مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه ترکیبیات، رمزنگاری و محاسبات، ص ۱۲۲ -۱۱۷

نرخ اطلاعات بهینه برای ساختارهای دسترسی گرافی

عباس چراغی چالشتری*، میترا شرافتی

۱- استادیار، ۲- دانشجوی کارشناسی ارشد، گروه ریاضی، دانشگاه خوانسار، خوانسار، ایران

(دریافت: ۱۳۹۷/۰۸/۲۵ پذیرش: ۱۳۹۸/۰۷/۰۲)

چکیده

در مقاله‌های بسیاری، نرخ اطلاعات بهینه برای ساختارهای دسترسی گرافی مورد بررسی قرار گرفته، اما تاکنون مقدار دقیق نرخ اطلاعات بهینه برای خانواده زیادی از ساختارهای دسترسی گرافی محاسبه نشده است. در این مقاله ما مقدار نرخ اطلاعات بهینه دو ساختار دسترسی گرافی با شش سهام‌دار، از ۹ ساختاری که مقدار نرخ اطلاعات بهینه آن‌ها محاسبه نشده، را به‌طور دقیق محاسبه می‌کنیم. همچنین در انتها، دسته جدیدی از گراف‌ها را معرفی و به محاسبه نرخ اطلاعات بهینه آن‌ها و در مواردی به ارائه کرانی برای این مقدار می‌پردازیم.

واژه های کلیدی: ساختار دسترسی گرافی، طرح تسهیم راز کامل، نرخ اطلاعات

۱- مقدمه

در تمام سطوح جامعه سامانه‌هایی مرسوم شده‌اند که با انتقال، ذخیره‌سازی و پردازش اطلاعات سرو کار دارند. جامعه‌ای که در آن زندگی می‌کنیم، معمولا جامعه اطلاعاتی نامیده می‌شود. اطلاع در جامعه ما شکل کلیدی به خود گرفته است. گاهی این اطلاعات از ارزش بالایی برخوردار هستند و نیازمند محفوظ ماندن از دسترس بیگانه می‌باشند. از این جهت همواره مبحث محرمانه بودن اطلاعات برای ما اهمیت دارد؛ از این‌رو، انسان درصدد برآمد که اطلاعات ارزشمند خود را رمزگذاری کند. هم-زمان با پیشرفت در زمینه محاسبات، نیاز به برون‌سپاری اطلاعات نیز افزایش یافت. بنابراین تامین و تضمین امنیت داده‌ها نیز بسیار ضرورت پیدا کرد. به این منظور روش‌های مختلفی برای رمزنگاری داده‌ها و الگوریتم‌های مختلفی برای تسهیم راز مطرح شد. هدف از طرح تسهیم راز آن است که یک راز به چندین بخش تقسیم شود و هر بخش به شرکت‌کنندگان در تسهیم راز ارسال شود. برای بازیابی راز، باید تعداد از پیش تعیین شده‌ای از شرکت‌کنندگان، سهم راز خود را برگردانند. این طرح، روشی برای تسهیم رازهای مختلف بین سهام‌داران است به طوری‌که زیرمجموعه‌های مجاز قادر به بازسازی راز باشند. حال اگر علاوه بر خاصیت مذکور زیرمجموعه‌های غیرمجاز نیز نتوانند حتی کوچکترین مقدار از راز را بازسازی کنند، گوییم یک طرح تسهیم راز کامل داریم. به مجموعه همه زیرمجموعه‌های مجاز که قادر به بازسازی راز باشند، ساختار دسترسی Γ گفته می‌شود. در این بین کوچکترین ساختار دسترسی ممکن را با Γ_0 نشان داده و پایه‌ی Γ 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 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 کارایی این روش به این‌صورت است: به‌ازای هر بیت از راز، چه تعداد بیت از اطلاعات سهام‌داران می‌بایست به خاطر سپرده شود؟

به نسبت بین اندازه راز با بیشترین مقدار سهم داده شده به هر شخص نرخ اطلاعات یک طرح تسهیم راز گفته می‌شود و چون علاقه‌مندیم که سهم داده شده به هر سهام‌دار کوچک باشد پس نرخ اطلاعات بهینه سختار دسترسی Γ با بیشینه این نسبت نشان داده می‌شود. 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 سهام-داران)، تمایل به کاهش دارد. ثانیاً، اگر سهم‌هایی که به سهام-داران 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 نرخ اطلاعات ساختارهای دسترسی را داشته باشیم. در راستای این هدف، یافتن کران‌های بالایی و پایینی روی نسبت اطلاعات ارزشمند خواهد بود.

