مقدار دقیق پیچیدگی بهینه‌ی گراف‌های کامل رشد یافته و چندبخشی کامل رشد یافته

میترا شرافتی*، عباس چراغی چالشتری

دانشکده ریاضی و کامپیوتر خوانسار

acheraghi78@yahoo.com

چکیده

در مقالات متعددی مقدار دقیق پیچیدگی بهینه برای ساختارهای دسترسی گراف‌های خاص مورد مطالعه قرار گرفته است. اما هنوز رده‌های بسیاری از گراف‌ها وجود دارند که مقدار دقیق پیچیدگی بهینه‌ی آن‌ها محاسبه نشده است. در این مقاله پیچیدگی بهینه‌ی ساختار دسترسی گراف‌های کامل رشد یافته و چندبخشی کامل رشد یافته بررسی شده است. در این مقاله نشان خواهیم داد که مقدار دقیق پیچیدگی بهینه، برای گراف‌های کامل رشد یافته و چندبخشی کامل رشد یافته‌ی از یک راس، برابر $\frac{3}{2}$ می‌باشد.

کلمات کلیدی: طرح تسهیم راز تام، ساختار دسترسی گرافی، تجزیه‌ی ایده‌آل، پیچیدگی.

۱. مقدمه

طرح تسهیم راز روشی برای تقسیم راز بین سهام‌داران است که تنها زیرمجموعه‌های مجاز قادر به بازگشایی راز باشند. اگر زیرمجموعه‌های غیرمجاز با استفاده از سهم‌های خود نتوانند کوچکترین اطلاعاتی از راز را بازگشایی کنند طرح را یک طرح تسهیم راز تام می‌نامیم.

به مجموعه‌ی همه‌ی افراد مجاز که قادر به بازگشایی راز هستند ساختار دسترسی Γ گفته می‌شود و کوچکترین ساختار دسترسی ممکن را پایه‌ی Γ یا Γ_0 نامیم.

در این مقاله ساختارهای دسترسی گرافی مورد مطالعه قرار گرفته‌اند که شامل کوچکترین زیر مجموعه‌های مجاز دو عضوی است. به عبارت دیگر هر دو نفر از n نفر قادر به بازگشایی راز هستند ولی یک نفر به تنهایی هیچ اطلاعاتی از راز را بدست نمی‌آورد.[1] همچنین لازم به ذکر است که ساختارهای دسترسی مورد مطالعه یکنوا هستند یعنی ابرمجموعه‌ی هر زیرمجموعه‌ی مجاز، خود یک مجموعه‌ی مجاز است.

* **Corresponding author:** دانشجوی کارشناسی ارشد با زمینه تخصصی رمزنگاری
Email: sherafatimitra@gmail.com

پیچیدگی یک طرح تسهیم راز نسبت بین بیشترین اندازه‌ی سهم داده شده به هر شخص به اندازه راز است و چون ما علاقه‌مندیم سهم کمتری به هر فرد تعلق گیرد پس پیچیدگی بهینه‌ی ساختار دسترسی Γ را با inf این نسبت نشان می‌دهیم[2]. در واقع تعریف می‌کنیم:

$$\sigma^*(\Gamma) = \inf_{\sum} \frac{\max_{p\epsilon P} H(p)}{H(K)}.$$

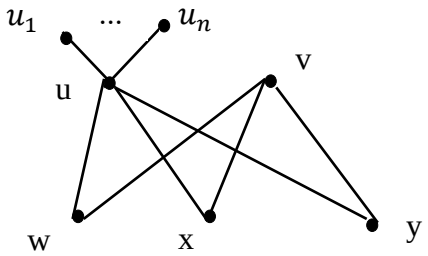
که $\sum$ بیانگر همه‌ی طرح‌های تسهیم راز پایه‌گذاری شده روی ساختار دسترسی Γ است.

$\sigma^*(\Gamma) = 1$، وضعیت بهینه است، چرا که به ازای هر راز یک سهم به هر فرد تعلق می‌گیرد نه بیشتر، بنابراین چنین طرحی را یک طرح تسهیم راز ایده‌آل می‌نامیم.

