
بسم الله الرحمن الرحیم

**دانشگاه الزهرا**
**دانشکده علوم پایه**
**گروه ریاضی**

**رساله جهت اخذ درجه دکتری**

**عنوان**

# طرح توزیع کلید و پوشش‌های دوبخشی کامل

نگارش
فرخ‌لقا معظمی گودرزی

استاد راهنما
**دکتر نسرین سلطانخواه**
استاد مشاور
**دکتر حسین حاجی‌ابوالحسن**

شهریور ۱۳۹۱

کلیه دستاوردهای این تحقیق متعلق به
دانشگاه الزهرا(س) است.

بسمه تعالی

دانشگاه الزهرا
دانشکده علوم پایه گروه ریاضی

عنوان:
# طرح توزیع کلید و پوشش دوبخشی کامل

استاد راهنما: دکتر نسرین سلطانخواه
دانشجو: فرخ‌لقا معظمی‌گودرزی

این پروژه تحت قرارداد پژوهشی شماره ۵۰۰/۶۰۷۹/ت مورخ ۹۰/۴/۱۸ از پشتیبانی معنوی و مادی موسسه تحقیقات ارتباطات و فناوری اطلاعات ایران بهره‌مند شده است.

تقدیم به تمام کسانی که معنی محبت و دوست داشتن را می دانند

مخصوصاً پدر و مادرم که معنی واقعی آن را به من آموختن.

# قدردانی

ستایش برای خداست آن نخستین بی‌آغاز و واپسین بی‌انجام. ستایش برای خداست که خود را به ما شناساند و شیوه سپاسگزاری از خود رابه ما آموخت و درهای علم به پروردگاریش را به روی ما گشود و ما را به اخلاص ورزیدن به توحید خود رهنمون ساخت.

در آغاز وظیفه خود می‌دانم از زحمات استاد راهنمای خود، سرکار خانم دکتر نسرین سلطانخواه، صمیمانه تشکر و قدردانی کنم.

همچنین از جناب آقای دکتر حسین حاجی‌ابوالحسن که با اخلاق گرم و صمیمی خود علم بی‌پایانشان را صمیمانه در اختیار من قرار دادند و در آماده سازی این رساله، به نحو احسن اینجانب را مورد راهنمایی قرار دادند، کمال امتنان را دارم.

از جناب آقایان دکتر بهمردی، دکتر اردوخانی، دکتر دانشگر و سرکار خانم دکتر اسلامی که زحمت مطالعه و داوری این رساله را تقبل فرمودند و با پیشنهادات ارزنده خود باعث بهبود این رساله شدند، تشکر و قدردانی می‌کنم.

در پایان، بوسه می‌زنم بر دستان خداوندگاران مهر و مهربانی، پدر و مادر عزیزم و بعد از خدا، ستایش می‌کنم وجود مقدس‌شان را. همچنین تشکر می‌کنم از برادران عزیزم به پاس عاطفه سرشار و گرمای امیدبخش وجودشان، که در این سردترین روزگاران، بهترین پشتیبان من بودند.

## چکیده

ارائه روش‌هایی که به کمک آن‌ها بتوان طرح‌های توزیع کلید امن و کم هزینه ساخت در علم رمزنگاری از اهمیت ویژه‌ای برخوردارند. الگوی توزیع کلید که با کمک یک خانواده عاری از پوشش ساخته می‌شود ابزاری است که چنین نیازی را برآورده می‌کند. الگوی توزیع کلید یک $(۰,۱)$-ماتریس $M$، $v \times n$ است، که در آن شخص $j$-ام کلید $k_i$ را دریافت می‌کند اگر و تنها اگر $M(i,j) = ۱$. یک $(r,w;d)$-خانواده عاری از پوشش خانواده‌ای از زیر مجموعه‌های مجموعه $X$ است که اشتراک هر $r$تا از مجموعه‌های این خانواده حداقل شامل $d$ عضو است که در اجتماع هیچ $w$تا از مجموعه‌های دیگر این خانواده قرار نمی‌گیرد. مینیمم اندازه مجموعه $X$ که برای آن یک $(r,w;d)$-خانواده عاری از پوشش با $t$ مجموعه وجود داشته باشد با نماد $N((r,w;d),t)$ نمایش داده می‌شود. یک $d$-پوشش دوبخشی کامل از گراف $G$ خانواده‌ای از زیرگراف‌های دوبخشی کامل $G$ هستند که هر یال $G$ حداقل توسط $d$تا از گراف‌های این خانواده پوشیده شود. کمترین تعداد دوبخشی‌های کامل که به کمک آن‌ها بتوان هر یال گراف $G$ را حداقل $d$ بار پوشاند عدد $d$-پوشش دوبخشی کامل نامیده می‌شود. در این رساله ابتدا به بررسی ویژگی‌های عدد $d$-پوشش دوبخشی کامل گراف‌ها در حالت کلی می‌پردازیم. سپس نشان می‌دهیم $N((r,w;d),t)$ برابر است با $d$-پوشش دوبخشی کامل گراف $I_t(r,w)$ که یک گراف دوبخشی است که مجموعه رأس‌های آن زیرمجموعه‌های $r$-عضوی و $w$-عضوی از یک مجموعه $t$ عضوی است. در این گراف یک رأس نظیر یک مجموعه $r$-عضوی به یک رأس نظیر یک مجموعه $w$-عضوی وصل است اگر وتنها اگر اشتراک مجموعه‌های نظیرشان تهی باشد. سپس کران‌هایی را برای پارامتر $N((r,w;d),t)$ ارائه می‌دهیم. همچنین مقدار دقیق $N((r,w;d),t)$ را در حالت‌های خاصی محاسبه می‌کنیم.