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

در این مقاله ساختارهای دسترسی گرافی مورد مطالعه قرار می‌گیرند که شامل کوچکترین زیرمجموعه‌های مجاز دو عضوی است. به‌عبارت‌دیگر اجتماع دو نفر از سهام‌داران قادر به بازسازی راز هستند اما یک نفر به تنهایی نمی‌تواند هیچ اطلاعاتی از راز را به‌دست آورد. هم‌چنین ساختارهای دسترسی بررسی شده دارای خاصیت یکنوایی هستند یعنی ابرمجموعه هر مجموعه مجاز خود یک مجموعه مجاز خواهد بود.

مقدار نرخ اطلاعات بهینه برای ساختارهای دسترسی گرافی با شش سهام‌دار در [۴-۷] مورد مطالعه قرار گرفته است. در [۴] همه ۱۱۲ ساختارهای دسترسی شش راسی گرافی مطالعه شده اما مقدار دقیق نرخ اطاعات بهینه ۹۴ مورد محاسبه شده است. در مقالات [۵-۶] نرخ اطلاعات بهینه ۸ مورد دیگر محاسبه شده و در [۷] نرخ اطلاعات یک مورد دیگر به‌طور دقیق مشخص شده است.

اما تا کنون مقدار دقیق نرخ اطلاعات ۹ ساختار دسترسی با ۶ سهام‌دار محاسبه نشده است. ما در این مقاله با ارائه طرحی خاص برای دو ساختار از این ۹ ساختار دسترسی گرافی، مقدار دقیق نرخ اطلاعات بهینه آن‌ها را به‌طور دقیق محاسبه می‌کنیم. در [۸] نیز به بررسی نرخ اطلاعات بهینه دسته جدیدی از گراف‌ها پرداخته شده که از حاصل ضرب دکارتی دوری به طول ۶ با گراف d–مکعب ساخته می‌شود که بیانگر گستردگی مبحث محاسبه نرخ اطلاعات بهینه گراف‌هاست.

درخت‌ها، دارای نرخ اطلاعات $\frac{k}{2(k-1)+1}$ هستند که در آن، k یک مقدار صحیح است [۹]. همچنین، برای هر d، دسته‌ای از گراف-های نامتناهی با بیشترین درجه d ساخته‌شده که نرخ دقیق اطلاعات آن‌ها $\frac{2}{d+1}$ است [۱۰]. گراف‌های کامل دارای نرخ اطلاعات ۱ هستند، مسیرهای با ۴ رأس یا بیش‌تر، همانند دورهای با طول حداقل ۵، دارای نرخ اطلاعات $\frac{2}{3}$ هستند. سیرماز [۱۱]، نرخ اطلاعات گراف‌های d–مکعبی را یافته و ثابت کرده است که نرخ اطلاعات این گراف‌ها برابر با $\frac{2}{d}$ می‌باشد.

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 نرخ اطلاعات بهینه ساختار دسترسی دو گراف که در [۴] به‌صورت بازه‌ای بررسی شده است را به‌صورت دقیق محاسبه خواهیم کرد. سپس در بخش سوم نرخ اطلاعات دقیق ساختار دسترسی گراف‌های چندبخشی رشد یافته محاسبه و در نهایت برای رده دیگری از گراف‌های رشد یافته کران‌هایی به‌صورت یک بازه کوچک ارائه خواهد شد.

۲- تعاریف و مفاهیم اولیه

در این بخش برخی تعاریف اولیه لازم در مقاله را بیان می‌نماییم. فرض کنید G یک گراف با مجموعه n راسی از رئوس به شکل V و یک مجموعه m یالی به‌صورت E باشد. هنگامی که تعداد یال‌ها و تعداد رأس‌ها متناهی باشد گراف را متناهی می‌گوییم. گرافی که مجموعه رأس‌ها و مجموعه یال‌های آن تهی باشد گراف تهی نامیده می‌شود. گرافی که تنها یک رأس داشته باشد گراف بدیهی و در غیر این‌صورت گراف غیربدیهی نامیده می‌شود. گراف ساده‌ای که بین همه‌ی n رأس آن یال وجود داشته باشد گراف کامل گویند و با K_n نمایش می دهند. زمانی که گراف هیچ یالی نداشته باشد گراف را خالی گویند. گراف t بخشی گرافی است که بتوان رئوس آن را به t بخش چنان افراز کرد که دو سر هیچ یالی در یک بخش قرار نگیرد. گراف چند بخشی کامل گرافی است که هر راس به تمامی رئوس دیگر بجز بخش خودش متصل باشد.

