

کران‌های جدیدی بر روی نسبت اطلاعات ضرب دکارتی کلاس‌هایی از گراف‌ها

عباس چراغی^{۱*}، محمد غلامی^۲

۱- استادیار، گروه ریاضی، دانشگاه خوارسار، خوارسار، ایران،

۲- دانشیار، دانشکده علوم ریاضی، دانشگاه شهرکرد، شهرکرد، ایران و محقق دانشکده علوم کامپیوتر،

پژوهشگاه دانش‌های بنیادین، تهران، ایران

(دریافت: ۱۳۹۶/۱۰/۲۳، پذیرش: ۱۳۹۷/۰۳/۰۶)

چکیده

در این مقاله، یک کران پایینی برای نسبت اطلاعات حاصل ضرب دکارتی یک درخت دلخواه با قطر حداقل ۳ و دور C_m برای هر $m \geq 3$ خواهیم یافت. علاوه بر این، بهترین نسبت اطلاعات طرح تسهیم راز کامل بر پایه گراف C_6^d را تعیین می‌کنیم که در آن، گراف حاصل از ضرب دکارتی دور به طول ۶ با گراف d -مکعب است. به‌طور 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، حاصل ضرب دکارتی

۱- مقدمه

نسبت اطلاعات این طرح، نسبت مابین بیشترین اندازه از سهم‌ها و اندازه مقدار راز است، درحالی‌که 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 بر پایه مشاهدات زیر است. در ابتدا، توجه داریم که امنیت هر دستگاهی با افزایش مقدار اطلاعاتی که می‌بایست مخفی نگه داشته شود (سهم سهام‌داران)، تمایل به کاهش دارد. ثانیاً، اگر سهم‌هایی که به سهام‌داران داده می‌شود، خیلی بزرگ باشد، آن‌گاه حافظه موردنیاز 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 رأس‌ها، همان مجموعه سهام‌داران و یال‌ها، مجموعه‌های مجاز کمینه هستند. در این مقاله، ما ساختارهای دسترسی بر پایه گراف‌ها را مورد مطالعه

طرح تسهیم راز، روشی برای توزیع اطلاعات در میان مجموعه‌های 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 بازیابی کرد. اگر علاوه بر این، مجموعه‌های غیرمجاز دارای هیچ اطلاعات اضافی در مورد راز نباشند، یعنی سهم‌های آنان به‌طور 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. شامیر [۱] و بلکلی [۲] در ابتدا مسئله 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 به دست نیاورند. این طرح‌ها، (n, k) -طرح‌های آستانه‌ای نامیده می‌شوند، مقدار k آستانه طرح نامیده می‌شود و n تعداد سهام‌داران می‌باشد. سؤال اصلی در مورد کارایی این روش به این صورت است: به‌ازای هر بیت از راز، چه تعداد بیت از اطلاعات سهام‌داران می‌بایست به خاطر سپرده شود؟

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

بلوندو در مرجع [۵] یک شکاف در مقادیر نسبت اطلاعات گراف‌ها را نشان داد؛ به‌طور دقیق‌تر، آن‌ها بر روی این مطلب که توسط بریکل و داوونپورت [۶] به دست آمده بود، تأکید 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 [۱۸] طرح‌های بهینه بررسی شده اند و در مرجع [۱۹]، 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، به‌طوری‌که کیو بیت‌ها در یک پایه کلاسیک اندازه‌گیری شده و ارسال آن‌ها بدون اختلال صورت می‌پذیرد. میمنی و نوروزی [۲۰] طرح‌های تسهیم راز بر پایه ضرب دکارتی، سه رده از گراف‌ها را معرفی کردند. آن‌ها به کمک این روش مقدار دقیق نسبت اطلاعات ساختارهای دسترسی گراف حاصل از ضرب دکارتی دور در دور، مسیر در دور و منشور را محاسبه نمودند؛ اما همچنان مقدار دقیق نسبت اطلاعات ساختارهای دسترسی بسیاری از رده‌های گراف‌ها که حاصل از ضرب دکارتی دو یا چند گراف است، حل نشده باقی‌مانده است. در این مقاله کران پایینی برای نسبت اطلاعات گراف‌های حاصل از ضرب دکارتی یک درخت دلخواه با قطر حداقل ۳ در یک دور به طول دلخواه محاسبه شده است. همچنین نسبت اطلاعات دقیق گراف حاصل از ضرب دکارتی دور به طول ۶ در یک گراف مکعبی معرفی گردیده است. طرح‌های تسهیم راز مطرح‌شده در این مقاله همگی کامل هستند؛ یعنی زیرمجموعه‌های مجاز می‌توانند راز را به‌دست آورند، درحالی‌که زیرمجموعه‌های غیرمجاز با استفاده از سهم‌هاشان نمی‌توانند هیچ‌گونه اطلاعاتی از راز به‌دست آورند.