در یک کد دودویی $\Gamma$ از طول $v$، یک $v$-کدکلمه $w = (w_۱,\ldots,w_v)$ توسط یک مجموعه $\{w^۱,\ldots,w^r\} \subseteq \Gamma$ از کدکلمه‌ها تولید می‌شود هرگاه برای هر $i = ۱,\ldots,v$، داشته باشیم $w_i \in \{w_i^۱,\ldots,w_i^r\}$. می‌گوییم یک کد، $r$-امن در برابر جعل از اندازه $t$ است هرگاه $|\Gamma| = t$ و برای هر $v$-کدکلمه‌ای که توسط دو مجموعه $C_۱$ و $C_۲$ از اندازه حداکثر $r$ تولید شده باشد آنگاه اشتراک این دو مجموعه ناتهی باشد. در این رساله نشان می‌دهیم که برای $t \geq ۲r$ یک کد $r$-امن در برابر جعل از اندازه $t$ و طول $v$ وجود دارد اگر و تنها اگر یک ۱-پوشش دوبخشی کامل برای گراف کنسر $\mathrm{KG}(t,r)$ وجود داشته باشد. سپس ارتباط $d$-پوشش دوبخشی کامل از گراف‌های کنسر را با خانواده‌های عاری از پوشش بیان می‌کنیم. در پایان به بررسی ویژگی‌های $d$-پوشش دوبخشی کامل گراف‌های کنسر می‌پردازیم.



**واژه‌های کلیدی:** *طرح توزیع کلید، الگوی توزیع کلید، خانواده‌های عاری از پوشش، پوشش دوبخشی کامل، کدهای ضدجعل*

# پیشگفتار

سیستم‌های رمزنگاری در حالت کلی به دو دسته عمده تقسیم می‌شوند. سیستم‌های رمزنگاری با کلید عمومی و سیستم‌های رمزنگاری با کلید خصوصی. در سیستم‌های رمزنگاری با کلید عمومی، امنیت سیستم مبتنی بر حل یک مسأله سخت در ریاضیات است. به عنوان مثال در سیستم‌های رمزنگاری $RSA$، $ELGAMAL$ و $NTRU$ که از مهم‌ترین سیستم‌های رمزنگاری با کلید عمومی هستند امنیت سیستم به ترتیب مبتنی بر سختی مسأله تجزیه اعداد، مسأله لگاریتم گسسته و مسأله پیدا کردن کوتاهترین فاصله در مشبکه‌هاست. در این سیستم‌های رمزنگاری برای رسیدن به یک امنیت مطلوب، نیازمندیم که از اعداد بسیار بزرگ استفاده کنیم. استفاده از اعداد بزرگ نیازمند صرف هزینه و وقت زیاد است. لذا این سیستم‌ها گران و کند هستند و در بسیاری از کاربردهای روزانه امکان استفاده از این سیستم‌های رمزنگاری وجود ندارد. البته قابل ذکر است که امروزه بعضی از افراد معتقدند که با گسترش علم و ساختن کامپیوترهایی با حجم محاسباتی بالا امکان تجزیه اعداد بزرگ و حل مسائل سخت هم وجود دارد و لذا امنیت این سیستم‌ها از دیدگاه این عده از افراد تضمین شده نیست. همچنین بعضی‌ها معتقدند که هر لحظه ممکن است شخصی پیدا شود و الگوریتم مناسبی برای حل این مسائل در زمان چندجمله‌ای ارائه دهد. بنابراین، امروزه تمایل بسیاری از افراد در استفاده از سیستم‌های رمزنگاری مبتنی بر کلید عمومی کمتر شده. در سیستم‌های رمزنگاری دسته دوم یعنی سیستم‌های رمزنگاری با کلید خصوصی امنیت مبتنی بر امنیت کلید است. یعنی در این سیستم‌ها تا زمانی که کلید سیستم لو نرفته باشد، سیستم رمزنگاری امن است. از جمله مهم‌ترین سیستم‌های رمزنگاری با کلید خصوصی می‌توان سیستم‌هایی مانند $DES$ و $AES$ را نام برد. مشکل اصلی و بزرگی که در این دسته از سیستم‌های رمزنگاری وجود دارد نحوه توزیع کلید بین دو نفری است که قرار است با هم مکاتبه داشته باشند. داشتن یک کانال امن برای ارسال کلید در دنیای واقعی عملاً غیر ممکن است و زمانی که تعداد افراد موجود در یک شبکه زیاد است، نمی‌توان این کار را از طریق حضوری انجام داد. بنابراین ارائه یک روش