در طرح‌های تسهیم راز بر پایه ساختارهای دسترسی گرافی، یک ساختار دسترسی توسط یک گراف تعریف می‌شود که در آن مجموعه رأس‌ها، همان مجموعه سهام‌داران و یال‌ها، مجموعه‌های مجاز مینیمال دو عضوی هستند. در این مقاله، ما ساختارهای دسترسی بر پایه گراف‌ها را مورد مطالعه قرار خواهیم داد و طرح تسهیم راز برای ساختار دسترسی بر پایه یک گراف را طرح تسهیم راز گرافی می‌نامیم. در طرح‌های تسهیم راز، مسئله یافتن کران روی اندازه سهم‌هایی که به سهام‌داران داده می‌شود.

فرض کنید که Γ یک ساختار دسترسی مشخص شامل تمامی مجموعه‌های مجازی باشد که قادر به بازسازی راز هستند. همچنین $\mathcal{P}$ مجموعه تمامی سهام‌داران، $\mathcal{S}_p$ مجموعه همه سهم‌های ممکنی است که به سهام‌دار دلخواه p تعلق گرفته است و $\mathcal{K}$ مجموعه همه رازهای ممکن می‌باشد.

تعریف ۲-۱. یک طرح تسهیم راز Σ، روشی برای توزیع یک راز دلخواه از مجموعه‌ی $\mathcal{K}$، در بین سهام‌داران مجموعه‌ی $\mathcal{P}$ است به طوری که هر زیرمجموعه مجاز دلخواه از ساختار دسترسی Γ بتوانند آن راز را بازسازی نمایند درحالی که هیچ زیرمجموعه‌ی غیرمجازی که متعلق به Γ نباشند، نتوانند هیچگونه اطلاعاتی راجع به آن راز به‌دست بیاورند.

بدیهی است که طبق تعریف فوق طرحی جذابیت بیشتر دارد که بتواند سهام‌داران بیشتری را راضی نگه دارد. از آنجایی که تمایل هر سهام‌دار به دریافت سهم کوچکتری با همان میزان امنیت قبل است، لذا ابزاری لازم است تا این میزان رضایت را در بین دو طرح مختلف روی یک ساختار دسترسی یکسان، تخمین بزند. نرخ اطلاعات روشی مناسب برای ارزیابی قدرت برتری یک طرح

نسبت به طرح دیگر است.

تعریف ۲-۲. فرض کنید Σ، طرح تسهیم رازی برای توزیع یک راز دلخواه از مجموعه $\mathcal{K}$، در بین سهام‌داران مجموعه $\mathcal{P}$ باشد. همچنین درنظر بگیرید که δ_p مجموعه همه سهم‌های ممکنی است که به سهام‌دار p تعلق یافته است. نرخ اطلاعات طرح خاص Σ به صورت زیر تعریف می‌شود [۳]:

$$\rho(\Sigma) = \frac{log_2|K|}{\max\limits_{p\in\mathcal{P}} log_2|S_p|} \qquad (1)$$

همچنین نرخ اطلاعات بهینه یک ساختار دسترسی Γ به صورت

$$\rho^*(\Gamma) = \sup_{\Sigma}\ \rho(\Sigma). \qquad (2)$$

تعریف می‌شود. که در آن بیشینه روی تمامی طرح‌های تسهیم راز Σ ای است که بر روی ساختار دسترسی Γ می‌توان ساخت. برای درک شهودی تعریف فوق و از آنجایی که مجموعه‌ی رازهای $\mathcal{K}$ یک خانواده متناهی است، $log_2|\mathcal{K}|$ را می‌توان طول رشته دودویی در نظر گرفت که برای نمایش هر کلید لازم است. همچنین $log_2|S_p|$ تعداد بیت‌هایی است که به‌عنوان سهم سهام‌دار p به او تعلق می‌گیرد. لذا $\rho(\Sigma)$ نسبت اطلاعات هرکلید به بیشترین اطلاعاتی است که به یک سهام‌دار اختصاص داده می‌شود. این پارامتر را می‌توان برای ارزیابی بهترین راندمان طرح‌های یک ساختار دسترسی مشخص استفاده نمود.