ساختار مقاله به‌صورت زیر سازمان‌دهی شده است. در بخش اول برخی تعاریف اولیه لازم برای طرح و اثبات ادعاهای مطرح‌شده در مقاله بیان شده است. در بخش دوم کران پایینی برای نسبت اطلاعات ساختار دسترسی گراف حاصل از ضرب دکارتی هر درخت n رأسی با قطر حداقل ۳ در یک دور به طول m معرفی شده است. درنهایت در بخش پایانی نسبت اطلاعات دقیق ساختار دسترسی گراف حاصل از ضرب دکارتی یک دور به طول ۶ در گراف مکعبی محاسبه شده است.

۲- برخی تعاریف اولیه

در این بخش برخی تعاریف اولیه لازم در مقاله را بیان می‌نماییم [۷-۸]. 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 در نظر می‌گیریم. s_i را سهم

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، مسئله یافتن کران روی اندازه سهم‌هایی که به سهام‌داران داده می‌شود یا به‌طور هم‌ارز نسبت اطلاعات، یکی از مسائل اساسی در این‌باره بوده و توجه زیادی را توسط محققین به خود جلب ساخته است. ارائه‌ی یک طرح با یک ساختار دسترسی مشخص در واقع ارائه یک کران بالا بر روی نسبت اطلاعات آن ساختار دسترسی است. بلوندو و همکارانش [۳] طرح‌های متفاوتی را برای ساختارهای دسترسی مختلف ارائه دادند و نسبت اطلاعات آن‌ها را محاسبه نمودند. سیرماز [۴] نشان داد که برای هر n سهام‌دار می‌توان یک ساختار دسترسی معرفی کرد به‌طوری‌که در هر طرح تسهیم راز کامل روی این ساختار دسترسی، نسبت سهم هر سهام‌دار حداقل $\frac{n}{\log n}$ برابر اندازه راز باشد.

در بسیاری از تحقیقاتی که تاکنون بر روی نسب اطلاعات انجام‌شده است تلاش شده تا نسبت اطلاعات دقیق رده‌های خاصی از ساختارهای دسترسی گرافی محاسبه گردد. به‌طور مثال نسبت اطلاعات برای اغلب گراف‌ها با حداکثر ۶ رأس در مراجع [۱۲-۵] مطرح‌شده، درحالی‌که متأسفانه نسبت اطلاعات برخی از این رده‌های گرافی هنوز به‌صورت بازه‌ای بیان شده است که اهمیت کران‌های دقیق ارائه‌شده در این مقاله را نشان می‌دهد. درخت‌ها، دارای نسبت اطلاعات $2 - \frac{1}{k}$ هستند که در آن، k یک مقدار صحیح است [۱۳]. همچنین، برای هر d ، دسته‌ای از گراف‌های نامتناهی با بیشترین درجه d ساخته شده که نسبت دقیق اطلاعات آن‌ها $\frac{d+1}{2}$ است [۱۴]. گراف‌های کامل دارای نسبت اطلاعات ۱ هستند، مسیرهای با ۴ رأس یا بیش‌تر، همانند دورهای با طول حداقل ۵، دارای نسبت اطلاعات $\frac{3}{2}$ هستند. سیرماز [۱۵]، نسبت اطلاعات گراف‌های d -مکعبی را یافته و ثابت کرده است که نسبت اطلاعات این گراف‌ها برابر با $d/2$ می‌باشد. با تعمیم گراف‌های مکعبی در مرجع [۱۶]، نسبت اطلاعات دسته‌ای از حاصل‌ضرب دکارتی گراف‌ها به دست آمده است.