مناسب برای توزیع کلید در دنیای رمزنگاری از ابتدای پیدایش این علم مسأله‌ای چالش برانگیز بوده و توجه بسیاری از محققان این علم را به خود جلب کرده است. شاید بتوان توزیع کلید دفی-هلمن را به‌عنوان یکی از ابتدایی‌ترین روش‌ها برای مسأله توزیع کلید دانست. این روش دارای ایده جالبی است که بعدها افراد دیگر از این ایده کمک گرفتند و با استفاده از آن سیستم‌های رمزنگاری با کلید عمومی را ابداع کردند. امنیت کلید در این توزیع کلید یک امنیت محاسباتی است. چون کلید در این توزیع کلید تا زمانی امن است که مسأله لگاریتم گسسته سخت باشد و الگوریتم مناسبی برای محاسبه لگاریتم گسسته وجود نداشته باشد. لذا استفاده از این روش مشکلات استفاده از سیستم‌های رمزنگاری با کلید عمومی را داراست، یعنی کند و پرهزینه است. اما در بیشتر کاربردها به دنبال روش‌هایی برای توزیع کلید هستیم که از نظر حجم محاسبه، هزینه و سرعت عمل مناسب باشند.

الگوی توزیع کلید یک $(۰,۱)$-ماتریس$v \times n$، $M$ است، که در آن شخص $j$-ام کلید $k_i$ را دریافت می‌کند اگر و تنها اگر $M(i,j) = ۱$. ماتریس$M$ را الگوی توزیع کلید می‌نامند. برای یک الگوی توزیع کلید $M$ و یک زیر مجموعه $P$ از شرکت کنندگان مجموعه کلید $P$ را به صورت

$$Keys(P) = \{i \mid M(i,j) = ۱, \quad U_j \in P\}$$

تعریف می‌کنیم. در حالتی که $Keys(P) \neq \varnothing$ افراد $P$ می‌توانند با هم کلید مشترک داشته باشند و کلید این گروه برابر است با حاصل جمع کلیدهای $k_i$ که $i$ عضوی از $Keys(P)$ است. حال اگر $M$ در بعضی از شرط‌های ترکیبیاتی صدق کند، آنگاه توزیع کلید در برابر ائتلاف بعضی از افراد شبکه می‌تواند امن باشد.

یک $(r,w;d)$-خانواده عاری از پوشش خانواده‌ای از زیر مجموعه‌های مجموعه $X$ است که اشتراک هر $r$تا از مجموعه‌های این خانواده حداقل شامل $d$ عنصر است که در اجتماع هیچ $w$تا از مجموعه‌های دیگر این خانواده قرار نمی‌گیرند. مینیمم اندازه مجموعه $X$ که برای آن یک $(r,w;d)$-خانواده عاری از پوشش با $t$ عضو وجود داشته باشد با نماد $N((r,w;d),t)$ نمایش داده می‌شود. اگر یک خانواده عاری از پوشش داشته باشیم به کمک آن می‌توان الگوی توزیع