قضیه ۲-۳. [۳] برای هر طرح تسهیم راز کامل Σ که روی یک ساختار دسترسی مشخص Γ ساخته شده باشد داریم:

$0 \le \rho(\Sigma) \le 1$ زمانی که نرخ اطلاعات یک طرح برابر ۱ باشد، حالت بهینه برای سهام‌داران اتفاق خواهد افتاد زیرا هر شخص به‌ازای یک راز به‌طور دقیق یک سهم دریافت خواهد کرد. بنابراین، چنین طرحی یک طرح ایده‌آل گفته می‌شود. در حقیقت مقدار نرخ اطلاعات بهینه بیانگر برتری یک طرح نسبت به طرح دیگر روی ساختار دسترسی مشخص Γ است. بنابراین، محاسبه دقیق و یا ارائه کرانی برای این پارامتر همواره مورد توجه بوده است. برای ارائه کران روی نرخ اطلاعات بهینه قضیه بعد می‌تواند سودمند باشد. در گراف G مجموعه رأس‌ها، همان مجموعه سهام‌داران و یال‌ها، مجموعه‌های مجاز کمینه Γ_0 هستند. نرخ اطلاعات بهینه این نوع ساختارهای دسترسی را با $\rho^*(G)$ نشان می‌دهیم. یکی از ابزاری که برای کران بالا نرخ اطلاعات بهینه استفاده می‌شود قضیه معروف زیر است.

قضیه ۲-۴. [۹] اگر G یک گراف و H زیرگراف القایی آن باشد آن‌گاه:

$$\rho^*(G) \le \rho^*(H).$$

قضیه (۲-۴)، بیانگر آن است که اگر ساختار دسترسی گرافی G دارای زیر گراف القایی به شکل H باشد طوری که نرخ اطلاعات بهینه آن محاسبه شده باشد آن‌گاه نرخ اطلاعات بهینه ساختار دسترسی G حداکثر برابر است با $\rho^*(H)$.

یکی از نتایج معروفی که برای نرخ اطلاعات بهینه ساختارهای دسترسی گرافی وجود دارد درخصوص وجود طرح‌های ایده‌آل است. به عبارت دیگر $\rho^*(G) = 1$ اگر و تنها اگر G یک گراف چندبخشی کامل باشد. اگر ساختار دسترسی گرافی یکریخت با یک گراف چندبخشی کامل نباشد نرخ اطلاعات هر طرح تسهیم راز روی آن یک جهش بزرگ دارد.

قضیه ۲-۵. [۳] فرض کنید G یک گراف همبند غیریکریخت با گراف چندبخشی کامل باشد آن‌گاه برای هر طرح تسهیم راز Σ روی این ساختار دسترسی داریم: $\rho(\Sigma) \le \frac{2}{3}$

تمامی ساختارهای دسترسی گرافی بررسی شده در این مقاله غیریکریخت با گراف چندبخشی کامل هستند، لذا کران بالای $\frac{2}{3}$ روی نرخ اطلاعات بهینه همگی این ساختارها وجود دارد. یکی از روش‌هایی که می‌توان نشان داد مقدار دقیق نرخ اطلاعات بهینه یک ساختار دسترسی گرافی غیر یکریخت با گراف‌های چندبخشی کامل برابر $\frac{2}{3}$ است، ارائه یک طرح خاص با نرخ اطلاعاتی برابر همین مقدار است. در بخش‌های بعد با استفاده از همین فن و روش‌های معروفی چون l-تجزیه استینسون مقادیر نرخ اطلاعات بهینه را به‌صورت دقیق محاسبه خواهیم کرد.

از آنجایی که محاسبه نرخ اطلاعات بهینه دقیق ساختارهای دسترسی گرافی بسیار مشکل است، در بیشتر مقالاتی که در این زمینه انجام شده کران‌هایی به شکل بازه‌ای برای آنها ارائه شده است. در بخش بعد، ما برای دو ساختار دسترسی گرافی مقدار بهینه دقیق محاسبه کرده‌ایم. سپس یک رده گراف با نرخ اطلاعات بهینه $\frac{2}{3}$ ارائه خواهیم داد و در پایان برای یک رده دیگری از ساختارهای دسترسی گرافی کران‌های به شکل یک بازه ارائه خواهیم داد.

