دانشگاه اصفهان

دانشکده علوم

گروه ریاضی

پایان نامه‌ی کارشناسی ارشد رشته‌ی ریاضی محض گرایش گروه

کدهای دوتایی روی گراف‌های قویاً منظم

اساتید راهنما:

دکتر جواد باقریان

دکتر رضا سبحانی

پژوهشگر: مسعود مجیدی

چکیده

در این پایان‌نامه، ابتدا رده‌های مختلف از گراف‌های قویاً منظم را معرفی و آن‌ها را مورد بررسی قرار می‌دهیم. سپس به کمک ماتریس مجاورت یک گراف قویاً منظم، کدهای دوتایی بدست می‌آوریم و پارامترهای کدهای تولید شده را تحلیل می‌کنیم. در انتها به صورت خاص کد روی گراف‌های قویاً منظم با کمتر از ۴۰ راس را بررسی نموده و پارامترهای آن‌ها را به صورت کامل به دست می‌آوریم.

فهرست مطالب

مقدمه

یکی از روش‌های مرسوم برای یافتن کد، استفاده از ابزارهای جبری است مانند استفاده از گروه‌ها، ماتریس‌ها و غیره. از جمله این روش‌ها می‌توان به کدهای دوتایی که از فضای سطری ماتریس‌ها به دست می‌آید، اشاره کرد. در سال ۱۹۹۸ همرز[۱] و پیترز[۲] در مقاله‌ی [۸] به مطالعه کدهای دوتایی که از فضای سطری گراف‌های قویاً منظم ساخته می‌شود، پرداخته‌اند. یک گراف قویاً منظم با پارامترهای (v, k, λ, μ) یک k-گراف منظم است که دارای v راس است به طوری که هر دو راس مجاور به طور مشترک با λ راس دیگر مجاور هستند و هر دو راس غیر مجاور به طور مشترک با μ راس دیگر مجاور هستند. ما در این پایان‌نامه ابتدا گراف‌های قویاً منظم را مورد بررسی قرار می‌دهیم و بعضی از خانواده‌های این گراف‌ها مثل گراف‌های مثلثی، گراف‌های لاتیس و گراف‌های پایلی را معرفی می‌کنیم. بعلاوه نشان می‌دهیم متمم هر گراف قویاً منظم گرافی قویاً منظم است.

در ادامه طرح‌های ترکیبیاتی را معرفی می‌کنیم و نشان می‌دهیم از هر طرح متقارن می‌توان گراف قویاً منظم به‌دست آورد. بعلاوه از گراف‌های قویاً منظم با پارامترهای (v, k, λ, λ)، طرح تولید می‌کنیم.

هم‌چنین ماتریس‌های هادامارد را تعریف می‌کنیم و از این ماتریس‌ها، گراف‌های قویاً منظم به دست می‌آوریم.

در پایان فصل ۱ دو-گراف‌ها و تعویض‌گرهای سیدل را تعریف می‌کنیم و با استفاده از تعویض‌گرهای سیدل از یک گراف قویاً منظم، گراف‌های قویاً منظم دیگری تولید می‌کنیم.

در فصل ۲، کد C را فضای تولید شده توسط سطرهای ماتریس مجاورت گراف‌های قویاً منظم قرار می‌دهیم و با استفاده از پارامترهای گراف قویاً منظم، بعد کد C را تعیین می‌کنیم. هم‌چنین برای گراف‌های قویاً منظم با کم‌تر از ۴۰ راس، کدهای متناظر را تولید می‌کنیم.

در فصل ۳ نخست یک کران برای کمترین فاصله‌ی کد C حاصل از فضای سطری تولید شده توسط $G = (I, A)$ به دست می‌آوریم، جایی‌که A یک ماتریس متقارن است و I ماتریس همانی است. سپس ثابت می‌کنیم، هرگاه A ماتریس مجاورت گراف قویاً منظم Γ با پارامترهای (v, k, λ, μ) و C کدی با ماتریس

[۱] Haemers

[۲] Peters

مولد $G = A$ یا $G = (I, A)$ باشد، آن‌گاه دوگان کد C می‌تواند با استفاده از کدگشایی اکثریت

$$\frac{k + \max(\lambda, \mu) - ۱}{۲ \max(\lambda, \mu)}$$

خطا را برای کد C تصحیح کند.

فصل ۱

تعاریف و قضایا

در این فصل تعاریف و قضایایی را می‌آوریم که در فصل‌های آینده مورد نیاز هستند.
در تمامی بخش‌های این پایان‌نامه I ماتریس همانی، J ماتریس مربعی با درایه‌های همه جا ۱، D ماتریس قطری و $\mathbf{1}$ ماتریس ستونی همه جا ۱ است.

