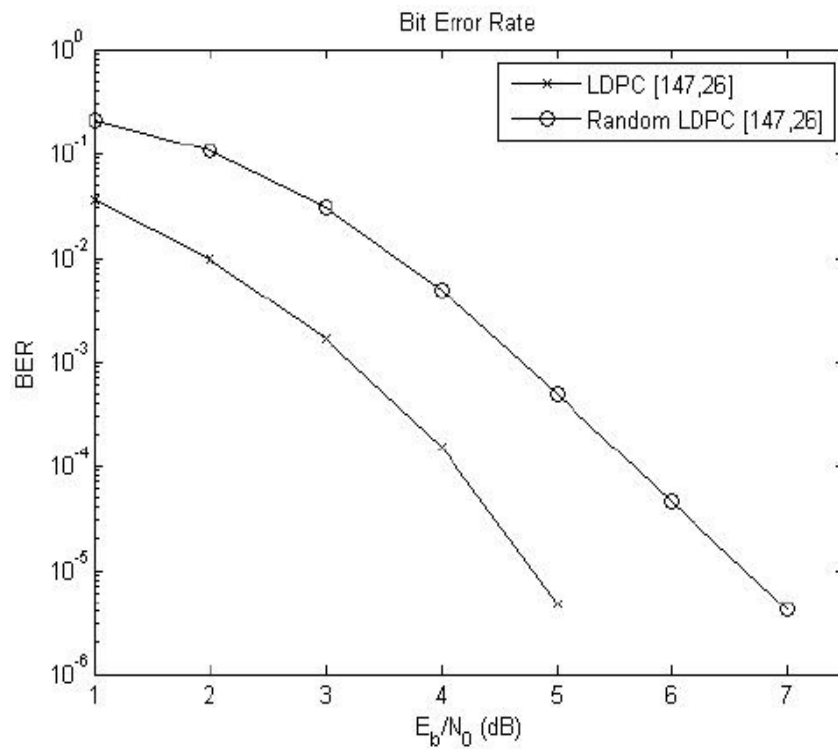
۵.۴ نتایج شبیه‌سازی کدهای LDPC ساخته شده توسط گراف‌های نیم متقارن مکعبی

در این بخش، نتایج شبیه‌سازی کدهای LDPC به دست آمده از گراف‌های نیم متقارن مکعبی روی کانال اختلال گاوسی افزودنی نشان داده شده است. این کدها با کدهای LDPC ساخته شده تصادفی با طول و ابعاد مشابه و یک ماتریس کنترل توازن با وزن ستونی برابر با سه مقایسه شده‌اند. برای کدهایی که به صورت تصادفی تولید شده‌اند از نرم‌افزاری برای کدهای LDPC که در مرجع [۴] در دسترس است، استفاده شده است. کدها با الگوریتم جمع-حاصلضرب کدگذاری شده‌اند و حداکثر تعداد تکرار روی 5° تنظیم شده است. شکل‌های ۶.۴ تا ۹.۴ عملکرد کدها را نشان می‌دهند.

