مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۱ -۵

کران‌های جدیدی بر روی نسبت اطلاعات ضرب دکارتی کلاس‌هایی از گراف‌ها

عباس چراغی[۱*]، محمد غلامی[۲]

۱- استادیار، گروه ریاضی، دانشکده ریاضی و کامپیوتر خوانسار ۲- دانشیار، دانشکده علوم ریاضی، دانشگاه شهرکرد، پژوهشگاه دانش‌های بنیادین
(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۷)

چکیده

در این مقاله، کران پایینی برای نسبت اطلاعات حاصل‌ضرب دکارتی یک درخت دلخواه با قطر حداقل ۳ و دور C_m برای هر $m \geq 3$ خواهیم یافت. علاوه براین، بهترین نسبت اطلاعات طرح تسهیم راز کامل برپایه گراف C_6^d را تعیین می‌کنیم که در آن، C_6^d گراف حاصل از ضرب دکارتی دور به طول ۶ با گراف d- مکعب است. به طور دقیق‌تر، نشان داده می‌شود که برای هر $d \geq 1$، نسبت اطلاعات C_6^d دقیقاً برابر با $\frac{d(d+3)+3}{2(d+1)}$ است.

واژه‌های کلیدی: طرح تسهیم راز، نسبت اطلاعات، حاصل‌ضرب دکارتی

۱- مقدمه

طرح تسهیم راز، روشی برای توزیع اطلاعات در میان مجموعه‌ای از سهام‌داران است، به‌طوری‌که تنها مجموعه‌های مجاز قادر به کشف راز باشند. راه‌کار اصلی تسهیم راز این است که داده محرمانه (راز) به بخش‌هایی تقسیم شود، به‌گونه‌ای که با زیرگروه‌های خاصی از این بخش‌ها، بتوان راز را بازیابی‌کرد. اگر علاوه بر این، مجموعه‌های غیرمجاز دارای هیچ اطلاعات اضافی در مورد راز نباشند، یعنی سهم‌های آنان به طور آماری از راز مستقل باشد، در این صورت طرح (تسهیم راز) کامل نامیده می‌شود. توصیف مجموعه‌های مجاز در میان تمامی زیرمجموعه‌های ممکن از سهام‌داران یک ساختار دسترسی نامیده می‌شود. Shamir [۱] و Blakley [۲] در ابتدا مساله طرح تسهیم راز را مطرح کرده و طرح‌های تسهیم رازی را ارائه دادند که هر زیرمجموعه A از سهام‌داران با اندازه $|A| \geq k$ قادر به بازسازی راز هستند و هر زیرمجموعه A از سهام‌داران با اندازه $|A| < k$ هیچ اطلاعاتی درباره راز به‌دست نیاورند. این طرح‌ها، (n,k)- طرح‌های آستانه‌ای نامیده می‌شوند، مقدار k آستانه طرح نامیده می‌شود و n تعداد سهام‌داران می‌باشد. سوال اصلی در مورد کارآیی این روش به این صورت است: به ازای هر بیت از راز، چه تعداد بیت از اطلاعات سهام‌داران می‌بایست به خاطر سپرده شود؟

نسبت اطلاعات این طرح، نسبت مابین بیش‌ترین اندازه از سهم‌ها و اندازه مقدار راز است، در حالی‌که نسبت یک ساختار دسترسی، کم‌ترین نسبت اطلاعات طرح‌هایی است که بر روی این ساختار دسترسی شناخته شده‌اند.

یکی از مسائل نظری و عملی در این مقوله، تعیین یا یافتن کران‌های قابل قبول برای نسبت اطلاعات ساختار دسترسی‌های متفاوت است که توسط تعدادی از پژوهشگران، توجه قابل قبولی را به خود منعطف ساخته است.

ارتباط عملی این موضوع برپایه مشاهدات زیر است. در ابتدا، توجه داریم که امنیت هر دستگاهی با افزایش مقدار اطلاعاتی که می‌بایست مخفی نگه داشته شود (یعنی سهم سهام‌داران)، تمایل به کاهش دارد. ثانیاً، اگر سهم‌هایی که به سهام‌داران داده می‌شود، خیلی بزرگ باشد، آن‌گاه حافظه مورد نیاز برای سهام‌داران خیلی بزرگ خواهد شد و در همان لحظه، الگوریتم‌های توزیع سهام ناکارآمد خواهند شد. بنابراین، مهم است بهترین نسبت اطلاعات ساختارهای دسترسی را داشته باشیم. در راستای این هدف، یافتن کران‌های بالایی و پایینی روی نسبت اطلاعات ارزشمند خواهد بود.