۱.۱ کد

تعریف ۱.۱.۱ مجموعه متناهی $\mathcal{A}=\{a_1,a_2,\cdots,a_q\}$، را در نظر بگیرید. فرض کنید $\mathcal{A}^n$ مجموعه همه‌ی رشته‌های به طول n روی $\mathcal{A}$ باشد. منظور از یک کد بلوکی به طول n روی $\mathcal{A}$، یک زیر مجموعه ناتهی از $\mathcal{A}^n$ است. به $\mathcal{A}$ الفبای این کد و به هر رشته در C، کدکلمه گویند. اگر C، شامل M کدکلمه باشد، آن‌گاه C را کدی به طول n و اندازه M گویند و آن را با (n,M)- کد نمایش می‌دهند.

تعریف ۲.۱.۱ فرض کنید x و y دو رشته به طول یکسان روی یک الفبا باشند. **فاصله همینگ**[۱] $d(x,y)$، برابر تعداد مکان‌هایی است که x و y در آن مکان‌ها دارای مقادیر متفاوت هستند.

مثال ۳.۱.۱ کد $C=\{0000,1100,0011,1001,0110,1111\}$ را روی میدان F_2 در نظر بگیرید. فاصله‌ی کدکلمات ۰۰۱۱ و ۱۱۰۰ برابر ۴ و فاصله‌ی کدکلمات ۱۱۱۱ و ۱۱۰۰ برابر ۲ است.

تعریف ۴.۱.۱ تابع $d: X\times X\longrightarrow \mathbb{R}$ را یک **متر** گوییم، هرگاه

۱) برای هر $x,y\in X$، $d(x,y)\geq 0$ و همچنین $d(x,y)=0$ اگر وتنها اگر $x=y$.

[۱] Hamming distance

۲) برای هر $x, y \in X$، $d(x,y) = d(y,x)$.

۳) برای هر $x, y, z \in X$، $d(x,y) \leq d(x,z) + d(y,z)$ (نامساوی مثلثی).

گزاره ۵.۱.۱ اگر A^n مجموعه تمامی کدکلمات به طول n روی الفبا A باشد، آن‌گاه فاصله همینگ یک متر روی A^n است.

اثبات. به قضیه‌ی (۴.۲.۱) در کتاب [۱۲] مراجعه شود. ■

تعریف ۶.۱.۱ فرض کنید A یک الفبا و C یک کد روی A باشد، **کمترین فاصله**[۲] کد C به صورت زیر تعریف می‌شود:

$$d(C) = \min_{c,d \in C} d(c,d)$$

که در آن d یک متر همینگ است.

تعریف ۷.۱.۱ یک (n, M, d)-کد، یک کد به طول n، اندازه M و کمترین فاصله d است.

تعریف ۸.۱.۱ دو (n, M)-کد q-تایی $C_۱$ و $C_۲$ را **معادل**[۳] گوییم، هرگاه جایگشتی چون σ روی n مختصات و جایگشت‌های $\pi_۱$، $\pi_۲$، $\cdots$، π_n روی الفبای کد موجود باشند به طوری که

$\pi_۱(c_{\sigma(۱)})\pi_۲(c_{\sigma(۲)})\cdots\pi_n(c_{\sigma(n)})) \in C_۲$ اگر و تنها اگر $c_۱c_۲\cdots c_n \in C_۱$.

۲.۱ کد خطی

مجموعه $(\mathbb{F}_q)^n$، یک فضای برداری با بعد n روی میدان $\mathbb{F}_q$ است. $(F_q)^n$ را با $V(n,q)$ نیز نمایش می‌دهیم.

تعریف ۱.۲.۱ کد $L \subseteq V(n,q)$ را **خطی**[۴] گوییم، اگر L زیر فضای $V(n,q)$ باشد. هرگاه L یک کد خطی و دارای بعد k روی $V(n,q)$ باشد، گوییم L یک $[n,k]$-کد است. اگر L دارای کمترین فاصله d باشد، آن‌گاه L را یک $[n,k,d]$-کد گوییم.

[۲] minimum distance

[۳] equivalence

[۴] linear

تعریف ۲.۲.۱ فرض کنید $x \in V(n,q)$. **وزن همینگ**[۵] x را که با $w(x)$ نمایش داده می‌شود، برابر تعداد مکان‌های غیر صفر x تعریف می‌شود. همچنین **وزن** یا کمترین وزن یک کد C را که با $w(C)$ نمایش داده می‌شود، برابر کم‌ترین وزن همه‌ی کدکلمات غیر صفر از کد C تعریف می‌شود.

تعریف ۳.۲.۱ اگر $x = x_۱x_۲\cdots x_n$ و $y = y_۱y_۲\cdots y_n$ دو عضو $V(n,۲)$ باشند. در این صورت اشتراک x و y را به صورت زیر تعریف می‌کنیم:

$$x \cap y := (x_۱y_۱, x_۲y_۲, \cdots, x_ny_n).$$

بنابراین $x \cap y$ در مکان iام ۱ است اگر وتنها اگر مکان iام x و y هر دو ۱ باشد.