در واقع مقدار پیچیدگی بهینه بیان‌گر برتری یک طرح به طرح دیگر روی ساختار دسترسی خاص Γ است به همین جهت محاسبه و یا ارائه‌ی کرانی منطقی برای این مقدار همواره مورد توجه بوده است. در همین راستا نرخ اطلاعات بهینه‌ی همه‌ی ساختارهای دسترسی همبند با چهار سهام‌دار در [3,4,5] محاسبه شده است. نرخ اطلاعات طرح تسهیم راز تام با پنج سهام‌دار توسط جکسون و مارتین در [6] بررسی شده است. در ۱۷۵ مورد از ۱۸۰ ساختار دسترسی همبند پنج سهام‌داری، مقدار دقیق نرخ اطلاعات بهینه مشخص شده است. علاوه بر این نرخ اطلاعات بهینه‌ی ساختارهای دسترسی همبند شش [7-11] و هفت [12-14] و نه رأسی[15] نیز تعیین گردیده اند. هم‌چنین ما در [2] با استفاده از خواص آنتروپی کران پایینی برای پیچیدگی پنج ساختار دسترسی گرافی با شش سهام‌دار ارائه دادیم. حال به بیان تعاریف و قضایای استفاده شده در این مقاله می‌پردازیم.

در این مقاله منظور از راس رشد یافته راسی است که به تعداد متناهی رأس جدید متصل گردد. هم‌چنین $|V(G)|$ نشانگر تعداد رئوس گراف G است.

مثال۱: در زیر $K^*_{2,3}$ را می‌بینید که از رأس u رشد یافته است.



تعریف۲: تمام گراف‌های چندبخشی کامل که تنها از یک راس رشد یافته‌اند را $K^*_{p_1,\dots,p_k}$ می‌نامیم.

هر گراف کامل در واقع گراف چندبخشی کاملی است که هر رأس آن به تنهایی یک بخش را تشکیل می‌دهد بنابراین تمامی احکام زیر برای K^*_n نیز برقرار است. لذا تنها به بررسی $K^*_{p_1,\dots,p_k}$ می‌پردازیم. در این مقاله مقدار پیچیدگی $k^*_{p_1,\dots,p_k}$ را برای $|V(K_{p_1,\dots,p_k})| \geq 3$ به روش تجزیه ایده‌آل [16] محاسبه خواهیم کرد.

قضیه۳:[16] فرض کنید $G=(V,E)$ یک گراف چندبخشی کامل باشد آن‌گاه یک طرح تسهیم راز ایده‌آل روی ساختار دسترسی با پایه‌ی E و سهام‌داران V وجود دارد.

طبق قضیه‌ی بالا تمام گراف‌های چندبخشی کامل یک طرح تسهیم راز ایده‌آل روی تمام رئوس و یال‌های خود بیان می‌کند از طرفی با استفاده از قضیه‌ی زیر کران پایینی برای پیچیدگی بهینه‌ی تمام گراف‌هایی که چند بخشی کامل نیستند بیان می‌کنیم.

قضیه۴:[16] فرض کنید G گراف همبندی باشد که چندبخشی کامل نیست و $\Gamma(G)$ ساختار دسترسی با پایه‌ی E است به طوری‌که E مجموعه یال‌های G باشد آن‌گاه:

$$\sigma^*(\Gamma(G)) \geq \frac{3}{2}$$

در واقع این قضیه بیان می‌کند که هرگز پیچیدگی بهینه‌ی یک ساختار دسترسی با پایه‌ی گرافی از $\frac{3}{2}$ کمتر نخواهد بود. حال به بیان یک مفهوم مهم نیازمندیم.