حالت خاص، زمانی است که یک ساختار دسترسی توسط یک گراف تعریف شود که در آن مجموعه راس‌ها، همان مجموعه سهام‌داران و یال‌ها، مجموعه‌های مجاز کمینه هستند. در این مقاله، ما ساختارهای دسترسی بر پایه گراف‌ها را مورد مطالعه

* رایانامه نویسنده مسئول: a.cheraghi@khn.ui.ac.ir

قرار خواهیم داد و طرح تسهیم راز برای ساختار دسترسی بر پایه یک گراف را طرح تسهیم راز آن گراف می‌نامیم. در طرح‌های تسهیم راز، مساله یافتن کران روی اندازه سهم‌هایی که به سهام‌داران داده می‌شود یا به طور هم ارز نسبت اطلاعات، یکی از مسائل اساسی در این باره بوده و توجه زیادی را توسط محققین به خود جلب ساخته است.

نسبت اطلاعات برای اغلب گراف‌ها با حداکثر ۶ راس در مراجع [۳-۸] مطرح شده است. درخت‌ها، دارای نسبت اطلاعات $2-\frac{1}{k}$ هستند که در آن، k یک مقدار صحیح است [۹]. هم‌چنین، برای هر d، دسته‌ای از گراف‌های نامتناهی با بیشترین درجه d ساخته شده که نسبت دقیق اطلاعات آنها $\frac{d+1}{2}$ است [۱۰]. برای نمونه، گراف‌های کامل دارای نسبت اطلاعات ۱ هستند، مسیرهای با ۴ راس یا بیش‌تر، همانند دورهای با طول حداقل ۵، دارای نسبت اطلاعات $\frac{3}{2}$ هستند. در مرجع [۱۱]، Csirmazنسبت اطلاعات گراف‌های d-مکعبی را یافته و ثابت کرده است که نسبت اطلاعات این گراف‌ها برابر با $d/2$ می‌باشد.

Brickell و Stinson [۵ و۱۲] چندین کران بالایی و پایینی برای نسبت اطلاعات ساختار دسترسی‌های مبتنی بر گراف‌ها یافته‌اند. Stinson [۱۲] نشان داد که نسبت اطلاعات یک گراف با بیش‌ترین درجه d حداکثر برابر با $\frac{d+1}{2}$ است. Brickell و Davenport [۴] نشان دادند که یک گراف دارای نسبت اطلاعات ۱ است اگر و تنها اگر گراف، دوبخشی کامل باشد. علاوه براین، Blundo در مرجع [۳] یک شکاف در مقادیر نسبت اطلاعات گراف‌ها را نشان داد؛ به طور دقیق‌تر، آن‌ها بر روی این مطلب که توسط Brickell و Davenport [۴] به‌دست آمده بود، تاکید کرده و نشان دادند که اگر گراف G یک گراف کامل دوبخشی نباشد، آن‌گاه هر طرح تسهیم راز برای آن گراف، دارای نسبت اطلاعات حداقل $\frac{3}{2}$ است.

در مرجع [۱۳] طرح‌های بهینه بررسی شده اند و در مرجع [۱۴]، نویسندگان یک $(3,3)$-طرح تسهیم راز آستانه‌ای شبه کوانتومی را طراحی نموده‌اند که فارغ از مولد کوانتومی، راز را با سه قسمت کلاسیک به اشتراک می‌گذارد، به طوری که qubitها در یک پایه کلاسیک اندازه‌گیری شده و ارسال آن‌ها بدون اختلال صورت می‌پذیرد.

طرح‌های تسهیم راز مطرح‌شده در این مقاله همگی کامل هستند. یعنی زیرمجموعه‌های مجاز می‌توانند راز را به‌دست آورند، درحالی‌که زیرمجموعه‌های غیر مجاز با استفاده از سهم‌هایشان نمی‌توانند هیچ‌گونه اطلاعاتی از راز به‌دست آورند.

۲- برخی تعاریف اولیه

فرض کنید Σ یک طرح تسهیم راز با مجموعه P از n سهام‌دار باشد. واسطه $p_0 \notin P$ و $Q = P \cup \{p_0\}$ را در نظر بگیرید. در یک طرح، سهم p_0 را راز درنظر می‌گیریم. s_i را سهم سهام‌دار $i \in Q$ فرض کنید. با توجه به همه $(n+1)$-تایی‌های ممکن $(s_{p_0}, s_1, s_2, ..., s_n)$ از سهم‌ها، نگاشت $\pi_i : E \to E_i$ را برای یک مجموعه مشخص E چنان تعریف می‌کنیم که برای هر $e \in E$ اعضاء $(\pi_i(e))_{i \in Q}$ سهم‌های یک راز باشند. ما فقط نگاشت‌های پوشا را در نظر می‌گیریم، بنابراین، برای هر سهام‌دار $i \in Q$ مجموعه E_i همان مجموعه همه سهم‌های ممکن سهام‌دار i-ام می‌باشد. اگر یک توزیع احتمال در E را درنظر بگیریم، آن‌گاه هر یک از نگاشت‌ها یک توزیع احتمال در E_i القاء می‌کند. بنابراین، می‌توان $H(E_i)$ را به‌عنوان Shannon entropy هر یک از متغیرهای تصادفی در نظر گرفت.