لم ۴.۲.۱ ۱) برای هر $x, y \in V(n,q)$ داریم

$$d(x,y) = w(x-y).$$

۲) برای هر $x, y \in V(n,۲)$ داریم

$$d(x,y) = w(x) + w(y) - ۲w(x \cap y).$$

اثبات. به لم (۴.۳.۴) از مرجع [۱۲] مراجعه شود. ■

قضیه ۵.۲.۱ برای کد خطی L داریم، $d(L) = w(L)$.

اثبات. به قضیه‌ی (۵.۳.۴) از مرجع [۱۲] مراجعه شود. ■

تعریف ۶.۲.۱ فرض کنید C کدی روی $(\mathbb{F}_q)^n$ باشد، **کد متمم**[۶] C، کدی است که از تعویض ۰ و ۱ های کدکلمات به دست می‌آید و آن را با C^c نمایش می‌دهند.

لم ۷.۲.۱ اگر $x, y \in V(n,۲)$، آن‌گاه $d(x,y^c) = n - d(x,y)$، جایی‌که y^c متمم کد کلمه‌ی $y \in C$ است.

اثبات. به لم (۸.۳.۴) از مرجع [۱۲] مراجعه شود. ■

[۵] Hamming weight

[۶] complement code

تعریف ۸.۲.۱ فرض کنید C یک $[n,k]$-کد دوتایی باشد. در این صورت **گروه خودریختی‌های**[۷] C که با $Aut(C)$ نمایش داده می‌شود، به صورت زیر تعریف می‌گردد:

$$Aut(C) = \{\pi \in S_n \mid \pi c \in C \quad \forall c \in C\},$$

جایی که π به صورت زیر عمل می‌کند:

$$\pi(c_۱, c_۲, \cdots, c_n) = (c_{\pi_۱}, c_{\pi_۲}, \cdots, c_{\pi_n}).$$

قضیه ۹.۲.۱ مجموعه $Aut(C)$ تحت عمل ترکیب توابع یک گروه است.

اثبات. واضح است. ■

مثال ۱۰.۲.۱ گروه خودریختی‌های کد $C = \{۰۰۰۰, ۱۱۰۰, ۰۰۱۱, ۱۱۱۱\}$ یک زیر گروه $S_۴$ از اندازه ۸ است. در واقع داریم:

$$Aut(C) = \{id, (۱۲), (۳۴), (۱۲)(۳۴), (۱۳)(۲۴), (۱۴)(۲۳), (۱۳۲۴), (۱۴۲۳)\}.$$

تعریف ۱۱.۲.۱ فرض کنید L یک $[n,k]$-کد باشد. ماتریس G را که یک ماتریس $k \times n$ است، **ماتریس مولد**[۸] کد L گوییم، هرگاه سطرهای G پایه کد L باشند.

اگر L یک $[n,k]$-کد روی میدان $\mathbb{F}_q$ با ماتریس مولد G باشد، آن‌گاه کدکلمات L ترکیبات خطی سطرهای G هستند؛ یعنی:

$$L = \{xG \mid x \in V(k,q)\}. \qquad (۱.۱)$$

معادله (۱.۱) روش بسیار ساده‌ای برای کدگذاری معرفی می‌کند. اگر منبع، به صورت همه‌ی کلمات به طول k روی الفبای q-تایی نمایش داده شود، آنگاه ما کلمه منبع $x \in V(k,q)$ را به کدکلمه xG کدگذاری می‌کنیم.

مثال ۱۲.۲.۱ فرض کنید L یک کد خطی با ماتریس مولد:

$$G = \begin{pmatrix} ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ \end{pmatrix}$$

[۷] automorphism group

[۸] generator matrix

باشد. کد L، عناصر $V(۳,۲)$ را کدگذاری می‌کند. در واقع برای هر

$$x = (x_۱, x_۲, x_۳) \in V(۳,۲)$$

کدکلمه متناظر عبارت است از:

$$[x_۱, x_۲, x_۳]\begin{pmatrix} ۱ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ \end{pmatrix} = [x_۱ + x_۳, x_۱ + x_۲, x_۲ + x_۳, x_۲].$$

اگر I_k ماتریس همانی از اندازه $k \times k$ باشد، آن‌گاه ماتریس مولد به فرم $G = (I_k \mid A)$ را ماتریس مولد در **شکل استاندارد** گوییم. فضای برداری $V(n,q)$ دارای یک ضرب داخلی است که به صورت طبیعی تعریف می‌شود. اگر $x = x_۱x_۲\cdots x_n$ و $y = y_۱y_۲\cdots y_n$ در $V(n,q)$ باشند، **ضرب نقطه‌ای** یا **ضرب اسکالر** x و y را که با $x \cdot y$ نمایش داده می‌شود، به صورت زیر تعریف می‌کنیم:

$$x.y = x_۱y_۱ + x_۲y_۲ + \cdots + x_ny_n.$$

تعریف ۱۳.۲.۱ فرض کنید L یک (n,k)-کد خطی باشد. مجموعه

$$L^{\perp} = \{x \in V(n,q) \mid x.c = ۰, \quad \forall c \in L\}$$

را **کد دوگان**[۹] L گوییم.