۳- نتایج اصلی

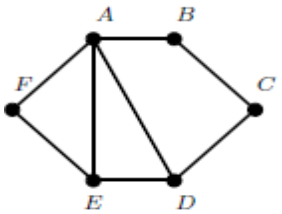
در [۴] تمامی ساختارهای دسترسی گرافی با ۶ راس مورد بررسی قرار گرفته اما مقدار دقیق نرخ اطاعات بهینه همه آن‌ها محاسبه نشده است. در [۶-۵] تنها نرخ اطلاعات بهینه ۸ مورد باقی مانده از گراف‌های شش راسی، محاسبه شده و در [۷] نرخ اطلاعات یک مورد دیگر به‌طور دقیق مشخص شده است.

اما تا کنون مقدار دقیق نرخ اطلاعات ۹ ساختار دسترسی با ۶

سهام‌دار محاسبه نشده است. ما در این بخش با ارائه طرحی خاص برای دو ساختار از این ۹ ساختار دسترسی گرافی، مقدار نرخ اطلاعات بهینه آن‌ها را به‌طور دقیق محاسبه می‌کنیم. ون دیجک در [۴] هریک از گراف‌های غیر یکریخت ۶ راسی را با یک ساختار دسترسی Γ_i شماره‌گذاری کرده است. ما برای دو ساختارهای دسترسی Γ_{55} و Γ_{70} (به ترتیب شکل ۱ و ۲) باقیمانده از این مقاله دو طرح جدید پیشنهاد و کران پایینی برای نرخ اطلاعات بهینه Γ_{55} و Γ_{70} ارائه می‌کنیم. ون دیجک در [۴] برای مقادیر ۷۰ و i=۵۵، کران بازه‌ای $\frac{3}{5}\leq\rho^*(\Gamma_i)\leq\frac{2}{3}$ ارائه داد، که تا کنون این کران بدون تغییر باقی مانده بود. در ادامه مقدار دقیق نرخ اطلاعات بهینه این دو ساختار محاسبه شده است.

قضیه ۳-۱. مقدار دقیق نرخ اطلاعات بهینه Γ_{55} برابر $\frac{2}{3}$ است.

اثبات: برای ساختار دسترسی Γ_{55} طرح خاصی با نرخ اطلاعات برابر $\frac{2}{3}$ به صورت زیر داریم که در آن منظور از S_A سهم‌های سهام‌دار 'A' است و راز یک زوج به‌صورت $K=(k_1,k_2)$ درنظرگرفته شده، به‌طوری که برای $i=1,\dots,5$ مقدار r_i و k_1 و k_2 به‌طور تصادفی از میدان گالوایی $GF(q)$ انتخاب شده است.



شکل (۱): Γ_{55}

سهم هریک از ۶ سهام‌دار را به‌صورت زیر درنظر بگیرید:

$$S_A=\{r_1+r_2+r_3+4k_1, r_3+2k_2, r_4+r_5+k_1-3k_2\}$$

$$S_B=\{r_1+3k_1, r_3, r_2\}$$

$$S_C=\{r_1+2k_1, r_3+2k_2, r_5+k_1-2k_2\}$$

$$S_D=\{r_1+r_5+4k_1-2k_2, r_3, r_4+r_2\}$$

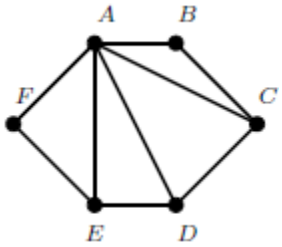
$$S_E=\{r_1+2r_3+r_4+r_5+3k_1+2k_2, r_3+r_4+2k_2, r_2\}$$

$$S_F=\{r_1+r_2+r_3+3k_1, r_3+r_4, r_5+K_1-2k_2\}$$

همان‌طور که ملاحظه می‌کنید سهم هر سهام‌دار برای توزیع دو راز، k_1 و k_2 حداکثر ۳ سهم است. لذا طبق تعریف نرخ اطلاعات، داریم $\rho(\Gamma_{55})\leq\frac{2}{3}$. طبق قضیه ۲-۴ حکم $\rho(\Gamma_{55})=\frac{2}{3}$ به‌دست می‌آید.

قضیه ۳-۲. مقدار دقیق نرخ اطلاعات بهینه Γ_{70} برابر $\frac{2}{3}$ است.