برای هر زیرمجموعه $A = \{i_1, ..., i_r\} \subset Q$، آنتروپی مشترک $H(E_{i_1}, ..., E_{i_r})$ را به صورت $H(A)$ می‌نویسیم و قرارداد مشابهی را برای آنتروپی شرطی قرار می‌دهیم. به‌طور مثال، داریم:

$$H(E_j \mid A) = H(E_j \mid E_{i_1}, ..., E_{i_r})$$

مجموعه Γ را ساختار دسترسی Σ درنظر بگیرید. از آن‌جا که نگاشت‌های π_i طرح تقسیم راز کامل Σ را تعریف می‌کنند، لذا $H(E_{p_0}) > 0$. درضمن اگر $A \in \Gamma$، داریم $H(E_{p_0} \mid A) = 0$. این تساوی بیانگر آن است که تمامی اطلاعات راز توسط یک مجموعه مجاز، مشخص می‌گردد. درحالی‌که اگر $A \notin \Gamma$ داریم:

$$H(E_{p_0} \mid A) = H(E_{p_0})$$

این تساوی بیانگر آن است که یک مجموعه غیرمجاز قادر به برملاکردن حتی یک بیت از اطلاعات راز نمی‌باشد.

به منظور اندازه‌گیری طول سهام هر طرح، از آنتروپی سهام آن طرح استفاده می‌شود. *نرخ* اطلاعات طرح تسهیم راز Σ به صورت $\rho(\Sigma) = \frac{H(E_0)}{\max_{i \in P} H(E_i)}$ تعریف می‌شود. مقدار $R(\Sigma) = 1/\rho(\Sigma)$ را نسبت *اطلاعات* طرح Σ گویند. هر دو مقدار ρ و R را به عنوان ضریب تاثیر یک طرح به کار می‌برند. این پارامترها را

می‌توان برای ارزیابی بهترین راندمان طرح‌های یک ساختار دسترسی مشخص استفاده نمود. نرخ اطلاعات *بهینه* $\rho(\Gamma)$ برای یک ساختار دسترسی Γ را انرخ‌های $\rho(\Sigma)$ روی تمامی طرح‌های Σ تعریف‌شده برای ساختار دسترسی Γ گویند. نسبت اطلاعات بهینه ساختار دسترسی Γ نیز به صورت $R(\Gamma)=1/\rho(\Gamma)$ تعریف می‌شود. در ادامه نسبت اطلاعات برخی ساختارهای دسترسی مبتنی بر ضرب دکارتی چندین گراف محاسبه و یا بر روی آن کران‌هایی معرفی می‌گردد.

۳- نسبت اطلاعات دسته‌ای از گراف‌ها

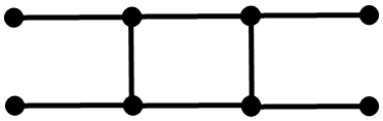
در ادامه به برخی قضایا و نتایج کاربردی در این مقاله می‌پردازیم.

زیرگراف H از گراف G که تنها با حذف زیرمجموعه‌ای از رئوس گراف G به‌دست می‌آید را زیر گراف القایی G گویند.

قضیه ۳-۱- [۱۵] اگر G یک گراف و H زیرگراف القایی آن باشد آن‌گاه:

$$R(H)\le R(G).$$

قضیه ۳-۲- [۱۵] فرض کنید G گراف نردبانی شکل (۱) باشد. آن‌گاه $R(G)=2$.



شکل (۱): گراف نردبانی

در نظریه گراف، حاصل ضرب دکارتی $G\square H$ از گراف‌های G و H گرافی است که مجموعه راس‌های $G\square H$ حاصل‌ضرب دکارتی $V(G)\times V(H)$ بوده و هر دو راس (u,u') و (v,v') مجاور هستند اگر و تنها اگر $u=v$ و u' در H با v' مجاور باشد یا $u'=v'$ و u در G با v مجاور باشد. حاصل‌ضرب دکارتی دارای خاصیت جابه‌جایی است، یعنی گراف‌های $G\square H$ و $H\square G$ به طور طبیعی یک‌ریخت هستند. این عملگر دارای خاصیت شرکت‌پذیری است، یعنی گراف‌های $F\square(G\square H)$ و $(F\square G)\square H$ به طور طبیعی یک‌ریخت هستند.