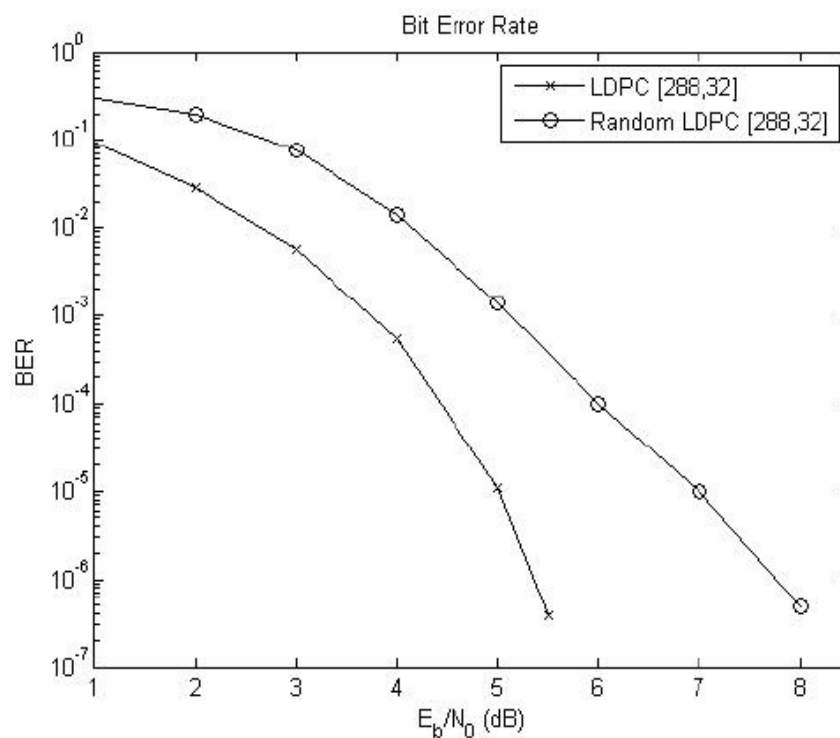
ملاحظه ۱.۵.۴. کدهای LDPC که از آن‌ها آگاه هستیم برای مقایسه با کدهای LDPC به دست آمده در این پایان نامه به دلیل پارامترهای مختلف کدها کافی نبودند. بنابراین، از بهترین ساختار تصادفی شناخته شده برای کدهای LDPC استفاده شده است. در مرجع [۱۳] ثابت شده است که این ساختار منجر به کدهای LDPC با عملکرد نزدیک به حد شانون می‌شود. علاوه بر این، بهترین نتایج در مورد کوچکترین وزن ستونی ممکن به دست آمد.



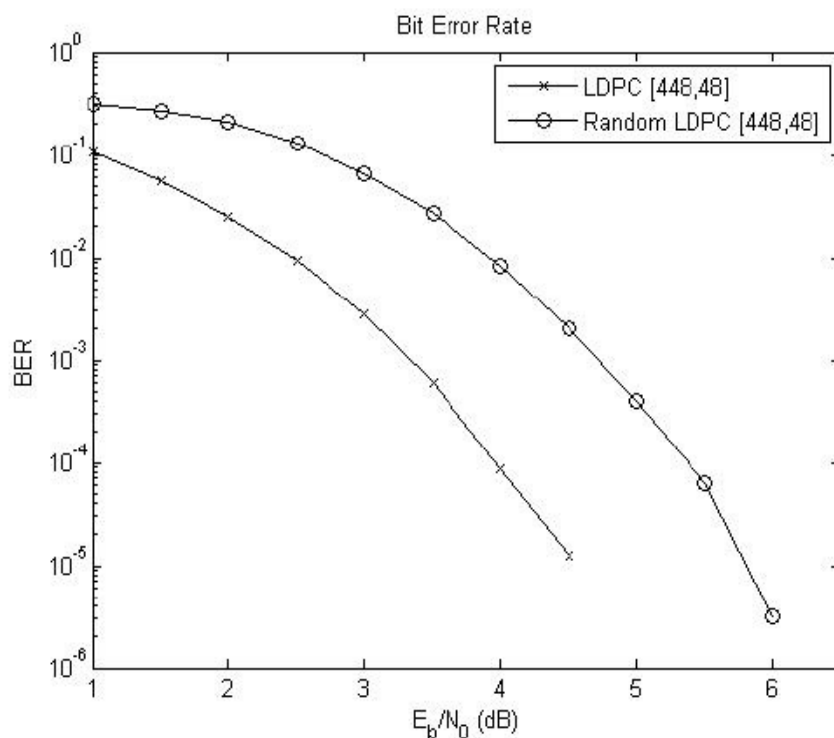
شکل ۶.۴: عملکرد BER کد LDPC [۵۶، ۱۲، ۱۶] به دست آمده از گراف Ljubljana.



شکل ۷.۴: عملکرد BER کد LDPC [۱۴۷،۲۶،۲۶] به دست آمده از گراف نیم متقارن مکعبی با ۲۹۴ رأس.