کلیدی ساخت که هر $r$ نفری دارای حداقل $d$ کلید مشترک هستند که در برابر ائتلاف هر $w$ نفری دارای امنیت بدون شرط است. در روش‌هایی که برای توزیع کلید ارائه می‌شود هزینه و امنیت دو پارامتر اساسی هستند. ارائه روش‌هایی که به کمک آن‌ها بتوان طرح‌های توزیع کلید امن و کم هزینه‌ای ساخت در علم رمزنگاری از اهمیت ویژه‌ای برخوردارند. الگوی توزیع کلید که با کمک یک خانواده عاری از پوشش ساخته می‌شود ابزاری است که چنین نیازهایی را برآورده می‌کند. خانواده‌های عاری از پوشش اولین بار در سال ۱۹۶۴ توسط کاتز و سینگلتون برای مطالعه رده خاصی از کدها تعریف شد. در سال ۱۹۸۵ اردوش این خانواده‌ها را به عنوان تعمیمی از سیستم‌های اسپرنر تعریف کرد و به مطالعه ویژگی‌های این خانواده از مجموعه‌ها پرداخت. در سال‌های اخیر از این خانواده‌ها در زمینه‌های مختلف رمزنگاری خصوصاً ساختن طرح‌های توزیع کلید استفاده شده است. برای ساختن این خانواده‌ها از طرح‌های بلوکی و دیگر ساختارهای ترکیبیاتی و گرافی، استفاده شده است. کاربرد بسیار وسیع این خانواده‌ها ما را بر آن داشت که در این رساله به مطالعه ویژگی‌های این ابزارهای ترکیبیاتی بپردازیم. یک $d$-پوشش دوبخشی کامل از گراف $G$ خانواده‌ای از زیرگراف‌های دوبخشی کامل $G$ هستند که هر یال $G$ حداقل توسط $d$تا از گراف‌های این خانواده پوشیده شود. کمترین تعداد دوبخشی‌های کاملی که به کمک آن‌ها بتوان هر یال $G$ را حداقل $d$ بار پوشاند عدد $d$-پوشش دوبخشی کامل نامیده می‌شود و با نماد $bc_d(G)$ نمایش داده می‌شود. در این رساله ارتباط مستقیمی بین خانواده‌های عاری از پوشش و پوشش دوبخشی کامل ایجاد می‌کنیم.

در فصل اول این رساله ابتدا به بررسی ویژگی‌های عدد $d$-پوشش دوبخشی کامل گراف‌ها در حالت کلی می‌پردازیم. سپس تعریف پوشش دوبخشی کامل کسری گراف‌ها را بیان می‌کنیم و به کمک آن کران‌هایی را برای عدد $d$-پوشش دوبخشی کامل گراف‌ها ارائه می‌دهیم. همچنین یک کران بالا برای عدد $d$-پوشش دوبخشی کامل حاصلضرب الفبایی گراف‌ها بیان می‌کنیم و در ادامه کران‌هایی را برای عدد $d$-پوشش دوبخشی کامل الحاق گراف‌ها و گراف‌های میسلسکی به دست می‌آوریم. در پایان این فصل تعمیمی که آلن برای پوشش دوبخشی کامل گراف‌ها ارائه داد

را مورد بررسی قرار می‌دهیم. مقاله‌های مستخرج از این فصل مقاله‌های [۳۱] و [۳۲] است.

در فصل دوم ابتدا مقدمه‌ای در مورد طرح توزیع کلید بیان می‌کنیم. سپس الگوی توزیع کلید و ارتباط آن با خانواده‌های عاری از پوشش را بیان می‌کنیم. در ادامه به بیان بعضی از کاربردهای خانواده‌های عاری از پوشش می‌پردازیم. سپس نشان می‌دهیم $N((r,w;d),t)$ با $d$-پوشش دوبخشی کامل گراف $I_t(r,w)$ برابر است. همچنین کران‌هایی را برای پارامتر $N((r,w;d),t)$ ارائه می‌دهیم. در انتها مقدار دقیق $N((r,w;d),t)$ را در حالتی که $t \leq r+w+\frac{r}{w}$ و همچنین برای بعضی از $d$ها محاسبه می‌کنیم. مقاله مستخرج از این فصل مقاله [۲۱] است.