فرض کنید که T_n یک درخت n راسی باشد. حاصل ضرب دکارتی درخت T_n با یک دور به طول m را با نماد $T_{n,m}$ نمایش می‌دهیم، در واقع $T_{n,m}=T_n\square C_m$.

بیش‌ترین فاصله موجود بین رئوس گراف را قطر گراف گویند.

قضیه ۳-۳- اگر T_n درخت n راسی با قطر حداقل ۳ باشد و $m\ge 4$. آن‌گاه $R(T_{n,m})\ge 2$.

اثبات: برای آن‌که نشان دهیم $R(T_{n,m})\ge 2$ کافی است نشان دهیم $T_{n,m}$ شامل یک زیر گراف القایی یک‌ریخت با گراف شکل (۱) است.

از آن‌جایی که قطر درخت T_n حداقل ۳ است، لذا T_n حداقل شامل یک مسیر القایی به فرم $P: a_1-a_2-a_3-a_4$ می‌باشد. به علاوه فرض کنید دور C_m به فرم $C_m: b_1-b_2-\cdots-b_m-b_1$ باشد. حال بر طبق شکل (۲) برخی رئوس $T_{n,m}$ را به صورت زیر نام‌گذاری می‌نماییم:

$$A=(a_2,b_1)\ ,\ B=(a_2,b_2),$$
$$C=(a_3,b_2)\ ,\ D=(a_4,b_2),$$

$$a=(a_1,b_3)\ ,\ b=(a_2,b_3),$$
$$c=(a_3,b_3)\ ,\ d=(a_3,b_4).$$

اگر $X:=\{A,B,C,D,a,b,c,d\}\subseteq V(T_{n.m})$ آن‌گاه به وضوح زیرگراف القایی $T_{n,m}[X]$ یک‌ریخت با گراف شکل (۱) است، لذا داریم:

$$2=R(T_{n,m}[X])\le R(T_{n,m}).$$

۴- نتایج اصلی

حال، فرض کنید گراف C_n دور به طول n و K_n گراف کامل با n راس باشد. تعریف کنید: $C_n^d=C_n\square K_2\square K_2\square\cdots\square K_2$ جایی که تعداد کپی‌های K_2 در این حاصل‌ضرب برابر با d است. به آسانی می‌توان بررسی کرد که برای هر $n\ge 2$ و $d\ge 0$، گراف C_n^d یک گراف $(d+2)$-منظم راس‌ترایا با $n\times 2^d$ راس است و برای n زوج، گراف C_n^d نیز یک گراف دوبخشی است. هدف اصلی این مقاله، قضیه زیر است که مقدار دقیق نسبت اطلاعات C_6^d را تعیین می‌کند و با $R(C_6^d)$ نمایش داده می‌شود.

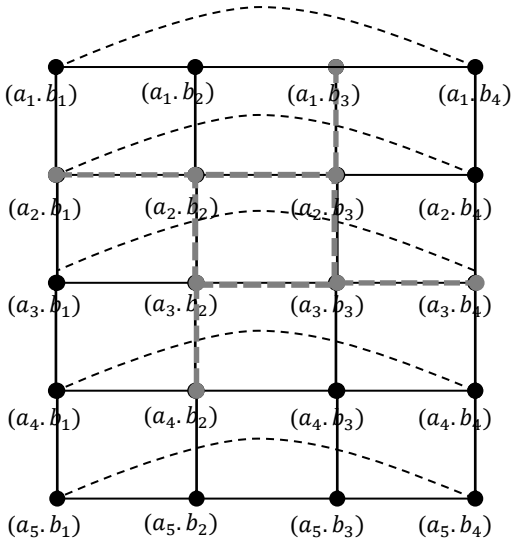
قضیه ۴-۴- برای عدد صحیح نامنفی d، نسبت اطلاعات C_6^d برابر با $\frac{d(d+3)+3}{2(d+1)}$ است.

برای اثبات قضیه فوق نیاز به بیان مطالب زیر است:

یک طرح تسهیم راز کامل S برای گراف G، خانواده‌ای از متغیرهای تصادفی ξ_v برای هر $v\in V(G)$ و متغیر تصادفی ξ برای راز در نظر گرفته می‌شود. بنابراین، اگر uv یالی از G باشد، آن‌گاه ξ_u و ξ_v به همراه یک‌دیگر قادر به تعیین متغیر تصادفی ξ خواهند بود. علاوه بر این، اگر A مجموعه مستقلی

از رئوس باشد، آن‌گاه ξ و مجموعه $\{\xi_v : v \in A\}$ به طور آماری مستقل هستند.