شکل ۸.۴: عملکرد BER کد LDPC [۲۸۸،۳۲،۵۶] به دست آمده از گراف نیم متقارن مکعبی با ۵۷۶ رأس.



شکل ۹.۴: عملکرد BER کد LDPC [۴۴۸،۴۸،۱۰۰] به دست آمده از گراف نیم متقارن مکعبی با ۸۹۶ رأس.

نتایج شبیه‌سازی به دست آمده نشان دهنده این است که کدهای ساخته شده از گراف‌های نیم متقارن مکعبی نسبت به کدهای LDPC که به طور تصادفی ساخته شده‌اند، عملکرد BER بهتری دارند.

واژه‌نامه انگلیسی به فارسی

Absorbing	جاذب
Adjacency matrix	ماتریس مجاورت
Arc-transitive	کمان-انتقالی
Automorphism	یکریخت
Binary	دودویی
Bit Node	رأس بیتی
Bipartite	دوبخشی
Bound	کران
Characteristic	مشخصه
Check Node	رأس کنترلی
Clique	خوشه
Coding	کدگذاری
Common neighbour	همسایه مشترک
Connected	همبند
Crossover probability	احتمال متقاطع
Cubic Graph	گراف مکعبی
Cycle	دور
Decoding	کدگشایی
Density	چگالی
Dependent	وابسته
Diagonal	قطر
Dimension	بعد
Distance	فاصله
Distributable	توزیع پذیر
Edge	یال
Eigenvalue	مقدار ویژه

Eigenvector	بردار ویژه
Equivalence	هم‌ارزی
Error-correcting	تصحیح‌گر خطا
Generator Polynomial	چندجمله‌ای مولد
Girth	کمر
Hamming distance	فاصله همینگ
Identity matrix	ماتریس همانی
Independence number	عدد استقلال
Irregular	نا منظم
Isomorphic	هم‌ریخت
Linear	خطی
Low-density	کم-چگال
Maximal	ماکسیمال
Multigraph	گراف چندگانه
Non-Diagonal	غیر قطری
Non-trivial	غیر بدیهی
Null space	فضای پوچ
Optimal	بهینه
Parity check	کنترل توازن
Polynomial	چندجمله‌ای
Rank	رتبه
Rate	نرخ
Reciprocal polynomial	چندجمله‌ای متقابل
regular	منظم
Self dual	خود-دوگان
Self-orthogonal	خود-متعامد
Semisymmetric	نیم متقارن
Simulation results	نتایج شبیه‌سازی
Singular	تکین
Sparse	کم چگال
Spectrum	طیف
Symmetric	مقارن
Syndrome	سندروم
Trapping set	مجموعه تله‌ای

Variance	واریانس
Vector Sum	جمع برداری
Vertex	رأس
Vertex-transitive	رأس-انتقالی
Weight	وزن

واژه‌نامه فارسی به انگلیسی

Crossover probability	احتمال متقاطع
Eigenvector	بردار ویژه
Dimension	بعد
Optimal	بهینه
Error-correcting	تصحیح‌گر خطا
Singular	تکین
Trapping	تله‌ای
Distributable	توزیع‌پذیر
Absorbing	جاذب
Density	چگالی
Polynomial	چندجمله‌ای
Reciprocal polynomial	چندجمله‌ای متقابل
Generator polynomial	چندجمله‌ای مولد
linear	خطی
Clique	خوشه
Self-dual	خود-دوگان
Self-orthogonal	خود-متعامد
Spectrum	طیف
Bipartite	دوبخشی
Binary	دودویی
Cycle	دور
Vertex	رأس
Vertex-Transitive	رأس-انتقالی
Bit Node	رأس بیتی
Control Node	رأس کنترلی
Rank	رتبه

