



دانشگاه صنعتی شاهرود

دانشکده علوم ریاضی

گروه ریاضی محض

پایان نامه

برای دریافت درجه کارشناسی ارشد در رشته

ریاضی ، گرایش جبر

عنوان

ویژگی‌های گراف‌های کیلی یکانی

استاد راهنما

دکتر حیدر جعفری

استاد مشاور

دکتر نادر جعفری راد

پژوهشگر

عفت کوشکی

۱۳۹۲

نام خانوادگی دانشجو: کوشکی		نام: عفت
عنوان: ویژگی‌های گراف‌های کیلی یکانی		
استاد راهنما: دکتر حیدر جعفری استاد مشاور: دکتر نادر جعفری راد		
مقطع تحصیلی: کارشناسی ارشد	رشته: ریاضی	گرایش: جبر
دانشگاه: صنعتی شاهرود تاریخ فارغ‌التحصیلی: ۱۳۹۲		دانشکده علوم ریاضی تعداد صفحات: ۷۳
واژگان کلیدی: گراف‌های کیلی یکانی، مقادیر ویژه گراف، ماتریس‌های دوری، خودریختی گرافی، قطر، همسایه مشترک، عدد خوشه و عدد رنگی گراف، همبندی و تقارن گراف،		
چکیده در این پایان‌نامه، گراف‌های کیلی یکانی را تعریف می‌کنیم و به بررسی تعدادی از ویژگی‌های این گراف می‌پردازیم. در ابتدا تعاریف و مفاهیم مقدماتی را بیان می‌کنیم. در بخش اول فصل دوم، بعضی از قضایا که در گراف‌ها برقرار است را بیان می‌کنیم و در بخش دوم این فصل، عدد رنگی، عدد خوشه، عدد استقلال، قطر و تعداد مثلث‌های گراف X_n را به دست می‌آوریم و نشان می‌دهیم X_n متقارن و همبندی راسی برابر با $\varphi(n)$ می‌باشد. در فصل سوم با استفاده از خاصیت دوری و متقارن بودن ماتریس‌های گراف‌های کیلی یکانی مقادیر ویژه این گراف‌ها را محاسبه می‌کنیم و سرانجام در فصل آخر اندازه خودریختی‌های این گراف‌ها را محاسبه می‌نماییم. این پایان‌نامه بر اساس مقاله [۶] و [۱۹] تهیه و تدوین شده است.		

تقدیم به همه آشنایی که

می خوانند بیشتر بدانند

خدایا...^۱

به من زیستنی عطا کن که در لحظه مرگ، بر بی‌ثمری لحظه‌ای که برای زیستن گذشته است، حسرت نخورم و مُردنی عطا کن که بر بیهودگیش، سوگوار نباشم. بگذار تا آن را، خود انتخاب کنم، اما آنچنان که تو دوست می‌داری.

تو می‌دانی و همه می‌دانند که شکنجه دیدن بخاطر تو، زندانی کشیدن بخاطر تو و رنج بردن به پای تو تنها لذت بزرگ زندگی من است، از شادی توست که من در دل می‌خندم، از امید رهایی توست که برق امید در چشمان خسته‌ام می‌درخشد و از خوشبختی توست که هوای پاک سعادت را در ریه‌هایم احساس می‌کنم. نمی‌توانم خوب حرف بزنم. نیروی شگفتی را که در زیر کلمات ساده و جمله‌های ضعیف و افتاده، پنهان کرده‌ام دریاب، دریاب.

تو می‌دانی و همه می‌دانند که زندگی از تحمیل لبخندی بر لبان من، از آوردن برق امیدی در نگاه من، از برانگیختن موج شعفی در دل من، عاجز است.

تو، چگونه زیستن را به من بیاموز، چگونه مردن را خود خواهم آموخت.

به من توفیق تلاش در شکست، صبر در نومیدی، رفتن بی‌همراه، جهاد بی‌سلاح، کار بی‌پاداش، فداکاری در سکوت، دین بی‌دنیا، مذهب بی‌عوام، عظمت بی‌نام، خدمت بی‌نان، ایمان بی‌ریا، خوبی بی‌نمود، گستاخی بی‌خامی، قناعت بی‌غرور، عشق بی‌هوس، تنهایی در انبوه جمعیت، و دوست داشتن بی‌آنکه دوست بداند، روزی کن.

^۱مناجاتی از دکتر علی شریعتی.

سپاس‌گزاری...

سپاس خداوندگار حکیم را که با لطف بی‌کران خود، آدمی را زیور عقل آراست.
در آغاز وظیفه خود می‌دانم از زحمات بی‌دریغ استاد راهنمای خود، جناب آقای دکتر سید حیدر جعفری، صمیمانه تشکر و قدردانی کنم که قطعاً بدون راهنمایی‌های ارزنده ایشان، این مجموعه به انجام نمی‌رسید.
از جناب آقای دکتر نادر جعفری راد که زحمت مطالعه و مشاوره این رساله را تقبل فرمودند و در آماده سازی این رساله، به نحو احسن اینجانب را مورد راهنمایی قرار دادند، کمال امتنان را دارم.
در پایان، بوسه می‌زنم بر دستان خداوندگاران مهر و مهربانی، پدر و مادر عزیزم و بعد از خدا، ستایش می‌کنم وجود مقدس‌شان را و تشکر می‌کنم از دوستان عزیزم به پاس عاطفه سرشار و گرمای امیدبخش وجودشان، بهترین پشتیبان من بودند.

عفت‌کوشی

۱۳۹۲

فهرست مطالب

۱	تعاریف و مفاهیم اولیه	۱
۲	۱.۱ مفاهیمی از گراف‌ها	۲
۹	۲.۱ گراف کیلی	۹
۱۱	۳.۱ مفاهیمی از نظریه اعداد	۱۱
۱۳	۴.۱ مفاهیمی از ترکیبات	۱۳
۱۴	۵.۱ مفاهیمی از گروه‌ها	۱۴
۱۵	۲ ویژگی گراف‌ها و گراف‌های کیلی یکانی	۱۵
۱۶	۱.۲ ویژگی گراف‌ها	۱۶
۲۲	۲.۲ گراف‌های کیلی یکانی	۲۲
۴۲	۳ مقادیر ویژه گراف‌های کیلی یکانی	۴۲
۴۳	۱.۳ مقادیر ویژه گراف‌های کیلی یکانی	۴۳
۵۵	۴ گروه خودریختی‌های گراف‌های کیلی یکانی	۵۵
۵۶	۱.۴ گروه خودریختی‌های گراف‌های کیلی یکانی	۵۶
۶۴	مراجع	۶۴

فصل ۱

تعاريف و مفاهيم اوليه

۱.۱ مفاهیمی از گراف‌ها

تذکر ۱.۱.۱. تعاریف و قضایای این بخش از مرجع [۱]، گرفته شده‌اند.

تعریف ۲.۱.۱. گراف G ، یک سه‌تایی مرتب $(V(G), E(G), \psi(G))$ است که تشکیل شده از یک مجموعه‌ی ناتهی $V(G)$ از راس‌ها، یک مجموعه‌ی $E(G)$ از یال‌ها و یک تابع وقوع $\psi(G)$ که به هر یال G ، یک زوج نامرتب از رأس‌های G را نسبت می‌دهد.

تعریف ۳.۱.۱. یال با دو انتهای یکسان را طوقه^۱ می‌نامیم.

تعریف ۴.۱.۱. یک یال را چندگانه^۲ می‌نامیم هرگاه بین دو راس بیشتر از یک یال وجود داشته باشد.

تعریف ۵.۱.۱. یک گراف، ساده^۳ است اگر هیچ طوقه‌ای نداشته باشد و بین هر دو رأس آن، بیش از یک یال نباشد.

تعریف ۶.۱.۱. گرافی که مجموعه یالهای آن تهی و مجموعه رأس آن تنها دارای یک رأس باشد، گراف بدیهی^۴ می‌نامیم.

تذکر ۷.۱.۱. از این به بعد گراف‌ها را ساده و بدون جهت در نظر می‌گیریم و عناصر $e \in E(G)$ را با مجموعه $\{u, v\}$ یا uv نمایش می‌دهیم که u و v دو انتهای یال e می‌باشند.

تعریف ۸.۱.۱. برای راس v از G ، مجموعه‌ی تمام راس‌هایی از G که با v مجاورند را با $N(v)$ نمایش می‌دهیم. به عبارت دیگر

$$N(v) = \{u \in V(G) : uv \in E(G)\}.$$

تعریف ۹.۱.۱. تعداد رئوسی که با راس v مجاورند را درجه^۵ ی راس v می‌نامیم و با $d_G(v)$ نمایش می‌دهیم. کمترین و بیشترین درجه‌ی رأس‌های G را به ترتیب با $\delta(G)$ و $\Delta(G)$ نمایش می‌دهیم.

^۱ Loop

^۲ Multiply

^۳ Simple

^۴ Evident

^۵ Degree

تعریف ۱۰.۱.۱. مرتبه^۶ G تعداد رأس‌های G است و با $|V(G)|$ نمایش می‌دهیم.

تعریف ۱۱.۱.۱. گراف‌های G_1 و G_2 ، **یکریخت**^۷ می‌نامیم (و می‌نویسیم $G_1 \cong G_2$)، اگر یک تابع یک به یک مانند ψ از $V(G_1)$ به روی $V(G_2)$ وجود داشته باشد به طوری که

$$uv \in E(G_1) \iff \psi(u)\psi(v) \in E(G_2).$$

تعریف ۱۲.۱.۱. **خودریختی**^۸ گراف یک یکریختی از گراف به‌روی خودش است. خودریختی‌های گراف G تحت عمل ترکیب توابع تشکیل یک گروه می‌دهیم که به آن گروه خودریختی‌های گراف می‌گوییم و با $Aut(G)$ نشان می‌دهیم. خودریختی در گراف‌های ساده را می‌توان به‌صورت جایگشتی روی مجموعه رئوس گراف که مجاورت را حفظ می‌کند نیز در نظر گرفت.

تعریف ۱۳.۱.۱. فرض کنیم x, y, u و v رئوسی دلخواه از گراف G باشند و x به y و u به v مجاور باشند در این صورت اگر خودریختی σ وجود داشته باشد به طوری که $\sigma(x) = u$ و $\sigma(y) = v$ ، آنگاه گراف G **متقارن**^۹ است.

تعریف ۱۴.۱.۱. گراف G را **یال-تراپا**^{۱۰} می‌نامیم هرگاه برای هر دو یال $xy, uv \in E(G)$ خودریختی σ از G وجود داشته باشد به طوری که یکی از شرایط $\sigma(x) = u$ و $\sigma(y) = v$ یا $\sigma(x) = v$ و $\sigma(y) = u$ برقرار باشد.

تعریف ۱۵.۱.۱. گراف G' را یک **زیر گراف**^{۱۱} G می‌گوییم (می‌نویسیم $G' \subseteq G$)، اگر $V(G') \subseteq V(G)$ ، $E(G') \subseteq E(G)$ و $\psi(G')$ از محدود کردن $\psi(G)$ به $E(G')$ حاصل شده باشد.

تعریف ۱۶.۱.۱. فرض کنید V' ، یک زیر مجموعه‌ی ناتهی از $V(G)$ باشد. زیر گرافی از G که مجموعه‌ی رأس‌های آن V' و مجموعه‌ی یال‌هایش برابر مجموعه‌ی همه‌ی یال‌هایی از G باشد که هر دو سر آن‌ها در V'

^۶ Order

^۷ Isomorph

^۸ Automorphism

^۹ Symetric

^{۱۰} Edge-transitive

^{۱۱} Subgraph

واقع است، زیر گراف القا شده توسط V' می‌نامیم و با $G[V']$ نمایش می‌دهیم. همچنین می‌گوییم $G[V']$ یک زیر گراف القایی^{۱۲} G است.

تعریف ۱۷.۱.۱. دنباله‌ی ناتهی $W = v_0 e_1 v_1 e_2 v_2 \dots e_k v_k$ که جمله‌های آن به طور متناوب راس‌ها و یال‌ها هستند را یک مسیر^{۱۳} می‌نامیم هرگاه یال‌های $e_1, \dots, e_k$ و راس‌های $v_0, \dots, v_k$ متمایز باشند و برای $1 \leq i \leq k$ ، دو انتهای e_i ، v_{i-1} و v_i باشند. راس‌های v_0 و v_k را به ترتیب مبدا و انتهای W و $v_1, \dots, v_{k-1}$ را راس‌های داخلی آن می‌نامیم. عدد صحیح k را طول W می‌نامیم.

تعریف ۱۸.۱.۱. مسیری که دارای طول مثبت و مبدا و انتهای آن یکی باشد را یک دور^{۱۴} می‌نامیم.

تعریف ۱۹.۱.۱. یک مسیر ماکسیمال^{۱۵} است هرگاه نتوان آن را از دو طرف ادامه داد.

تعریف ۲۰.۱.۱. دور را فرد(زوج)^{۱۶} می‌نامیم هرگاه طول آن فرد(زوج) باشد. هر دور به طول k را k -دور می‌نامیم و با C_k نمایش می‌دهیم.

تعریف ۲۱.۱.۱. هر دور به طول ۳ در گراف G را یک مثلث^{۱۷} می‌نامیم.

تعریف ۲۲.۱.۱. دوری که شامل تمام رئوس گراف G باشد را دور همیلتنی^{۱۸} می‌نامیم.

تعریف ۲۳.۱.۱. گراف G را همبند^{۱۹} می‌گوییم هرگاه بین هر دو راس دلخواه u و v از G ، مسیری در G موجود باشد. در غیر این صورت G را ناهمبند می‌نامیم.

تعریف ۲۴.۱.۱. یالی که دو راس غیر مجاور در یک دور از گراف G را به هم وصل می‌کند را وتر^{۲۰} می‌نامیم.

^{۱۲}Induced Subgraph

^{۱۳}Path

^{۱۴}Cycle

^{۱۵}maximal

^{۱۶}Odd(Even)

^{۱۷}Tringle

^{۱۸}Hamilton cycle

^{۱۹}Connected

^{۲۰}Chord

تعریف ۲۵.۱.۱. دور القایی در گراف G که هیچ وتري نداشته باشد را حفره^{۲۱} می‌نامیم.

تعریف ۲۶.۱.۱. گراف ساده‌ای با مجموعه رئوس گراف G که در آن دو راس مجاورند اگر و تنها اگر آن راس‌ها در G مجاور نباشند را مکمل^{۲۲} گراف G می‌نامیم و با $\bar{G}$ نمایش می‌دهیم.

تعریف ۲۷.۱.۱. زیر گراف G' از گراف G را پادحفره^{۲۳} می‌نامیم هرگاه مکمل حفره در G باشد.

تعریف ۲۸.۱.۱. (فرض کنید مجموعه رئوس یک گراف، به چند مجموعه چنان تقسیم شود که حداقل از یک راس یکی به هیچ یک از راسهای دیگر مجموعه‌ها، مسیری وجود نداشته باشد، آنگاه گراف از قطعاتی تشکیل شده است. این قطعات را مولفه‌های گراف می‌نامیم.) یک زیر گراف همبند ماکسیمال از گراف G را یک مولفه^{۲۴} از گراف G می‌نامیم.

تعریف ۲۹.۱.۱. اگر u و v در G متصل باشند، طول کوتاه‌ترین مسیر بین u و v در G را فاصله^{۲۵} u و v در G ، می‌نامیم و با $d(u, v)$ نشان می‌دهیم.

تعریف ۳۰.۱.۱. ماکزیمم فاصله در گراف G را قطر^{۲۶} G می‌نامیم و با $diam(G)$ نشان می‌دهیم.

تعریف ۳۱.۱.۱. گراف ساده G را خود مکمل^{۲۷} می‌نامیم هرگاه در شرط $G \cong \bar{G}$ صدق کند.

تعریف ۳۲.۱.۱. گراف G را که درجه‌ی هر راس آن k باشد k -منظم^{۲۸} می‌نامیم.

تعریف ۳۳.۱.۱. گراف G را کامل^{۲۹} می‌نامیم هرگاه هر دو راس متمایز آن مجاور باشند. گراف کامل با n

راس را با K_n نمایش می‌دهیم.

^{۲۱} Holed

^{۲۲} Complement

^{۲۳} Anti holed

^{۲۴} Component

^{۲۵} Distance

^{۲۶} Diameter

^{۲۷} Self-Complement

^{۲۸} K -regular

^{۲۹} Complete

تعریف ۳۴.۱.۱. فرض کنیم G یک گراف باشد زیر مجموعه H از رئوس G را یک خوشه^{۳۰} می نامیم هر گاه زیر گراف القایی از H یک گراف کامل باشد. اندازه بزرگترین مجموعه القا کننده یک خوشه در گراف G را عدد خوشه‌ای^{۳۱} G می نامیم و با $\omega(G)$ نشان می دهیم.

تعریف ۳۵.۱.۱. گراف G را k -رنگ پذیر^{۳۲} گوئیم، در صورتی که بتوان هر یک از k رنگ را به یکی از رئوس آن تخصیص داد، به طوری که هیچ دو راس مجاور هم رنگ نباشند. اگر G با کمتر از k رنگ قابل رنگ آمیزی نباشد، G را k -رنگی^{۳۳} می گوئیم، یا بطور معادل گوئیم عدد رنگی^{۳۴} G یعنی $\chi(G)$ برابر k است.

تعریف ۳۶.۱.۱. کمترین تعداد رنگ هایی که بتوان یال های گراف G را رنگ آمیزی کرد به طوری که هیچ دو یال مجاور یک رنگ نباشند را عدد رنگی یالی^{۳۵} گراف G می نامیم و با $\chi'(G)$ نمایش می دهیم.

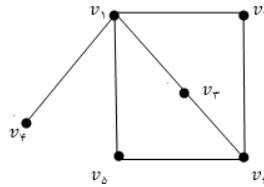
تعریف ۳۷.۱.۱. زیر مجموعه S از $V(G)$ را یک مجموعه ی مستقل^{۳۶} می نامیم هرگاه هیچ دو راسی از S در G مجاور نباشد. ماکزیمم مرتبه یک مجموعه ی مستقل در G را عدد استقلال^{۳۷} G می نامیم و آن را با $\alpha(G)$ نشان می دهیم.

تعریف ۳۸.۱.۱. گراف G را دو بخشی^{۳۸} می نامیم هرگاه مجموعه رئوس آن را بتوان به دو قسمت X و Y افراز کرد به طوری که هر یال یک انتها در X و یک انتها در Y داشته باشد. چنانچه هر راس از X به هر راس از Y وصل باشد G را گراف دو بخشی کامل می نامیم و معمولا با $K_{r,s}$ نشان می دهیم که در آن r و s به ترتیب تعداد رئوس در X و Y است.

مثال ۳۹.۱.۱. گراف زیر با مجموعه رئوس $V(G) = v_1, v_2, \dots, v_6$ دو بخشی است. چون $V(G)$ را

^{۳۰} Clique^{۳۱} Clique number^{۳۲} K -Colourable^{۳۳} K -chromatic^{۳۴} Chromatic number^{۳۵} Edge chromatic number^{۳۶} Independent set^{۳۷} Independent number^{۳۸} Bipartite

می‌توان به زیر مجموعه‌های $V_1 = \{v_1, v_6\}$ ، $V_2 = \{v_2, v_3, v_4, v_5\}$ افراز کرد. همچنین هر یال G راس‌های این دو مجموعه را به هم وصل می‌کند.



تعریف ۴۰.۱.۱. مینیم تعداد یال‌هایی که با حذف آن‌ها از گراف G یک گراف ناهمبند یا بدیهی حاصل شود را **همبندی یالی**^{۳۹} در گراف G می‌نامیم و آن را با $\lambda(G)$ نمایش می‌دهیم.

تعریف ۴۱.۱.۱. مینیم تعداد راس‌هایی که با حذف آن‌ها از گراف G یک گراف ناهمبند یا بدیهی حاصل شود را **همبندی راسی**^{۴۰} در گراف G می‌نامیم و آن را با $k(G)$ نمایش می‌دهیم.

تعریف ۴۲.۱.۱. زیر مجموعه V از مجموعه یال‌های گراف همبند G را **مجموعه برشی یالی**^{۴۱} G می‌نامیم هرگاه $G - V$ ناهمبند باشد.

تعریف ۴۳.۱.۱. زیر مجموعه S از مجموعه راسی G را **مجموعه برشی راسی**^{۴۲} G می‌نامیم هرگاه $G[V(G) - S]$ ناهمبند باشد.