اندازه متغیر تصادفی ξ توسط آنتروپی اندازه‌گیری می‌شود (که محتوای اطلاعاتی نامیده می‌شود) و آن را با نماد $H(\xi)$ نمایش می‌دهند، این روش توسط Blundo در سال ۱۹۹۵ مطرح گردید. نسبت اطلاعات هر راس $v \in V(G)$ برابر با $\frac{H(\xi_v)}{H(\xi)}$ است. این تساوی بیان می‌کند که برای هر بیت راز، چه میزان بیت اطلاعات توسط v به خاطر سپرده می‌شود.



شکل (۲): ضرب دکارتی مسیر با دور

نسبت اطلاعات میانگین و نسبت اطلاعات در بدترین حالت S به ترتیب همان نسبت اطلاعات میانگین در بین تمامی سهام‌داران و بیش‌ترین نسبت اطلاعات در بین آن‌ها است. فرض کنید S یک طرح تسهیم راز کامل روی گراف G باشد، به طوری‌که متغیرهای تصادفی ξ_v برای هر $v \in V(G)$ و متغیر تصادفی ξ برای راز درنظر گرفته می‌شوند. برای هر زیرمجموعه A از رئوس تعریف می‌کنیم:

$$f(A) := \frac{H(\xi_v : v \in A)}{H(\xi)}$$

واضح است که نسبت اطلاعات میانگین S همان میانگین اعضای مجموعه‌ی $\{f(v) : v \in V\}$ می‌باشد. در بدترین حالت، نسبت اطلاعات برابر با بیش‌ترین مقدار در این مجموعه است. با استفاده از خواص استاندارد توابع آنتروپی **[۴]** داریم:

الف) خاصیت مثبت‌بودن: $f(\varnothing) = 0$ و در حالت کلی $f(A) \geq 0$

ب) خاصیت یک‌نوایی: اگر $A \subseteq B \subseteq V(G)$ آنگاه $f(A) \leq f(B)$

ج) خاصیت زیرمدولی:

$$f(A) + f(b) \geq f(A \cap B) + f(A \cup B)$$

یک نتیجه معروف در نظریه اطلاع آن است که اگر ξ و ς دو متغیر تصادفی باشند، متغیر تصادفی ς، مقدار ξ را تعیین می‌کند اگر و تنها اگر $H(\varsigma\xi) = H(\xi)$.

هم‌چنین ξ و ς به طور آماری مستقل هستند اگر:

$$H(\varsigma\xi) = H(\varsigma) + H(\xi).$$

با توجه به این مطلب و تعریف طرح تسهیم راز کامل، خواص زیر را نیز خواهیم داشت:

د) یکنوایی قوی: اگر $A \subseteq B$ همچنین A یک مجموعه مستقل و مجموعه B وابسته باشد، آن‌گاه:

$$f(A) + 1 \leq f(B)$$

ه) زیرمدولی قوی: اگر هیچ‌یک از مجموعه‌های A و B مستقل نباشند، اما $A \cap B$ مستقل باشد، آن‌گاه:

$$f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$$

- **کران پایین نسبت اطلاعات**

روش‌های معروف آنتروپی که در سال ۱۹۷۹ نشان داده شد، به صورت زیر بیان می‌گردد. به سادگی دیده می‌شود برای هر تابع حقیقی f که در خواص (الف) تا (ه) صدق کرده و مقدار متوسط آن روی مجموعه رئوس G حداقل برابر با r باشد، آن‌گاه، نسبت اطلاعات گراف G حداقل برابر با r خواهد بود **[۳]**.

اثبات قضیه ۴-۴- برای اثبات کران پایین $\frac{d(d+3)+3}{2(d+1)}$ بر روی نسبت اطلاعات C_6^d کافی است نشان دهیم برای هر تابع f با مقدار حقیقی که در خواص (الف) تا (ه) صدق کند، داریم:

$$\sum_{v \in V(C_6^d)} f(v) \geq 3 \times 2^d (d + 2 + \frac{1}{d+1}).$$

این همان نامساوی است که می‌بایست ثابت شود. برای این منظور، مجموعه رئوس گراف C_6^d را به دو قسمت مستقل مجزای A_d و B_d با اندازه یکسان تقسیم می‌کنیم. لذا، داریم:

$$|A_d| = |B_d| = 3 \times 2^d.$$

رئوس A_d فقط همسایه‌هایی در B_d و رئوس در B_d فقط همسایه‌هایی در A_d دارند. گراف $C_6^{d+1} = C_6^d \square K_2$ شامل دو نسخه