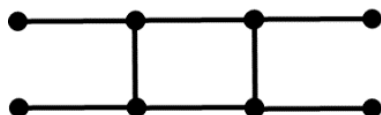
استینسون و بریکل [۷ و ۱۷] چندین کران بالایی و پایینی برای نسبت اطلاعات ساختار دسترسی‌های مبتنی بر گراف‌ها یافته‌اند. استینسون [۱۷] نشان داد که نسبت اطلاعات یک گراف با بیشترین درجه d حداکثر برابر با $\frac{d+1}{2}$ است. بریکل و داوونپورت [۶] نشان دادند که یک گراف دارای نسبت اطلاعات ۱ است اگر و تنها اگر گراف، دوبخشی کامل باشد. علاوه بر این،

گراف G به دست می‌آید را زیر گراف القایی G گویند.

قضیه ۳-۱. [۲۱] اگر G یک گراف و H زیرگراف القایی آن باشد آن‌گاه:

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

قضیه ۳-۲. [۲۱] 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 رأس‌های $G \square H$ حاصل ضرب دکارتی $V(G) \times V(H)$ بوده و هر دو رأس (u, u') و (v, v') مجاور هستند اگر و تنها اگر $u = v$ و $u' = v'$ مجاور باشد یا $u = v$ و $u' = v'$ مجاور باشد. حاصل ضرب دکارتی دارای خاصیت جابه‌جایی است، یعنی گراف‌های $G \square H$ و $H \square G$ به‌طور طبیعی یک‌ریخت هستند. این عملگر دارای خاصیت شرکت‌پذیری است، یعنی گراف‌های $F \square (G \square H)$ و $(F \square G) \square H$ به‌طور طبیعی یک‌ریخت هستند. در مورد حاصل ضرب دکارتی مسیر P_m به طول m و دور C_n به طول n ، مقدار دقیق نسبت اطلاعات با توجه به قضیه زیر به دست آمده است:

قضیه ۳-۳. [۲۰] برای هر $m, n \geq 4$ می‌توان گفت

$$R(P_m \square C_n) = 2$$

فرض کنید که T_n یک درخت n رأسی 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. در ادامه، تعمیمی از قضیه ۳-۳ را بیان می‌کنیم که اثبات آن برگرفته‌شده از مرجع [۲۰] است.

قضیه ۳-۴. اگر T_n درخت n رأسی با قطر حداقل ۳ باشد و

$$R(T_{n,m}) \geq 2 \quad m \geq 4.$$

اثبات: برای آن که نشان دهیم $R(T_{n,m}) \geq 2$ 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 به طول ۳ است. این مسیر القایی را به فرم

سهام‌دار $i \in Q$ فرض کنید. با توجه به همه $(n+1)$ -تایی‌های ممکن $(s_{p_0}, s_1, s_2, \dots, s_n)$ از سهام‌ها، نگاشت $\pi_i: E \rightarrow E_i$ را برای یک مجموعه‌ی مشخص E چنان تعریف می‌کنیم که برای هر $e \in E$ اعضای $(\pi_i(e))_{i \in Q}$ سهام‌های یک راز باشند. ما فقط نگاشت‌های پوشا را در نظر می‌گیریم، بنابراین، برای هر سهام‌دار $i \in Q$ مجموعه E_i همان مجموعه همه سهام‌های ممکن سهام‌دار i است. اگر یک توزیع احتمال در E را در نظر بگیریم، آن‌گاه هر یک از نگاشت‌ها یک توزیع احتمال در E_i القاء می‌کند. بنابراین، می‌توان $H(E_i)$ را به‌عنوان آنتروپی شانون هر یک از متغیرهای تصادفی در نظر گرفت.