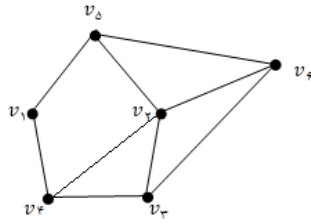
مثال ۴۴.۱.۱. همانطور که در شکل ۱.۱ و ۲.۱ می‌بینیم، در گراف G ، S و U به ترتیب مجموعه برشی یالی و مجموعه برشی راسی G هستند، که در آن $S = \{v_1, v_2, v_3\}$ ، $U = \{v_1v_5, v_2v_5, v_2v_6, v_3v_6\}$.

^{۳۹} Edge connectivity

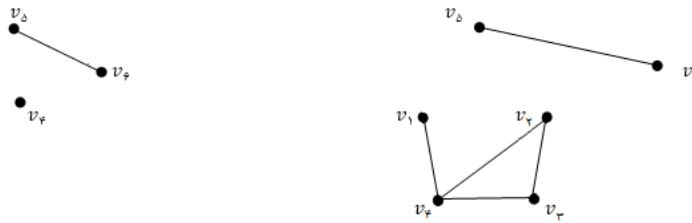
^{۴۰} Vertex connectivity

^{۴۱} Edge cut

^{۴۲} Vertex cut



شکل ۱.۱: گراف G



شکل ۲.۱: در شکل سمت راست گراف $G - U$ و در سمت چپ گراف $G - S$ را می‌بینید.

تعریف ۴۵.۱.۱. مجموعه S از یال‌های گراف G را **جداساز**^{۴۳} دو راس u و v در G می‌نامیم هرگاه $G[V(G) - S]$ یک گراف ناهمبند باشد به طوری که u و v در مولفه‌های متفاوت قرار گیرند. به عبارت دیگر S ، u و v را جدا می‌کند هرگاه $G - S$ شامل هیچ $u - v$ مسیر نباشد.

تعریف ۴۶.۱.۱. دو $u - v$ مسیر Q_1 و Q_2 از گراف G را **یال-مجزا**^{۴۴} می‌نامیم هرگاه Q_1 و Q_2 هیچ یال مشترکی نداشته باشند.

تعریف ۴۷.۱.۱. مسیرهای Q_1 و Q_2 با دو انتهای u و v ، به طور **داخلی مجزا**^{۴۵} هستند هرگاه $V(Q_1) \cap V(Q_2) = \{u, v\}$.

تعریف ۴۸.۱.۱. اگر گراف G همبند و شامل یال e باشد به طوری که $G - e$ ناهمبند شود. e را یک **پل**^{۴۶} از G می‌نامیم.

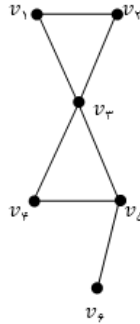
^{۴۳} Separator

^{۴۴} Edge-disjoint

^{۴۵} Internally disjoint

^{۴۶} Bridge

مثال ۴۹.۱.۱. در شکل زیر یال $e = v_5 v_6$ تنها پل گراف است.



تعریف ۵۰.۱.۱. فرض کنیم $v_1, \dots, v_n$ رئوس گراف باشند. ماتریس مجاورت^{۴۷} گراف G ماتریسی $n \times n$ مانند $A(G) = [a_{ij}]$ است که در آن a_{ij} برابر با تعداد یال‌هایی است که v_i را به v_j متصل می‌کند. فرض کنید G گرافی ساده باشد و بین v_i و v_j یالی واقع باشد آنگاه $a_{ij} = 1$ و در غیر اینصورت $a_{ij} = 0$.

۲.۱ گراف کیلی

تذکر ۱.۲.۱. تمام مطالب ارجاع داده نشده این بخش به مرجع [۹] باز می‌گردد.

فرض کنید G یک گروه متناهی با عنصر همانی 1 است و فرض کنید S یک مجموعه‌ی مولد برای G باشد با این ویژگی که $1 \notin S$ و برای هر $s \in S$ ، $s^{-1} \in S$.

تعریف ۲.۲.۱. گراف کیلی^{۴۸} $\Gamma = \text{Cay}(G, S)$ گراف ساده‌ای است که مجموعه‌ی رئوس و مجموعه‌ی یال‌های آن به‌صورت زیر می‌باشند.

$$V(\Gamma) = G \quad \text{و} \quad E(\Gamma) = \{ \{g, h\} \mid g^{-1}h \in S \}$$

لم ۳.۲.۱. گراف کیلی $\Gamma = \text{Cay}(G, S)$ یک گراف همبند است اگر و تنها اگر مجموعه S مولد G باشد.

^{۴۷}Adjacency matrix

^{۴۸}Cayley graph

برهان. ($\Leftarrow$) فرض کنید Γ یک گراف همبند باشد. بنابراین برای هر $x, y \in V(\Gamma)$ یک مسیر بین x و y در G وجود دارد. فرض کنید $x, v_1, v_2, \dots, v_n, y$ مسیری بین x و y باشد که $v_1, v_2, \dots, v_n \in G$ در این صورت $yv_n^{-1}, v_nv_{n-1}^{-1}, \dots, v_1x^{-1} \in S$. از طرفی $yx^{-1} = (yv_n^{-1})(v_nv_{n-1}^{-1}) \dots (v_1x^{-1})$ در نتیجه yx^{-1} با عناصر S تولید شده است. اگر x عنصر همانی در نظر بگیریم در نتیجه هر عنصر G توسط مجموعه S تولید می شوند.

($\Rightarrow$) فرض کنید g و h عناصر مجاور در Γ باشند. بنابراین $s_1 \in S$ وجود دارد به طوریکه $gh^{-1} = s_1$ $g = s_1h$ در نتیجه با ضرب s_1 در h به g می رسیم. بنابراین با ضرب از چپ عنصر دیگر S می توانیم به رئوس دیگر گراف برسیم. (هر راس G را می توان به صورت حاصل ضربی از عناصر S نوشت). فرض کنید $xy^{-1} \in S$ از آنجایی که S یک مجموعه مولد برای G است لذا $s_1, s_2, \dots, s_k \in S$ وجود دارند که $yx^{-1} = s_1s_2 \dots s_k \Rightarrow y = s_1s_2 \dots s_kx$ $\square$

تعریف ۴.۲.۱. فرض کنیم $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ گروه دوری جمعی و $U_n = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$ مجموعه ییکال های $\mathbb{Z}_n$ باشد. در این صورت به گراف کیلی که در آن Γ برابر با گروه جمعی $\mathbb{Z}_n$ و دارای مجموعه مولد U_n باشد را **گراف کیلی یکانی**^{۴۹} می نامیم که دارای مجموعه رئوس $V(X_n) = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ و مجموعه یال $E(X_n) = \{\{a, b\} \mid a, b \in \mathbb{Z}_n, (a-b, n) = 1\}$ است و با $X_n = \text{Cay}(\mathbb{Z}_n, U_n)$ نمایش می دهیم.

^{۴۹}Unitary Cayley graph

۳.۱ مفاهیمی از نظریه اعداد

تذکر ۱.۳.۱. تعاریف و قضایای به کار رفته در این قسمت از منبع [۲۳]، گرفته شده‌اند.

قضیه باقیمانده چینی ۲.۳.۱. فرض کنیم $b_1, b_2, \dots$ و $m_1, m_2, \dots$ اعداد صحیح و m_k اعداد طبیعی دو به دو متباین باشند. در این صورت دستگاه زیر دقیقاً یک جواب منحصر بفرد به پیمانه $m_1 m_2 \dots m_k$ دارد:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

تعریف ۳.۳.۱. تابع موبیوس را به صورت زیر تعریف می‌کنیم:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \dots p_k \text{ اگر } n \text{ خالی از مربع باشد} \\ 0 & \text{اگر } n \text{ خالی از مربع نباشد} \end{cases}$$

تعریف ۴.۳.۱. اگر n یک عدد طبیعی باشد، تعداد اعداد طبیعی کوچکتر یا مساوی n که نسبت به n اول هستند را تابع φ -اوایلر^{۵۰} می‌نامیم و با $\varphi(n)$ نمایش می‌دهیم.

تعریف ۵.۳.۱. تعداد جفت، از اعداد متوالی که هر کدام نسبت به n اول هستند را با $\varphi_2(n)$ نمایش می‌دهیم که

$$\varphi_2(n) = n \prod_{p|n} \left(1 - \frac{2}{p}\right).$$

قضیه ۶.۳.۱. اگر m, n اعداد طبیعی باشند به طوری که $(m, n) = 1$ ، آنگاه $\varphi(mn) = \varphi(m)\varphi(n)$. (اصطلاحاً می‌گوییم تابع φ ضربی است).

قضیه اساسی حساب ۷.۳.۱. هر عدد طبیعی $n \geq 1$ را می‌توان بصورت حاصلضربی از اعداد اول نمایش داد که این نوع نمایش صرف نظر از ترتیب عوامل منحصر بفرد است.

^{۵۰} Euler

مثال ۸.۳.۱. فرض کنید $m > 1$ و $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ که در آن p_i ها اعداد اول متمایز و α_i ها اعداد طبیعی هستند. چون p_i ها دو به دو نسبت به هم اول هستند لذا با استفاده پی در پی از قضیه فوق داریم:

$$\begin{aligned}\varphi(p_1^{\alpha_1} \dots p_r^{\alpha_r}) &= (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_r^{\alpha_r} - p_r^{\alpha_r-1}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r}) \\ &= n \prod_{p|n} (1 - \frac{1}{p}).\end{aligned}$$

گزاره ۹.۳.۱. فرض کنیم $m = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ و $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ که در آن p_i ها اعداد اول فرد متمایزاند و $p_1 < p_2 < \dots < p_r$ ، در این صورت اگر برای هر $1 \leq i \leq r$ ، $\beta_i \leq \alpha_i = 1$ ، آنگاه

$$n = m \Leftrightarrow \varphi(n) = \varphi(m)$$

برهان. ($\Rightarrow$) بدیهی است.

($\Leftarrow$) فرض کنیم $\varphi(n) = \varphi(m)$ و برای هر $1 \leq i \leq r$ ، $\beta_i \leq \alpha_i$ پس $\varphi(p_i^{\alpha_i}) \leq \varphi(p_i^{\beta_i}) < 1$. در نتیجه برای هر i ، $\varphi(p_i^{\beta_i}) = \varphi(p_i^{\alpha_i})$ ، لذا $p_i^{\beta_i-1}(p_i-1) = p_i^{\alpha_i-1}(p_i-1)$. اگر $\beta_i = 0$ ، آنگاه $\varphi(p_i^{\alpha_i}) = 1$ به عبارت دیگر $p_i^{\alpha_i-1}(p_i-1) = 1$ که غیر ممکن است. چون $p_i \neq 2$ بنابراین $\alpha_i = \beta_i = 1$. در نتیجه $n = m$. $\square$

لم ۱۰.۳.۱. فرض کنید که m و d اعداد طبیعی هستند و $d | m$ آنگاه تعداد اعداد صحیح

به طوری که $(k, m) = d$ برابر $\varphi(\frac{m}{d})$ است.

اگر $M = \{d_1, d_2, \dots, d_k\}$ مجموعه مقسوم علیه‌های مثبت m باشد، آنگاه

$$\sum_{d|m} \varphi(d) = m$$

برهان. گروه دوری $(\mathbb{Z}_m, +)$ را در نظر می‌گیریم. می‌دانیم برای هر d که $d | m$ ، $\mathbb{Z}_m$ فقط یک زیر گروه d

عضوی دارد و لذا $\mathbb{Z}_m$ دقیقا $\varphi(d)$ عضو از مرتبه d دارد. لذا $m = \sum_{\substack{x \in \mathbb{Z}_m \\ o(x)=d}} 1 = \sum_{d|m} \varphi(d)$. $\square$

۴.۱ مفاهیمی از ترکیبات

قانون ضرب ۱.۴.۱. فرض کنید یک دنباله به طول r رویدادهای E_1 به E_r وجود داشته باشد به طوری که

$$(1) \quad E_i \text{ می تواند به } n_i \text{ طریق رخ دهد } (i = 1, 2, \dots, r).$$

(۲) تعداد طریقی که رویداد در دنباله می تواند رخ دهد به تقدم و تاخر وقوع رویدادها در دنباله بستگی ندارد. بنابراین $(n_1) \times (n_2) \times (n_3) \times \dots \times (n_r)$ راه وجود دارد که رویداد در دنباله رخ دهند.

تعریف ۲.۴.۱. دسته X از n شی مجزا را در نظر بگیرید یک r -تبدیل از X یک ترکیب در سطری از هر r شی از X می باشد که r حداکثر برابر با n است. تعداد کل r -تبدیل با n شی ϵ مجزا با $P(n, r)$ نشان می دهیم. تعداد طریقی که یک رویداد می تواند رخ دهد به این که رویدادهای قبل آن چطور رخ داده است بستگی ندارد بنابراین با استفاده از قانون ضرب شمارش داریم:

$$P(n, r) = n(n-1)(n-2) \dots (n-r+1).$$

۵.۱ مفاهیمی از گروه‌ها

تذکر ۱.۵.۱. تمام مطالب ارجاع داده نشده این بخش به منبع [۲] باز می‌گردد.

تعریف ۲.۵.۱. گروه Γ و مجموعه‌ی ناتهی X را در نظر می‌گیریم. فرض کنید به‌ازای هر g از Γ و هر x از X ، عضو یکتایی از X که آن را با علامت $x \bullet g$ نشان می‌دهیم وجود داشته باشد به‌طوری‌که

$$(۱) \text{ به‌ازای هر } x \text{ از } X, x \bullet 1 = x$$

$$(۲) \text{ به‌ازای هر } g_1 \text{ و } g_2 \text{ از } \Gamma \text{ و هر } x \text{ از } X, x \bullet (g_1 g_2) = (x \bullet g_1) \bullet g_2.$$

در این صورت گوییم Γ بر X عمل می‌کند و $\bullet$ را عمل Γ بر X گوییم. برای سهولت در نوشتن، به‌جای $x \bullet g$ از xg استفاده می‌کنیم.

تعریف ۳.۵.۱. فرض کنیم G بر V عمل کند در این صورت برای $x \in V$ مدار x ^{۵۱} را به صورت $orb(x) = \{xg \mid g \in G\}$ نمایش می‌دهیم.

^{۵۱} Orbit

فصل ۲

ویژگی گراف‌ها و گراف‌های کیلی یکانی

در بخش اول این فصل به بیان قضایای کلی در مورد گراف‌ها که برای اثبات ویژگی‌های گراف‌های کیلی یکانی مورد استفاده قرار می‌گیرند می‌پردازیم و در بخش دوم نشان می‌دهیم X_n منظم و از درجه $\varphi(n)$ می‌باشد و عدد رنگی و عدد خوشه آن برابر با کوچکترین عامل اول n است. با استفاده از خاصیت متقارن و یال-تراپا بودن گراف X_n نشان می‌دهیم $k(X_n) = \varphi(n)$. همچنین تعداد مثلث‌های گراف‌های کیلی و تعداد همسایه‌های مشترک را برای هر یال واقع در گراف محاسبه می‌نماییم.

۱.۲ ویژگی گراف‌ها

تذکر ۱.۱.۲. تمام قضایای ذکر شده در این بخش برگرفته از مرجع [۳] می‌باشد.

تعریف ۲.۱.۲. برای دو راس u و v از گراف غیر بدیهی G بیشترین تعداد $u - v$ مسیرهای به طور داخلی مجزا در G و بیشترین تعداد $u - v$ مسیرهای یال-مجزا در G را به ترتیب با $M(u, v)$ و $M'(u, v)$ نمایش می‌دهیم.

تعریف ۳.۱.۲. فرض کنید گراف G همبند باشد، اگر $uv \notin E(G)$ ، آنگاه $k(u, v)$ کمترین تعداد راس‌هایی است که u و v را جدا می‌کند.

تعریف ۴.۱.۲. برای دو رأس مجزای u و v از گراف G کمترین تعداد یال‌هایی که u و v را جدا می‌کند را با $\lambda(u, v)$ نمایش می‌دهیم.

قضیه منگر ۵.۱.۲.^۱ فرض کنیم G یک گراف نابدیهی باشد، در این صورت برای هر دو رأس u و v از G داریم:

$$\lambda(u, v) = M'(u, v).$$

تعریف ۶.۱.۲. گراف G را n - همبند یالی می‌نامیم هرگاه $\lambda(G) \geq n$ و گراف G را n - همبند می‌نامیم هرگاه $k(G) \geq n$.

^۱Menger

نتیجه ۷.۱.۲. گراف G ، n - همبند یالی است اگر و تنها اگر هر دو راس از G حداقل با n مسیر یال-مجزا به هم وصل شوند.

برهان. فرض کنیم برای $n \geq 1$ ، $\lambda(G) \geq n$. (برهان خلف) فرض کنیم که دو راس u و v از G وجود داشته باشند که دقیقاً با l مسیر یال-مجزا که $l < n$ به هم متصل می‌شوند، لذا بنا به قضیه قبل G شامل مجموعه E از l یال است که u و v را جدا می‌کند. در نتیجه $\lambda(u, v) = l$ که یک تناقض است. برعکس، فرض کنیم هر دو راس از G حداقل با n مسیر یال-مجزا به هم وصل شوند. (برهان خلف) فرض کنیم که $\lambda(G) < n$ ، در این صورت یک مجموعه برشی یالی E با تعداد $\lambda(G)$ عضو وجود دارد. فرض کنیم u و v راس‌هایی متعلق به مولفه‌های مجزا در $G - E$ باشند. پس E مجموعه‌ای از یال‌هاست که u و v را جدا می‌کند. بنابراین $\lambda(u, v) \leq |E| = \lambda(G) < n$ که یک تناقض است. $\square$

قضیه منگر ۸.۱.۲. ^۲ فرض کنیم u و v دو راس غیر مجاور در گراف G باشند در این صورت

$$k(u, v) = M(u, v).$$

نتیجه ۹.۱.۲. برای $n \geq 1$ ، گراف G ، n - همبند است، اگر و تنها اگر هر دو راس G حداقل با n مسیر به طور داخلی مجزا به هم وصل شوند.

برهان. گراف G همبند (۱ - همبند) است اگر و تنها اگر مسیری وجود داشته باشد که هر دو راس از G را به هم وصل کند. بنابراین نتیجه برای $n = 1$ بدست می‌آید.

فرض کنیم $n \geq 2$ و G ، n - همبند باشد، در این صورت $|V(G)| \geq n + 1$. به برهان خلف، فرض کنید که G شامل دو راس u و v با حداکثر $n - 1$ مسیر به طور داخلی مجزا باشد. فرض کنیم $uv \notin E(G)$ ، در این صورت بنا به قضیه قبل مجموعه S با حداکثر $n - 1$ راس که u و v را جدا می‌کند وجود دارد. پس $G - S$ ناهمبند است و $k(G) \leq n - 1$ که غیرممکن است. حال فرض کنیم $uv \in E(G)$ ، در این صورت $G - uv$ شامل حداکثر $n - 2$ مسیر به طور داخلی مجزا است. بنا به قضیه قبل،

^۲Menger

مجموعه S با حداکثر $n - 2$ راس که u و v را در $G - uv$ جدا می‌کند، وجود دارد. فرض کنیم u و v هر دو راس‌های منفرد در $S - (G - uv)$ باشند، در این صورت $S - (G - uv)$ شامل یک مولفه سوم است. فرض کنیم $S' = S \cup \{u\}$ و دقت کنید که $G - S'$ ناهمبند است لذا $|S'| \leq n - 1$ که غیر ممکن است. بنابراین می‌توانیم فرض کنیم u یا v در $S - (G - uv)$ منفرد نیستند و u به یک مولفه غیر بدیهی از $S - (G - uv)$ تعلق دارد، در این صورت $S \cup \{u\}$ یک مجموعه برشی راسی با حداکثر $n - 1$ عضو در G است که تناقض است.

بعکس، فرض کنیم G گرافی است که هر دو راس آن با حداقل n مسیر به طور داخلی مجزا به هم وصل شده باشد. در این صورت، $V(G) \geq n + 1$ ایجاب می‌کند، به شرط کامل بودن G ، گراف G ، n - همبند باشد. ($k(G) \geq n$). حال فرض کنیم G نه کامل و نه n - همبند باشد. در این صورت G شامل یک مجموعه برشی راسی S با حداکثر $n - 1$ عنصر است. فرض کنیم u, v راس‌هایی از مولفه‌های مجزای $G - S'$ باشند. در این صورت S راس‌های u و v را جدا می‌کند. بنا به قضیه قبل، حداکثر $n - 1$ ، $u - v$ مسیر به طور داخلی مجزا در G وجود دارد که خلاف فرض است.