در یک کد دودویی $\Gamma$ از طول $v$، یک $v$-کدکلمه $w$ می‌تواند توسط یک مجموعه $\{w^1,\ldots,w^r\} \subseteq \Gamma$ از کدکلمه‌ها تولید شود هرگاه برای هر $i=1,\ldots,v$، داشته باشیم $w_i \in \{w_i^1,\ldots,w_i^r\}$. می‌گوییم یک کد، $r$-امن در برابر جعل از اندازه $t$ است هرگاه $|\Gamma|=t$ و برای هر $v$-کدکلمه‌ای که توسط دو مجموعه $C_1$ و $C_2$ از اندازه حداکثر $r$ تولید شده باشد اشتراک این دو مجموعه ناتهی باشد.

در فصل سوم از این رساله نشان می‌دهیم که برای $t \geq 2r$ یک کد $r$-امن در برابر جعل از اندازه $t$ و طول $v$ وجود دارد اگر و تنها اگر یک، ۱-پوشش دوبخشی کامل برای گراف کنسر $\mathrm{KG}(t,r)$ وجود داشته باشد. سپس ارتباط $d$-پوشش دوبخشی کامل از گراف‌های کنسر را با خانواده‌های عاری از پوشش بیان می‌کنیم. در پایان به بررسی ویژگی‌های $d$-پوشش دوبخشی کامل گراف‌های کنسر می‌پردازیم و با کمک روش‌های احتمالاتی یک کران بالا برای عدد $d$-پوشش دوبخشی کامل گراف‌های کنسر ارائه می‌دهیم. مقاله مستخرج از این فصل مقاله [۲۲] است.

# فهرست مطالب

# فصل ۱
# پوشش دوبخشی کامل

## ۱.۱ مقدمه

گراف $G$ را **دوبخشی** نامند هرگاه مجموعه رأس‌های آن را بتوان به دو مجموعه $X$ و $Y$ افراز کرد به‌قسمی که هر یال گراف یک رأسش در $X$ و رأس دیگرش در $Y$ باشد. گراف دوبخشی $G$ با مجموعه رأس‌های $V = X \cup Y$ را **دوبخشی کامل** نامند هرگاه هر رأس از $X$ به تمام رأس‌های $Y$ وصل باشد. یک **پوشش دوبخشی کامل** برای گراف $G$ خانواده‌ای از زیرگراف‌های دوبخشی کامل گراف $G$ مانند $\{G_۱, G_۲, \ldots, G_t\}$ است به‌گونه‌ای که برای هر یال از گراف حداقل یک $۱ \leq i \leq t$ وجود داشته باشد که $G_i$ شامل آن یال باشد. کمترین تعداد دوبخشی‌های کامل در یک پوشش دوبخشی کامل **عدد پوشش دوبخشی کامل** نامیده می‌شود و با نماد $bc(G)$ نمایش داده می‌شود. این پارامتر در نظریه گراف توجه افراد زیادی را به خود جلب کرده و مقاله‌های زیادی برای بررسی ویژگی‌های این پارامتر در گراف‌ها نوشته شده است که از جمله می‌توان به مراجع [۱، ۳، ۱۹، ۲۳، ۴۶] اشاره کرد. این پارامتر تعمیم‌های جالب و پرکاربردی دارد به عنوان مثال آلن در [۱] تعمیمی از این پارامتر را به صورت زیر ارائه داد.

**تعریف ۱.۱.۱.** *فرض کنید $K$ مجموعه‌ای متشکل از $k$ عدد صحیح و مثبت باشد. یک پوشش کامل دوبخشی از گراف $G$ از نوع $K$ نامیده می‌شود هرگاه برای هر یال از گراف $G$ تعداد*

*دوبخشی‌های کاملی که شامل آن یال هستند عددی از مجموعه $K$ باشد.* ♠

آلن کاربرد هندسی جالب توجهی از این پارامتر برای گراف کامل بیان کرد. سپس کران‌های بالا و پایینی برای این پارامتر در گراف‌های کامل ارائه داد. در این رساله ما تعمیم دیگری از این پارامتر را تعریف می‌کنیم و نشان می‌دهیم که این تعمیم برای بعضی از گراف‌های خاص که در فصل‌های بعد تعریف می‌شوند ارتباط مستقیمی با مفهوم الگوی توزیع کلید و بعضی دیگر از مفاهیم رمزنگاری دارد. لذا ابتدا در این فصل این تعمیم از پوشش دوبخشی کامل را بیان می‌کنیم و به بررسی ویژگی‌های این پارامتر برای گراف‌ها در حالت کلی می‌پردازیم. سپس نگاهی کوتاه به تعمیم آلن می‌اندازیم و کران به‌دست آمده برای این پارامتر را تا حدی بهبود می‌بخشیم. سپس در فصل‌های بعد به مبحث توزیع کلید و ارتباط آن با این مفهوم گرافی می‌پردازیم. مقاله‌های مستخرج از این فصل مقاله‌های [۳۱] و [۳۲] است.