اثبات: برای ساختار دسترسی Γ_{70} طرح خاصی با نرخ اطلاعات $\frac{2}{3}$ ارائه کردیم که در زیر می‌بینید.



شکل (۲): Γ_{70}

$$S_A=\{r_1+r_2+r_3+4k_1, r_3+2k_2+k_1, 2r_4+r_5+k_1-3k_2\}$$

$$S_B=\{r_1+3k_1+2k_2, r_3, r_2\}$$

$$S_C=\left\{r_1+\frac{5}{2}k_1+3k_2, r_3-2k_2-k_1, r_5+k_1-2k_2+2r_4\right\}$$

$$S_D=\{r_1+r_2+3k_1-2K_2, r_3, 2r_4+r_5-6k_2+k_1\}$$

$$S_E=\{r_1+r_2+2r_3+r_4+r_5+4k_1, r_5+2r_4+k_1-2k_2, r_4-r_3-k_1\}$$

$$S_F=\{r_1+r_2+r_4+3k_1, r_3+r_4-2k_2, r_5+k_1-2k_2\}$$

از آنجایی که سهم همه سهام‌داران کمتر یا مساوی ۳ است و با توجه به اینکه تنها ۲ راز بین این ۶ سهام‌دار توزیع شده است، لذا نرخ اطلاعات بهینه برای این ساختار دسترسی حداقل برابر $\frac{2}{3}$ است. بنابراین طبق قضیه ۲-۵ کران بالای نرخ اطلاعات برای این ساختار دسترسی برابر $\frac{2}{3}$ است. بنابراین مقدار نرخ اطلاعات بهینه‌ی این ساختار دسترسی دقیقا برابر $\frac{2}{3}$ خواهد شد. ■

در بخش بعدی نرخ اطلاعات بهینه یک دسته‌ی دیگر از گراف‌ها به طور دقیق محاسبه شده است.

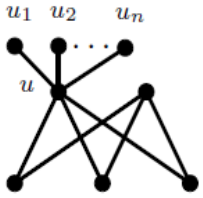
۴- نرخ اطلاعات بهینه گراف چندبخشی رشد یافته

در این مقاله، عبارت "*راس رشد یافته*" به معنای راسی است که به تعداد متناهی راس جدید متصل شده است. هم‌چنین $|V(G)|$ نشان‌دهنده‌ی رئوس گراف G است. اکنون دسته‌ی جدیدی از گراف‌ها را معرفی می‌کنیم.

تعریف ۴-۱. فرض کنید $K_{p_1,\dots,p_k}$ یک گراف k-بخشی کامل باشد. اگر $u\in V(K_{p_1,\dots,p_k})$ ، منظور از گراف k-بخشی رشد یافته

از راس u گراف $K_{p_1,\dots,p_k}$ است که از راس u به n راس دیگر رشد یافته است و آن را با $K^u{}_{p_1,\dots,p_k}$ نشان می‌دهیم.

مثال ۴-۲. در شکل (۳) گراف $K^u{}_{2,3}$ که از راس u رشد یافته، ترسیم شده است.



شکل (۳): $K^u{}_{2,3}$

با توجه به تعریف نرخ اطلاعات بهینه یک ساختار دسترسی، برای ارائه کران پایین روی این پارامتر کافیست که یک طرح تسهیم راز با نرخ اطلاعاتی برابر آن کران پایین ارائه دهیم. یکی از ابزارهای معروف برای ساخت یک طرح تسهیم راز گرافی، روش l-تجزیه استینسون است.

تعریف ۴-۳. [۳] فرض کنید Γ ساختار دسترسی با پایه Γ_0 باشد. یک تجزیه ایده‌آل روی پایه Γ_0 بر روی مجموعه رازهای $\mathcal{K}$ شامل خانواده‌هایی از زیرساختارهای دسترسی به‌صورت $\{\Gamma_1, \Gamma_2, \cdots, \Gamma_n\}$ است به‌طوری‌که خواص زیر را دارا باشند:

- $\Gamma_k \subseteq \Gamma_0$ برای $1 \le k \le n$
- $\bigcup_{k=1}^{n} \Gamma_k = \Gamma_0$
- به‌ازای $1 \le k \le n$ برای هر ساختار دسترسی Γ_k با مجموعه راز $\mathcal{K}$ روی زیرمجموعه سهام‌داران $\mathcal{P}_k = \bigcup_{B \in \Gamma_k} B$، یک طرح ایده‌آل وجود داشته باشد.