□

نتیجه ۱۰.۱.۲. اگر G یک گراف نا بدیهی باشد، آنگاه $\lambda(G) = \min\{\lambda(u, v) \mid v \in V(G) - \{u\}\}$

برهان. فرض کنیم u راسی از گراف نا بدیهی G از مرتبه p باشد. اگر U یک مجموعه برشی یالی از G دارای تعداد عناصر $\lambda(G)$ باشد، آنگاه u متعلق به یکی از دو مولفه $G - U$ است. فرض کنیم v راسی باشد که به مولفه دیگر $G - U$ تعلق دارد. U دو راس u و v را جدا می‌کند بنابراین $\lambda(u, v) = \lambda(G)$. در نتیجه برای هر راس u از G یک راس v از G وجود دارد به طوری که $\lambda(u, v) = \lambda(G)$. پس

$$\lambda(G) = \min\{\lambda(u, v) \mid v \in V(G) - \{u\}\}$$

□

نتیجه ۱۱.۱.۲. $k(G) = \min\{k(u, v) \mid uv \notin E(G)\}$

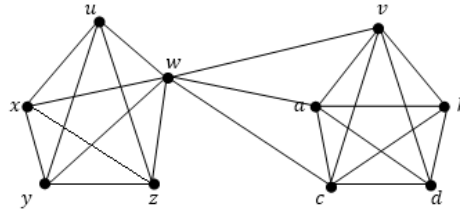
برهان. فرض کنیم مرتبه گراف G ، n و درجه هر راس آن $n - 1$ باشد. در این صورت G کامل است و $k(G) = n - 1$. فرض کنیم G کامل نباشد. اگر S یک مجموعه برشی راسی با $k(G)$ عنصر باشد، آنگاه $G - S$ ناهمبند است. فرض کنیم u و v راس‌هایی از G باشند که در مولفه‌های مجزای $G - S$ قرار دارند. در این صورت S راس‌های u, v را جدا می‌کند. بنابراین $k(u, v) \leq k(G)$. همچنین اگر S' مجموعه‌ای از $k(u, v)$ راس باشد که u, v را جدا می‌کند، آنگاه $G - S'$ ناهمبند است و $k(G) \leq k(u, v)$. پس $k(u, v) = k(G)$. بنا به قضیه ۶.۱.۲، $k(u, v) = M(u, v)$. در نتیجه دو راس غیر مجاور u, v از G وجود دارند که $k(G) = M(u, v)$. چون برای تمام جفت‌های x, y از راس‌های G ، $k(G) \leq k(x, y)$ لذا $k(G) = \min\{k(u, v) \mid uv \notin E(G)\}$. $\square$

قضیه ویتنی ۱۲.۱.۲. ^۳ برای هر گراف G ، $k(G) \leq \lambda(G) \leq \delta(G)$.

برهان. فرض کنیم v راسی از G باشد به طوری که درجه v برابر با $\delta(G)$ باشد. با حذف $\delta(G)$ یال متصل به v از G گراف G' را تولید می‌کند که v در این گراف منفرد است. بنابراین گراف G' ناهمبند یا بدیهی است. بنابراین $\lambda(G) \leq \delta(G)$. اگر $\lambda(G) = 0$ ، آنگاه گراف G ناهمبند یا بدیهی است، بنابراین $k(G) = 0$. اگر $\lambda(G) = 1$ ، آنگاه گراف G همبند و شامل یک پل است. لذا $G \cong K_2$ یا گراف G همبند و شامل حداقل یک راس برشی است. پس در هر دو حالت $k(G) = 1$. حال فرض می‌کنیم $\lambda(G) \geq 2$ و U یک مجموعه برشی یالی از G با تعداد عناصر $\lambda(G)$ باشد. فرض کنیم $e = uv$ یالی از U باشد. اگر یال‌های $U - e$ از G حذف شوند، آنگاه گراف به دست آمده H_1 ، همبند و e یک پل آن است. حال برای هر یال در $U - e$ یک راس واقع بر آن (گراف) و متمایز از u و v انتخاب می‌کنیم. اگر با حذف این راس‌ها (حداکثر $\lambda(G) - 1$) گراف ناهمبند H_2 حاصل شود، آنگاه $\lambda(G) - 1 < \lambda(G) \leq k(G)$. اگر H_2 همبند باشد، آنگاه $H_2 \cong K_2$ یا چون H_2 یک زیر گراف القایی H_1 است، زیر گراف H_2 دارای یک راس برشی است. در هر حالت، یک راس از H_2 وجود دارد که حذف آن یک گراف ناهمبند یا بدیهی را نتیجه می‌دهد. بنابراین $k(G) \leq \lambda(G)$. $\square$

^۳ Witni

مثال ۱۳.۱.۲. شکل زیر گراف G را با $k(G) = ۱$ ، $\lambda(G) = ۳$ و $\delta(G) = ۴$ نشان می‌دهد.



تعریف ۱۴.۱.۲. فرض کنیم $C(G)$ مجموعه تمام مجموعه‌های برشی G با کاردینال $k(G)$ باشد. زیرگراف

P را یک بخش^۴ از گراف G می‌نامیم هرگاه برای $C \in C(G)$ ، P یک مولفه از $G[V(G) - C]$ باشد.

تعریف ۱۵.۱.۲. فرض کنیم P یک جز بر حسب C است. $P(G) = \min_C \{ \min\{|V(P)| \mid P \text{ یک جز بر حسب } C \text{ است} \}$ که

$|C| = k(G)$. اگر $|V(P)| = P(G)$ ، آنگاه P را بخش اتومیک^۵ گراف می‌نامیم.

لم ۱۶.۱.۲. [۲۴] فرض کنیم $n \geq ۲$ و G همبند باشد، در این صورت:

$$P(G) \geq ۲.۱$$

$$k(G) < \min\{d(v) \mid v \in V(G)\}.۲$$

قضیه ۱۷.۱.۲. [۲۴] در یک گراف همبند بخش‌های اتومیک گراف، متمایز هستند.

برهان. فرض کنیم $P_۱$ و $P_۲$ دو بخش اتومیک گراف بر حسب $c_۱$ و $c_۲$ باشند و $u_۱ = V(P_۱)$ ،

$R_۱ = V(G) - (u_۱ \cup c_۱)$ ، $u_۲ = V(P_۲)$ و $R_۲ = V(G) - (u_۲ \cup c_۲)$. بنا به لم قبل داریم:

$$|R_۱| = |R_۲| \text{ و } |u_۱| = |u_۲| = P(G) \text{ و } |c_۱| = |c_۲| = K(G)$$

□

^۴Part

^۵Atomic

قضیه ۱۸.۱.۲. اگر گراف G همبند و یال-ترایا باشد، آنگاه

$$k(G) = \min\{d(v) \mid v \in V(G)\}.$$

برهان. فرض کنیم (فرض خلف)، $k(G) \neq \min\{d(v) \mid v \in V(G)\}$ ، لذا بنا به لم قبل یک بخش اتومیک مانند P با حداقل دو راس وجود دارد. چون G و P همبند هستند رئوس $x, y, z \in V(G)$ وجود دارند بطوری که $\{x, y\} \in E(P)$ و $\{x, y\} \in E(G) - E$ چون G یال ترایاست، پس $\bar{h} \in \text{Aut}(G)$ وجود دارد بطوری که $\bar{h}(x) = x$ و $\bar{h}(y) = z$ یا $\bar{h}(y) = x$ و $\bar{h}(x) = z$ ، در هر دو صورت $\bar{h}(p) \neq p$ و $\bar{h}(p) \neq \circ$ و $p \cap \bar{h}(p) \neq \circ$ که با قضیه قبل در تناقض است. چون $\bar{h}(p)$ و p ، بخش‌های اتومیک متمایز هستند. $\square$

تعریف ۱۹.۱.۲. فرض کنید $V(G)$ مجموعه رئوس و $E(G)$ مجموعه یالهای گراف G باشند، هرگاه مجموعه یال‌ها به جای زوجهای نامرتب زوجهای مرتب باشد آنگاه G را یک گراف جهتدار می‌نامیم. فرض کنید $e \in E(G)$ و u ابتدا و v انتهای e باشند، در این صورت اعضای $E(G)$ را کمان می‌نامیم و با (u, v) نمایش می‌دهیم.

تعریف ۲۰.۱.۲. [۹] یک مجموعه مرتب $[\alpha] = (\alpha_0, \alpha_1, \dots, \alpha_t)$ از $t+1$ راس گراف G که برای $1 \leq i \leq t$ ، $(\alpha_{i-1}, \alpha_i) \in E(G)$ و برای $1 \leq i \leq t-1$ ، $\alpha_{i-1} \neq \alpha_{i+1}$ را t -کمان می‌نامیم.

تعریف ۲۱.۱.۲. [۹] گراف G ، t -ترایا می‌نامیم هرگاه گروه خودریختی‌های G روی مجموعه t -کمان در G ترایا باشد، اما روی $t+1$ -کمان ترایا نباشد

نتیجه ۲۲.۱.۲. [۹] گروه خودریختی‌های G روی 1 -کمان ترایاست اگر و تنها اگر G متقارن باشد. همچنین یک گراف متقارن برای $t \geq 1$ ، t -ترایاست.

قضیه ویزینگ ۲۳.۱.۲. ^۶ فرض کنیم G یک گراف ساده باشد، در این صورت $\chi'(G) = \Delta(G) + 1$ یا

$$\chi'(G) = \Delta(G)$$

قضیه ۲۴.۱.۲. [۱] گراف G دو بخشی است اگر و تنها اگر هیچ دور فردی نداشته باشد.

^۶Vzing

۲.۲ گراف‌های کیلی یکانی

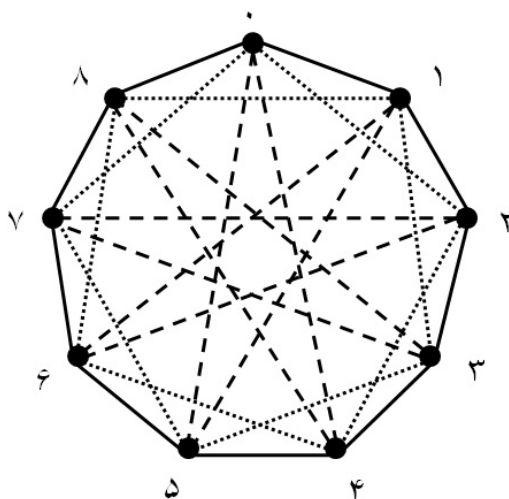
لم ۱.۲.۲. گراف‌های کیلی یکانی همبند هستند.

برهان. مجموعه رئوس گراف‌های کیلی یکانی، مجموعه $\mathbb{Z}_n$ می‌باشد. تفاضل هر دو راس متوالی نسبت به

n اول می‌باشد لذا بین هر دو راس متوالی یک یال وجود دارد لذا گراف همبند است. $\square$

ملاحظه ۲.۲.۲. گرافهای کیلی یکانی را با X_n نمایش می‌دهیم که n مرتبه گراف می‌باشد.

مثال ۳.۲.۲. گراف کیلی یکانی X_n برای $n = 9$ به صورت زیر رسم می‌شود:



گزاره ۴.۲.۲. گراف $X_n = Cay(\mathbb{Z}_n, U_n)$ ، منظم و از درجه $\varphi(n)$ است.

برهان. فرض کنیم x راسی دلخواه از گراف X_n باشد. اگر $|y - x| \in U_n$ ، آنگاه راس $y \in V(X_n)$ با راس

x مجاور است. چون $\mathbb{Z}_n$ یک گروه است، هر $y \in \mathbb{Z}_n$ را می‌توان به صورت $x + i$ نوشت که $0 < i < n$.

همچنین برای اینکه x و y مجاور باشند باید $i \neq 0$. بنابراین

$$\begin{aligned} N(x) &= \{x+i \mid 0 < i < n, (x+i-x, n) = 1\} \\ &= \{x+i \mid 0 < i < n, (i, n) = 1\} \\ &= \{x+i \mid i \in U_n\}. \end{aligned}$$

بنابراین $d(x) = |N(x)| = \varphi(n)$ و لذا حکم برقرار است. $\square$

گزاره ۵.۲.۲. فرض کنیم n مرتبه گراف باشد. اگر $n = p$ ، آنگاه گراف G کامل است و اگر $n = p^\alpha$ ، آنگاه گراف، p - بخشی کامل است.

برهان. اگر $n = p$ ، آنگاه برای هر a و b در $\mathbb{Z}_p$ ، $0 < a-b < p$ ، در نتیجه $(a-b, p) = 1$. بنابراین بین هر دو راس دلخواه از گراف X_p یک یال وجود دارد. لذا گراف حاصل گرافی کامل است. حال اگر $n = p^\alpha$ باشد، برای $0 \leq i < p$ مجموعه A_i را به صورت زیر تعریف می کنیم:

$$A_i = \{x \in \mathbb{Z}_n \mid x \equiv i \pmod{p}\} = [i].$$

برای هر $a, b \in A_i$ ، $((a-b), n) \neq 1$ در نتیجه رئوس واقع در هر مجموعه دو به دو نامجاور می باشند در نتیجه هر مجموعه، یک مجموعه مستقل در گراف می باشد. باقیمانده تقسیم هر $x \in \mathbb{Z}_n$ بر p منحصر بفرد است در نتیجه هر $x \in \mathbb{Z}_n$ دقیقاً در یکی از کلاس‌ها قرار دارد. در نتیجه

$$A_0 \cup A_1 \cup \dots \cup A_{p-1} = \mathbb{Z}_n$$

$$A_i \cap A_j = \emptyset, 0 \leq i, j < p$$

به عبارت دیگر این p مجموعه شامل تمام رئوس گراف می باشند و یک راس نمی تواند در بیش از یک مجموعه قرار گیرد در نتیجه A_i ها، یک افرازی برای رئوس گراف می باشند. فرض کنید a و b دو راس دلخواه غیر واقع در یک مجموعه باشند و $a = k_1 p + i, b = k_2 p + j$ که $0 \leq k_1, k_2 < p^{\alpha-1}$ در نتیجه

$$(k_1 p + i - (k_2 p + j), p^\alpha) = ((k_1 - k_2)p + (i - j), p^\alpha) = 1.$$

در نتیجه هر دو راس دلخواه غیر واقع در یک مجموعه مجاور هستند، در نتیجه گراف، p -بخشی و کامل است. $\square$

قضیه ۶.۲.۲. برای $n \geq 2$ ، گراف کیلی یکانی X_n دو بخشی است اگر و تنها اگر n زوج باشد.

برهان. ($\Rightarrow$) چون n زوج است عناصر یکال $\mathbb{Z}_n$ اعدادی فرد هستند. تفاضل هر دو راس فرد (زوج)، عددی زوج می باشد. بدیهی است که دو عدد زوج نسبت به هم اول نیستند بنابراین هیچ دو راس فرد (زوج) مجاور نیستند. لذا مجموعه‌ی رئوس زوج و مجموعه‌ی رئوس فرد، تشکیل دو افراز از مجموعه‌ی رئوس گراف می دهند.

($\Leftarrow$) اگر گراف دو بخشی باشد بنابر قضیه ۲۴.۱.۲، گراف دارای هیچ دور فردی نیست دنباله رئوس 0 و 1 و $\dots$ و $n-1$ و یک دور در گراف می باشند. طول این دور n می باشد چون گراف دارای دوری به طول فرد نیست در نتیجه n زوج است. $\square$

نتیجه ۷.۲.۲. اگر n زوج باشد، آنگاه X_n دارای هیچ دور با طول فرد نیست. به ویژه برای n زوج X_n بدون مثلث است.

نتیجه ۸.۲.۲. برای $n = 2^t$ گراف X_n یک گراف دو بخشی کامل $K_{2^{t-1}, 2^{t-1}}$ است. این گراف‌ها 2^{t-1} -منظم هستند و تعداد یال‌های گراف برابر با مربع درجه گراف می باشد.

برهان. بنابر گزاره ۶.۲.۲، گراف G دو بخشی کامل است و تعداد یال‌های گراف برابر با

$$\frac{2^t \times 2^{t-1}}{2} = (2^{t-1})^2$$

است. $\square$

تعریف ۹.۲.۲. فرض کنید $a, b, c \in \mathbb{Z}_n$. اگر $\pm(a-c)$ و $\pm(c-b)$ و $\pm(b-a)$ عناصر یکال $\mathbb{Z}_n$ باشند در این صورت زیر گراف القایی با رئوس a و b و c یک مثلث در X_n می باشد و با $\{a, b, c\}$ نمایش می دهیم.

تعریف ۱۰.۲.۲. مجموعه تمام مثلث‌هایی با رئوس مشترک a و b را با T_{ab} نمایش می‌دهیم. اگر $a = 0$ و $b = 1$ ، آنگاه به چنین مثلث‌هایی، مثلث‌های بنیادی می‌گوییم.

$$\text{لم ۱۱.۲.۲. برای } n \text{ های فرد، } |T_{0,1}| = \varphi_2(n) = n \prod_{p|n} \left(1 - \frac{2}{p}\right).$$

برهان. سه تایی $\{0, 1, b\}$ یک مثلث بنیادی است اگر و تنها اگر $(b-1) \in U_n$ و $b \in U_n$ اگر و تنها اگر $b-1$ و b زوج اعداد متوالی باشند که هر یک نسبت به n اول هستند. بنابراین تعداد مثلث‌های بنیادی در گراف X_n برابر است با تعداد جفت، از اعداد متوالی که هر یک از آنها نسبت به n اول باشند. در نتیجه بنابر تعریف ۵.۳.۱، $|T_{0,1}| = \varphi_2(n)$. $\square$

قضیه ۱۲.۲.۲. اگر p کوچکترین عامل اول n باشد، آنگاه زیرگراف تولید شده با راس‌های

$$\{0, 1, 2, \dots, p-1\} \text{ یک زیرگراف کامل ماکسیمال است.}$$

برهان. زیرگراف تولید شده با $0, 1, 2, \dots, p-1$ را با Ω نمایش می‌دهیم. بنابر قضیه ۵.۲.۲، زیر گراف القایی با مرتبه کوچکترین عامل اول n یک گراف کامل است. حال فرض کنیم $a \in V(X_n)$ راس دلخواهی باشد که $a \notin V(\Omega)$. نشان می‌دهیم راس a حداقل با یکی از رئوس گراف Ω مجاور نیست. به برهان خلف فرض می‌کنیم a با تمام رئوس مجاور باشد لذا

$$(a-0, n) = 1, (a-1, n) = 1, \dots, (a-p+1, n) = 1$$

که $a-1, a-2, \dots, a-p+1, p$ عدد صحیح متوالی هستند. لذا یکی از آنها بر p بخش پذیر است. بنابراین i بی وجود دارد به طوری که $(a-i, p) \neq 1$ در نتیجه $(a-i, n) \neq 1$. لذا با فرض در تناقض است. پس حکم برقرار است. $\square$

گزاره ۱۳.۲.۲. در یک گراف کامل، $\chi(K_n) = \omega(K_n) = n$.

ملاحظه ۱۴.۲.۲. چون راس‌های یک خوشه باید رنگ‌های متفاوتی داشته باشند لذا همواره $\chi(G) \geq \omega(G)$.

قضیه ۱۵.۲.۲. فرض کنیم p کوچکترین عامل اول n باشد. در این صورت:

$$\chi(X_n) = \omega(X_n) = p \cdot 1$$

$$\chi(\overline{X_n}) = \omega(\overline{X_n}) = \frac{n}{p} \cdot 2$$

برهان. فرض کنیم $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ که $2 \leq p_1 < p_2 < \cdots < p_r$ و p_i ها اعداد اول هستند.