قضیه ۱۴.۲.۱ ۱) اگر G ماتریس مولد کد L باشد، آن‌گاه

$$L^{\perp} = \{x \in V(n,q) \mid xG^T = ۰\}.$$

۲) دوگان $[n,k]$-کد خطی L، یک $[n,n-k]$-کد خطی است.

۳) برای هر کد خطی L داریم، $(L^{\perp})^{\perp} = L$.

اثبات. به قضیه‌ی (۳.۱.۵) از مرجع [۱۲] مراجعه شود. ■

[۹] dual code

توجه داشته باشید که $L \cap L^{\perp}$ همیشه برابر صفر نیست. اما بنابر قضیه (۱۴.۲.۱) داریم

$$\dim(L) + \dim(L^{\perp}) = n$$

فرض کنید L یک کد خطی با ماتریس مولد $k \times n$، به فرم استاندارد $G = (I_k \mid A)$ باشد. قرار دهید

$$H = (-A^T \mid I_{n-k})$$

جایی که A^T ترانهاده ماتریس A است. داریم

$$GH^T = (I_k \mid A)\begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = -A + A = 0$$

پس سطرهای H بر G عمود است و چون $\mathrm{rank}(H) = n - k = \dim(L^T)$، بنابراین H ماتریس مولد برای کد دوگان، $L^{\perp}$ است. به H **ماتریس بررسی توازن**[۱۰] L گوییم.

قضیه ۱۵.۲.۱ فرض کنید L یک $[n, k, d]$-کد خطی با ماتریس بررسی توازن H باشد. در این صورت d کوچک‌ترین عدد صحیح r است به طوری که r ستون از ماتریس H وابسته خطی باشند. (یعنی، d ستون H وجود دارند که وابسته خطی هستند، اما هر $d - 1$ ستون از H مستقل خطی‌اند.)

اثبات. به قضیه (۴.۱.۵) از مرجع [۱۲] مراجعه شود. ■

تعریف ۱۶.۲.۱ به کد خطی L **خود متعامد**[۱۱] گوییم، هرگاه $L \subseteq L^{\perp}$.

قضیه ۱۷.۲.۱ فرض کنید G ماتریس مولد یک کد خطی دوتایی L باشد. در این صورت L خود عمود است اگر و تنها اگر سطرهای مجزای G بر هم عمود باشند و وزن سطرها بر ۲ بخش پذیر باشد.

اثبات. اثبات واضح است. ■

قضیه ۱۸.۲.۱ اگر سطرهای مجزای ماتریس مولد G از کد خطی دوتایی L بر هم عمود باشند و وزن سطرهای G بر ۴ بخش پذیر باشند، آن‌گاه L خود عمود است و وزن همه‌ی کدکلمات L بر ۴ بخش پذیر هستند.

اثبات. خود عمود بودن از قضیه قبل معلوم است. برای قسمت دوم داریم:

$$w(u+v) = w(u) + w(v) - 2w(u \cap v).$$

چون u و v برهم عمودند، لذا $w(u \cap v)$ مضربی از ۲ است. پس $w(u)$، $w(v)$ و $w(u \cap v)$ مضربی از ۴ هستند در نتیجه وزن هر کدکلمه از L مضربی از ۴ است. ■

[۱۰] parity check matrix

[۱۱] self orthogonal

تعریف ۱۹.۲.۱ کد L را **خود دوگان**[۱۲] گوییم، هرگاه $L = L^{\perp}$.

به راحتی می‌توان دید که برای خود دوگان بودن یک کد C باید طول کد زوج باشد. در حقیقت، $[n, k]$ - کد C خود دوگان است اگر و تنها اگر C، خود عمود بوده و داشته باشیم $k = n/۲$.

تعریف ۲۰.۲.۱ برای هر (n, M) کد C، فرض کنید A_k برابر تعداد کدکلمات C به وزن k باشد. $A_۱, A_۲, \cdots , A_n$ را **توزیع وزنی**[۱۳] C می‌نامیم. به جمع

$$W_C(s) = \sum_{k=۰}^{n} A_k s^k$$

شمارنده وزنی[۱۴] C گوییم.