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

$$H(E_j | A) = H(E_j | E_{i_1}, \dots, E_{i_r})$$

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

$$H(E_{p_0} | A) = H(E_{p_0})$$

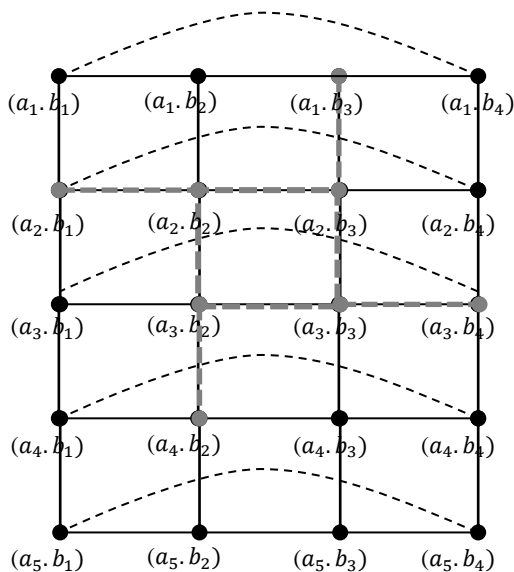
این تساوی بیانگر آن است که یک مجموعه غیرمجاز قادر به بر ملا کردن حتی یک بیت از اطلاعات راز نیست.

به‌منظور اندازه‌گیری طول سهام هر طرح، از آنتروپی سهام آن طرح استفاده می‌شود. نرخ اطلاعات طرح تسهیم راز Σ به‌صورت $\rho(\Sigma) = \frac{H(E_0)}{\max_{i \in P} H(E_i)}$ تعریف می‌شود. مقدار $R(\Sigma) = 1/\rho(\Sigma)$ را نسبت اطلاعات طرح Σ گویند. هر دو مقدار ρ و R را به‌عنوان ضریب تأثیر یک طرح به کار می‌برند. این پارامترها را می‌توان برای ارزیابی بهترین راندمان طرح‌های یک ساختار دسترسی مشخص استفاده نمود. نرخ اطلاعات بهینه برای یک ساختار دسترسی Γ را بیشترین نرخ $\rho(\Sigma)$ روی تمامی طرح‌های Σ تعریف شده برای ساختار دسترسی Γ گویند. نسبت اطلاعات بهینه ساختار دسترسی Γ نیز به‌صورت $R(\Gamma) = 1/\rho(\Gamma)$ 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

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 طوری که متغیرهای تصادفی ξ_v برای هر $v \in V(G)$ و متغیر تصادفی ξ برای راز در نظر 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 مجموعه $\{f(v) : v \in V(G)\}$ است. در بدترین حالت، نسبت اطلاعات برابر با بیشترین مقدار در این مجموعه است. با استفاده از خواص استاندارد توابع آنتروپی [۸] داریم:

الف) خاصیت مثبت بودن: $f(\emptyset) = 0$ 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 ζ دو متغیر تصادفی باشند، متغیر تصادفی ζ ، مقدار ξ را تعیین می‌کند اگر و تنها اگر $H(\xi|\zeta) = 0$. همچنین ξ و ζ به طور آماری مستقل هستند اگر:

در نظر بگیرید. به علاوه فرض کنید دور $P: a_1 - a_2 - a_3 - a_4$ به فرم $C_m: b_1 - b_2 - \dots - b_m - b_1$ 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 طبق قضیه ۱-۳ داریم:

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

۴- نتایج اصلی

حال، فرض کنید گراف C_n دور به طول n و K_n گراف کامل با n رأس باشد. تعریف کنید: $C_n^d = C_n \square K_2 \square \dots \square K_2$ جایی که تعداد کپی‌های K_2 در این حاصل ضرب برابر با d است. به آسانی می‌توان بررسی کرد که برای هر $n \geq 2$ و $d \geq 0$ ، گراف C_n^d یک گراف $(d+2)$ -منظم راس‌ترایا با $n \times 2^d$ رأس است و برای n زوج، گراف C_n^d نیز یک‌گراف 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 ۱-۴. 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 بلوندو [۵] مطرح گردید. نسبت اطلاعات هر رأس $v \in V(G)$ برابر با $\frac{H(\xi_v)}{H(\xi)}$ است. این تساوی بیان می‌کند که

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 تک عضوی b است.

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

با توجه به تعریف مجموعه‌های A_d و B_d 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 ۴-۲. 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:

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

اثبات ادعا: برای اثبات ادعا از استقرا روی d استفاده می‌کنیم. فرض کنیم نامساوی فوق به‌ازای $d=1$ 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:

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

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:

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

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

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 آنروپی که در سال ۱۹۷۹ نشان داده‌شد، به‌صورت زیر بیان می‌گردد. به‌سادگی 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 [۵].