فرض کنیم $V(\Omega) = \{0, 1, \dots, p_1 - 1\}$ مجموعه رئوس زیر گراف تولید شده با p_1 راس در گراف X_n

باشد. بنابر قضیه ۵.۲.۲، گراف Ω کامل است و بنابر گزاره ۱۳.۲.۲ $\chi(X_{p_1}) = \omega(X_{p_1}) = p_1$ در نتیجه

$$\omega(X_n) \geq p_1 \text{ با توجه به برقراری رابطه } \chi(X_n) \geq \omega(X_n) \text{، نتیجه می‌گیریم که}$$

$$\chi(X_n) \geq \omega(X_n) \geq p_1. \quad (1.2)$$

بدیهی است که برای هر $0 \leq m \leq n - 1$ ، باقیمانده m به پیمانه p_1 منحصر بفرد می‌باشد. فرض کنیم

m یک راس گراف و $m \equiv k_m \pmod{p_1}$ به راس m رنگ k_m را اختصاص می‌دهیم. فرض کنید که

$$[k_m] = \{kp_1 + k_m \mid 0 \leq k \leq n - 1, 0 \leq k_m < p_1\} \text{ در نتیجه}$$

$$\forall (k_1 p_1 + k_m), (k_2 p_1 + k_m) \in [k_m], (k_1 p_1 + k_m) - (k_2 p_1 + k_m), n = ((k_1 - k_2)p_1, n) \neq 1$$

دو رأس m و m' مجاور و نیستند بنابراین این دو رأس در گراف دارای رنگ یکسان هستند.

$$\forall (k_1 p_1 + k_m) \in [k_m], (k_2 p_1 + k_{m'}) \in [k_{m'}], i \neq j, 0 \leq k_m, k_{m'} < p_1, 0 \leq k_1, k_2 \leq n - 1$$

$$(k_1 p_1 + k_m) - (k_2 p_1 + k_{m'}) = (k_1 - k_2)p_1 + (k_m - k_{m'})$$

$$\Rightarrow (k_1 - k_2)p_1 + (k_m - k_{m'}), n = 1.$$

در نتیجه رئوس متعلق به هر کلاس به رئوس دیگر کلاسها مجاور می‌باشند در نتیجه در گراف دارای رنگهای

متمایز می‌باشند، لذا نتیجه می‌گیریم که

$$\chi(X_n) \leq p_1. \quad (2.2)$$

از روابط (۱.۲) و (۲.۲) نتیجه می‌گیریم که

$$p_1 \geq \chi(X_n) \geq \omega(X_n) \geq p_1 \Rightarrow \chi(X_n) = \omega(X_n) = p_1.$$

حال به اثبات قسمت ۲ می‌پردازیم. اجتماع کلاس‌هایی به پیمانه p_1 در $\mathbb{Z}_n$ برابر با مجموعه $\mathbb{Z}_n$ است. بنابراین هر کلاس دارای $\frac{n}{p_1}$ راس از گراف است. همانطور که قبلاً نشان دادیم، رئوس متعلق به هر کلاس در گراف X_n دو به دو غیر مجاورند و با توجه به تعریف گراف مکمل، رئوس متعلق به هر کلاس در $\bar{X}_n$ دو به دو مجاور می‌باشند. بنابراین رئوس متعلق به هر کلاس $\bar{X}_n$ یک زیر گراف کامل در $\bar{X}_n$ با $\frac{n}{p_1}$ راس است. فرض کنید Ω' زیر گراف القایی با مجموعه رئوس $[0]$ در X_n باشد. چون این گراف کامل است در نتیجه

$$\chi(\Omega') = \omega(\Omega') = \frac{n}{p_1} \Rightarrow \chi(\bar{X}_n) \geq \omega(\bar{X}_n) \geq \frac{n}{p_1}$$

مجموعه‌های $\{kp_1, kp_1 + 1, \dots, (k+1)p_1 - 1\}$ که $0 \leq k \leq \frac{n}{p_1}$ ، از رئوس گراف را در نظر می‌گیریم. رئوس واقع در هر مجموعه در گراف $\bar{X}_n$ دو به دو غیر مجاور هستند. بنابراین این رئوس در $\bar{X}_n$ هم‌رنگ می‌باشند. چون تعداد این مجموعه‌ها $\frac{n}{p_1}$ است لذا تمام رئوس گراف $\bar{X}_n$ را نمی‌توان با بیش از $\frac{n}{p_1}$ رنگ آمیزی کرد. بنابراین $\chi(\bar{X}_n) \leq \frac{n}{p_1}$. لذا $\chi(\bar{X}_n) = \omega(\bar{X}_n) = \frac{n}{p_1}$. $\square$

قضیه ۱۶.۲.۲. برای $n \geq 2$ هیچ گراف کیلی یکانی خود کامل وجود ندارد.

برهان. به برهان خلف، فرض کنیم X_n یک گراف خود کامل باشد. بنابراین $X_n \cong \bar{X}_n$ پس بنا به خواص یکرختی دو گراف $\chi(X_n) = \chi(\bar{X}_n)$ و بنابر قضیه قبل، $\chi(X_n) = p$ و $\chi(\bar{X}_n) = n/p$ ، لذا داریم: $p = \frac{n}{p}$ در نتیجه $n = p^2$ که p یک عدد اول است. چون $\bar{X}_n \cup X_n = K_n$ درجه نظم گراف کامل K_n ، $n - 1$ است و همچنین درجه نظم دو گراف یکرخت یکسان است لذا X_n و $\bar{X}_n$ دارای درجه نظم یکسان هستند که برابر با $\varphi(n)$ است. لذا $2\varphi(n) = n - 1$ حال با جاگذاری $n = p^2$ ، داریم:

$$2\varphi(p^2) = p^2 - 1.$$

از طرفی می‌دانیم $\varphi(p^2) = p(p - 1)$. لذا $2\varphi(p^2) = 2p(p - 1) = p^2 - 1$ که غیرممکن است. $\square$

گزاره ۱۷.۲.۲. فرض کنیم $a \in U_n$. اگر $n \geq 3$ ، آنگاه برای $0 \leq k \leq n-1$ ، دنباله $x_k \equiv ka \pmod{n}$ یک دور همیلتنی در X_n است. این دور را با C_a نمایش می‌دهیم.

برهان. از آنجایی که هر عضو از مجموعه U_n مولدی برای $\mathbb{Z}_n$ است. لذا برای هر $a \in U_n$ ضرب عدد صحیح $(0 \leq k \leq n-1)$ ، در a به پیمانه n تمام عناصر گروه $\mathbb{Z}_n$ تولید می‌شود بنابراین دور C_a متشکل از رئوس $a, 2a, \dots, (n-1)a$ ، 0 ، از تمام رئوس گراف می‌گذرد و برای هر $0 \leq k, k+1 \leq n-1$ داریم:

$$x_{k+1} - x_k = a \Rightarrow (x_{k+1} - x_k, n) = 1.$$

بین هر دو رأس غیر متوالی یال وجود ندارد بنابراین دنباله $x_0, \dots, x_{n-1}$ یک دور همیلتنی در X_n است.

□

لم ۱۸.۲.۲. فرض کنیم $n \geq 3$. در این صورت تعداد دورهای همیلتنی یال-مجزا به صورت C_a که $\frac{\varphi(n)}{2}$ است که $E(X_n)$ را افراز می‌کنند. $a \in U_n$

برهان. فرض کنیم $\pm u_1, \pm u_2, \dots, \pm u_r$ عناصر یکال $\mathbb{Z}_n$ باشند. بنابر گزاره قبل دنباله رئوس دور همیلتنی C_{u_i} به صورت 0 و u_i و $\dots$ و $(n-1)u_i$ می‌باشد. فرض کنید $\{a, b\}$ یک یال در C_{u_i} باشد بنابراین $k \in \mathbb{Z}_n$ وجود دارد به طوری که $a = ku_i$ و $b = (k+1)u_i$ بدون اینکه از کلیت قضیه کم شود، فرض می‌کنیم $L(a) = ku_i, L(b) = (k+1)u_i$ و $L(a) > L(b)$. بنابراین $L(a) - L(b) = u_i$ و $L(b) - L(a) = -u_i$. در نتیجه $\{a, b\}$ یک یال در C_{-u_i} است بنابراین C_{u_i} و C_{-u_i} دارای مجموعه

یال‌های یکسان هستند و برای هر یال $(x_{n-k} - x_{n-k-1}) \in C_{-u_i}$ داریم:

$$|x_{n-k} - x_{n-k-1}| \in U_n \Leftrightarrow |(n-k)(-u_i) - (n-k-1)(-u_i)| \in U_n$$

$$\Leftrightarrow |(k+1)(-u_i) - k(-u_i)| \in U_n$$

$$\Leftrightarrow |ku_i - (k+1)u_i| \in U_n$$

$$\Leftrightarrow (x_k, x_{k+1}) \in C_{u_i}$$

لذا دوره‌های همیلتن C_{u_i} و C_{-u_i} بر هم منطبق هستند. حال برای هر j که $i \neq j$ ، $u_i \neq \pm u_j$ در نتیجه C_{-u_i} و $C_{\pm u_j}$ و $L(a) - L(b) \neq \pm u_j$ بنابراین مجموعه یال‌های C_{u_i} از هر دور همیلتن X_n به جز C_{-u_i} متمایز است. چون تعداد عناصر یکال U_n ، $\varphi(n)$ است و $C_{-u_i} = C_{u_i}$ ، بنابراین تعداد دوره‌های همیلتن یال - مجزا به صورت C_{u_i} ، $\frac{\varphi(n)}{2}$ است.

حال نشان می‌دهیم اجتماع دوره‌های همیلتن یال مجزای C_{u_i} که $u_i \in U_n$ برابر با $E(X_n)$ است. هر دور همیلتن از تمام رئوس گراف (فقط یکبار) می‌گذرد، در نتیجه $\cup_{i=1}^r C_{u_i}$ دارای مجموعه رئوس یکسان با رئوس گراف X_n است. حال نشان می‌دهیم که مجموعه یال‌های گراف X_n و $\cup_{i=1}^r C_{u_i}$ یکسان هستند. یال‌های واقع در هر دور همیلتنی در مجموعه یال‌های گراف قرار دارند، بنابراین برای هر i که $1 \leq i \leq r$ ، $C_{u_i} \subseteq E(X_n)$ ، در نتیجه $\cup_{i=1}^r C_{u_i} \subseteq E(X_n)$ از طرفی

$$\forall \{x, y\} \in E(X_n) \Rightarrow (y - x, n) = 1$$

$$\Rightarrow y - x \in U_n, \exists i, \text{ s.t. } y - x = u_i \quad 1 \leq i \leq r$$

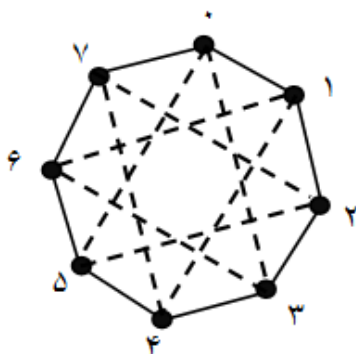
$$\Rightarrow \{x, y\} \in C_{u_i} \Rightarrow \{x, y\} \in \cup_{i=1}^r C_{u_i}$$

□

لذا C_{u_i} ، $E(X_n)$ را افزاز می‌کنند.

مثال ۱۹.۲.۲. در شکل زیر گراف کیلی یکانی $X_8 = \text{Cay}(\mathbb{Z}_8, U_8)$ اجتماع دو دور همیلتن متمایز می‌باشد

که $C_1 = C_7$ و $C_3 = C_5$ است.



قضیه ۲۰.۲.۲. در گراف‌های کیلی یکانی، اگر n زوج باشد، آنگاه $\chi'(X_n) = \varphi(n)$ و اگر n فرد باشد،

$$\text{آنگاه } \chi'(X_n) = \varphi(n) + 1.$$

برهان. اگر n زوج باشد بنابر قضیه ۶.۲.۲، گراف دو بخشی است و هر دور دارای طول زوج است، آنگاه هر دور را می‌توانیم با دو رنگ، رنگ آمیزی کنیم. بنا به لم قبل X_n به $\frac{\varphi(n)}{2}$ دور همپلتن یال-مجزا تجزیه می‌شود. بنابراین X_n دقیقاً با $\varphi(n)$ رنگ، رنگ آمیزی می‌شود. در نتیجه $\chi'(X_n) \leq \varphi(n)$. حال با توجه به اینکه ماکزیمم درجه گراف X_n ، $\varphi(n)$ است و بنا به قضیه ویزینگ، $\chi'(X_n) \geq \varphi(n)$. بنابراین $\chi'(X_n) = \varphi(n)$. برای رنگ آمیزی درست یک گراف (منظور از رنگ آمیزی درست یک گراف، رنگ آمیزی یال‌های گراف به طوری که هیچ دو یال مجاور، یکرنگ نباشند)، هر دو یال که دارای یک انتها مشترک باشند، دارای رنگ یکسان نیستند. بنابراین برای n های فرد، بیشتر از $\frac{n-1}{2}$ یال از یک رنگ در گراف وجود ندارد لذا با $\varphi(n)$ رنگ، حداکثر $\varphi(n)(\frac{n-1}{2})$ یال از گراف را می‌توانیم رنگ آمیزی کنیم. در صورتیکه تعداد کل یال‌های گراف $\varphi(n)(\frac{n}{2})$ می‌باشد. بنابراین $\chi'(X_n)$ بزرگتر از $\varphi(n)$ است. از طرفی $\varphi(n)$ ماکزیمم درجه در X_n است. لذا بنا به قضیه ویزینگ، $\chi'(X_n) = \varphi(n) + 1$ است. $\square$

گزاره ۲۱.۲.۲. $\lambda(X_n) = \varphi(n)$.

برهان. اگر $n < 3$ ، آنگاه $X_n \cong K_2$ ، لذا $\lambda(X_n) = 1$ و حکم برقرار است. فرض کنیم $n \geq 3$. ابتدا نشان

می‌دهیم که $\lambda(X_n) \geq \varphi(n)$. فرض کنیم v و w دو راس در $V(X_n)$ باشند. بنا به لم قبل X_n به $\frac{\varphi(n)}{2}$

دور همیلتنی یال-مجزا تجزیه می‌شود. بنابراین حداقل $\varphi(n)$ مسیر از v به w وجود دارد که دارای مجموعه یال‌های مجزا هستند. درجه هر راس گراف X_n ، $\varphi(n)$ است لذا از v به w حداقل $\varphi(n)$ مسیر وجود دارد. بنا به قضیه منجر، برای غیر همبند بودن v و w باید حداقل $\varphi(n)$ یال را حذف کنیم. چون v و w رئوس دلخواه گراف X_n بودند، بنابراین بنابر نتیجه ۷.۱.۲

$$\lambda(X_n) \geq \varphi(n). \quad (۳.۲)$$

از طرفی هر راس دلخواه گراف X_n را می‌توان با حذف $\varphi(n)$ یال از گراف X_n جدا کرد در نتیجه گراف ناهمبند می‌شود، بنابراین

$$\lambda(X_n) \leq \varphi(n). \quad (۴.۲)$$

لذا از رابطه (۳.۲) و (۴.۲) نتیجه می‌گیریم که $\lambda(X_n) = \varphi(n)$ و اثبات کامل است. $\square$

قضیه ۲.۲.۲. برای $a, b \in \mathbb{Z}_n$ تبدیل آفین را به صورت $\tau_{(a,b)} : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ با ضابطه $x \mapsto ax + b$ در نظر می‌گیریم. در این صورت $\tau_{(a,b)}$ یک خودریختی از X_n است اگر و تنها اگر $a \in U_n$.

برهان. ابتدا نشان می‌دهیم $\tau_{(a,b)}$ یک تابع دو سوپی می‌باشد.

$$\tau_{(a,b)}(x) = \tau_{(a,b)}(y) \Rightarrow ax + b = ay + b$$

$$\Rightarrow a(x - y) + b - b = 0 \Rightarrow a(x - y) = 0$$

$$\Rightarrow ax = ay \Rightarrow x = y$$

در نتیجه $\tau_{(a,b)}$ یک به یک می‌باشد. چون $(a, n) = 1$ بنابراین s و t در $\mathbb{Z}$ وجود دارند به طوری که $ar + ns = 1$ در نتیجه $ar \equiv 1 \pmod{n}$. فرض کنید b عدد صحیح و ثابت باشند، برای هر $y \in \mathbb{Z}_n$ ، $y - b \in \mathbb{Z}_n$ و

$$a(r(y - b)) = y - b \Rightarrow a(r(y - b)) + b = y$$

قرار می‌دهیم $x = r(y - b)$ بنابراین $x \in \mathbb{Z}_n$ وجود دارد به طوری که $\tau_{(a,b)}(x) = y$. در نتیجه $\tau_{(a,b)}$ یک خودریختی در X_n است، بنابراین برای هر $x \in \mathbb{Z}_n$ ، $\tau(x) \in \mathbb{Z}_n$ و برای هر $a, b, c, d \in \mathbb{Z}_n$ که

$$(d, c) \in E(X_n) \Leftrightarrow (\tau_{(a,b)}(d), \tau_{(a,b)}(c)) \in E(X_n)$$

در نتیجه

$$(\tau_{(a,b)}(c) - \tau_{(a,b)}(d), n) = 1 \Rightarrow (a(c - d), n) = 1 \Rightarrow (a, n) = 1 \Rightarrow a \in U_n$$

($\Rightarrow$) فرض می‌کنیم که $a \in U_n$ و $(d, c) \in E(X_n)$ ، لذا داریم:

$$(a, n) = 1, ((c - d), n) = 1 \Rightarrow (a(c - d), n) = 1$$

$$\Rightarrow (ac - ad, n) = 1$$

$$\Rightarrow \forall b \in \mathbb{Z}, ((ac + b) - (ad + b), n) = 1$$

$$\Rightarrow (\tau_{(a,b)}(c) - \tau_{(a,b)}(d), n) = 1$$

$$\Rightarrow (\tau_{(a,b)}(c), \tau_{(a,b)}(d)) \in E(X_n)$$

□

لذا $\tau_{a,b}$ یک خودریختی است.

قضیه ۲.۲.۲. $A(X_n) = \{\tau_{(a,b)} \mid a \in U_n, b \in \mathbb{Z}\}$ یک زیرگروه از $Aut(X_n)$ است.

برهان. نشان می‌دهیم $A(X_n)$ تحت ترکیب توابع بسته است. اگر $a = 1$ و $b = 0$ ، آنگاه $\tau_{(1,0)}(x) = x$

بنابراین تابع همانی در $A(X_n)$ قرار دارد. فرض کنیم $\tau_{(a,b)} \in A(X_n)$ و قرار می‌دهیم:

$$a' = a^{-1}, b' = -a^{-1}b$$

برای هر $x \in \mathbb{Z}_n$ داریم:

$$\tau_{(a',b')} \circ \tau_{(a,b)}(x) = \tau_{(a',b')}(ax + b) = a'(ax + b) + b'$$

$$= a'ax + (a'b + b') = \tau_{(1,0)}(x) = x$$

چون a و b دلخواه می‌باشند لذا هر عضو مجموعه $A(X_n)$ وارون دارد. حال نشان می‌دهیم ترکیب دو عضو در $A(X_n)$ عضوی از $A(X_n)$ است. فرض کنیم $x \in \mathbb{Z}_n$ ، $a, c \in U_n$ و $b, d \in \mathbb{Z}_n$. لذا داریم:

$$\tau_{(a,b)} \circ \tau_{(c,d)}(x) = \tau_{(a,b)}(cx + d) = (ac)x + (ad + b)$$

چون U_n گروه ضربی می‌باشد و $a, b \in U_n$ لذا $ac \in U_n$ و چون $\mathbb{Z}_n$ گروه جمعی است بنابراین $ad + b \in \mathbb{Z}_n$

پس $\tau_{(a,b)} \circ \tau_{(c,d)} \in A(X_n)$ و $A(X_n)$ یک زیرگروه $Aut(X_n)$ است. $\square$

قضیه ۲۴.۲.۲. برای $n \geq 2$ ، X_n متقارن است.

برهان. فرض کنیم x و y دو راس مجاور و u و v نیز دو راس مجاور دیگر در گراف X_n باشند بنابراین $(v - u), (y - x) \in U_n$ لذا $(y - x)^{-1} \in U_n$ عناصر s و t را به صورت زیر در نظر می‌گیریم $s = (v - u)(y - x)^{-1} \in U_n$ و $t = u - ((v - u)(y - x)^{-1})x \in \mathbb{Z}_n$ فرض کنید $h_{s,t} \in A(X_n)$ در نتیجه

$$\begin{cases} h_{s,t}(x) = sx + t = u \\ h_{s,t}(y) = sy + t = v \end{cases}$$

در نتیجه یک خودریختی در $A(X_n)$ وجود دارد که دو راس مجاور در یک گراف را به دو راس مجاور دیگر

گراف می‌برد لذا گراف X_n متقارن است. $\square$

قضیه ۲۵.۲.۲. در گراف کیلی یکانی X_n ، $k(X_n) = \varphi(n)$.

برهان. نشان دادیم X_n همبند و متقارن است در نتیجه بنا بر نتیجه ۲۲.۱.۲، X_n یال تراياست. بنا بر قضیه

۱۸.۱.۲، برای هر گراف همبند و یال ترايا داریم:

$$k(X_n) = \min\{d(v) \mid v \in V(X_n)\}$$

چون گراف X_n منظم و درجه هر راس $\varphi(n)$ است، بنابراین $k(X_n) = \varphi(n)$. $\square$

تعریف ۲۶.۲.۲. برای اعداد صحیح n و s که $n \geq 2$ ، تعداد جواب‌های معادله هم‌نهشتی

$$x + y \equiv s \pmod{n} \quad (5.2)$$

که $x, y \in U_n$ را با $F_n(s)$ نمایش می‌دهیم.