۳.۱ کد همینگ

کد همینگ احتمالاً مشهورترین کد در میان تصحیح کننده‌ی خطاست. این کد به طور مستقل توسط مارسل گُلی[۱۵] در سال ۱۹۴۹ و ریچارد همینگ [۱۶] در سال ۱۹۵۰ کشف شد. برای ساخت کد همینگ ابتدا توجه کنید که بنابر قضیه (۱۵.۲.۱) کمترین فاصله از $[n, k]$ - کد خطی با ماتریس بررسی توازن H برابر کوچک‌ترین عدد صحیح m است که سطرهای H وابسته خطی‌اند، لذا هیچ دو ستون از ماتریس بررسی توازن $[n, k, ۳]$ - کد خطی، وابسته خطی نیستند. یعنی هیچ ستونی مضرب اسکالری از ستون دیگر نیست، ولی سه ستون وجود دارد که وابسته خطی‌اند. اکنون ماتریس بررسی توازن کد همینگ $[n, k, ۳]$ را به صورت زیر می‌سازیم:
نخست بردار غیر صفر $c_۱$ از $V_۱ = V(r, q)$ را برمی‌داریم. سپس بردار غیر صفر $c_۲$ را از

$$V_۲ = V_۱ - \{\alpha c_i \mid \alpha \neq ۰\}$$

برمی‌داریم. این روند را برای انتخاب همه‌ی بردارهای غیر صفر ممکن ادامه می‌دهیم، چون

$$|\{\alpha c_i \mid \alpha \neq ۰\}| = q - ۱,$$

[۱۲] self dual

[۱۳] weight distribution

[۱۴] weight enumerator

[۱۵] Marcel Golay

[۱۶] Richard Hamming

پس ماتریس بررسی توازن دارای $\frac{q^r-1}{q-1}$ ستون مختلف است. ستون‌های ماتریس بررسی توازن دو به دو مستقل خطی‌اند، ولی سه ستون وجود دارد که وابسته خطی‌اند. ماتریس حاصل، ماتریس بررسی توازن $[n,k,3]$ کد خطی است که در آن،

$$n=\frac{q^r-1}{q-1},\qquad k=n-r. \tag{2.1}$$

به این کد، **کد همینگ** از مرتبه‌ی r گوییم.

توجه داشته باشید که انتخاب ستون‌ها منحصر به فرد نیست. پس ماتریس‌های همینگ مختلف با پارامتر یکسان داریم. با این وجود می‌توانیم از یک ماتریس همینگ، ماتریس همینگ دیگری (با همان پارامترها) را بدست آوریم (با استفاده از جایگشت‌ها و ضرب ستون‌ها در اسکالر غیر صفر)، لذا کدهای همینگ از مرتبه‌ی یکسان، معادل هستند.

حالت دوتایی از کد همینگ بسیار استفاده می‌شود. $H_2(r)$، یک $[n,k,3]$-کد است که:

$$n=2^r,\qquad k=2^r-1-r.$$

اگر $q=2$ آن‌گاه ستون‌های ماتریس همینگ از مرتبه‌ی r، نمایش دوتایی تمام 2^r-1 عدد غیر صفر $1,2,\cdots,2^r-1$ است.

مثال ۱.۳.۱ ماتریس بررسی توازن برای کد همینگ $H_2(3)$ برابر است با

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

فصل ۲

گراف‌های قویاً منظم

۱.۲ گراف قویاً منظم

تعریف ۱.۱.۲ یک **گراف**[۱] ساده Γ شامل مجموعه راس‌های V و مجموعه یال‌های E است، جایی‌که یک یال یک زوج نامرتب از دو راس متمایز X است. اگر $xy \in E$ یک یال باشد، گوییم راس‌های x و y مجاور هستند.

تعریف ۲.۱.۲ فرض کنید $\Gamma = (V, E)$ یک گراف باشد. **درجه‌ی**[۲] راس $x \in V$ برابر تعداد راس‌هایی است که با x در گراف Γ مجاور هستند.

تعریف ۳.۱.۲ یک **گراف منظم** از درجه‌ی k یک گراف ساده است که درجه هر راس آن k باشد.

تعریف ۴.۱.۲ یک **گراف قویاً منظم** با پارامترهای (v, k, λ, μ) که آن را معمولاً با $SRG(v, k, \lambda, \mu)$ نمایش می‌دهند، عبارت است از یک گراف ساده بدون طوقه از مرتبه‌ی v که در شرایط زیر صدق می‌کند.

۱) منظم از درجه‌ی k است.

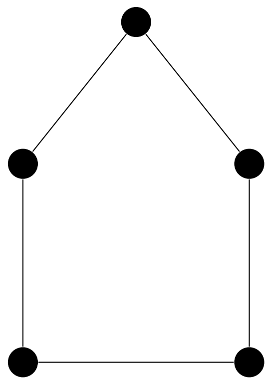
۲) برای هر دو راس مجاور، λ راس وجود دارند که با هر دو مجاور هستند.

۳) برای هر دو راس غیر مجاور، μ راس وجود دارند که با هر دو مجاور هستند.

[۱] graph

[۲] order

برای مثال یک پنج ضلعی[۳] (شکل (۱.۲)) یک گراف قویاً منظم با پارامترهای $(۵, ۲, ۰, ۱)$ است.