اثبات قضیه ۴-۱. با توجه به تعریف ارائه‌شده برای تابع f در قسمت قبل، 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:

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

این همان نامساوی است که برای اثبات کران پایین 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 دو نسخه C_6^d به روش فوق به ترتیب 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 A'_d و B_d باشند؛ بنابراین، تقسیم رئوس گراف C_6^{d+1} به‌صورت زیرمجموعه‌های از هم جدای مستقل $A_{d+1} = A_d \cup A'_d$

اما به سادگی می توان دید:

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

بنابراین:

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

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

اکنون به ادامه اثبات قضیه ۴-۱ می پردازیم:

فرض کنید $d \geq 1$. با توجه به نحوه تعریف گراف C_6^d و بر اساس آنچه شرح داده شد، می توان مجموعه رئوس این گراف را به صورت $V(C_6^d) = A_d \cup B_d$ از آنجایی که در هر یک از بخش های مستقل مجزای A_d و B_d دقیقاً 3×2^d رأس وجود دارد؛ لذا می توانیم بین رئوس این دو دسته یک تطابق کامل در نظر بگیریم. اگر (a, b) یکی از یال های 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 تک عضوی b است. نامساوی فوق برقرار است چراکه $A_d - \{a\}$ یک مجموعه مستقل رأسی است، در حالی که bA_d چنین نیست. با در نظر گرفتن رابطه فوق برای هر یک از زوج جملات حاصل از مجموع های 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:

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

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

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

سمت راست نامساوی فوق همان کران پایین مورد نظر است و

این اثبات را تمام می کند، زیرا:

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

• کران بالای نسبت اطلاعات

برای اثبات کران بالا از روش تجزیه استینسون [۱۷] استفاده خواهیم کرد. استینسون در مقاله خود روشی برای طرح های تسهیم راز در حالت کلی ارائه داده است که به آن ساختار λ - تجزیه گویند. این روش، یک ساختار بازگشتی برای تولید یک طرح تسهیم راز با استفاده از طرح های تسهیم راز کوچک تر به عنوان بلوک هایی از طرح اصلی است. این روش در ساختار دسترسی یک گراف، بر پایه یافتن یک پوشش از آن گراف است به طوری که هر یال از این گراف می بایست در حداقل λ تا از زیرگراف های این پوشش قرار گیرد. قضیه زیر نحوه استفاده از چنین پوششی را برای معرفی یک کران بر روی ساختار دسترسی گراف های حاصل از ضرب دکارتی معرفی شده در این مقاله بیان می کند.

قضیه ۴-۳. [۱۷] فرض کنید G_i خانواده ای از زیرگراف های G باشد به طوری که هر یال از گراف G متعلق به حداقل λ تا از G_i ها باشد. به ازای رأس $v \in V(G)$ تعریف کنید: اگر $v \notin V(G_i)$ تعریف می کنیم $r_i(v) = 0$ و در غیر این صورت $r_i(v) = R(G_i)$. آن گاه:

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

با توجه به قضیه فوق، نتیجه زیر را می توان در مورد حاصل ضرب دکارتی یک گراف منظم با گراف کامل دو رأسی به دست آورد:

نتیجه ۴-۴. برای هر گراف d -منظم G داریم:

$$R(G \square K_2) \leq 1 + \left(1 - \frac{1}{d}\right) R(G)$$

اثبات: کافی است در گراف $G \square K_2$ ، هر یک از نسخه های گراف G را $d-1$ بار و زیرگراف های حاصل از ضرب هر یک از یال های G با گراف K_2 را یک بار توسط مربع ها ببوشانیم. در این صورت، هر یال دقیقاً در d تا از این پوشش ها آمده و هر رأس متعلق به دقیقاً d تا از این مربع ها و $d-1$ نسخه G است؛ بنابراین، طبق قضیه ۴-۶ داریم:

$$R(G \square K_2) \leq \frac{d \times 1 + (d-1)R(G)}{d} = 1 + \left(1 - \frac{1}{d}\right) R(G).$$

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

لم ۴-۵. به ازای مقدار صحیح نامنفی d داریم:

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

اثبات: با توجه به آن که C_6^d حاصل ضرب دکارتی دور به طول ۶ با گراف مکعبی است لذا تمامی دوره های به طول ۴ در گراف

جدول (۱): نسبت اطلاعات به همراه کران‌های بالایی و پایینی

d	lower	upper	R	lgap	ugap
۱	۱/۲	۲	۷/۴	۵/۴	۱/۴
۲	۱	۵/۲	۱۳/۶	۷/۶	۱/۳
۳	۳/۲	۳	۲۱/۸	۹/۸	۳/۸
۴	۲	۷/۲	۳۱/۱۰	۱۱/۱۰	۲/۵
۵	۵/۲	۴	۴۳/۱۲	۱۳/۱۲	۵/۱۲
۶	۳	۹/۲	۵۷/۱۴	۱۵/۱۴	۳/۷
۷	۷/۲	۵	۷۳/۱۶	۱۷/۱۶	۷/۱۶
۸	۴	۱۱/۲	۹۱/۱۸	۱۹/۱۸	۴/۹
۹	۹/۲	۶	۱۱۱/۲۰	۲۱/۱۰	۹/۲۰
۱۰	۵	۱۳/۲	۱۳۳/۲۲	۲۳/۲۲	۵/۱۱

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 بر این، بهترین نسبت اطلاعات، طرح تسهیم راز کامل بر پایه گراف C_6^d را تعیین کردیم که در آن، گراف حاصل از ضرب دکارتی دور به طول ۶ با گراف d -مکعب است.

به‌طور 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 استینسون استفاده شد. در بیشتر مقالاتی که تاکنون به این موضوع پرداخته‌اند کران‌های غیردقیق و به‌صورت بازه‌ای ارائه شده است، درحالی‌که در این مقاله نتیجه اصلی به‌صورت یک کران دقیق معرفی گردیده است. خواننده علاقه‌مند می‌تواند نسبت اطلاعات دقیق گراف‌های بسیاری که هنوز تعیین نگردیده است را مورد مطالعه قرار دهد.

۶- تقدیر و تشکر

نویسنده دوم، از حمایت پژوهشگاه دانش‌های بنیادین به‌خاطر حمایت مالی با شماره طرح CS1397-4-74 تقدیر و تشکر می‌نماید.

مکعبی و دوره‌های به طول ۶ در C_6^d ، یک پوشش برای این گراف ایجاد می‌کند. این پوشش به‌اختصار ۲-رخ نامیده می‌شود. به‌وضوح، C_6^d یک گراف $(d+2)$ -منظم است که دارای 6×2^d رأس می‌باشد. از آنجایی‌که هر زوج از یال‌های شامل رأس v تشکیل یک ۲-رخ می‌دهند، بنابراین، هر رأس دقیقاً روی $1 - \binom{d+2}{2}$ تا ۲-رخ قرار می‌گیرد. حال، به‌سادگی 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. به‌عبارت‌دیگر، ۲-رخ‌ها تشکیل یک $(d+1)$ -پوشش از C_6^d می‌دهند. از طرفی در این پوشش هر رأس دقیقاً $\frac{d^2+3d+1}{2}$ بار توسط ۲-رخ‌ها پوشیده می‌شوند. با توجه به نحوه محاسبه نسبت اطلاعات ارائه‌شده در قضیه ۴-۶ توسط یک پوشش مشخص از گراف G ، داریم:

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

حال، قضیه اصلی از لم ۴-۲ و لم ۴-۵ نتیجه شده و به‌صورت زیر است:
قضیه ۴-۶. 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 گراف‌های حاصل از ضرب دکارتی، معرفی شده در این مقاله هست.

اگرچه قضیه ۴-۶ در این مقاله مقدار دقیق نسبت اطلاعات گراف C_6^d را مشخص می‌کند، برخی کران‌های بالایی و پایینی برای این نسبت اطلاعات را می‌توان از مراجع [۱۵ و ۱۷] به‌دست آورد. در واقع، از آنجایی‌که C_6^d یک گراف $(d+2)$ -منظم است، داریم $R(C_6^d) \leq \frac{d+3}{2}$ و نیز از آنجایی‌که گراف d -مکعبی را به‌عنوان زیرگراف القایی خود در برمی‌گیرد داریم $R(C_6^d) \geq R(Q_d) = \frac{d}{2}$. در جدول (۱) مقدار دقیق نسبت اطلاعات C_6^d که با R نمایش داده شده است با این کران‌های بالایی و پایینی مقایسه شده است. همچنان‌که از این جدول دیده می‌شود، فاصله R با کران بالایی که با $UGAP$ نشان داده شده، از فاصله آن با کران پایینی، یعنی $LGAP$ ، کمتر می‌باشد، به‌عبارت‌دیگر R به کران بالایی نزدیک‌تر است.