مجزا از C_6^d است که مابین رئوس آن‌ها نظیر به نظیر یک تطابق کامل وجود دارد. فرض کنید رئوس هر دونسخه C_6^d به روش فوق به‌ترتیب به‌صورت $A_d \cup B_d$ و $A'_d \cup B'_d$ تقسیم شده باشند، به‌طوری‌که تطابق‌های کامل بین A_d و B'_d و هم‌چنین بین B_d و A'_d باشند. بنابراین، تقسیم رئوس گراف C_6^{d+1} به صورت زیرمجموعه‌های از هم جدای مستقل $A_{d+1} = A_d \cup A'_d$ و $A'_d \cup B'_d$ انجام می‌گردد. با استفاده از این تجزیه، می‌توان از استقرا روی d برای اثبات کران پایین $R(C_6^d)$ استفاده کرد. در مراحل استقرا از نمادگذاری زیر استفاده خواهیم کرد که در آن منظور از bA اجتماع مجموعه A با مجموعه تک‌عضوی b می‌باشد.

$$[[A,B]] = \sum_{b\in B} f(bA) - \sum_{a\in A} f(A-\{a\}).$$

در زمان استفاده از این نام‌گذاری فرض می‌کنیم که مجموعه‌های A و B دارای اندازه‌های یکسان هستند. اکنون، می‌توانیم ثابت کنیم که کران پایین $R(C_6^d)$ برابر با $\frac{d(d+3)+3}{2(d+1)}$ است.

لم ۴-۵- برای هر $d \geq 1$ داریم:

$$R(C_6^d) \geq \frac{d(d+3)+3}{2(d+1)}.$$

اثبات: برای اثبات لم فوق به بیان ادعای زیر نیازمندیم.

ادعا: برای گراف C_6^d با افراز رئوس آن به مجموعه‌های مستقل $A_d \cup B_d$ داریم:

$$\sum_{v\in C_6^d} f(v) \geq [[A_d, B_d]] + 3\times 2^d (d+1+\frac{1}{d+1}) \qquad (۱)$$

اثبات ادعا: برای اثبات ادعا از استقرا روی d استفاده می‌کنیم**.** فرض کنیم نامساوی فوق به ازای $d=1$ برقرار باشد. اکنون با فرض این‌که نامساوی برای هر دو نسخه C_6^d با مجموعه رئوس v_d و v'_d در گراف C_6^{d+1} با مجموعه رئوس V_{d+1}، برقرار باشد، با تقسیم‌بندی رئوس این گراف به فرم $A_{d+1} = A_d \cup A'_d$ و $B_{d+1} = B_d \cup B'_d$ ثابت می‌کنیم حکم برای C_6^{d+1} نیز برقرار است. اکنون بر اساس فرض استقرا بیان شده داریم:

$$\sum_{v\in V_{d+1}} f(v) = \sum_{v\in V_d} f(v) + \sum_{v\in V'_d} f(v) = [[A_d, B_d]] +$$
$$[[A'_d, B'_d]] + 3\times 2^{d+1}(d+1+\frac{1}{d+1}) \qquad (۲)$$

می‌توان نشان داد:

$$[[A_d, B_d]] + [[A'_d, B'_d]] \geq$$
$$[[A_d A'_d, B_d B'_d]] + 6\times 2^d$$

با ترکیب این نامساوی با معادله (۲) داریم:

$$\sum_{v\in C_6^{d+1}} f(v) \geq [[A_d A'_d, B_d B'_d]] +$$
$$3\times 2^{d+1}(d+1+\frac{1}{d+1}) + 6\times 2^d.$$

اما به سادگی می‌توان دید:

$$3\times 2^{d+1}(d+1+\frac{1}{d+1}) + 6\times 2^d \geq$$
$$3\times 2^{d+1}(d+2+\frac{1}{d+2}),$$

بنابراین:

$$\sum_{v\in C_6^{d+1}} f(v) \geq [[A_d A'_d, B_d B'_d]] +$$
$$3\times 2^{d+1}(d+2+\frac{1}{d+2}),$$

و لذا حکم برای $d+1$ برقرار بوده و ادعا ثابت می‌شود.