شکل ۱.۲: گراف پنج ضلعی

در حالت کلی دو گراف قویاً منظم با پارامترهای یکسان، یکریخت نیستند. برای مثال گراف ۴ × ۴-شبکه[۴] یک گراف قویاً منظم با پارامتر $(۱۶, ۶, ۲, ۲)$ است که یکریخت با $K_۴ \times K_۴$ است. در گراف ۴ × ۴-شبکه، راس‌ها، زوج‌های (i, j) هستند که $i, j \in \{۰, ۱, ۲, ۳\}$ و بعلاوه زوج‌های (i, j) و (i', j') مجاورند اگر و تنها اگر $i = i'$ یا $j = j'$. از طرف دیگر **گراف شریخانده**[۵] شکل (۲.۲) یک گراف قویاً منظم با پارامترهای $(۱۶, ۶, ۲, ۲)$ است. اما بنابر مثال (۱۲.۲) از مرجع [۴]، گراف‌های ۴ × ۴-شبکه و شریخانده یکریخت نیستند.

تعریف ۵.۱.۲ به گراف قویاً منظم با پارامترهای $SRG(۲۷, ۱۶, ۱۰, ۸)$، **گراف اشلافلی**[۶] گوییم. این گراف به شکل (۳.۲) است. همچنین گراف قویاً منظم با پارامترهای $SRG(۲۷, ۱۶, ۱۰, ۸)$ منحصر به فرد است.

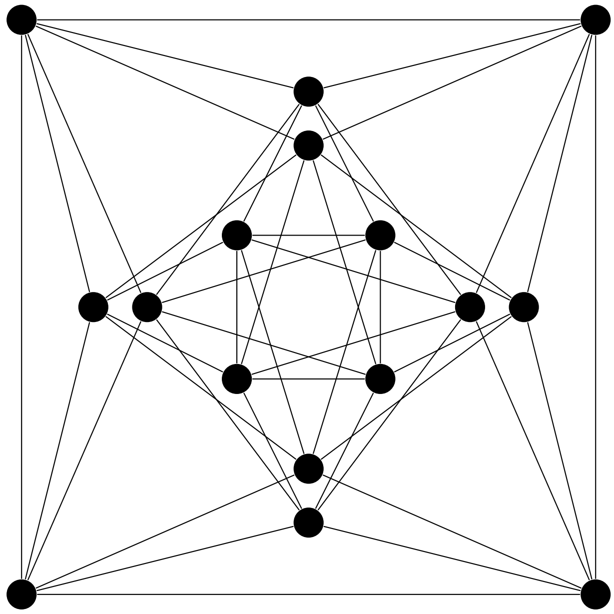
گزاره ۶.۱.۲ گراف Γ یک گراف قویاً منظم با پارامترهای (v, k, λ, μ) است اگر و تنها اگر متمم آن $\overline{\Gamma}$ یک گراف قویاً منظم با پارامترهای $(v, v-k-۱, v-۲k+\mu-۲, v-۲k+\lambda)$ باشد.

اثبات. فرض کنید $\overline{\Gamma}$ متمم گراف Γ باشد. درجه‌ی هر راس $\overline{\Gamma}$ برابر $v-k-۱$ است. نخست نشان می‌دهیم تعداد راس‌های مجاور با دو راس مجاور برابر $۲-۲k+\mu-$ است. اگر x و y دو راس مجاور در $\overline{\Gamma}$ باشند، آن‌گاه x و y در Γ غیر مجاورند. هر راس z که با x و y در $\overline{\Gamma}$ مجاور باشد در Γ با x و y غیر مجاور است.