قضیه ۴-۵. [۳] (**ساختار l-تجزیه**) فرض کنید Γ ساختار دسترسی با پایه‌ی Γ_0، مقدار $\ell \ge 1$ یک عددصحیح، $\mathcal{K}$ مجموعه همه رازهای ممکن و برای هر $1 \le h \le \ell$ مجموعه $\mathcal{D}_h = \{\Gamma_{h,1}, \dots, \Gamma_{h,n_h}\}$ یک تجزیه ایده‌آل روی Γ_0 با مجموعه راز $\mathcal{K}$ باشد. اگر w تعداد کل سهام‌داران و $\mathcal{P}_{h,j}$ نشان‌دهنده مجموعه سهام‌داران $\Gamma_{h,j}$ باشد، برای هر سهام‌دار p_i تعریف کنید

$$R_i = \sum_{h=1}^{l} |\{j : p_i \in \mathcal{P}_{h,j}\}|$$

آن‌گاه، یک طرح تسهیم راز کامل روی Γ با نرخ اطلاعات $\rho(\Gamma) = \frac{l}{R}$ وجود دارد که در آن:

$$R = max\{R_i : 1 \le i \le w\}$$

تعریف ۴-۶. گراف ستاره‌ای n راسی، یک گراف کامل دو بخشی است که یک بخش آن تنها یک راس u و باقی رئوس در بخش دیگر هستند. در حقیقت گراف ستاره‌ای با n راس، گراف $K_{1,n-1}$ است و ما آن را با ST^u نمایش می‌دهیم. اکنون با استفاده از قضیه l-تجزیه استینسون، نرخ اطلاعات بهینه $K^u{}_{p_1,\dots,p_k}$ را محاسبه می‌کنیم.

قضیه۴-۷. برای هر $|V(K_{p_1,\dots,p_k})| \ge 3$ داریم

$$\rho^*(K^u_{p_1,\dots,p_k}) = \frac{2}{3}.$$

اثبات: ابتدا یک تجزیه ایده‌آل برای این ساختار دسترسی ارائه خواهیم کرد. برای همه $K^u_{p_1,\dots,p_k}$ها (با $|V(K_{p_1,\dots,p_k})| \ge 3$) می‌توان دو تجزیه ایده‌آل به روش زیر ارائه کرد. در حقیقت $\mathcal{D}_i$، برای $i = 1$ و 2 تجزیه‌های ایده‌آلی روی $K^u_{p_1,\dots,p_k}$است. لازم به ذکر است که نمادهای استفاده شده در زیر از قضیه ۴-۵ گرفته شده است.

$$\Gamma_{1,1} = \{K_{p_1,\dots,p_k}\}$$

$$\Gamma_{1,2} = \{ST^u : |V(ST^u)| = n+1\}$$

که در آن، منظور از ST^u گراف ستاره با مرکز u و n راس جدید در بخش دیگری است.

$$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$$

همچنین تجزیه ایده‌آل زیر را درنظر بگیرید:

$$\Gamma_{2,1} = \{K_{p_1,\dots,p_j-1,\dots,p_k}\}$$

منظور از $K_{p_1,\dots,p_j-1,\dots,p_k}$ گرافی است که از حذف راس u از گراف k-بخشی کامل به‌دست می‌آید.

$$\Gamma_{2,2} = \{STC^u : |V(STC^u)| = (|V(G)| - p_j) + n\}$$

که در آن، منظور از STC^u گراف ستاره با مرکز u و تمام رئوس مجاور u از $K^u_{p_1,\dots,p_k}$ در بخش دیگری است.

$$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$$

اکنون طبق قضیه‌ی ۴-۵ برای محاسبه $\rho^*(K^u_{p_1,\dots,p_k})$، باید R را محاسبه کنیم. به عبارت دیگر مقدار R بیانگر بیشترین حضور رئوس در زیرتجزیه‌های ایده‌آل است. برای محاسبه R، ابتدا رئوس

$K^u_{p_1,\dots,p_k}$ را به سه دسته تقسیم می‌کنیم.

$$V_1 = \{v \in K^u_{p_1,\dots,p_k} \ : \ v \in K^u_{p_1,\dots,p_k} \setminus K_{p_1,\dots,p_k}\}$$

در واقع V_1 مجموعه رئوس جدید اضافه شده به گراف چندبخشی کامل است

$$V_2 = V(STC^u)$$

یعنی V_2 مجموعه رئوس ستاره در تجزیه ایده‌آل دوم است

$$V_3 = \{v \in K^u_{p_1,\dots,p_k} \ : \ v \in K_{p_1,\dots,p_k} \setminus V_2\}$$

به راحتی می‌توان دید که $V(K^u_{p_1,\dots,p_k}) = \bigcup_{i=1}^{3} V_i$.