## ۲.۱ پوشش دوبخشی کامل

در این بخش بحث را با تعریف زیر که یکی از تعاریف اصلی در سرتاسر این رساله است شروع می‌کنیم.

**تعریف ۱.۲.۱.** *یک خانواده از زیرگراف‌های دوبخشی کامل از گراف $G$ یک $d$-پوشش دوبخشی کامل نامیده می‌شود هرگاه هر یال $G$ حداقل توسط $d$ تا از گراف‌های این خانواده پوشیده شود. (توجه کنید که بعضی از زیرگراف‌های دوبخشی کامل در این خانواده می‌توانند تکراری باشند.) کمترین تعداد دوبخشی‌های کامل که به کمک آن‌ها بتوان هر یال گراف $G$ را حداقل $d$ بار پوشاند* ***عدد $d$-پوشش دوبخشی کامل*** *نامیده می‌شود و با نماد $bc_d(G)$ نمایش داده می‌شود.* ♠

در ادامه این بخش تعاریف و نمادهای لازم را بیان می‌کنیم همچنین مشاهده‌های ساده‌ای که در مورد $d$-پوشش دوبخشی کامل گراف‌ها وجود دارد را ارائه می‌دهیم. سپس در بخش‌های بعدی به

بیان قضیه‌های کلی‌تر می‌پردازیم. در این رساله تمامی گراف‌هایی که در نظر می‌گیریم گراف ساده هستند. فرض کنید $V(G)$ و $E(G)$ به ترتیب نمایش دهنده مجموعه رأس‌ها و مجموعه یال‌های گراف $G$ باشند. نگاشت $\phi : V(G) \to V(H)$ را یک **همریختی** بین $G$ و $H$ نامند هرگاه تابع $\phi$ مجاورت را حفظ کند. به عبارت دیگر $\phi$ یک همریختی است هرگاه، اگر $uv$ یالی از $G$ باشد آنگاه $\phi(u)\phi(v)$ یالی از $H$ باشد. به‌علاوه اگر هر یال $H$ تصویر یالی از $G$ باشد این همریختی را یک **همریختی پوشای-یالی** می‌نامند. دو گراف $G$ و $H$ را **یکریختی** گویند هرگاه یک همریختی یک به یک و پوشا از $G$ به $H$ وجود داشته باشد. گراف ساده $G$ **رأس-ترایا** است هرگاه برای هر دو رأس دلخواه $u$ و $v$ یک یکریختی $\phi : G \to G$ وجود داشته باشد به‌گونه‌ای که $\phi(u) = v$. مشابهاً گراف ساده $G$ **یال-ترایا** نامیده می‌شود هرگاه برای هر دویال دلخواه $u_۱v_۱$ و $u_۲v_۲$ از گراف $G$ یک یکریختی مانند $\phi$ وجود داشته باشد به‌گونه‌ای که $\phi(u_۱)\phi(v_۱) = u_۲v_۲$.

در این رساله نماد $B(G)$ نمایش دهنده بیشترین تعداد یال‌های یک زیر گراف دوبخشی کامل از گراف $G$ است. با یک مشاهده ساده می‌توان دید که $d|E(G)| \leq bc_d(G)B(G)$. بنابراین لم زیر به‌سادگی نتیجه می‌شود.

**لم ۲.۲.۱.** [۳۲] *برای هر گراف $G$ داریم $d\frac{|E(G)|}{B(G)} \leq bc_d(G)$.*

**تعریف ۳.۲.۱.** *زیرمجموعه $K$ از مجموعه رأس‌های گراف $G$ را یک **پوشش** برای گراف $G$ نامند هرگاه هر یال گراف $G$ حداقل یکی از رأس‌هایش در مجموعه $K$ باشد. تعداد رأس‌هایی که در کوچکترین پوشش گراف $G$ قرار گرفته است **عدد پوششی** گراف $G$ نامیده می‌شود و با نماد $\beta(G)$ نمایش داده می‌شود.* ♠

یک ستاره درختی است با $n$ رأس که یک رأس از درجه $n-۱$ دارد و بقیه رأس‌های آن از درجه ۱ هستند. رأس از درجه $n-۱$ مرکز ستاره نامیده می‌شود. گراف $k$-مکعب $Q_k$ گرافی است که