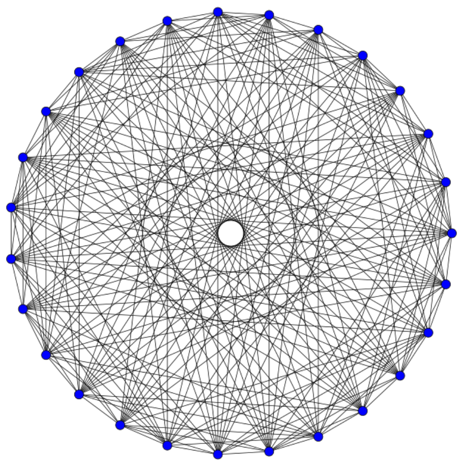
[۳]pentagon

[۵]Shrikhande graph

[۶]Schlafli graph



شکل ۲.۲: گراف شریخانده



شکل ۳.۲: گراف اشلافلی

راس‌های x و y در Γ هر کدام با k راس مجاور هستند. پس از v، $2k$ را کم می‌کنیم، اما چون راس‌های مجاور با هر دو را دو بار کم کردیم و تعداد راس‌های مجاور با راس‌های غیر مجاور x و y در Γ برابر μ است، لذا μ را اضافه کردیم. در نتیجه تعداد راس‌های مجاور با دو راس x و y در $\overline{\Gamma}$ برابر $v - 2k + \mu - 2$ است. حال نشان می‌دهیم تعداد راس‌های مجاور با دو راس غیرمجاور برابر $v - 2k + \lambda =$ است. اگر x و y دو راس غیر مجاور در $\overline{\Gamma}$ باشند، آن‌گاه راس‌های x و y در Γ مجاور هستند. هر راس z که با x و y در $\overline{\Gamma}$ مجاور باشد، با x و y در Γ غیر مجاور است. تعداد راس‌های غیر مجاور با x و y در Γ برابر $v - 2k + \lambda$ است. در نتیجه تعداد راس‌های مجاور با دو راس غیرمجاور برابر $v - 2k + \lambda =$ است. ■

تعریف ۷.۱.۲ **گراف خطی** وابسته به گراف Γ، گراف $L(\Gamma)$ است، به طوری که یال‌های Γ راس‌های $L(\Gamma)$

هستند و دو راس در $L(\Gamma)$ مجاور هستند اگر و تنها اگر یال‌های متناظر با آن‌ها در Γ در یک راس مجاور باشند.

تعریف ۸.۱.۲ **گراف کامل**، گراف ساده‌ای است که هر دو راس در آن مجاورند. گراف کامل m راسی را با K_m نمایش می‌دهند.

تعریف ۹.۱.۲ گراف خطی گراف کامل m راسی را **گراف مثلثی**[۷] گوییم و آن را با $T(m)$ نشان می‌دهیم.

با توجه به بخش (۴.۱) از مرجع [۸] نشان می‌دهیم گراف مثلثی یک گراف قویاً منظم با پارامترهای $(\frac{۱}{۲}m(m-۱), ۲(m-۲), m-۲, ۴)$ است. ابتدا نشان می‌دهیم λ برابر $m-۲$ است، فرض کنید x و y دو راس مجاور در $T(m)$ باشند، لذا یال‌های x و y در راسی چون z در K_n مجاورند. در این صورت هر راس که مجاور با x و y در $T(m)$ باشد، یالی بوده که با یال‌های x و y در K_n مجاور بوده است. تعداد یال‌ها در K_n که با x و y مجاور هستند برابر است با $(m-۳)+۱ = m-۲$. ولی $m-۳$ برابر تعداد یال‌هایی است که با x و y در راس z در K_n مجاورند و مقدار ۱ آن یالی است که راس‌های u و v را به هم وصل می‌کند، جایی که u راسی است که توسط یال x به راس z وصل شده است و v راسی است که توسط یال v به راس z وصل شده است. بعلاوه μ برابر ۴ است، زیرا دو راس غیر مجاور در $T(m)$ دو یال غیر مجاور در K_n هستند. تعداد یال‌های مجاور با دو یال غیر مجاور در K_n برابر ۴ است، لذا تعداد راس‌های مجاور با دو راس غیر مجاور در $T(m)$ برابر ۴ است. در نتیجه $\mu = ۴$.
برای مثال $T(۵)$ یک گراف قویاً منظم با پارامترهای $(۱۰, ۶, ۳, ۴)$ است. متمم $T(۵)$ گراف قویاً منظم با پارامترهای $(۱۰, ۳, ۰, ۱)$ است. به $\overline{T(۵)}$ گراف پترسن [۸] گوییم(۴.۲).

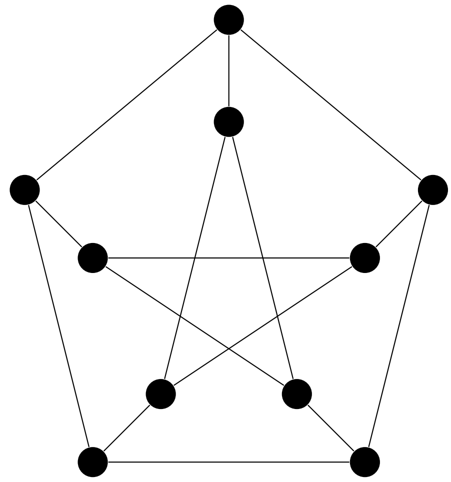
۲.۲ مقادیر ویژه

فرض کنید Γ یک گراف باشد. ماتریس مجاورت گراف Γ برابر ماتریسی مانند $A = [a_{ij}]$ است، به طوری‌که $a_{ij} = ۱$، اگر راس i و راس j مجاور باشند. در غیر این صورت $a_{ij} = ۰$. برای گراف‌های k منظم داریم $A1 = k1$. لذا برای گراف k-منظم، k یک مقدار ویژه ماتریس مجاورت A است. برای اطلاعات بیشتر به مرجع [۶] مراجعه فرمایید.