اکنون به ادامه اثبات قضیه ۴-۴ می‌پردازیم:

فرض کنید $d \geq 1$ و $V(C_6^d) = A_d \cup B_d$ افراز مجزای رئوس به مجموعه‌های مستقل راسی باشد. از آن‌جایی که در هر یک از بخش‌های مستقل مجزای A_d و B_d دقیقاً 3×2^d راس وجود دارد؛ لذا می‌توانیم بین رئوس این دو دسته یک تطابق کامل درنظر بگیریم. اگر (a,b) یکی از یال‌های این تطابق باشد، با توجه به خاصیت یک‌نوایی قوی داریم:

$$f(bA_d) - f(A_d - \{a\}) \geq 1,$$

که در آن منظور از bA_d اجتماع مجموعه A_d با مجموعه تک‌عضوی b می‌باشد. نامساوی فوق برقرار است چرا که $A_d - \{a\}$ یک مجموعه مستقل راسی است، درحالی‌که bA_d چنین نیست. با درنظرگرفتن رابطه فوق برای هر یک از زوج جملات حاصل از مجموع‌های زیر داریم:

$$[[A_d, B_d]] = \sum_{b\in B_d} f(bA_d) - \sum_{a\in A_d} f(A_d - \{a\}) \geq 3\times 2^d.$$

بنابراین:

$$\sum_{v\in C_6^d} f(v) \geq 3\times 2^d (d+1+\frac{1}{d+1}) + 3\times 2^d =$$
$$3\times 2^d (d+2+\frac{1}{d+1})$$

از آن‌جایی‌که 6×2^d راس در C_6^d وجود دارد، پس حداقل یک راس $v \in C_6^d$ وجود دارد به طوری که:

$$f(v) \geq \frac{3\times 2^d (d+2+\frac{1}{d+1})}{6\times 2^d}$$

و این اثبات را تمام می‌کند، زیرا:

$$R(G) \geq \frac{d(d+3)+3}{2(d+1)}.$$

- **کران بالای نسبت اطلاعات**

برای اثبات کران بالا از روش تجزیه [۱۲] استفاده خواهیم کرد. در این مقاله روشی برای طرح‌های تسهیم راز در حالت کلی ارائه شده است که به آن ساختار λ -تجزیه گویند. این روش، یک ساختار بازگشتی برای تولید یک طرح تسهیم راز با استفاده از طرح‌های تسهیم راز کوچک‌تر به عنوان بلوک‌هایی از طرح اصلی است. این روش در ساختار دسترسی یک گراف، بر پایه یافتن یک پوشش از آن گراف است به‌طوری‌که هر یال از این گراف می‌بایست در حداقل λ تا از زیرگراف‌های این پوشش قرار گیرد. قضیه زیر نحوه استفاده از چنین پوششی را برای معرفی یک کران بر روی ساختار دسترسی گرافی بیان می‌کند.

قضیه۴-۶- [۱۲] فرض کنید G_i خانواده‌ای از زیرگراف‌های G باشد به‌طوری‌که هر یال از گراف G متعلق به حداقل λ تا از G_i-ها باشد. به ازای راس $v \in V(G)$ تعریف کنید:

اگر $v \notin V(G_i)$ تعریف می‌کنیم $r_i(v)=0$ و در غیر این صورت $r_i(v)=R(G_i)$. آن‌گاه:

$$R(G) = sup_{v\in G} \frac{\sum_i r_i(v)}{\lambda}$$

حال، قضیه فوق را برای یافتن کران بالایی مطلوب برای $R(C_6^d)$ به کار می بریم.

لم ۴-۷- به ازای مقدار صحیح نامنفی d داریم:

$$R(C_6^d) \leq \frac{d(d+3)+3}{2(d+1)}$$

اثبات: در این‌جا پوششی از C_6^d توسط دورهای به طول ۴ و ۶ ارائه می‌دهیم و این پوشش‌ها را به اختصار ۲-رخ نامیده می‌شود، به‌طوری‌که هر یال دقیقاً $d+1$ بار و هر راس دقیقاً $\frac{d^2+3d+1}{2}$ بار توسط ۲-رخ‌ها پوشیده می‌شوند که در نتیجه لم ۴-۷ به عنوان نتیجه‌ای از قضیه ۴-۶ اثبات می‌شود.

به وضوح، C_6^d یک گراف $(d+2)$- منظم است که دارای 6×2^d راس می‌باشد. توجه دارید که هر زوج از یال‌های شامل راس v تشکیل یک ۲-رخ می‌دهند. بنابراین، هر راس دقیقاً روی $\binom{d+2}{2}-1$ تا ۲-رخ قرار می گیرد. حال، به سادگی می‌توان بررسی کرد که تمامی ۲-رخ‌ها یک پوشش برای C_6^d تشکیل می‌دهند به‌طوری‌که هر یال از C_6^d مشمول در حداقل $d+1$ از این ۲-رخ‌ها است. بنابراین، ۲-رخ‌ها تشکیل یک $(d+1)$- پوشش از C_6^d می‌دهند. با توجه به مطالب فوق داریم:

$$R(G) \leq \frac{\binom{d+2}{2}-1+\frac{3}{2}}{d+1} = \frac{d(d+3)+3}{2(d+1)}$$

حال، قضیه اصلی از لم **۴-۵** و لم **۴-۷** نتیجه شده و به صورت زیر می‌باشد:

قضیه ۴-۸- برای مقدار صحیح نامنفی d، داریم:

$$R(C_6^d) = \frac{d(d+3)+3}{2(d+1)}.$$

قضیه فوق در واقع مبین یک مقدار دقیق برای نسبت اطلاعات یک رده نامتناهی از گراف‌ها می‌باشد.