تعریف ۲۷.۲.۲. فرض کنید $p_1, p_2, \dots, p_k$ عامل‌های اول n باشند و $n \geq 2$. برای اعداد صحیح s و x

که $x \equiv s \pmod{n}$ ، تعداد مقادیری که x به پیمانه p_i نمی‌تواند اختیار کند را با $\varepsilon(p_i)$ نمایش می‌دهیم.

لم ۲۸.۲.۲. برای اعداد صحیح n و s که $n \geq 2$ ، $F_n(s) = n \prod_{p|n, p \nmid s} \left(1 - \frac{\varepsilon(p)}{p}\right)$ است که

$$\begin{cases} 1 & p \mid s \\ 2 & p \nmid s \end{cases}$$

برهان. فرض کنیم $p_1, p_2, \dots, p_r$ عامل‌های اول متمایز n باشد و $m = p_1 p_2 \dots p_r$ و $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$

که $\alpha_i \geq 1$. اگر x و y در رابطه (۵.۲) صدق کنند، آنگاه

$$x + y \equiv s \pmod{n} \Rightarrow y \equiv s - x \pmod{n}$$

لذا y به طور یکتا توسط x به پیمانه n تعیین می‌شود. بنابراین کافی است تعداد انتخاب‌های ممکن x را پیدا

کنیم. بازه اعداد صحیح $\{0, 1, \dots, n-1\} = [0, n-1]$ را به بازه‌های مجزای $I_k = [(k-1)m, km-1]$

افراز می‌کنیم که $k = 1, \dots, \frac{n}{m}$. بنا به قضیه باقیمانده چینی، برای هر عدد صحیح $x \in I_k$ داریم:

$$x \equiv x_i \pmod{p_i}, \quad 0 \leq x_i \leq p_i - 1, \quad 0 \leq i \leq r$$

بنابراین

$$p_i \nmid x_i \Rightarrow (x_i, p_i) = 1, \quad (x_i, n) = 1 \Rightarrow x_i \neq 0$$

بنابراین x در صورتی رابطه (۵.۲) صدق کند که $x \in I_k \cap U_n$. (یا به عبارت دیگر باید $x_i \neq 0$ حال اگر

برای $0 < s'_i < p_i$ و $x_i = s'_i$ ، آنگاه

$$\begin{cases} x \equiv x_i \pmod{p_i} \\ s \equiv s'_i \pmod{p_i} \\ x_i = s'_i \end{cases} \Rightarrow x \equiv s'_i \pmod{p_i} \quad (6.2)$$

و با جایگذاری در رابطه (۵.۲) داریم:

$$x \equiv s - y \pmod{n} \Rightarrow x \equiv s'_i - y \pmod{p_i} \quad (۷.۲)$$

از رابطه (۶.۲) و (۷.۲) نتیجه می‌شود $y \equiv 0 \pmod{n}$ و $y \notin U_n$ که با فرض تناقض دارد، لذا $s'_i \neq x_i$.

اگر $s'_i = 0$ چون

$$\begin{cases} s \equiv s'_i \pmod{p_i} \Rightarrow p_i \mid s \\ x_i \neq s'_i \Rightarrow p_i \nmid x_i \end{cases}$$

لذا $0 \leq x_i < p_i - 1$ و $x_i \neq 0$ بنابراین $\varepsilon(p_i) = 1$. حال اگر $s'_i \neq 0$ ،

$$\begin{cases} s \equiv s'_i \pmod{p_i} \Rightarrow p_i \nmid s \\ x_i \equiv s'_i \Rightarrow p_i \mid x_i \end{cases}$$

در این صورت x_i نمی‌تواند مقادیر $s'_i, 0$ را اختیار کند. بنابراین در این حالت $\varepsilon(p_i) = 2$ ، در نتیجه برای

$x \in I_k \cap U_k$ تعداد $(p_1 - \varepsilon(p_1)) \dots (p_r - \varepsilon(p_r))$ انتخاب در رابطه (۵.۲) صدق می‌کنند. چون x ها متعلق

به I_k هستند و تعداد این بازه‌های مجزا $\frac{n}{m}$ است، لذا با ضرب عدد $\frac{n}{m}$ در عبارت فوق داریم:

$$\begin{aligned} F_n(s) &= \frac{n}{m} (p_1 - \varepsilon(p_1)) \dots (p_r - \varepsilon(p_r)) = \frac{n}{m} (p_1 (1 - \frac{\varepsilon(p_1)}{p_1})) \dots \frac{n}{m} (p_r (1 - \frac{\varepsilon(p_r)}{p_r})) \\ &= \frac{n}{m} m (1 - \frac{\varepsilon(p_1)}{p_1}) \dots (1 - \frac{\varepsilon(p_r)}{p_r}) \\ &= n \prod_{\substack{p \mid n, p \text{ اول}}} (1 - \frac{\varepsilon(p)}{p}) \end{aligned}$$

□

قضیه ۲۹.۲.۲. تعداد همسایه‌های مشترک رئوس متمایز a و b در گراف‌های کیلی یکانی برابر با $F_n(a - b)$

است.

برهان. فرض کنیم a و b و z عناصری در $V(X_n)$ باشند. راس z همسایه مشترک رئوس a و b است اگر و

تنها اگر $(a - z, n) = (z - b, n) = 1$. بنابراین عناصر منحصر به فرد x و y در $\mathbb{Z}_n$ وجود دارند به طوری

که $a - z \equiv x \pmod{n}$ و $z - b \equiv y \pmod{n}$ هستند. بنابراین

$$z \equiv a - x \equiv b + y \pmod{n}.$$

از برقراری رابطه $a - x \equiv b + y \pmod{n}$ نتیجه می‌گیریم که $x + y \equiv a - b \pmod{n}$ که $x, y \in U_n$ و این همان معادله همنهشتی لم قبل می‌باشد که تعداد جواب‌های معادله برابر با $F_n(a - b)$ است. بنابراین تعداد همسایه‌های مشترک a و b برابر $F_n(a - b)$ است. $\square$

نتیجه ۳۰.۲.۲. تعداد همسایه‌های مشترک هر جفت از رئوس مجاور در X_n یکسان و برابر با

$$\lambda(n) = \prod_{p|n, p \text{ اول}} \left(1 - \frac{1}{p}\right) \text{ است.}$$

برهان. بنا به لم ۲۸.۲.۲، تعداد همسایه‌های مشترک a و b برابر با $F_n(a - b)$ است و بنا به قضیه ۲۹.۲.۲، $F_n(a - b)$ برابر با تعداد جواب‌های معادله همنهشتی $x + y \equiv a - b \pmod{n}$ است که $x, y \in U_n$. اگر a و b مجاور باشند و p یک عامل اول دلخواه n باشد، آنگاه $(a - b, p) = 1$ و لذا $p \nmid (a - b)$. بنابراین $\varepsilon(p) = 2$ و با جاگذاری در $F_n(a - b)$ داریم:

$$F_n(a - b) = n \prod_{p|n, p \text{ اول}} \left(1 - \frac{1}{p}\right) = \lambda(n).$$

$\square$

گزاره ۳۱.۲.۲. تعداد مثلث‌ها در X_n برابر با $\frac{n^3}{6} \prod_{p|n, p \text{ اول}} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^2}\right)$ است.

برهان. اگر n زوج باشد، آنگاه بنا به نتیجه ۷.۲.۲، گراف X_n بدون مثلث است. حال فرض می‌کنیم n فرد باشد. برای رئوس مجاور a و b که $a, b \in V(X_n)$ ، T_{ab} برابر با تعداد رئوسی از گراف است که در شرط $(a - c), (c - b) \in U_n$ صدق کنند در نتیجه $\{c | a - c \equiv 1 \pmod{n}, c - b \equiv 1 \pmod{n}\}$. لذا بنا به قضیه قبل، تعداد همسایه‌های مشترک برای یال ab برابر است با

$$|\{c | a - c \equiv c - b \equiv 1 \pmod{n}\}| = (\lambda_n)$$

در نتیجه $|T_{ab}| = (\lambda_n)$. چون تعداد یال‌های گراف X_n برابر $\frac{n\varphi(n)}{2}$ است و هر یال سه بار شمرده می‌شود

لذا $T(n)$ برابر با $\frac{n\varphi(n)}{2} \frac{\lambda_n}{3}$ است که با جایگذاری $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ حکم ثابت می‌شود. $\square$

قضیه ۲.۲.۲. برای $n \geq 2$ داریم:

$$\text{diam}(X_n) = \begin{cases} 1 & \text{اگر } n \text{ یک عدد اول باشد} \\ 2 & \text{اگر } \alpha > 1, n = 2^\alpha \\ 2 & \text{اگر } n \text{ فرد باشد و اول نباشد} \\ 3 & \text{اگر } n \text{ زوج و دارای یک عامل اول فرد باشد} \end{cases}$$

برهان. اگر n یک عدد اول باشد، آنگاه هر راس X_n با هر راس دیگر آن مجاور است. در نتیجه $X_n = K_n$

و $\text{diam}(X_n) = 1$. در سه حالت دیگر چون X_n گراف کامل نیست پس

$$\text{diam}(X_n) \geq 2. \quad (۸.۲)$$

حال اگر $\alpha > 1$ و $n = 2^\alpha$ ، آنگاه بنا به گزاره ۵.۲.۲، این گراف دو بخشی کامل است و رئوس آن به دو بخش $X = \{0, 2, 4, \dots, n-2\}$ و $Y = \{1, 2, \dots, n-1\}$ افراز می‌شوند. اگر دو راس دلخواه $a, b \in V(X_n)$ در یک افراز نباشند، آنگاه بنا به خاصیت گراف‌های دو بخشی کامل $d(a, b) = 1$. اگر a و b هر دو در یک افراز از رئوس $V(X_n)$ باشند، آنگاه a و b در گراف مجاور نیستند. فرض کنیم $a, b \in X$ لذا $c \in Y$ وجود دارد به طوری که a, b با c مجاور است بنابراین $d(a, b) = 2$ ، در نتیجه $\text{diam}(X_n) \leq 2$. در نتیجه بنا بر رابطه (۸.۲) $\text{diam}(X_n) = 2$.

حال اگر n فرد باشد و اول نباشد، آنگاه عدد ۲، مقسمی از n نیست. بنا به قضیه ۲.۲.۲، تعداد همسایه‌های مشترک رئوس متمایز a و b برابر با $F_n(a-b)$ می‌باشد، لذا $(1 - \frac{\varepsilon(p_i)}{p_i}) \neq 0$ ، بنابراین $F_n(a-b) \neq 0$ پس برای هر دو راس متمایز گراف، یک همسایه مشترک وجود دارد. بنابراین

$$\text{diam}(X_n) \leq 2 \quad (۹.۲)$$

لذا از (۸.۲) و (۹.۲) نتیجه می‌گیریم که $\text{diam}(X_n) = 2$.

اگر n زوج و دارای یک عامل اول فرد p باشد، آنگاه $(p-0, n) \neq 1$. بنابراین رئوس 0 و p مجاور نیستند. به برهان خلف فرض کنیم z یک همسایه مشترک برای رئوس 0 و p باشد، بنابراین $(p-z, n) = (z-0, n) = 1$. چون $p \in U_n$ زوج می‌باشد پس $p \in U_n$ چون $(p-z, n) = 1$ لذا z نمی‌تواند عدد فردی باشد. بنابراین $z \notin U_n$ در نتیجه $(z-0, n) \neq 1$. لذا فرض خلف نادرست است بنابراین رئوس 0 و p دارای همسایه مشترک نیستند

و $d(o, p) \neq 2$ در نتیجه

$$\text{diam}(X_n) \geq d(o, p) \geq 3 \quad (10.2)$$

اگر a و b دو راس متمایز و غیر مجاور در گراف X_n باشند که دارای همسایه مشترک هستند. بنا به قضیه ۲۹.۲.۲، z یک همسایه مشترک a و b است اگر و تنها اگر $1 = (z - b, n) = (a - z, n)$. این در صورتی برقرار است که a و b هر دو زوج یا هر دو فرد باشند. فرض کنیم a و b دو راس متمایز و غیرمجاور در X_n باشند که دارای همسایه مشترک نباشد. بنابراین a و b هر دو زوج یا هر دو فرد نیستند لذا فرض می‌کنیم a زوج و b فرد باشد. گراف X_n منظم و از درجه $\varphi(n)$ است بنابراین راس a دارای $\varphi(n)$ همسایه است که اعدادی فرد هستند. فرض کنیم c یکی از همسایه‌های a باشد بنابراین c فرد است. چون b و c هر دو فرد هستند لذا مجاور نیستند. نشان دادیم هر دو راس فرد دارای همسایه مشترک هستند لذا b و c دارای همسایه مشترک مانند d می‌باشند. با عبور در امتداد رئوس a, c, d و b نتیجه می‌شود که

$$d(a, b) \leq 3 \quad (11.2)$$

از (۱۰.۲) و (۱۱.۲) داریم:

$$\text{diam}(X_n) = 3$$

□

تعریف ۳۳.۲.۲. اگر هر حفره و پاد حفره در گراف G دارای طول زوج باشد، گراف G را **برژ^v** می‌نامیم.

تعریف ۳۴.۲.۲. گراف G را **تام^h** می‌نامیم، اگر برای هر زیر گراف القایی H در G ، عدد رنگی H برابر با اندازه بزرگترین زیر گراف کامل (خوشه) H باشد.

قضیه ۳۵.۲.۲. [۱۱] $(SPGT)$: گراف G تام است اگر و تنها اگر G و $\bar{G}$ دارای هیچ حفره فردی نباشد.

لم ۳۶.۲.۲. اگر n فرد و تنها دو عامل اول متمایز داشته باشد، آنگاه $\bar{X}_n$ دارای هیچ حفره فرد نیست.

^vBerge

^hperfect

برهان. به برهان خلف فرض می‌کنیم $\bar{X}_n$ دارای حفره فرد C'_{2k+1} باشد و به ترتیب از رئوس $x_0, x_1, \dots$ و x_{2k} می‌گذرد و p_1 و p_2 عامل‌های اول n باشند. بنابراین برای هر یال $\{x_j, x_{j+1}\}$ در $\bar{X}_n$,

$$(x_{j+1} - x_j, n) \neq 1 \Rightarrow p_1 \mid (x_{j+1} - x_j) \text{ یا } p_2 \mid (x_{j+1} - x_j).$$

پس برای هر دو یال متوالی $\{x_j, x_{j+1}\}$ و $\{x_{j+1}, x_{j+2}\}$ در C'_{2k+1} داریم:

$$((x_{j+2} - x_{j+1}), n) \neq 1 \Rightarrow p_1 \mid (x_{j+2} - x_{j+1}) \text{ یا } p_2 \mid (x_{j+2} - x_{j+1}).$$

از اینکه $p_1 \mid (x_{j+1} - x_j)$ نتیجه می‌گیریم که $(x_{j+1} - x_j) \equiv 0 \pmod{p_1}$. در نتیجه عنصر $s \in \mathbb{Z}$ وجود دارد به طوری که $x_{j+1} - x_j = sp_1$. همچنین از اینکه $p_1 \mid (x_{j+2} - x_{j+1})$ نتیجه می‌گیریم که $(x_{j+2} - x_{j+1}) \equiv 0 \pmod{p_1}$. لذا عنصر $t \in \mathbb{Z}$ وجود دارد به طوری که $x_{j+2} - x_{j+1} = tp_1$. با قرار دادن این دو معادله در یک دستگاه و حل آنها داریم:

$$x_{j+2} - x_j = (s + t)p_1 \Rightarrow x_{j+2} - x_j \equiv 0 \pmod{p_1} \Rightarrow \{x_{j+2}, x_j\} \in E(\bar{X}_n)$$

بنابراین $\{x_{j+2}, x_j\}$ یک وتر در دور C'_{2k+1} می‌باشد و این تناقض با حفره بودن C'_{2k+1} دارد. $\square$

قضیه ۳۷.۲.۲. [۱۱] اگر هر حفره و پادحفره گراف G دارای طول زوج باشد، آنگاه گراف G ، برژ است.

قضیه ۳۸.۲.۲. [۱۱] یک گراف برژ است اگر و تنها اگر تام باشد.

تذکر ۳۹.۲.۲. مکمل دور القایی به طول k در گراف را با (C'_k) نمایش می‌دهیم.

لم ۴۰.۲.۲. اگر n ، فرد و دارای حداقل سه عامل اول متمایز باشد، آنگاه X_n شامل یک دور القایی با طول ۵ است.

برهان. فرض کنیم $p_1, p_2, \dots, p_r$ عامل‌های متمایز n باشند که $r \geq 3$ و برای $1 \leq i \leq r$ ، $p_i \neq 2$ و، $p_1 < p_2 < \dots < p_r$ ، $m = p_1 p_2 \dots p_r$ چون در هر گراف $C'_5 = (C'_5)$ یکریخت است. لذا کافیت نشان

دهیم گراف $\overline{X}_n$ شامل یک دور به طول ۵ است. در نتیجه با استفاده از خواص یکریختی دو گراف نتیجه می‌گیریم که X_n یک دور به طول ۵ دارد. رئوس x_0, x_1, x_2, x_3 را به صورت زیر تعریف می‌کنیم:

$$x_0 = 0, \quad x_1 = p_r, \quad x_2 = p_r + p_1 \dots p_{r-1}, \quad x_3 = 2p_r + p_1 \dots p_{r-1} \quad (12.2)$$

بنا به قضیه باقیمانده چینی عنصر یکتای $x_4 \in \mathbb{Z}_m$ وجود دارد که

$$x_4 \equiv 0 \pmod{p_1}$$

$$x_4 \equiv 2p_r \pmod{p_2}$$

$$x_4 \equiv 0 \pmod{p_j} \quad j = 1, \dots, r-1$$

$$x_4 \equiv 2p_1 \dots p_{r-1} + 2p_r \pmod{p_r}$$

با یک مقایسه ساده در می‌یابیم که رئوس $x_0, \dots, x_4$ متمایزاند و یک دور در $\overline{X}_n$ تعریف می‌کنند. در صورتی x_i, x_j یک یال در گراف $\overline{X}_n$ می‌باشد که رئوس x_i و x_j در گراف X مجاور نباشند. بنابراین برای رئوس $x_0, \dots, x_4$ در $\overline{X}_n$ داریم:

$$x_1 - x_0 = x_3 - x_2 = p_r \Rightarrow x_1 - x_0 \equiv x_3 - x_2 \pmod{p_r}$$

$$x_2 - x_1 \equiv x_4 - x_0 \pmod{p_1}$$

$$x_4 - x_3 \equiv 0 \pmod{p_2}$$

بنابراین یال‌های $\{x_0, x_1\}, \{x_1, x_2\}, \{x_2, x_3\}, \{x_3, x_4\}$ و $\{x_4, x_0\}$ در $\overline{X}_n$ قرار دارند.

حال نشان می‌دهیم که دور C'_5 در $\overline{X}_n$ وتر ندارد. کافی است نشان دهیم یال‌های $\{x_3, x_1\}, \{x_4, x_2\}$

در $\overline{X}_n$ قرار ندارند.

$$x_2 - x_0 = p_r + p_1 \dots p_r \Rightarrow (x_2 - x_0, m) = 1 \Rightarrow \{x_0, x_2\} \notin E(\overline{X}_n)$$

با به کارگیری استدلال مشابه برای یال‌های $\{x_0, x_3\}$ و $\{x_1, x_3\}$ همین نتیجه حاصل می‌شود. حال برای

$\{x_1, x_4\}$ با توجه به رابطه (۱۲.۲) و روابط همنهشتی برای x_4 داریم:

$$x_4 - x_1 \equiv -p_r \pmod{p_1} \Rightarrow p_1 \nmid (x_4 - x_1)$$

$$x_4 - x_1 \equiv p_r \pmod{p_2} \Rightarrow p_2 \nmid (x_4 - x_1)$$

$$x_4 - x_1 \equiv -p_r \pmod{p_j} \quad j = 3, \dots, r-1 \Rightarrow p_j \nmid (x_4 - x_1)$$

$$x_4 - x_1 \equiv 2p_1 \dots p_{r-1} \pmod{p_r} \Rightarrow p_r \nmid (x_4 - x_1)$$

در نتیجه $(x_4 - x_1, m) = 1$ ، بنابراین $\{x_4, x_1\} \notin E(\bar{X}_n)$ به طور مشابه $\{x_2, x_4\} \notin E(\bar{X}_n)$.

□

قضیه ۴۱.۲.۲. برای $n \geq 2$ گراف X_n تام است اگر و تنها اگر n زوج باشد یا n فرد و دارای حداکثر دو عامل اول متمایز باشد.