Syndrome	سندروم
Independence number	عدد استقلال
Non-trivial	غیر بدیهی
Non-Diagonal	غیر قطری
Distance	فاصله
Hamming Distance	فاصله همینگ
Vector Space	فضای برداری
Null Space	فضای پوچ
Diagonal	قطر
Bound	کران
Coding	کدگذاری
Decoding	کدگشایی
Arc-transitive	کمان-انتقالی
Girth	کمر
Low-density	کم-چگال
Sparse	کم وزن
Parity check	کنترل توازن
Multigraph	گراف چندگانه
Cubic graph	گراف‌های مکعبی
Adjacency matrix	ماتریس مجاورت
Identity matrix	ماتریس همانی
Maximal	ماکسیمال
Symmetric	متقارن
Independent	مستقل
Characteristic	مشخصه
Eigenvalue	مقدار ویژه
Regular	منظم
Irregular	نا منظم
Simulation results	نتایج شبیه‌سازی
Rate	نرخ
Semisymmetric	نیم متقارن
Dependent	وابسته
Variance	واریانس
Weight	وزن

Equivalence	هم‌ارزی
Connected	همبند
Common neighbor	همسایه مشترک
Isomorphic	هم‌ریخت
Edge	یال
Automorphic	یک‌ریخت

مراجع

- [1] R. Balakrishnan and K. Ranganathan, *A Textbook of Graph Theory*, Springer, New York, 2012.
- [2] W. Bosma, J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, 1994. <http://magma.maths.usyd.edu.au/magma>.
- [3] D. J. C. MacKay and R. M. Neal, Near shannon limit performance of Low Density Parity Check codes, *Electronics Letters* 32 (1997), 457-458.
- [4] R. M. Neal, Software for Low Density Parity Check (LDPC) codes, Release of 2012-02-11. <http://www.cs.utoronto.ca/radford/>.
- [5] M. Harada, K. Saito, Binary linear complementary dual codes, *Cryptogr. Commun.* 11 (2019), 677-696.
- [6] M. Conder and B. McKay, G. Royle, Cubic symmetric graphs (The Foster Census), Online available at <http://staffhome.ecm.uwa.edu.au/00013890/remote/foster/>, Accessed on 18/01/2020.
- [7] R. G. Gallager, Low-Density Parity-Check Codes, *MIT Press*, Cambridge, MA, 1963.
- [8] R. Diestel, *Graph theory*, Springer-Verlag, Berlin Heidelberg, 2017.
- [9] M. Greferath, C. Robing and L. Storme, Current Research Topics in Galois Geometry, *Galois geometries and low-density parity-check codes*, Nova Science Publishers, 2011, 245-275.
- [10] W. C. Haffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [11] A. Nilli, On the second eigenvalue of a graph, *Discrete Math.* 91 (1991), 207- 210.

-
- [12] J. L. Massey, Linear codes with complementary duals, *Discrete Math.* 106/107 (1992), 337-342.
 - [13] D. J. C. MacKay and R. M. Neal, Near Shannon Limit Performance of Low Density Parity Check Codes, *Electronics Letters* 32 (1997), 457-458.
 - [14] C. Pacher, P. Grabenweger and D. E. Simos, Weight distribution of the syndrome of linear codes and connections to combinatorial designs, 2016 IEEE Int. *Symp. Info. (ISIT)*, 2016, 3038-3042.
 - [15] J. Rosenthal and P. O. Vontobel, Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis, 38th Allerton Conference on Communication, *Control and Computing*, 2000, 248-257.
 - [16] T. Shibuya, M. Onikubo and K. Sakaniwa, On Tanner's Lower Bound for the Minimum Distance of Regular LDPC Codes Based on Combinatorial Designs, *IEICE Trans. Fundamentals E86-A* (2003), 2428-2434.
 - [17] S. K. Chilappagari, D. V. Nguyen, B. V. Vasic and M. W. Marcellin, Girth of the Tanner graph and error correction capability of LDPC codes, 46th Annual Allerton Conference on Communication, *Control and Computing*, 2008, 1238- 1245.
 - [18] M. Conder and R. Nedela, A refined classification of symmetric cubic graphs, *J. Algebra* 322 (2009), 722-740.
 - [19] A. Bretto and L. Gillibert, G-graphs: An efficient tool for constructing symmetric and semisymmetric graphs, *Discrete Appl. Math.* 156 (2008), 2719–2739.
 - [20] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi, Orthogonal direct sum masking, a smartcard friendly computation paradigm in a code, with Builtin protection against sidechannel and fault attacks, *Proceedings of WISTP 2014. Lecture Notes in Computer Science 8501*, 2014, 40–56.
 - [21] A. K. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* 78 (1997), 405–408.
 - [22] M. Conder, A. Malnic, D Marusic and P. Potocnik, A census of semisymmetric cubic graphs on up to 768 vertices, *J. Algebraic Combin.* 23 (2006), 255–294.
 - [23] V. Toto-Zarasoia, A. Roumy and C. Guillemot, Maximum Likelihood BSC Parameter Estimation for the Slepian-Wolf Problem, *IEEE Commun. Lett.* 15 (2011), 232–234.