مجموعه رأس‌های آن $k$ -تایی‌هایی با درایه‌های ۰ و ۱ هستند و دو رأس در این گراف مجاورند اگر و فقط اگر دقیقاً در یک مؤلفه متمایز باشند. به‌وضوح $k$ -مکعب $Q_k$ دارای $2^k$ رأس و $k2^{k-1}$ یال است و گرافی دوبخشی است. باتوجه به دوبخشی بودن گراف $Q_k$، اگر ستاره‌هایی به مرکز رأس‌های یکی از بخش‌های این گراف را $d$ بار در نظر بگیریم، $d$-پوشش دوبخشی کاملی از گراف با اندازه $d2^{k-1}$ حاصل می‌شود. از طرف دیگر بزرگترین زیرگراف دوبخشی کامل در $Q_k$ با شرط $k \geq 5$ یک ستاره با $k$ یال است. بنابراین با استفاده از لم (۲.۲.۱) داریم، $bc_d(Q_k) \geq d2^{k-1}$. پس می‌توان نتیجه گرفت برای $k \geq 5$، $bc_d(Q_k) = d2^{k-1}$ و این نشان می‌دهد که کران پایین ارائه شده در لم (۲.۲.۱) می‌تواند برای بعضی از گراف‌ها به تساوی تبدیل شود.

فرض کنید دور با $n$ رأس را با نماد $C_n$ نمایش دهیم، در این‌صورت لم زیر را می‌توان به آسانی نتیجه گرفت.

**لم ۴.۲.۱.** [۳۲] *فرض کنید $d$ و $n$ اعداد صحیح مثبتی باشند. در این‌صورت*

$$bc_d(C_n) = \begin{cases} d & n = 4, \\ \frac{n}{2}d & n = 2k,\ n \geq 6, \\ \frac{d}{2}n & n = 2k+1,\ d = 2k', \\ \frac{d-1}{2}n + \lfloor \frac{n}{2} \rfloor + 1 & n = 2k+1,\ d = 2k'+1 \end{cases}$$

## ۱.۲.۱ پوشش دوبخشی کامل کسری

معمولاً پارامترهایی که در نظریه گراف تعریف می‌شوند اعداد صحیحی هستند. اما می‌توان حالت غیر صحیح این پارامترها را نیز تعریف کرد. در این بخش قصد داریم این کار را در حالت کلی انجام دهیم. سپس تعاریف و قضیه‌های موجود در این زمینه را برای پوشش دوبخشی کامل گراف‌ها استفاده می‌کنیم. در انتها به کمک این تعاریف و قضیه‌های موجود، نتایجی درباره $d$-پوشش دوبخشی کامل ارائه می‌دهیم.

ابرگراف $\mathcal{H}$ زوج $(S, \mathcal{X})$ است که $S$ یک مجموعه متناهی و $\mathcal{X}$ خانواده‌ای از زیرمجموعه‌های

$S$ است. مجموعه $S$ را مجموعه رأس‌های ابرگراف می‌نامند و معمولاً آن را با نماد $V(\mathcal{H})$ نمایش می‌دهند. مجموعه $\mathcal{X}$ را نیز مجموعه یال‌های ابرگراف می‌نامند. درجه رأس $v$ در یک ابرگراف تعداد یال‌هایی است که رأس $v$ را شامل می‌شوند. یک **پوشش یالی** برای ابرگراف $\mathcal{H}$ خانواده $\{X_1, \ldots, X_j\}$ از یال‌های ابرگراف است به‌گونه‌ای که $S \subseteq X_1 \cup \cdots \cup X_j$. کوچکترین $j$ی که برای آن یک پوشش از اندازه $j$ وجود داشته باشد **عدد پوششی یالی** نامیده می‌شود و با نماد $k(\mathcal{H})$ نمایش داده می‌شود. مسأله پوشش دارای یک دوگان طبیعی است. از این دیدگاه که به‌جای پوشاندن رأس‌های گراف توسط یال‌ها، یال‌ها را توسط رأس‌ها بپوشانیم. فرض کنید $\mathcal{H}$ یک ابر گراف باشد. یک **بسته بندی رأسی** برای $\mathcal{H}$ زیر مجموعه $Y$ از $V(\mathcal{H})$ است با این ویژگی که از هر یال $\mathcal{H}$ حداکثر یک رأس در $Y$ قرار دارد. **عدد بسته بندی** که با نماد $p(\mathcal{H})$ نمایش داده می‌شود اندازه بزرگترین بسته بندی موجود برای ابرگراف $\mathcal{H}$ است. دو پارامتری که برای ابرگراف‌ها تعریف کردیم پارامترهای بسیار مهمی هستند چون با تعریف ابرگراف‌های مناسب می‌توان بسیاری از پارامترهای گراف را با این دو پارامتر معادل کرد. به عنوان مثال فرض کنید ابرگراف $\mathcal{H}(G)$ متناظر با گراف داده شده $G$، ابرگرافی باشد که $S = V(G)$ و یال‌های آن مجموعه‌های مستقل در گراف $G$ باشند. در این‌صورت عدد رنگی رأسی گراف $G$ همان $k(\mathcal{H}(G))$ است. همچنین عدد تطابقی $G$ همان $p(\mathcal{H})$ است.