۵- نتیجه‌گیری

در این مقاله، نسبت اطلاعات ساختارهای دسترسی گرافی طرح‌های تسهیم راز مورد مطالعه قرار گرفت. به این منظور کران پایینی برای نسبت اطلاعات حاصل ضرب دکارتی یک درخت دلخواه با قطر حداقل ۳ و دور C_m برای هر $m \geq 3$ یافتیم. برای یافتن این کران پایین از نسبت اطلاعات یک زیرگراف القایی معروف و شناخته‌شده در این گراف استفاده شد. علاوه براین، بهترین نسبت اطلاعات، طرح تسهیم راز کامل بر پایه گراف C_6^d را تعین کردیم که در آن، C_6^d گراف حاصل از ضرب دکارتی دور به طول ۶ با گراف d- مکعب است. به طور دقیق‌تر، برای هر $d \geq 1$، ثابت کردیم که $R(C_6^d) = \frac{d(d+3)+3}{2(d+1)}$. جهت ارائه کران بالای نسبت اطلاعات C_6^d، از پوشش این گراف توسط زیرگراف‌هایی با نسبت اطلاعات معین به روش تجزیه Stinson استفاده شد. در بیش‌تر مقالاتی که تاکنون به این موضوع پرداخته‌اند کران‌های غیردقیق و به صورت بازه‌ای ارائه شده است، درحالی‌که در این مقاله نتیجه اصلی به صورت یک کران دقیق معرفی گردیده است.

خواننده علاقمند می‌تواند نسبت اطلاعات دقیق گراف‌های بسیاری که هنوز تعیین نگردیده است را مورد مطالعه قرار دهد.

۶- مراجع

[1] A. Shamir, "How to share a secret," Comm. ACM, 22,vol. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safe guarding cryptographic keys," in AFIPS Conference Proceedings, New York, United States of America, pp. 313-317, June 4-7, 1979.

[3] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, “Graph decomposition and secret sharing schemes,” Journal of Cryptology, vol. 8, pp. 39-64, 1995.

[4] E. F. Brickell and D. M. Davenport, “On the classification of ideal secret sharing schemes,” Journal of Cryptology, vol. 4, pp. 123-134, 1991.

[5] E. F. Brickell and D. R. Stinson, “Some improved bounds on the information rate of perfect secret sharing schemes,” Journal of Cryptology, vol. 5, pp. 153-166, 1992.

[6] M. Dijk, “On the information rate of perfect secret sharing schemes”, Designs Codes and Cryptography, vol. 6, pp. 143-160, 1995.

[7] W. A. Jackson and K. M. Martin, “Perfect secret sharing schemes on five participants,” Designs Codes and Cryptography, vol. 9, pp. 267-286, 1996.

[8] C. Padro, “Lecture notes in secret sharing,” Available at http://eprint.iacr.org/2012/674, 2012.

[9] L. Csirmaz and G. Tardos, “Optimal information rate of secret sharing schemes on trees”, IEEE Trans. Inf. Theory, vol. 59, pp. 2527-2530, 2013.

[10] L. Csirmaz and P. Ligeti, “On an infinite family of graphs with information ratio 2−1/k”, Computing, vol. 85, pp. 127-136, 2009.

[11] L. Csirmaz, “Secret sharing on the d-dimensional cube,” Designs Codes and Cryptography, vol. 74, pp. 719-729, 2015.

[12] D. R. Stinson, “Decomposition construction for secret sharing schemes,” IEEE Trans. Inf. Theory, vol 40, pp. 118-125, 1994.

[13] W. Wang, Z. Li, and Y. Song, “The optimal information rate of perfect secret sharing schemes,” In 2011 International Conference on Business Management and Electronic Information (BMEI), Guangzhou, China, May 13-15, pp. 207-212, 2011.

[14] Z. Karimifard, S. Mashhadi, and D. Ebrahimi Bagha, “Semiquantum Secret Sharing Using Three Particles Without Entanglement,” Journal Of Electronical & Cyber Defence, vol. 4, no. 3, 2016.

[15] L. Csirmaz, “Secret sharing on infinite graphs,” Tetra Mountains Mathematical Publication, vol. 41, pp.1-18, 2008.