برهان. ($\Leftarrow$) فرض کنید گراف تام باشد بنابر قضیه ۳۸.۲.۲، گراف برژ است و همچنین بنابر قضیه ۳۵.۲.۲ X_n و $\bar{X}_n$ دارای هیچ حفره فردی نیست. از اینکه X_n و $\bar{X}_n$ دارای هیچ حفره فردی نیست، نتیجه می‌گیریم که n زوج است و از اینکه X_n برژ است نتیجه می‌شود که n فرد است و نمی‌تواند بیش از دو عامل اول متمایز داشته باشد بنابراین n فرد و حداکثر دو عامل اول متمایز دارد.

($\Rightarrow$) فرض کنیم n زوج باشد، بنابراین گراف دارای هیچ دور فرد نیست و X_n هیچ زیرگراف القایی ندارد که دور به طول ۵ باشد در نتیجه گراف برژ و بنابر قضیه ۳۴.۲.۲، گراف تام است. حال با برهان خلف نشان می‌دهیم که اگر n فرد و بیش از دو عامل اول داشته باشد گراف X_n نمی‌تواند تام باشد. فرض کنیم n فرد و بیش از دو عامل اول داشته باشد لذا بنا به لِم ۴۰.۲.۲، گراف X_n دارای یک دور القایی به طول ۵ است، در نتیجه گراف برژ نیست و همچنین گراف تام نمی‌باشد لذا برهان خلف باطل است و n نمی‌تواند بیش از دو عامل اول متمایز داشته باشد.

□

فصل ۳

مقادیر ویژه گراف‌های کیلی یکانی

در این فصل مقادیر ویژه گراف‌های کیلی یکانی را محاسبه می‌کنیم و نشان می‌دهیم اگر n عامل خالی از مربع نداشته باشد، آنگاه همه مقادیر ویژه گراف X_n ناصفر و عامل‌های صحیحی از $\varphi(n)$ هستند.

۱.۳. مقادیر ویژه گراف‌های کیلی یکانی

تذکر ۱.۱.۳. فضای برداری مختلط با بعد n را با $\mathbb{C}^n$ نمایش می‌دهیم. تعاریف و قضایای (مربوط به ماتریس‌های دوری) ارجاع داده نشده در این قسمت از مرجع [۱۲]، گرفته شده‌اند.

تعریف ۲.۱.۳. فرض کنید $n \geq 2$ و $\nu = (v_0, v_1, \dots, v_{n-1})$ یک بردار سطری در $\mathbb{C}^n$ باشد. عملگر انتقال $T: \mathbb{C}^n \rightarrow \mathbb{C}^n$ را به صورت $T(v_0, v_1, \dots, v_{n-1}) = (v_{n-1}, v_0, v_1, \dots, v_{n-2})$ تعریف می‌کنیم.

تعریف ۳.۱.۳. ماتریس متناظر به ν ، ماتریس $n \times n$ ی است که k -امین سطر ماتریس با $T^{k-1}(\nu)$ که $k = 1, \dots, n$ بدست می‌آید. این چنین ماتریسی را دوری می‌نامیم و به صورت زیر نمایش می‌دهیم:

$$V = \text{circ}\{\nu\} = \begin{pmatrix} v_0 & v_1 & \dots & v_{n-1} \\ v_{n-1} & v_0 & \dots & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 & v_2 & \dots & v_0 \end{pmatrix}$$

تعریف ۴.۱.۳. فرض کنید

$$\delta_{i,j} = \begin{cases} 1 & i = j & \text{هرگاه} \\ 0 & i \neq j & \text{هرگاه} \end{cases}$$

که $i = 0, 1, \dots, n-1$. در این صورت $e_i = (\delta_{i,0}, \dots, \delta_{i,n-1})$ ها یک پایه متعامد یکه برای ماتریس دوری V می‌باشند.

قضیه ۵.۱.۳. [۹] فرض کنیم W ماتریس دوری است که اولین سطر آن $[0, 1, 0, \dots, 0]$ است. در این صورت مقادیر ویژه W برابر با $1, w, w^2, \dots, w^{n-1}$ است که $w = \exp(\frac{\sqrt[n]{n}}{n})$.

تعریف ۶.۱.۳. فرض کنیم $W_i = \text{circ}\{e_i\}$ که $0 \leq i \leq n-1$. در این صورت هر ماتریس دوری را می‌توان به صورت استاندارد زیر نشان داد.

$$\text{circ}(v_0, v_1, \dots, v_{n-1}) = \sum_{i=1}^{n-1} v_i W^i.$$

نتیجه ۷.۱.۳. $W^i = W_i$, $W_1 = W$, $W_i W_j = W_{i+j}$, $W_0 = I$.

تعریف ۸.۱.۳. فرض کنید X یک متغیر ثابت باشد. چند جمله ای مشخصه ماتریس دوری $V =$

$\text{circ}\{v_0, v_1, \dots, v_{n-1}\}$ ، به صورت زیر تعریف می کنیم:

$$P_V(X) = \sum_{i=1}^{n-1} v_i X^i.$$

قضیه ۹.۱.۳. فرض کنید $n \geq 2$ ، $\nu = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{C}^n$ و $V = \text{circ}\{\nu\}$. اگر $\omega = \exp(\frac{2\pi i}{n})$ ،

n -امین ریشه اولیه مختلط واحد باشد، آنگاه

$$\det V = \det \begin{pmatrix} v_0 & v_1 & \dots & v_{n-1} \\ v_{n-1} & v_0 & \dots & v_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 & v_2 & \dots & v_0 \end{pmatrix} = \prod_{l=0}^{n-1} \left(\sum_{j=0}^{n-1} v_j \omega^{jl} \right).$$

قضیه ۱۰.۱.۳. فرض کنید $\omega = \exp(\frac{2\pi i}{n})$ ، n -امین ریشه اولیه مختلط واحد باشد و برای $l = 0, 1, \dots, n-1$

$x_l = \frac{1}{\sqrt{n}}(1, \omega^l, \omega^{2l}, \dots, \omega^{(n-1)l}) \in \mathbb{C}^n$ ، ماتریس متناظر به تبدیل خطی که برای هر l ، l -امین

بردار واحد e_l را به x_l می برد به صورت زیر می باشد:

$$E = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & \omega & \dots & \omega^{n-2} & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{n-2} & \dots & \omega^{(n-2)^2} & \omega^{(n-1)(n-2)} \\ 1 & \omega^{n-1} & \dots & \omega^{(n-2)(n-1)} & \omega^{(n-1)^2} \end{pmatrix}$$

قضیه ۱۱.۱.۳. فرض کنید D_V ماتریس قطری باشد که عناصر قطر اصلی آن به ترتیب $\lambda_0, \lambda_1, \dots$ و

λ_{n-1} باشند. در این صورت $E^{-1}VE = D_V$.

قضیه ۱۲.۱.۳. برای $l = 0, 1, \dots, n-1$ ، $\lambda_l = P_V(\omega^l)$.

برهان. بنابر قضایای جبر خطی $\lambda_l = \det(D_V)$ و $\det(E^{-1}VE) = \det(V)$.

همچنین در قضیه ۱۱.۱.۳، داریم:

$$E^{-1}VE = D_V \Rightarrow \det(E^{-1}VE) = \det(D_V).$$

در نتیجه

$$\prod_{l=0}^{n-1} \left(\sum_{j=1}^{n-1} v_j \omega^{jl} \right) = \prod_{l=0}^{n-1} \lambda_l$$

□ لذا $\lambda_l = P_V(\omega^l)$ ، و بنابر تعریف ۸.۱.۳، $\lambda_l = \sum_{j=1}^{n-1} v_j \omega^{jl}$

تعریف ۱۳.۱.۳. گراف G را دوری می‌نامیم هرگاه دارای ماتریس مجاورت دوری باشد.

تعریف ۱۴.۱.۳. مقادیر ویژه گراف G همان مقادیر ویژه ماتریس مجاورت G است.

تذکر ۱۵.۱.۳. ماتریس مجاورت گراف X_n یک ماتریس متقارن است که عناصر روی قطر اصلی آن صفر می‌باشد.

برهان. چون گراف X_n بدون جهت می‌باشد در نتیجه اگر بین رئوس v_i و v_j یالی موجود باشد، بین v_j و v_i نیز همان یال موجود است در نتیجه ماتریس مجاورت گراف متقارن می‌باشد. از اینکه گراف X_n ساده می‌باشد (بدون طوقه)، نتیجه می‌شود که درایه a_{ii} در ماتریس مجاورت X_n برای $1 \leq i, j \leq n$ ، صفر است. □ در نتیجه حکم برقرار است.

قضیه ۱۶.۱.۳. [۹] فرض کنیم λ یک مقدار ویژه حقیقی در ماتریس مجاورت G باشد، در این صورت مرتبه تکرار λ برابر با بعد فضای بردار ویژه متناظر به λ است.

قضیه ۱۷.۱.۳. ماتریس مجاورت گراف‌های کیلی یکانی، یک ماتریس دوری است.

برهان. ماتریس مجاورت گراف X_n را بر حسب ترتیب طبیعی رئوس $\mathbb{Z}_n$ در نظر می‌گیریم. چون گراف ساده است لذا برای هر $i \in V(X_n)$ راس i با i مجاور نیست. در نتیجه راس $i+1$ با $i+1$ نیز مجاور

نیست و بر عکس. برای هر $i, j \in V(X_n)$ ، اگر $(j - i, n) = 1$ ، آنگاه $((i + 1) - (j + 1), n) = 1$ و بر عکس. در نتیجه i با j مجاور است اگر و تنها اگر $i + 1$ با $j + 1$ مجاور باشد. لذا هر سطر ماتریس با یک گام انتقال درایه‌های سطر قبلی به دست می‌آید. بنابراین ماتریس مجاورت گراف‌های کیلی یکانی، یک ماتریس دوری هستند. $\square$

نتیجه ۱۸.۱.۳. اگر اولین سطر ماتریس مجاورت در یک گراف دوری $[0, a_1, \dots, a_{n-1}]$ باشد، آنگاه ماتریس دوری متناظر آن به صورت زیر می باشد

$$A_n = \begin{pmatrix} 0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & 0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & 0 \end{pmatrix}$$

نتیجه ۱۹.۱.۳. [۲۲] فرض کنیم $w = \exp(\frac{\sqrt{-1}\pi i}{n})$ ، n - امین ریشه اولیه مختلط واحد A_n باشد و ضرایب چندجمله‌ای $P_n(W) = \sum_{j=1}^n a_j W^j$ درایه‌های سطر اول A_n باشد. در این صورت مقادیر ویژه A_n برابر است با

$$\lambda_r = p_n(w^r) = \sum_{j=0}^{n-1} a_j w^{rj} \quad (1.3)$$

تعریف ۲۰.۱.۳. [۲۲] برای $r, n \in \mathbb{Z}$ و $k \in \mathbb{N}$ و $r \geq 1$ تابع $C(r, n) = \sum_{k \pmod{r}} \exp(\frac{\sqrt{-1}\pi i k n}{r})$ را جمع رامانوجان می‌نامیم که $(k, r) = 1$ است.

قضیه ۲۱.۱.۳. [۲۲] برای هر $r, n \in \mathbb{Z}$ داریم:

$$c(n, r) = \sum_{d|(n, r)} d \mu\left(\frac{r}{d}\right)$$

همچنین تمام مقادیر $c(n, r)$ صحیح است و

$$c(n, r) = \sum_{k \pmod{r}} \cos\left(\frac{\sqrt{-1}\pi k n}{r}\right)$$

که $(k, r) = 1$ است.

اتحاد هلدر ۲۲.۱.۳. [۲۲] برای هر $n, r \geq 1$ داریم:

$$c(n, r) = \frac{\varphi(r)\mu(m)}{\varphi(m)}$$

که $m = \frac{r}{(n, r)}$ است.

قضیه ۲۳.۱.۳. برای ماتریس دوری A_n داریم:

$$\lambda_r = C(r, n) = \mu(t_r) \frac{\varphi(n)}{\varphi(t_r)} \quad (۲.۳)$$

که $t_r = \frac{n}{(r, n)}$ و $0 \leq r \leq n-1$ است.

برهان. درایه (k, i) -ام در ماتریس دوری A_n را با $a_{(i-k)}$ نمایش می‌دهیم. فرض کنیم $(i-k) = j$

باشد، در این صورت $a_j = \begin{cases} 1 & (j, n) = 1 \\ 0 & (j, n) > 1 \end{cases}$ است. بنابراین با جایگذاری در رابطه (۱.۳)، اگر

$(j, n) > 1$ ، آنگاه $a_j = 0$ لذا $\lambda_r = 0$. اگر $(j, n) = 1$ ، آنگاه $a_j = 1$ می‌باشد در نتیجه $\lambda_r = \sum_{j=1}^{n-1} w^{rj}$

بنابراین بنا به تعریف تابع رامانوجان $\lambda_r = \sum_{j=1}^{n-1} w^{rj} = C(r, n)$ که $(j, n) = 1$ است. در نتیجه بنابر اتحاد

هلدر $\lambda_r = C(r, n) = \mu(t_r) \frac{\varphi(n)}{\varphi(t_r)}$ است که $t_r = \frac{n}{(r, n)}$. $\square$

قضیه ۲۴.۱.۳. برای $n \geq 2$ گزاره‌های زیر برقراراند:

۱. هر مقدار ویژه ناصفر X_n یک عامل از $\varphi(n)$ است.

۲. اگر m ماکزیمم عامل خالی از مربع n باشد، آنگاه $\lambda_{min} = \mu(m) \frac{\varphi(n)}{\varphi(m)}$ یک مقدار ویژه ناصفر X_n

با مینیمم مقدار قدر مطلق و مرتبه تکرار $\varphi(m)$ است. بعلاوه هر مقدار ویژه X_n مضربی از λ_{min}

است. همچنین اگر n فرد باشد، آنگاه λ_{min} تنها مقدار ویژه ناصفر X_n با مینیمم مقدار قدر مطلق

است. اگر n زوج باشد، آنگاه λ_{min} یک مقدار ویژه X_n با مرتبه تکرار $\varphi(m)$ است.

برهان. قسمت ۱:

بنا به خاصیت ضربی تابع φ -اویلر، اگر t یک عامل از n باشد، آنگاه $\varphi(n) \mid \varphi(t)$. بنا به رابطه

(۲.۳) مقادیر ویژه گراف X_n برابر با $\lambda_r = \mu(t_r) \frac{\varphi(n)}{\varphi(t_r)}$ است و بنا به تعریف تابع موبیوس $\mu(t_r) = 0$

یا $\mu(t_r) = \pm 1$. اگر $\mu(t_r) = 0$ ، آنگاه $\lambda_r = 0$. اگر $\mu(t_r) = +1$ ، آنگاه $\lambda_r = \frac{\varphi(n)}{\varphi(t_r)}$. بنابراین $\lambda_r \varphi(t_r) = \varphi(n)$ و $\lambda_r \mid \varphi(n)$. در نتیجه λ_r یک عامل از $\varphi(n)$ است. اگر $\mu(t_r) = -1$ ، آنگاه $\lambda_r = -\frac{\varphi(n)}{\varphi(t_r)}$. بنابراین $-\lambda_r \varphi(t_r) = \varphi(n)$ و $-\lambda_r \mid \varphi(n)$. در نتیجه $-\lambda_r$ یک عامل از $\varphi(n)$ است. بنابراین مقادیر ویژه ناصفر X_n ، $\varphi(n)$ را عاد می‌کنند.

قسمت ۲:

فرض کنیم m ماکزیمم عامل خالی از مربع n باشد. برای اینکه $\lambda_r \neq 0$ باید $\mu(t_r) \neq 0$ یا به عبارت دیگر t_r خالی از مربع باشد بنابراین t_r یک عامل از m است. بنا به رابطه (۲.۳)، λ_r دارای مینیمم مقدار است اگر و تنها اگر $\varphi(t_r) = \varphi(m)$. این معادله همیشه دارای جواب بدیهی $t_r = m$ است. در نتیجه

$$\lambda_r = \lambda_{min} = \mu(m) \frac{\varphi(n)}{\varphi(m)} \quad (۳.۳)$$

و برای $1 \leq r \leq n-1$ داریم:

$$\begin{aligned} \lambda_r = \lambda_{min} &\Leftrightarrow t_r = \frac{n}{(r, n)} = m \Leftrightarrow (r, n) = \frac{n}{m} \\ &\Leftrightarrow r \in Q = \left\{ x \frac{n}{m} \mid 0 \leq x < m, (x, m) = 1 \right\} \end{aligned}$$

و $|Q| = \varphi(m)$. بنابراین مرتبه تکرار λ_{min} برابر با اندازه Q ، $\varphi(m)$ است. اگر λ_r یک مقدار ویژه ناصفر دلخواه از X_n باشد، آنگاه t_r یک عامل m و همچنین $\varphi(t_r) \mid \varphi(m)$ و عدد صحیحی مانند k وجود دارد که $\varphi(m) = k\varphi(t_r)$. با جایگذاری در رابطه (۲.۳) داریم:

$$\lambda_r = \mu(t_r) \frac{\varphi(n)}{\frac{\varphi(m)}{k}} = k\mu(t_r) \frac{\varphi(n)}{\varphi(m)}$$

از آنجا که برای مقادیر ویژه ناصفر λ_r ، $\mu(t_r) = \pm 1$ لذا $\lambda_r = \pm k \frac{\varphi(n)}{\varphi(m)}$.

با توجه به رابطه (۳.۳) و اینکه $\mu(m) = \pm 1$ داریم:

$$\lambda_{min} = \pm \frac{\varphi(n)}{\varphi(m)} \Rightarrow \lambda_r = \pm k \lambda_{min}.$$

t_r یک عامل از m می‌باشد بنابراین $kt_r = m$. برای n ، فرد $\varphi(t_r) = \varphi(m)$ تنها دارای جواب بدیهی $t_r = m$ است لذا $k = 1$ و $\mu(\frac{m}{k}) = \mu(t_r)$. بنابر خاصیت ضربی تابع موبیوس، $\mu(t_r) = \mu(m)\mu(k^{-1})$. چون $k \in \mathbb{Z}_n$ و $k = 1$ بنابراین

$$\mu(t_r) = -\mu(m) \implies \lambda_r = -\mu(m) \frac{\varphi(n)}{\varphi(m)} = -\lambda_{min}.$$

حال اگر n زوج باشد، آنگاه $\frac{m}{2}$ یک عدد فرد است. از طرفی $\varphi(\frac{m}{2}) = \varphi(m)$ ، در نتیجه اگر $t_r \mid m$ در این صورت $\varphi(t_r) = \varphi(m)$ دارای جواب دیگر $t_r = \frac{m}{2}$ است و

$$\lambda_r = \mu(t_r) \frac{\varphi(n)}{\varphi(m)} = \mu(\frac{m}{2}) \frac{\varphi(n)}{\varphi(\frac{m}{2})} = \lambda'_{min}$$

و

$$\begin{aligned} \lambda_r = \lambda'_{min} &\Leftrightarrow t_r = \frac{m}{2} \Leftrightarrow \frac{n}{(r, n)} = \frac{m}{2} \\ &\Leftrightarrow r \in Q = \{x \frac{2n}{m} \mid 0 < x < m, (x, m) = 1\} \quad |Q| = \varphi(m) \end{aligned}$$

□

در نتیجه مرتبه تکرار λ'_{min} ، $\varphi(m)$ است.

گزاره ۲۵.۱.۳. [۹] فرض کنیم G یک گراف منظم از درجه k باشد، در این صورت:

۱. k یک مقدار ویژه G است.

۲. اگر G همبند باشد، آنگاه مرتبه تکرار k برابر یک است.

۳. برای هر مقدار ویژه λ از G ، $|\lambda| \leq k$.

گزاره ۲۶.۱.۳. [۹] فرض کنیم G گراف دو بخشی و λ یک مقدار ویژه با مرتبه تکرار $m(\lambda)$ در G باشد،

در این صورت $-\lambda$ نیز یک مقدار ویژه G است و $m(-\lambda) = m(\lambda)$ در نتیجه $\lambda_{min} = -\lambda_{max}$.

نتیجه ۲۷.۱.۳. در گراف‌های کیلی یکانی از مرتبه n ، $\varphi(n) = |\lambda_{max}|$ می‌باشد.

نتیجه ۲۸.۱.۳. مقادیر ویژه ناصفر گراف‌های دو بخشی به صورت $(\lambda, -\lambda)$ ظاهر می‌شوند و مرتبه تکرار یکسان دارند.