- [24] C. Schlegel, On the Dynamics of the Error Floor Behavior in (Regular) LDPC Codes, *IEEE Trans. Inform. Theory* 56 (2010), 3248–3264.
- [25] R. M. Tanner, A Recursive Approach to Low Complexity Codes, *IEEE Trans. Inform. Theory* 27 (1981), 533–547.
- [26] Y. Q. Feng, M. Ghasemi and C. Wang, Cubic semisymmetric graphs of order $6p^3$, *Discrete Math.* 310 (2010), 2345–2355.
- [27] M. Greferath, C. Roßing and L. Storme, Galois geometries and low-density parity-check codes, *L. Storme, J. De Beule, Current Research Topics in Galois Geometry*, Nova Science Publishers, 2011, 245–275.
- [28] F. Ivanov and V. Zyablov, LDPC codes based on Steiner quadruple systems and permutation matrices, *Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory*, Svetlogorsk, Russia, 2014, 175–180.
- [29] J.-L. Kim, U. N. Peled, I. Perepelitsa and V. Pless, Explicit construction of families of LDPC codes with no 4-cycles, *IEEE Trans. Inform. Theory* 50 (2004), 2378–2388.
- [30] A. Malnic, D. Marusic and C. Wang, Cubic edge-transitive graphs of order $2p^3$, *Discrete Math.* 274 (2004), 187–198.
- [31] R. M. Neal, Software for Low Density Parity Check (LDPC) codes, Release of 2012-02-11. <http://www.cs.utoronto.ca/radford/>.
- [32] Q. Diao, Y.Y. Tai, S. Lin and K. Abdel-Ghaffar, Trapping Set Structure of LDPC Codes on Finite Geometries, *IEEE Int. Symp. on Inf. Theory* (2013), 3088–3092.
- [33] D. Crnkovic, S. Rukavina and M. Simac, LDPC codes from geodetic graphs obtained from block designs, *Graphs Combin.* 35 (2019), 451–469.
- [34] W. E. Ryan, S. Lin, *Channel Codes: Classical and Modern*, Cambridge University Press, 2009.
- [35] R. M. Tanner, Minimum-distance bounds by graph analysis, *IEEE Trans. Inform. Theory* 47 (2001), 808–821.
- [36] P. Potocnik, P. Spiga, G. Verret, On the nullspace of arc-transitive graphs over finite fields, *J. Algebr. Comb.* 36 (2012), 389–401.

Abstract

Low-density parity-check (LDPC) codes have been the subject of much interest due to the fact that they can perform near the Shannon limit. In this thesis, some kinds of constructions of LDPC codes from cubic (semi-)symmetric graphs are presented. The constructed codes are $(3,3)$ -regular and the vast majority of the corresponding Tanner graphs have girth greater than four. Some properties of the obtained codes are analysed, and some bounds for the code parameters, specially for the dimension and the minimum distance, are presented. Furthermore, an expression for the variance of the syndrome weight of the constructed codes are given. Information on the LDPC codes constructed from bipartite cubic symmetric graphs with less than 200 vertices is presented as well. Some of the constructed codes are optimal, and some have an additional property of being self-orthogonal or linear codes with complementary dual (LCD codes).



Faculty Of Mathematical Sciences

MSc Thesis in Cryptography and Coding

Constructing LDPC codes from cubic symmetric graphs

By: Yasaman Mohammad Niya

Supervisor:

Dr Abdollah Alhevaz

January 2022