۷- منابع

- [12] M. Gharahi and S. Khazaei, "Reduced access structures with four minimal qualified subsets on six participants," *Adv. Math. Commun.* vol. 12, pp. 199-214, 2018.
- [13] L. Csirmaz and G. Tardos, "Optimal information rate of secret sharing schemes on trees," *IEEE Trans. Inf. Theory*, vol. 59, pp. 2527-2530, 2013.
- [14] L. Csirmaz and P. Ligeti, "On an infinite family of graphs with information ratio $2-1/k$," *Computing*, vol. 85, pp. 127-136, 2009.
- [15] L. Csirmaz, "Secret sharing on the d-dimensional cube," *Design. Code. Cryptogr.* vol. 74, pp. 719-729, 2015.
- [16] A. Cheraghi, G. Raeisi and M. Gholami, "On the information ratio of a class of graphs," *First International Conference on Combinatorics, Cryptography and Computation, I4C2016, IUST, Nour branch, Mazandaran, Iran, Sep. 2016.*
- [17] D. R. Stinson, "Decomposition construction for secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 40, pp. 118-125, 1994.
- [18] 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.
- [19] 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.
- [20] H. Maimani, Z. Norozi, "Secret sharing based on Cartesian product of graphs", *Iranian J. Math. Sci. Info*, vol. 8, pp. 31-38, 2013.
- [21] L. Csirmaz, "Secret sharing on infinite graphs," *Tetra Mount. Math. Pub.* vol. 41, pp.1-18, 2008.
- [1] A. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, 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, et al., "On the information rate of secret sharing schemes," *Theor. Comput. Sci.*, vol. 154, no. 2, pp. 283-306, 1996.
- [4] L. Csirmaz, "The size of a share must be large," *J. Cryptol*, vol. 10, pp. 223-231, 1997.
- [5] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, "Graph decomposition and secret sharing schemes," *J. Cryptol*, vol. 8, pp. 39-64, 1995.
- [6] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptol*, vol. 4, pp. 123-134, 1991.
- [7] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *J. Cryptol*, vol. 5, pp. 153-166, 1992.
- [8] J. Martí-Farré and P. Carles "On secret sharing schemes, matroids and polymatroids," *J. Math. Cryptol*, vol. 4, pp. 95-120, 2010.
- [9] M. Van Dijk, "On the information rate of perfect secret sharing schemes," *Design. Code. Cryptogr.*, vol. 6, pp. 143-160, 1995.
- [10] W. A. Jackson and K. M. Martin, "Perfect secret sharing schemes on five participants," *Design. Code. Cryptogr.* vol. 9, pp. 267-286, 1996.
- [11] C. Padro, "Lecture notes in secret sharing," Available at <http://eprint.iacr.org/2012/674>, 2012.

Some New Bounds on the Information Ratio of the Cartesian Product of Some Classes of Graphs**A. Cheraghi*, M. Gholami**

University of Khansar

(Received: 13/01/2018, Accepted: 27/05/2018)

ABSTRACT

In this paper, we find a lower-bound for the information ratio of the cartesian product of an arbitrary tree with diameter at least 3 and a cycle C_m for every $m \geq 3$. Moreover, we determine the best information ratio of the perfect secret sharing scheme based on C_6^d the graph constructed from the cartesian product of a cycle of length 6 with the d -dimensional cube Q_d . More precisely, it is shown that for every $d \geq 1$, the information ratio of C_6^d is exactly $\frac{d(d+3)+3}{2(d+1)}$.

Keywords: Secret Sharing Scheme, Information Ratio, Cartesian Product.

* Corresponding Author Email: : a.cheraghi@khn.ui.ac.ir