قضیه ۲۹.۱.۳. اگر n خالی از مربع باشد، آنگاه $\mu(n)$ یک مقدار ویژه X_n با مرتبه تکرار $\varphi(n)$ می‌باشد.

برهان. اگر n خالی از مربع باشد، آنگاه n ماکزیمم عامل خالی از مربع n است. لذا بنا به (۳.۳) داریم:

$$\lambda_r = \lambda_{\min} = \mu(n) \frac{\varphi(n)}{\varphi(n)} = \mu(n)$$

و

$$\lambda_r = \lambda_{\min} \Leftrightarrow t_r = n, \quad \frac{n}{(r, n)} = n \Leftrightarrow (r, n) = 1$$

$$\Leftrightarrow r \in Q = \{x \mid 0 < x < n, (x, n) = 1\} \Rightarrow |Q| = \varphi(n).$$

□

قضیه ۳۰.۱.۳. گراف X_n دارای یکی از مقادیر ویژه ± 1 است اگر و تنها اگر n عدد مربع-آزاد باشد.

برهان. اگر n مربع-آزاد باشد، آنگاه بنا به قضیه قبل $\lambda_{\min} = \mu(n)$ و $\mu(n) \neq 0$. اگر تعداد عامل‌های اول آن فرد باشد، آنگاه $\mu(n) = -1$. اگر تعداد عامل‌های اول آن زوج باشد، آنگاه $\mu(n) = +1$ لذا در هر دو حالت X_n یکی از مقادیر ویژه $+1$ و -1 را داراست.

بعکس، اگر X_n یکی از مقادیر ویژه ± 1 را دارا باشد، آنگاه عنصر $r_1 \in \mathbb{Z}_n$ وجود دارد به طوری که

$$\lambda_{r_1} = \pm 1 \text{ با توجه به رابطه (۲.۳) داریم:}$$

$$\lambda_{r_1} = \mu(t_{r_1}) \frac{\varphi(n)}{\varphi(t_{r_1})} = \pm 1 \Rightarrow \varphi(n) = \varphi(t_{r_1}), \quad \mu(t_{r_1}) = \pm 1$$

بنابراین $\lambda_{r_1} = \mu(t_{r_1}) = \pm 1$. چون $\varphi(n) = \varphi(t_{r_1})$ دارای جواب بدیهی $n = t_{r_1}$ است لذا $\mu(n) = \pm 1$

□

و n خالی از مربع است.

قضیه ۳۱.۱.۳. گراف‌های کیلی یکانی X_n دارای هر دو مقدار ویژه ± 1 با مرتبه تکرار $\varphi(n)$ است اگر و تنها اگر n عدد خالی از مربع و زوج باشد.

برهان. ($\Leftarrow$) بنا به رابطه (۲.۳) مقادیر ویژه برای گراف‌های کیلی یکانی برابر با $\lambda_r = \mu(t_r) \frac{\varphi(n)}{\varphi(t_r)}$ است که $t_r = \frac{n}{(r,n)}$. بنابراین r_1 و r_2 وجود دارد به طوری که $1 \leq r_1, r_2 \leq n-1$ و $\lambda_{r_1} = \mu(t_{r_1}) \frac{\varphi(n)}{\varphi(t_{r_1})} = -1$ و $\lambda_{r_2} = \mu(t_{r_2}) \frac{\varphi(n)}{\varphi(t_{r_2})} = +1$.

در نتیجه باید $\varphi(t_{r_1}) = \varphi(n)$ و $\mu(t_{r_1}) = +1$ و $\varphi(t_{r_2}) = \varphi(n)$ و $\mu(t_{r_2}) = -1$. چون مقادیر ویژه λ_{r_1} و λ_{r_2} مخالف صفر هستند لذا t_{r_1} و t_{r_2} عامل‌های خالی از مربع هستند. همچنین اگر n فرد باشد، روابط $\varphi(n) = \varphi(t_{r_1})$ و $\varphi(n) = \varphi(t_{r_2})$ دارای تنها جواب $n = t_{r_1}$ و $n = t_{r_2}$ است. در نتیجه $n = t_{r_1} = t_{r_2}$ و $\lambda_{r_1} = \lambda_{r_2}$ که یک تناقض است. لذا n زوج است. از طرفی X_n حداقل یکی از مقادیر ویژه ± 1 را دارد در نتیجه بنا به قضیه قبل، n خالی از مربع است.

($\Rightarrow$) فرض کنیم n خالی از مربع باشد. چون n مربع-آزاد است پس حداقل یک عامل خالی از مربع دارد، بنابراین X_n دارای مقدار ویژه ناصفر است و $\lambda_r = \mu(t_r) \frac{\varphi(n)}{\varphi(t_r)}$. $\lambda_{min} = \mu(n)$ چون مقادیر ویژه صحیح هستند لذا $|\lambda_{min}| = 1$. بنا به قضیه ۲۷.۱.۳ اگر n زوج باشد، آنگاه $\lambda_{min} = -1$ یک مقدار ویژه X_n است. لذا هر دو مقدار ویژه $+1$ و -1 وجود دارد و دارای مرتبه تکرار $\varphi(n)$ هستند. $\square$

قضیه ۳۲.۱.۳. فرض کنیم m ماکزیمم عامل خالی از مربع n و M مجموعه عامل‌های مثبت m باشد، آنگاه گزاره‌های زیر برای گراف‌های کیلی یکانی X_n ، $n \geq 2$ برقرارند.

(الف). تکرار هر جمله دنباله $S = (\mu(t) \frac{\varphi(n)}{\varphi(t)})_{t \in M}$ با مرتبه تکرار $\varphi(t)$ ، دنباله $\tilde{S}$ به طول m و شامل تمام مقادیر ویژه ناصفر X_n است که هر مقدار ویژه به اندازه مرتبه تکرار آن ظاهر می‌شود.

(ب). مرتبه تکرار مقدار ویژه صفر در X_n برابر با $n - m$ است.

(ج). اگر $\alpha(\lambda)$ مرتبه تکرار مقدار ویژه λ در X_n باشد، آنگاه $\lambda \alpha(\lambda)$ مضربی از $\varphi(n)$ است.

برهان. (الف). فرض کنیم $\tilde{S}$ جملات دنباله S با مرتبه تکرارشان باشد. تعداد جملات دنباله $\tilde{S}$ برابر با $\sum_{t \in M} \varphi(t)$ است. برای هر $m, t, t \in M$ را عادی می‌کند. بنا به قضیه ۱۰.۳.۱، $\sum_{t|m} \varphi(t) = m$. بنابراین طول دنباله $\tilde{S}$ ، m است. وقتی که $t_r \notin M$ ، t_r یک عامل خالی از مربع نیست. لذا $\mu(t_r) = 0$ و $\lambda_r = 0$. برای هر $t_r \in M$ که $0 < r \leq n-1$ و $t_r = \frac{n}{(r,n)}$ زیر دنباله $\tilde{T}$ از مقادیر ویژه ناصفر X_n به صورت $\tilde{T} = (\mu(t_r) \frac{\varphi(n)}{\varphi(t_r)})_{t_r \in M}$ در نظر می‌گیریم. فرض کنیم t یک عضو دلخواهی از M باشد. برای $0 < r \leq n-1$ داریم:

$$t_r = t \Leftrightarrow (r, n) = \frac{n}{t}$$

$$\Leftrightarrow r \in Q_t = \{x \frac{n}{t} \mid 0 < x < t, (x, t) = 1\} \quad |Q_t| = \varphi(t)$$

در نتیجه برای هر $t \in M$ ، هر جمله $\tilde{T}$ ، $\varphi(t)$ بار ظاهر می‌شود. اگر هر جمله $\tilde{T}$ را تنها یک بار برداریم، آنگاه دنباله S به دست می‌آید و لذا $\tilde{T}$ و $\tilde{S}$ دارای عناصر برابر هستند.

(ب). بنا به قسمت الف تعداد مقادیر ویژه ناصفر X_n ، m است. تعداد مقادیر ویژه در ماتریس‌ها برابر با بعد ماتریس است. از آنجا که بعد ماتریس متناظر با گراف‌های کیلی n است بنابراین تعداد تکرار مقدار ویژه صفر $n - m$ است.

(ج). اگر $\lambda = 0$ ، آنگاه $\lambda \alpha(\lambda) = 0$ و حکم برقرار است. حال فرض کنیم $\lambda \neq 0$ بنابراین عنصر $t \in M$ وجود دارد به طوری که $\lambda = \mu(t) \frac{\varphi(n)}{\varphi(t)}$ بنا به قسمت الف، برای هر $t \in M$ ، مرتبه تکرار هر مقدار ویژه ناصفر در X_n ، $\varphi(t)$ می‌باشد. اگر تعداد

$$|T \in M | \lambda_T = \lambda_t| = |\{T \in M \mid \mu(T) = \mu(t), \varphi(T) = \varphi(t)\}| = k_t$$

در نظر بگیریم، بنابراین مرتبه تکرار λ_t برابر با $k_t \varphi(t)$ است. در نتیجه

$$\lambda_t \alpha(\lambda_t) = \mu(t) \frac{\varphi(n)}{\varphi(t)} k_t \varphi(t) = \mu(t) k_t \varphi(t).$$

□

تعریف ۳۳.۱.۳. فرض کنیم D مجموعه‌ای از عامل‌های سره و مثبت عدد صحیح $n > 1$ باشد. در این

صورت گراف X_n با مجموعه رئوس $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ و مجموعه یال‌های

$$E(X_n(D)) = \{\{a, b\} \mid a, b \in \mathbb{Z}_n, (a-b, n) \in D\}$$

را $gcd-graph$ می‌نامیم و آن را با $X_n(D)$

نمایش می‌دهیم.

تعریف ۳۴.۱.۳. اگر $D = \{d_1, d_2, \dots, d_k\}$ ، آنگاه $X_n(D) = X_n(\{d_1, d_2, \dots, d_k\})$ و در حالت خاص

$$X_n(1) = X_n$$

گزاره ۳۵.۱.۳. $gcd-graph$ از مرتبه n یکرخت با یک گراف دوری از مرتبه n است.

برهان. کافیت نشان دهیم، ماتریس مجاورت $X_n(D)$ یک ماتریس دوری است. برای هر $i, j \in V(X_n(D))$

چون $(i-i, n) \notin D$ بنابراین $((i+1) - (i+1), n) \notin D$ و برعکس، در نتیجه $a_{ii} = a_{(i+1)(i+1)}$. اگر

$(j-i, n) \in D$ ، آنگاه $((j+1) - (i+1), n) \in D$ و برعکس، لذا $a_{ij} = a_{(i+1)(j+1)}$ و هر راس ماتریس

با یک گام انتقال، درایه‌های سطر قبلی به دست می‌آید. بنابراین ماتریس مجاورت $X_n(D)$ یک گراف دوری

است. پس گراف‌های $X_n(D)$ با گراف‌های دوری هم مرتبه شان یکرخت هستند.

□

قضیه ۳۶.۱.۳. مقادیر ویژه گراف $X_n(D)$ برابر با $\lambda_r = \sum_{d \in D} C(r, \frac{n}{d})$ است که $0 \leq r \leq n-1$ و

$$(t, \frac{n}{d}) = 1$$

برهان. بنا به گزاره قبل، گراف $X_n(D)$ یک گراف دوری است. درایه (k, i) -ام در ماتریس دوری متناظر

با $X_n(D)$ را با a_{i-k} نمایش می‌دهیم. فرض کنیم $(i-k) = j$ باشد. در این صورت

$$a_j = \begin{cases} 1 & \text{اگر } (j, n) \in D \\ 0 & \text{اگر } (j, n) \notin D \end{cases}$$

مقادیر ویژه برای گراف‌های دوری بنا بر (۱.۳) برابر با

$$\lambda_r = \sum_{j=0}^{n-1} a_j w^{rj} \quad 0 \leq r \leq n-1$$

و $w = \exp(\frac{2\pi i}{n})$ است. اگر $a_j = 0$ ، آنگاه $\lambda_r = 0$. اگر $(j, n) \in D$ ، آنگاه $a_j = 1$ و $\lambda_r =$

$$\sum_{d \in D} \sum_{1 \leq j < n} w^{rj} \quad \text{است. از طرفی بنا به لم ۹.۳.۱،}$$

$$\{j \mid 1 \leq j < n, (j, n) = d\} = \{td \mid 1 \leq t < \frac{n}{d}, (t, \frac{n}{d}) = 1\}$$

بنابراین

$$\begin{aligned} \lambda_r &= \sum_{d \in D} \sum_{1 \leq t < \frac{n}{d}} w^{r(td)} = \sum_{d \in D} \sum_{1 \leq t < \frac{n}{d}} \exp(\frac{2\pi i}{n} rtd) \\ &\Rightarrow \lambda_r = \sum_{d \in D} C(r, \frac{n}{d}) \quad 0 \leq r \leq n-1 \end{aligned}$$

□

که $(t, \frac{n}{d}) = 1$ است.

فصل ۴

گروه خودریختی های گراف های کیلی یکانی

۱.۴ گروه خودریختی های گراف های کیلی یکانی

برای گراف G تعداد همسایگی های مشترک رئوس a و b را با $N(a, b)$ نمایش می دهیم. همچنین در فصل ۳ نشان دادیم که $N(a, b) = F_n(a - b)$.

تعریف ۱.۱.۴. خودریختی گرافی یک تابع دو سویی از $V(G)$ به $V(G)$ می باشد که مجاورت را حفظ می کند و با $Aut(G)$ نمایش می دهیم.

قضیه ۲.۱.۴. فرض کنیم $n = p^k$ که p عددی اول است. و $k \geq 1$ در این صورت

$$|Aut(X_n)| = p!((p^{k-1})!)^p$$

برهان. فرض کنیم $0 \leq i \leq p-1$ ، مجموعه c_i را به صورت زیر تعریف می کنیم.

$$c_i = \{a \mid 0 \leq a < p^k, a \equiv i \pmod{p}\}$$

در فصل ۳ نشان دادیم که رئوس متعلق به هر کلاس دو به دو نامجاور هستند و رئوس هر کلاس، به رئوس همه کلاس های دیگر X_n مجاور می باشند. فرض کنیم a و b دو راس در کلاس c_i و $f \in Aut(X_n)$ همچنین فرض کنید $f(a) \in c_j$ که $0 \leq i, j \leq p-1$. از اینکه $p \mid a - b$ نتیجه می گیریم که a و b نامجاورند در نتیجه $f(a)$ و $f(b)$ نامجاورند و لذا $p \mid f(a) - f(b)$. چون $f(a) \in c_j$ لذا $f(b) \in c_j$. در نتیجه رئوس کلاس c_i به رئوس کلاس c_j تصویر می شوند. چون i دلخواه بود نتیجه می گیریم که کلاس ها تحت خودریختی f جا به جا می شوند. فرض کنیم c_i به c_j تصویر شده باشد، چون رئوس کلاس c_i یک مجموعه مستقل هستند لذا $Aut(c_i) = |c_i|! = (p^{k-1})!$ (تعداد این کلاس ها p می باشد) تعداد جایگشت هایی که این کلاسها را جا به جا می کند $p!$ می باشد. جابجایی رئوس و کلاسها، مستقل از یکدیگر هستند بنابر قانون ضرب شمارش در ترکیبات، تعداد خودریختی های X_n برابر با $p!((p^{k-1})!)^p$ است. $\square$

تعریف ۳.۱.۴. برای $0 \leq i < p_j$ و $1 \leq j \leq k$ ، قرار می دهیم

$$c_i^{(j)} = \{a \mid 0 \leq a < n, a \equiv i \pmod{p_j}\}.$$

در فصل دوم نشان دادیم که عدد رنگی X_n برابر با کوچکترین عامل اول n و دقیقاً p_1 کلاس رنگی در X_n وجود دارد. بنابراین مجموعه های $c_0, c_1, \dots, c_{p_1-1}^1$ ماکزیمال مجموعه های مستقل می باشند. این کلاس ها تحت خودریختی f جابجا می شوند. در ادامه نشان می دهیم کلاس های به پیمان p که $p|n$ تحت خودریختی f جابجا می شوند.

لم ۴.۱.۴. فرض کنید f یک خودریختی از X_n باشد و $p_i | n$ در این صورت

$$p_i | a - b \Leftrightarrow p_i | f(a) - f(b), \quad 1 \leq a, b \leq n - 1, \quad 1 \leq i \leq k \quad (1.4)$$

برهان. ($\Rightarrow$) فرض کنیم f یک خودریختی و $p_i | f(a) - f(b)$. قرار می دهیم $f(a) = a', f(b) = b'$ در نتیجه

$$p_i | f(a) - f(b) \Rightarrow p_i | a' - b'$$

چون f^{-1} یک خودریختی است لذا

$$p_i | f^{-1}(a') - f^{-1}(b') \Rightarrow p_i | a - b.$$

لذا حکم ثابت شد.

($\Rightarrow$) برهان خلف، فرض کنیم حکم برقرار نباشد و $2 \leq j \leq k$ بزرگترین اندیسی باشد که $p_j | a - b$

و $p_j \nmid f(a) - f(b)$. رئوس $(a, b) = (i, i + p_j)$ را در نظر می گیریم به طوری که $p_j \nmid f(i) - f(i + p_j)$

و $0 \leq i \leq n - 1 - p_j$ باشد. با توجه به قضیه ۲۹.۲.۲،

$$N(i, i + p_j) = F_n(p_j) = (p_1 - 2) \dots (p_{j-1} - 2)(p_j - 1)(p_{j+1} - 2) \dots (p_k - 2) \frac{n}{p_1 p_2 \dots p_k}.$$

برای s هایی که $1 \leq s, j \leq k, s < j$ ، چون $p_s \nmid (i + p_j - i)$ لذا $p_s \nmid (f(i + p_j) - f(i))$ در نتیجه برای

$$\varepsilon(p_s) = 2, \quad s < j$$

$$.N(f(i), f(i + p_j)) = (p_1 - \varepsilon(p_1)) \dots (p_{j-1} - \varepsilon(p_{j-1}))(p_j - 2)(p_{j+1} - 2) \dots (p_k - 2) \frac{n}{p_1 p_2 \dots p_k}$$

خودریختی f تعداد همسایه های مشترک رئوس را حفظ می کند. بنابراین

$$N(i, i + p_j) = N(f(i), f(i + p_j)).$$

اگر $\varepsilon(p_1) = \varepsilon(p_2) = \dots = \varepsilon(p_k) = 2$ ، آنگاه $\frac{p_j - 2}{p_j - 1} < 1$ که یک تناقض است.

بنابراین s ، $1 \leq s \leq j - 1$ وجود دارد به طوری که $\varepsilon(p_s) = 1$ و $\frac{N(f(i), f(i + p_j))}{N(i, i + p_j)} \geq \frac{(p_s - 1)(p_j - 2)}{(p_s - 2)(p_j - 2)} > 1$

که باز هم یک تناقض است. در نتیجه $p_j \mid f(i) - f(i + p_j)$. بنابراین برای رئوس دلخواه $a, b \in X_n$ که

$$a < b \text{ و } a - b \mid p_j \text{ داریم:}$$

$$p_j \mid f(a) - f(a + p_j) + (f(a + p_j) - f(a + 2p_j)) + \dots + (f(b - p_j) - f(b)) = f(a) - f(b)$$

در نتیجه کلاس هایی به پیمانه p_j تحت خودریختی f جابجا شده است. چون j دلخواه بود لذا برهان کامل

□

است.