- **تعریف۵**:[16] فرض کنید Γ ساختار دسترسی با پایه‌ی Γ_0 باشد. یک تجزیه ایده‌آل Γ_0 برای مجموعه کلید $\mathcal{K}$ شامل $\{\Gamma_1,\dots,\Gamma_n\}$ است به‌طوری‌که خواص زیر را دارا باشند:
- $\Gamma_k \subseteq \Gamma_0$ برای $1 \leq k \leq n$
- $\bigcup_{k=1}^{n} \Gamma_k = \Gamma$
- برای $1 \leq k \leq n$ روی مجموعه کلید $\mathcal{K}$ طرح ایده‌آلی وجود دارد به طوری که روی زیرمجموعه‌ی سهام‌داران برای ساختار دسترسی با پایه‌ی Γ_k داشته باشیم $\mathcal{P}_k = \bigcup_{B \in \Gamma_k} B$.

با داشتن یک تجزیه‌ی ایده‌آل و بهره‌مندی از قضیه‌ی زیر مقدار دقیق پیچیدگی $K^*_{p_1,\dots,p_k}$، به ازای $|V(k_{p_1,\dots,p_k})| \geq 3$ را محاسبه می‌کنیم.

قضیه۶:[16] فرض کنید Γ ساختار دسترسی با پایه‌ی Γ_0 و $\ell \geq 1$ یک عددصحیح و $\mathcal{K}$ مجموعه کلید باشد و برای $1 \leq h \leq \ell$، $\mathcal{D}_h = \{\Gamma_{h,1}, \dots, \Gamma_{h,n_h}\}$ یک تجزیه ایده‌آل روی Γ_0 با مجموعه کلید $\mathcal{K}$ و اگر $\mathcal{P}_{h,j}$ نشان‌دهنده‌ی مجموعه‌ی شرکت‌کننده‌های $\Gamma_{h,j}$ باشد برای هر شرکت‌کننده‌ی p_i تعریف می‌کنیم

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

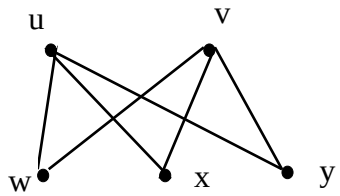
آنگاه یک طرح تسهیم راز تام روی Γ با نرخ اطلاعات $\sigma(\Gamma) = \frac{R}{\ell}$ وجود دارد به طوری‌که

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

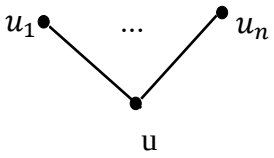
حال به دنبال ارائه‌ی تجزیه‌ی ایده‌آل برای $K^*_{p_1,\dots,p_k}$ ها هستیم.

طبق تعریف $K^*_{p_1,\dots,p_k}$، به وضوح هر $K^*_{p_1,\dots,p_k}$ را می‌توان به یک $K_{p_1,\dots,p_k}$ و یک ستاره (Star) تجزیه کرد. برای تفهیم بیشتر به مثال زیر توجه کنید.

مثال۷:یک تجزیه ایده‌آل برای گراف $K^*_{2,3}$ که در مثال ۱ بیان شد، ارائه می‌دهیم.