حال تعداد حضور رئوس هریک از این سه دسته را بررسی می‌کنیم.

- رئوس واقع در V_1 در دو زیرتجزیه $\Gamma_{1,2}$ و $\Gamma_{2,1}$ حضور دارند و بنابراین، به هر کدام از این رئوس دو سهم تعلق می‌گیرد..
- رئوس واقع در V_2 در سه زیرتجزیه $\Gamma_{1,1}$ و $\Gamma_{1,2}$ و $\Gamma_{2,1}$ حضور دارند و سهم هرکدام از آنها ۳ سهم است.
- رئوس واقع در V_3 در دو زیرتجزیه $\Gamma_{1,1}$ و $\Gamma_{2,1}$ و $\Gamma_{2,2}$ حضور دارند.

درنتیجه بیشترین سهم هر سهام‌دار ۳ سهم است و بنابراین، $R=3$. طبق قضیه ۴-۵ طرحی برای $K^u_{p_1,\dots,p_k}$ با نرخ اطلاعات برابر $\frac{2}{3}$ وجود دارد. همچنین چون $K^u_{p_1,\dots,p_k}$ گراف چندبخشی کامل نیست، پس $\rho^*(K^u_{p_1,\dots,p_k}) \leq \frac{2}{3}$. در نتیجه حکم قضیه اثبات شد.

۵-کران پایین نرخ اطلاعات

به ساده‌گی می‌توان نشان داد که اگر گراف‌های چندبخشی کامل را از دو راس رشد دهیم، کران پایین جدیدی برای نرخ اطلاعات آن‌ها برابر $\frac{1}{2}$ است. اما مقدار دقیق نرخ اطلاعات آن‌ها تاکنون محاسبه نشده که می‌تواند برای ادامه تحقیقات قابل توجه باشد. همچنین به‌راحتی می‌توان نشان داد که دورهای رشد یافته از یک راس، کران پایین جدیدی برابر $\frac{2}{5}$ دارند که مقدار دقیق نرخ اطلاعات این دسته نیز پیشنهاد نویسندگان برای ادامه این تحقیق است.

۶- نتیجه‌گیری

محاسبه نرخ اطلاعات بهینه ساختارهای دسترسی یکی از چالش برانگیزترین مباحث در موضوع طرح‌های تسهیم راز است. از آنجایی که هر ساختار دسترسی در حالت کلی یک ابرگراف است، بنابراین، بررسی ساختارهای دسترسی گرافی ابزاری مناسب برای مطالعه این پارامتر است. در این مقاله به بررسی مقدار نرخ اطلاعات برخی گراف‌هایی پرداختیم که تا کنون محاسبه نشده بود. همچنین به معرفی دسته جدیدی از گراف‌ها پرداخته شده و مقدار نرخ اطلاعات آن‌ها به‌طور دقیق بیان شد.

۷- مراجع

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

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

[3] D. R. Stinson and M. Paterson, "Cryptography theory and practice," 4th edition. Chapman and Hall/CRC, 2018.

[4] M. Van Dijk, "On the information rate of perfect secret sharing schemes," Designs Codes and Cryptography, vol. 6, pp. 143-169, 1995.

[5] M. Gharahi, and M. Hadian, "The complexity of the graph access structures on six participants," Designs Codes and Cryptography, vol. 67, pp. 169-173, 2013.

[6] M. Gharahi and M. Hadian, "Perfect secret sharing schemes for graph access structures on six participants," Journal of Mathematical Cryptology, vol. 7, pp. 143-146, 2013.

[7] C. Padro, and L. Vazquez, and A. Yang, "Finding lower bounds on the complexity of secret sharing schemes by linear programming," Discrete Applied Mathematics, vol. 161, pp. 1072-1084, 2013.

[8] A. Cheraghi and M. Gholami, "Some New Bounds on the Information Ratio of the Cartesian Product of Some Classes of Graphs," Journal of Electronical & Cyber Defence, vol. 6, pp. 135-142, 2019.

[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.