قضیه ۵.۱.۴. اگر $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ نمایش متعارف n باشد و $p_1 < p_2 < \dots < p_k$ ، آنگاه

$$|Aut(X_n)| = p_1! p_2! \dots p_k! \left(\left(\frac{n}{p_1 p_2 \dots p_k} \right)! \right)^{p_1 p_2 \dots p_k}$$

برهان. فرض کنیم $f \in Aut(X_n)$ و $m = p_1 p_2 \dots p_k$ بزرگترین عامل مربع-آزاد n باشد. دو راس a

و b در X_n مجاور هستند اگر و تنها اگر $(a - b, m) = 1$ و کلاس های $D_0, D_1, \dots, D_{m-1}$ را که

$D_i = \{a \mid 0 \leq a < n, a \equiv i \pmod{m}\}$ است را در نظر می گیریم. اندازه هر کلاس D_i برابر با $\frac{n}{m}$

است. برای رئوس دلخواه $a, b \in D_i$ ، $a - b \mid m$ در نتیجه $(a - b, n) \neq 1$ و هر کلاس به پیمانه m یک

مجموعه مستقل از رئوس است. لذا بنا بر لم قبل $m \mid f(a) - f(b)$ و کلاس های $D_0, D_1, \dots, D_{m-1}$

تحت خودریختی f جابجا می شوند. فرض کنیم $a \in D_i$ و $b \in D_j$ که $0 \leq i, j \leq m - 1$ رئوس دلخواه

در کلاس های متمایز باشند، رئوس a و b مجاورند اگر و تنها اگر $(m(k - l) + (i - j), n) = 1$. اگر $i - j$

نسبت به n اول باشد، آنگاه رئوس D_i و D_j یک زیرگراف دو بخشی کامل در X_n را تشکیل می دهند، در غیر

اینصورت هیچ یالی بین D_i و D_j وجود ندارد. چون کلاس های $\{D_0, D_1, \dots, D_{m-1}\}$ تحت خودریختی

f جابجا می شوند و هر کلاس یک مجموعه مستقل است پس تعداد خودریختی های f برای $D_i = f(D_j)$ دقیقاً $|D_i|! = (\frac{n}{m})!$ است. برای شمردن تعداد جایگشت های کلاس های D_i فرض کنیم $0 \leq i \leq m-1$ دلخواه باشد و $i_1, i_2, \dots$ و i_k به ترتیب باقیمانده i به پیمانه $p_1, p_2, \dots$ و p_k باشند. برای هر $1 \leq s \leq k$ قرار می دهیم:

$$c_{i_s}^{(s)} = \{0 \leq a < n \mid a \equiv i_s \pmod{p_s}\}$$

برای هر $a \in D_i$

$$m \mid a - i \Rightarrow p_1 \mid a - i, p_2 \mid a - i, \dots, p_k \mid a - i \Rightarrow a \equiv i \pmod{p_1}, a \equiv i \pmod{p_2}, \dots, a \equiv i \pmod{p_k}$$

از طرفی

$$i \equiv i_1 \pmod{p_1}, i \equiv i_2 \pmod{p_2}, \dots, i \equiv i_k \pmod{p_k}$$

در نتیجه

$$a \equiv i_1 \pmod{p_1}, a \equiv i_2 \pmod{p_2}, \dots, a \equiv i_k \pmod{p_k} \Rightarrow a \in C_{i_1}, a \in C_{i_2}, \dots, a \in C_{i_k}^k$$

بنابراین

$$D_i \subseteq c_{i_1}^{(1)} \cap c_{i_2}^{(2)} \cap \dots \cap c_{i_k}^{(k)}. \quad (2.4)$$

برای اندیس های $i_1, i_2, \dots$ و i_k دستگاه همبستگی زیر را در نظر بگیرید

$$x \equiv i_1 \pmod{p_1}$$

$$x \equiv i_2 \pmod{p_2}$$

$$\vdots$$

$$x \equiv i_k \pmod{p_k}$$

بنابر قضیه باقیمانده چینی این دستگاه یک جواب منحصر بفرد i به پیمانه m دارد. با توجه به فرض، i تنها جواب دستگاه می باشد. از اینکه $a \equiv i \pmod{p_j}$ که $1 \leq j \leq k$ ، نتیجه می گیریم که $a \equiv i \pmod{m}$. بنابراین برای هر j ، $c_{i_s}^{(j)} \subset D_i$ به عبارت دیگر

$$p_j \nmid x \Rightarrow m \nmid x \Rightarrow c_{i_s}^{(j)} \subset D_i, \quad 1 \leq j \leq k, \quad 1 \leq s \leq k$$

در نتیجه

$$c_{i_1}^{(1)} \cap c_{i_2}^{(2)} \cap \dots \cap c_{i_k}^{(k)} \subseteq D_i \quad (3.4)$$

از (۲.۴) و (۳.۴) نتیجه می گیریم که $D_i = c_{i_1}^{(1)} \cap c_{i_2}^{(2)} \cap \dots \cap c_{i_k}^{(k)}$. بنا به لم قبل، برای هر عدد اول p_s که $1 \leq s \leq k$ خودریختی f کلاس های $c_{j_1}^s, c_{j_2}^s, \dots, c_{j_{p_s-1}}^s$ را جابجا می کند. بنابراین اندیس های $j_1, j_2, \dots, j_k$ و j_k که $0 \leq j_s < p_s$ و $1 \leq s \leq k$ وجود دارد به طوری که $f(c_{i_s}^{(s)}) = c_{j_s}^{(s)}$ یک تابع دو سویی است لذا

$$f(c_{i_1}^{(1)} \cap c_{i_2}^{(2)} \cap \dots \cap c_{i_k}^{(k)}) = f(c_{i_1}^{(1)}) \cap f(c_{i_2}^{(2)}) \cap \dots \cap f(c_{i_k}^{(k)})$$

و

$$f(D_i) = c_{j_1}^{(1)} \cap c_{j_2}^{(2)} \cap \dots \cap c_{j_k}^{(k)} = D_j$$

اگر جایگشت اندیس های به پیمانه p_s را با h_s نمایش می دهیم، آنگاه برای $s = 1, 2, \dots, k$ ضابطه $f(D_i) \mapsto D_j$ برقرار است اگر و تنها اگر $h_s(i_s) = j_s$. بنابراین مجموعه $f(D_i)$ به وسیله جایگشت های کلاس های $c_{j_s}^{(s)}$ به دست می آید. چون این جایگشت ها مستقل هستند. کران بالا برای تعداد حالت های ممکن برای جایگشت های کلاس های D_i برابر با ضرب تعداد جایگشت های کلاس های $c_{j_s}^{(s)}$ که $p_1! p_2! \dots p_k!$ می باشد. فرض کنید $h_i : \mathbb{Z}_{p_i} \rightarrow \mathbb{Z}_{p_i}$ نمایانگر تعدادی جایگشت های کلاس های $c_{j_s}^{(s)}$ که

۱.۴. گروه خودریختی های گراف های کیلی یکانی. ضریب c_{p_i} جواب دستگاه همبستگی زیر است

$$C_{p_i} \equiv 1 \pmod{p_i}$$

$$C_{p_i} \equiv 0 \pmod{p_j}, 1 \leq j \leq k, j \neq i.$$

فرض کنید برای هر $1 \leq l \leq m-1$ و $l_i \equiv \text{mod } p_i$ که $l_i \equiv \text{mod } p_i$ و $0 \leq l_i \leq p_i-1, i=1, 2, \dots, k$ جایگشت $p(l)$ جواب دستگاه $p(l) \equiv \sum_{i=1}^k c_{p_i} h_i(l_i) \pmod{m}$ باشد. در اینصورت چون $m \nmid p(l)$ لذا $n \nmid p(l)$ بنابراین

$$(p(l') - p(l''), n) = 1 \Leftrightarrow \sum_{i=1}^k c_{p_i} (h_i(l'_i) - h_i(l''_i), n) = 1$$

$$\Leftrightarrow p_i \nmid h_i(l'_i) - h_i(l''_i), i=1, 2, \dots, k$$

$$\Leftrightarrow p_i \nmid l'_i - l''_i, i=1, 2, \dots, k$$

$$\Leftrightarrow (\sum_{i=1}^k c_{p_i} (l'_i - l''_i), n) = 1$$

$$\Leftrightarrow (l' - l'', n) = 1.$$

بنابراین دقیقاً $p_1! p_2! \dots p_k!$ حالت برای جابجایی کلاس های $\{D_0, D_1, \dots, D_{m-1}\}$ وجود دارد. چون رؤس تشکیل دهنده کلاس ها، می توانند بدون شرط تصویر شوند لذا بنا به قانون ضرب مرتبه گروه خودریختی های X_n برابر با $p_1! p_2! \dots p_k! ((\frac{n}{m})!)^m$ است. $\square$

در فصل ۲، تبدیل آفین را معرفی کردیم و نشان دادیم که $A(X_n)$ زیر گروه $AUT(X_n)$ می باشد.

قضیه ۱.۴.۶. برای هر $n \geq 2$ ، $|A(X_n)| = n \cdot \varphi(n)$.

برهان. $A(X_n) = \{\tau_{a,b} | a \in U_n, b \in \mathbb{Z}_n\}$ لذا تعداد انتخاب ها برای a ، $\varphi(n)$ است و تعداد انتخاب های

n, b می باشد چون این انتخاب ها مستقل از یکدیگر هستند در نتیجه $|A(X_n)| = n \cdot \varphi(n)$. $\square$

قضیه ۷.۱.۴. برای هر $n \geq ۲$ ، $|A(X_n)| \leq |AUT(X_n)|$ و تساوی برقرار است اگر و تنها اگر $n \in \{۲, ۳, ۴, ۶\}$.

برهان. در قضیه ۲۸.۲.۲، نشان دادیم که مجموعه $A(X_n)$ زیرگروه مجموعه $AUT(X_n)$ می باشد بنابراین $|A(X_n)| \mid |AUT(X_n)|$ در نتیجه $|A(X_n)| \leq |AUT(X_n)|$. با جایگذاری مقادیر مجموعه ها با توجه به قضایای قبل، داریم:

$$\frac{|AUT(X_n)|}{|A(X_n)|} = \frac{p_1! p_2! \cdots p_k!}{p_1 p_2 \cdots p_k (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)} \cdot \left(\frac{(p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1})!}{p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1}} \right)^2 \cdot ((p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1})!)^{(p_1 p_2 \cdots p_k - 2)}$$

بنابراین

$$|A(X_n)| = |AUT(X_n)| \Leftrightarrow \begin{cases} ((p_1 - 2)!(p_2 - 2)! \cdots (p_k - 2)! = 1 \\ \text{و} \\ (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1})!^{(p_1 p_2 \cdots p_k - 2)} = 1 \\ \text{و} \\ ((p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1} - 1)!)^2 = 1 \end{cases}$$

عبارت

$$(p_1 - 2)!(p_2 - 2)! \cdots (p_k - 2)! = 1 \Leftrightarrow \forall 1 \leq i \leq k, (p_i - 2)! = 1$$

در نتیجه این تساوی در صورتی برقرار است، اگر و تنها اگر تنها عامل های اول n ، ۲ و ۳ باشند. برای $n \geq ۲$ ،

$$p_i \neq 0 \Rightarrow p_i^{\alpha_i-1} \neq 0 \Rightarrow (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1}) \neq 0$$

بنابراین جمله

$$(p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1})!^{(p_1 p_2 \cdots p_k - 2)} = 1 \Leftrightarrow (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1})! = 1$$

$$\Leftrightarrow (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1}) = 1$$

$$\Leftrightarrow \forall 1 \leq i \leq k, p_i^{\alpha_i-1} = 1$$

$$\Leftrightarrow \alpha_i - 1 = 0$$

در نتیجه n عدد خالی از مربع می باشد و عامل

$$((p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} - 1)!)^2 = 1 \Leftrightarrow (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} - 1)! = 1$$

$$\Leftrightarrow p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} = 1$$

یا

$$\Leftrightarrow p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} = 2$$

جمله

$$p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} = 1 \Leftrightarrow \alpha_i - 1 = 0$$

لذا n عدد خالی از مربع است و

$$(p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1}) = 2 \Leftrightarrow k = 1, p_1 = 2, \alpha_1 = 2$$

در این صورت n دو برابر عدد خالی از مربع می باشد. بنابراین تساوی این دو مقدار در صورتی برقرار می باشد

که $n \in \{2, 3, 4, 6\}$. بنابراین برای $n = 5, n > 6$ ، $|A(X_n)| < AUT(X_n)$ است. $\square$

مراجع

- [۱] باندی، مورتی، (۱۳۷۸)، نظریه‌ی گراف و کاربردهای آن، ترجمه د معظمی، چاپ اول، مرکز نشر دانشگاهی، تهران.
- [۲] علیرضا. جمالی، (۱۳۸۰)، مباحثی در نظریه‌ی گروه‌ها، چاپ اول، انتشارات مبتکران، تهران.
- [۳] گری چارتراند، آرتروود اولرمن، (۱۳۸۳)، نظریه الگوریتمی و کاربردی گراف‌ها، چاپ اول، انتشارات دانشگاه صنعتی امیرکبیر، تهران.
- [۴] ارزنگ. علی آبادی، (۱۳۸۵)، نظریه اعداد، چاپ اول، انتشارات پیام نور، تهران.
- [5] J. L. R. Alfonsin, and B.A. Reed. Perfect graphs. John Wiley and Sons, New York-Chichester-Brisbane, 2001
- [6] M. Basic and A. Ilic. On the automorphism group of integral circulant graphs (2009).
- [7] R. Balakrishnan and K. Ranganathan. A Textbook Of Graph Theoy, Springer-verlag New York, Inc , New York, 2000.
- [8] P. Berrizbeitia, and R.E. Giudic. On cycles in the sequence of unitary Cayley graphs. Discrete Math. 282, 1-3 (2004), 239-243.
- [9] N. Biggs. Algebra graph theory , Second Edition. Cambridge Mathematical Laibrary. Cambridge University Press 1993.
- [10] F. Boesch, and R. Tindell. Circulants and their connectivities. J. Graph Theory 8 (1984), 487-499.
- [11] Chudnovsky, Robertson, Seymour, Thomas. The strong perfect graph theorem. Annals of math. 164 (2002), 51-229.
- [12] P.J. Davis. Circulant matrices. A Wiley-Interscience Publication, Pure and Applied Mathematics. John Wiley and Sons, New York-Chichester-Brisbane, 1979.
- [13] I.J. Dejter. Totally multicolored subgraphs of complete Cayley graphs, Congressus. Num. 70, (1990), 53-64.
- [14] I.J. Dejter, and R.E. Giudici. On unitary cayley graphs , J. combin.math.18(1995), 121-124
- [15] E.D. Fuchs. Longest induced cycles in circulant graphs. The Electronic J. Comb. 12(2005), 1-12.
- [16] E.D. Fuchs, and J Sinz. Longest induced cycles in Cayley graphs. eprint arXiv:math/04103008 (2008) 1-16
- [17] R.E. Giudici and E. Lima de Sa, Chromatic uniqueness of certain bipartite graphs, Congressus Numerantium, 76 (1990), 69-75.

-
- [18] R. Gould. Graph Theory, *The Benjamin/ Commings Publishing Company, Inc, Menlo Park, California*, 1988.
- [19] W. Klortz and T. Sander. Some properties of unitary Cayley graphs, *electron.j. combin.***14** (2007).
- [20] D.H. Lehmer. On Eulers totient function *Bull. Amer.math.Soc.* **38** (1932), 745-751
- [21] B. Maheswari and M. Lavaku. Enumeration of triangles and Hamilton Cycles in quadratic residue Cayley graphs, *Journal of Mathematics, volume 1, no 1, (2009)* 95-103.
- [22] P.J. Mccarthy. Introduction to arithmetical function *Universitext. Springer-Verlage, New York*, 1986
- [23] H.E. Rose. A course in number theory *Oxford Science Publications. Oxford University Press*, 1994
- [24] M.E. watkins. connectivity of transitive graphs *J-comb. theory* **8** (1970), 23-29

واژه‌نامه فارسی به انگلیسی

<i>cut</i>	برش
<i>vertex cut</i>	برشی راسی
<i>minimum cut</i>	برش مینیمم
<i>edge cut</i>	برش یالی
<i>bridge</i>	پل
<i>incidence function</i>	تابع وقوع
<i>chromatic polynomial</i>	چند جمله‌ای رنگی
<i>Strong Perfect Graph Conjecture</i>	حدس قوی گراف تام
<i>degree</i>	درجه
<i>automorphism</i>	خودریختی
<i>clique</i>	خوشه
<i>cycle</i>	دور
<i>even(odd) cycle</i>	دور زوج(فرد)
<i>hamilton cycle</i>	دور همیلتنی
<i>vertex</i>	راس
<i>vertex-transitive</i>	راس-ترایا
<i>internal vertices</i>	راس‌های داخلی

<i>vertex colouring</i>	رنگ آمیزی راسی
<i>subgraph</i>	زیر گراف
<i>induced subgraph</i>	زیر گراف القایی
<i>edge-disjoint</i>	یال-مجزا
<i>network</i>	شبکه
<i>loop</i>	طوقه
<i>length</i>	طول
<i>independence number</i>	عدد استقلال
<i>chromatic number</i>	عدد رنگی
<i>edge chromatic number</i>	عدد رنگی یالی
<i>diameter</i>	قطر
<i>graph</i>	گراف
<i>bipartite graph</i>	گراف دو بخشی
<i>complete graph</i>	گراف کامل
<i>regular graph</i>	گراف منظم
<i>disconnected graph</i>	گراف غیر همبند
<i>connected graph</i>	گراف همبند
<i>k-chromatic graph</i>	گراف k - رنگی
<i>k-regular graph</i>	گراف k - منتظم
<i>k-connected graph</i>	گراف k - همبند
<i>adjacency matrix</i>	ماتریس مجاورت
<i>triangle</i>	مثلث

<i>adjacent</i>	مجاور
<i>independent set</i>	مجموعه مستقل
<i>path</i>	مسیر
<i>internally-disjoint paths</i>	مسیرهای مجزای داخلی
<i>hamilton path</i>	مسیر همبستگی
<i>component</i>	مولفه
<i>connectivity</i>	همبندی
<i>edge connectivity</i>	همبندی یالی
<i>edge</i>	یال
<i>cut edge</i>	یال برشی
<i>edge-transitive</i>	یال-ترا یا

واژه‌نامه انگلیسی به فارسی

<i>adjacency matrix</i>		ماتریس مجاورت
<i>adjacent</i>		مجاور
<i>automorphism</i>		خودریختی
<i>bridge</i>		پل
<i>bipartite graph</i>		گراف دو بخشی
<i>chromatic number</i>		عدد رنگی
<i>chromatic polynomial</i>		چند جمله‌ای رنگی
<i>clique</i>		خوشه
<i>complete graph</i>		گراف کامل
<i>component</i>		مولفه
<i>connected graph</i>		گراف همبند
<i>connectivity</i>		همبندی
<i>cut</i>		برش
<i>cut edge</i>		یال برشی
<i>cycle</i>		دور
<i>degree</i>		درجه
<i>diameter</i>		قطر

<i>disconnected graph</i>	گراف غیر همبند
<i>edge</i>	یال
<i>edge chromatic number</i>	عدد رنگی یالی
<i>edge connectivity</i>	همبندی یالی
<i>edge cut</i>	برش یالی
<i>edge-disjoint</i>	یال-مجزا
<i>edge-transitive</i>	یال-ترایا
<i>even(odd) cycle</i>	دور زوج(فرد)
<i>graph</i>	گراف
<i>hamilton cycle</i>	دور همیلتنی
<i>hamilton path</i>	مسیر همیلتنی
<i>incidence function</i>	تابع وقوع
<i>independent set</i>	مجموعه مستقل
<i>independence number</i>	عدد استقلال
<i>induced subgraph</i>	زیر گراف القایی
<i>internally-disjoint paths</i>	مسیرهای مجزای داخلی
<i>internal vertices</i>	راس‌های داخلی
<i>k-chromatic graph</i>	گراف k - رنگی
<i>k-connected graph</i>	گراف k - همبند
<i>k-regular graph</i>	گراف k - منتظم
<i>length</i>	طول
<i>loop</i>	طوقه

<i>minimum cut</i>	برش مینیمم
<i>network</i>	شبکه
<i>path</i>	مسیر
<i>regular graph</i>	گراف منظم
<i>Strong Perfect Graph Conjecture</i>	حدس قوی گراف تام
<i>subgraph</i>	زیر گراف
<i>triangle</i>	مثلث
<i>vertex</i>	راس
<i>vertex colouring</i>	رنگ آمیزی راسی
<i>vertex cut</i>	برشی راسی
<i>vertex-transitive</i>	راس-ترایا

Surname: Koshkee

Name: Efat

Title: Some Properties Of Unitary Cayley Graphs

Supervisor: Dr.Heydar Jafari

Advisor: Dr.Nader Jafari rad

Degree: Master of Science

Subject: Pure Mathematics

Field: Algebra

Shahrood University of Technology

Faculty Of Mathematical Sciences

Date: 2012

Number of pages: 73

Keywords: unitary cayley graph, clique number,chromatic number,vertex connectivity , eigenvalues, independence number

Abstract

The unitary cayley graph X_n has vertex set $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$. vertices a and b are adjacent, if $\gcd(a - b, n) = 1$. For X_n chromatic number, the clique number, the independence number, the diameter and the vertex connectivity are determined. We deside under perfect ness of X_n and show that all nonzero eigenvalues of X_n are integers dividing the value $\varphi(n)$ of the Euler function.



*Shahrood University of Technology
Faculty Of Mathematical Sciences*

*Dissertation Submitted in Partial
Fulfillment of The Requirements For The
Degree of Master of Science in
Pure Mathematics*

Some Properties Of Unitary Cayley Graphs

Supervisor

Dr. Heydar Jafari

Advisor

Dr. Nader Jafari rad

by

Efat Koshkee

2012