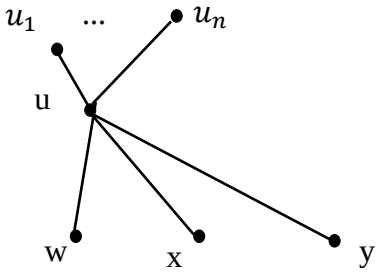
$\Gamma_{1,1}$



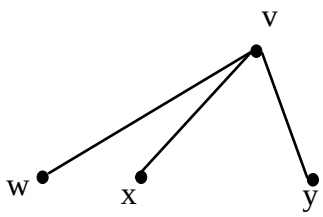
$\Gamma_{1,2}$

حال ادعا می‌کنیم هر $K^*_{p_1,\dots,p_k}$ را می‌توان به $K_{p_1,\dots,p_j-1,\dots,p_k}$ و یک ستاره (و یا به $K_{p_1,\dots,p_{j-1},p_{j+1},\dots,p_k}$ و یک ستاره) تجزیه کرد. برای این منظور از گراف $K^*_{p_1,\dots,p_k}$ راس u (که در واقع رأس رشد یافته‌ی ماست) و تمام یال‌های متصل به این رأس را برمی‌داریم. مشاهده می‌شود علاوه براین‌که یال‌های رشدیافته‌ی $K^*_{p_1,\dots,p_k}$ جداشده، یال‌هایی که یک سرشان در گراف چندبخشی کامل است نیز حذف خواهد شد و گراف $K_{p_1,\dots,p_j-1,\dots,p_k}$ به وجود می‌آید. (توجه کنید که اگر رأس u به تنهایی یک بخش از k تا بخش گراف $K^*_{p_1,\dots,p_k}$ را تشکیل دهد، آن‌گاه با حذف این رأس گراف $K_{p_1,\dots,p_{j-1},p_{j+1},\dots,p_k}$ و یک ستاره به وجود خواهد آمد.)

مثال۸: تجزیه‌ی ایده‌آل دیگری از $K^*_{2,3}$ ارائه می‌دهیم.



$\Gamma_{2,1}$



$\Gamma_{2,2}$

همان‌طور که در بالا بیان شد برای همه‌ی $K^*_{p_1,\dots,p_k}$ ها (به ازای $|V(K_{p_1,\dots,p_k})| \geq 3$) می‌توان دو تجزیه‌ی ایده‌آل به شیوه‌ی زیر ارائه داد.

$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$
$\Gamma_{1,1} = \{K_{p_1,\dots,p_k}\}$
$\Gamma_{1,2} = \{Star: |V(Star)| = n+1\}$
$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$
$\Gamma_{2,1} = \{K_{p_1,\dots,p_j-1,\dots,p_k}\}$
$\Gamma_{2,2} = \{Star: |V(Star)| = (|V(G)| - p_j) + n\}$

لازم به ذکر است که نماد گذاری بالا برگرفته از قضیه‌ی 6 است. در واقع $\mathcal{D}_i$ ها تجزیه‌ی ایده‌آل روی Γ هستند.

حال برای محاسبه‌ی $\sigma(\Gamma)$ کافی است به محاسبه‌ی R بپردازیم. از طرفی مقدار R معادل است با بیشترین حضور هر راس در زیرتجزیه‌های ایده‌آل. برای محاسبه‌ی R ابتدا رئوس $K^*_{p_1,\dots,p_k}$ را به سه دسته تقسیم خواهیم کرد.

$V_1 = \{v \in K^*_{p_1,\dots,p_k} : v \in K^*_{p_1,\dots,p_k} \setminus K_{p_1,\dots,p_k}\}$
$V_2 = \{A\}$

$V_3 = \{v \in K^*_{p_1,\ldots,p_k} : v \in K_{p_1,\ldots,p_k} \backslash A\}$

به راحتی می‌توان دید $V(K^*_{p_1,\ldots,p_k}) = \bigcup_{i=1}^{3} V_i$.

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

- رئوس واقع در V_1 در دو زیرتجزیه‌ی $\Gamma_{1,2}$ و $\Gamma_{2,1}$ حضور دارند.
- رئوس واقع در V_2 در دو زیرتجزیه‌ی $\Gamma_{1,1}$ و $\Gamma_{1,2}$ و $\Gamma_{2,1}$ حضور دارند.
- رئوس واقع در V_3 در دو زیرتجزیه‌ی $\Gamma_{1,1}$ و $\Gamma_{2,1}$ و $\Gamma_{2,2}$ حضور دارند.

قضیه۹: برای هر $|V(K_{p_1,\ldots,p_k})| \geq 3$ داریم، $\sigma^*(K^*_{p_1,\ldots,p_k}) = \frac{3}{2}$.