مسأله پوشش در ابرگراف‌ها را می‌توان به صورت یک مسأله برنامه ریزی خطی بیان کرد. برای این منظور فرض کنید ماتریس $M$ یک $(0,1)$-ماتریس باشد که سطرهای آن با عناصر $S$ برچسب گذاری شده باشد و ستون‌های آن با یال‌های ابرگراف. درایه $ij$-ام در این ماتریس ۱ است اگر وتنها اگر $s_i \in X_j$. ماتریس $M$ را **ماتریس مجاورت** ابرگراف $\mathcal{H}$ می‌نامند. واضح است که $X$ بردار مشخصه یک پوشش است اگر و تنها اگر $MX \geq 1$. بنابراین $k(\mathcal{H})$ مقدار صحیح مسأله

برنامه ریزی خطی زیر است

$$\begin{array}{ll} minimize & j^tX \\ & MX \geq j. \end{array}$$

مشابهاً بردار $Y$ بردار مشخصه متناظر با یک بسته بندی است اگر و تنها اگر $M^tY \leq ۱$.

بنابراین $p(\mathcal{H})$ مقدار صحیح مسأله برنامه ریزی خطی زیر است

$$\begin{array}{ll} maximize & j^tY \\ & M^tY \leq j \end{array}.$$

بنابراین مسأله پوشش، مسأله دوگان برنامه ریزی خطی، مسأله بسته‌بندی است. با توجه به توضیح‌های داده شده اولین تعریف طبیعی برای اینکه یک پارامتر صحیح در نظریه گراف‌ها را به یک پارامتر غیر صحیح تبدیل کرد تعریف زیر است.

**تعریف ۵.۲.۱.** ***عدد پوشش کسری*** *و* ***عدد بسته بندی کسری*** *که به ترتیب با نمادهای* $k_f(\mathcal{H})$ *و* $p_f(\mathcal{H})$ *نمایش داده می‌شود به صورت جواب‌های مسائل برنامه ریزی خطی زیر تعریف می‌شوند*

$$\begin{array}{ll} minimize & j^tX \\ & MX \geq j \end{array} \qquad \begin{array}{ll} maximize & j^tY \\ & M^tY \leq j \end{array}$$

♠

با توجه به قضیه دوگانی در برنامه ریزی خطی داریم $k_f(\mathcal{H}) = p_f(\mathcal{H})$. عدد پوششی کسری و عدد بسته‌بندی کسری با روش دیگری نیز تعریف می‌شوند. در آخر نشان می‌دهند که این دو تعریف با هم معادلند. فرض کنید $\mathcal{H} = (S, \mathcal{X})$ یک ابرگراف باشد و $t$ عدد صحیح و مثبتی باشد. یک **پوشش $t$-تایی** از $\mathcal{H}$ یک مجموعه چندگانه $\{X_۱, X_۲, \ldots, X_j\}$ از یال‌های ابرگراف است که هر رأس ابرگراف حداقل در $t$تا از $X_i$ها قرار دارد. کوچکترین $j$ی که یک پوشش $t$-تایی از اندازه $j$ برای ابرگراف $\mathcal{H}$ داشته باشیم **عدد $t$-پوشش** نامیده می‌شود و با نماد $k_t(\mathcal{H})$ نمایش داده می‌شود. واضح است که $k_t$ در خاصیت زیر صدق می‌کند

$$k_{s+t}(\mathcal{H}) \leq k_s(\mathcal{H}) + k_t(\mathcal{H}).$$