قضیه ۱.۲.۲ فرض کنید Γ یک گراف قویاً منظم از درجه‌ی k باشد. در این صورت گزاره‌های زیر برقرار هستند:

[۷] Triangular Graph

[۸] Petersen Graph



شکل ۴.۲: گراف پترسن

۱) k یک مقدار ویژه است.

۲) اگر Γ همبند باشد آن‌گاه چندگانگی k برابر ۱ است.

۳) برای هرمقدار ویژه λ از Γ داریم $|\lambda| \leq k$.

اثبات. ۱) واضح است.

۲) فرض کنید $x = [x_1, x_2, \cdots, x_v]^T$ یک بردار ویژه غیر صفر برای مقدار ویژه k باشد. فرض کنید x_j در x دارای بیشترین مقدار قدر مطلق باشد، یعنی برای هر $1 \leq i \leq v$، $|x_i| \leq |x_j|$. چون $(Ax)_j = kx_j$، داریم

$$\sum_{i=1}^{v} a_{j,i} x_i = kx_j. \tag{1.2}$$

در سمت چپ معادله اخیر سطر jام A را در x ضرب کردیم، حاصل‌ضرب برابر جمع روی k راس v_i مجاور با v_j است. با توجه به ماکزیمم بودن x_j، برای تمام راس‌های مجاور x_j داریم، $x_i = x_j$. اگر Γ همبند باشد با ادامه دادن این فرایند روی دیگر x_iها نتیجه می‌گیریم که همه مقادیر x با هم معادل هستند، لذا x مضربی از 1 است. پس فضای بردار ویژه مرتبط با مقدار k دارای بعد ۱ است.

۳) فرض کنید $Ay = \lambda y \neq 0$ و y_i دارای بزرگ‌ترین مقدار قدر مطلق در y باشد. با توجه به (۱.۲) داریم $\sum_{i=1}^{v} a_{j,i} x_i = kx_j$. پس

$$|\lambda||y_i| = |\sum_{i=1}^{k} y_i| = \sum_{i=1}^{k} |y_i| \leq k|y_i|.$$

در نتیجه $|\lambda| \leq k$. ■

تعریف ۲.۲.۲ مقدار ویژه λی مخالف k را تحدید شده[۹] گوییم، اگر بردار ویژه مقدار ویژه λ عمود بر بردار 1 باشد، یعنی حاصل‌ضرب داخلی بردار ویژه متناظر با λ در 1 برابر صفر شود.

لم ۳.۲.۲ برای گراف همبند k-منظم، مقادیر ویژه تحدید شده، مقادیر ویژه متفاوت با k هستند.

اثبات. فرض کنید ρ یک مقدار ویژه متفاوت با k برای گراف k-منظم Γ با ماتریس مجاورت A باشد. فرض کنید y بردار ویژه ρ باشد. داریم $A1 = k1$ و $Ay = \rho y$. لذا

$$A1 = k1 \Rightarrow y^T A1 = y^T k1 \Rightarrow \rho y^T 1 = k y^T 1.$$

چون $k \neq \rho$، تساوی آخر در معادله اخیر نتیجه می‌دهد $y^T 1 = ۰$، لذا y بر 1 عمود است. ■

قضیه ۴.۲.۲ برای گراف ساده همبند غیر کامل وغیر تهی Γ از مرتبه‌ی v، با ماتریس مجاورت A شرایط زیر معادلند؛

۱) Γ یک گراف قویاً منظم با پارامترهای (v, k, λ, μ) است.

۲) برای مقادیر حقیقی λ و μ و k داریم، $A^۲ = (\lambda - \mu)A + (k - \mu)I + \mu J$.

۳) Aدقیقاً دو مقدار ویژه تحدید شده دارد.

اثبات. ابتدا توجه می‌کنیم که معادله‌ی $A^۲ = (\lambda - \mu)A + (k - \mu)I + \mu J$ را می‌توان به صورت زیر نوشت

$$A^۲ = kI + \lambda A + \mu(J - I - A). \qquad (۲.۲)$$

با توجه به قضیه‌ی (۲.۲) از مرجع [۶] داریم:
(۱) ⇐ (۲) چون A ماتریسی متقارن است، لذا حاصل‌ضرب سطر iام A در ستون jام A برابر حاصل‌ضرب سطر iام در سطر jام A است. حاصل‌ضرب سطر iام در سطر i برابر k است. اگر راس iام و راس jام مجاور باشند، آن‌گاه حاصل‌ضرب سطر iام در سطر jام برابر λ است و اگر سطر iام و سطر jام غیر مجاور باشند، آن‌گاه حاصل‌ضرب سطر iام در سطر jام برابر μ است. در نتیجه $A^۲$ به صورت معادله (۲.۲) است.
(۲) ⇐ (۱) واضح است.
(۲) ⇐ (۳) فرض کنید ρ یک مقدار ویژه تحدید شده باشد و u بردار ویژه متناظر با ρ و عمود بر 1 باشد. پس

[۹] restricted