اثبات: طبق قضیه‌ی ۴ نشان دادیم پیچیدگی بهینه برای تمام گراف‌هایی که چندبخشی کامل نیستند بزرگتر یا مساوی $\frac{3}{2}$ است و چون $K^*_{p_1,\ldots,p_k}$ ها چندبخشی کامل نیستند پس پیچیدگی بهینه برای این دسته از گراف‌ها نیز بزرگتر یا مساوی $\frac{3}{2}$ خواهد شد. همچنین با استفاده از قضیه‌ی ۶ طرح ایده‌آلی با پیچیدگی $\frac{3}{2}$ برای $K^*_{p_1,\ldots,p_k}$ ها ارائه کردیم بنابراین پیچیدگی بهینه برای $K^*_{p_1,\ldots,p_k}$ ها دقیقا برابر $\frac{3}{2}$ خواهد شد.

2. نتیجه‌گیری

محاسبه‌ی مقدار دقیق پیچیدگی بهینه‌ی گراف‌ها در حالت کلی بسیار مسأله‌ی دشواری است. لذا محاسبه‌ی مقدار دقیق یک رده‌ی خاص از اهمیت ویژه‌ای برخوردار می‌باشد. در این مقاله طبق قضیه‌ی ۹ که بیان شد، مقدار دقیق پیچیدگی بهینه‌ی گراف‌های کامل و چندبخشی کاملی که تنها از یک راس رشد یافته اند برابر $\frac{3}{2}$ می‌شود. در ادامه‌ی این تحقیق می‌توان مقدار دقیق پیچیدگی بهینه‌ی طیف گسترده‌تری از گراف‌ها را مورد بررسی قرار داد.

3. مراجع

1. Shamir, A. (1979), "How to share a secret", Communications of the ACM, 22(11), 612-613.
۲. شرافتی، میترا. چراغی چالشتری، عباس. (۱۳۹۵)، "بهبود کران پایین پیچیدگی برای ساختار دسترسی گرافی با شش سهام‌دار"،اولین کنفرانس بین المللی ترکیبیات، محاسبات، رمزنگاری، دانشگاه علم و صنعت، واحد نور.
3. Stinson, D.R. (1992), "An explication of secret sharing schemes", Designs Codes and Cryptography, 2, 357-390.
4. Capocelli, R.M. and De Santis, A. and Gargano, L. and Vaccaro, U. (1993), "On the size of shares of secret sharing schemes", Journal of Cryptograghy, 6(3), pp 157-169.

5. Simmons, G.J. and Jackson, W.A. and Martin, K.M. (1991) "The geometry of shared secret schemes", Bulletin of the Institute of Combinatorics and its Applications, Appl. 1, 71-88.
6. Jackson, W. and Martin, K.M. (1996), "Perfect secret sharing schemes on five participants", Designs Codes and Cryptograghy, 9(3), 267-286.
7. Van Dijk, M.. (1995),"On the information rate of perfect secret sharing schemes", Designs Codes and Cryptograghy, 6(2), 143-169.
8. Sun, H.M and Chen, B.L. (2002)," Weighted decomposition construction for perfect secret sharing schemes", Computers and Mathematics with Applications, 43(6-7), 877-887.
9. Gharahi, M. and Hadian, M. (2013), "The complexity of the graph access structures on six participants", Designs Codes and Cryptography, 67(2), 169-173.
10. Padro, C. and Vazquez. , L. and Yang, A. (2013), "Finding lower bounds on the complexity of secret sharing schemes by linear programming", Discrete Applied Mathematics, 161(7-8), 1072-1084.
11. Gharahi, M. and Hadian, M. (2013), "Perfect secret sharing schemes for graph access structures on six participants", Journal of Mathematical Cryptology, 7(2), 143-146.
12. Song, Y. and Li, ZH. and Wang, W.C. (2012), "The information rate of secret sharing schemes based on seven participants by connect gragh", Lecture Notes in Electrical Engineering, 127, 637-645.
13. Wang, W.C and Li, Z.H and Song, Y. (2011), "The optional information rate of perfect secret sharing schemes", In: Proceeding of the 2011 International Conference on Business Management and Electronic Information, 207-212.
14. Li, Z.H and Song, Y. and Li, M. (2014) "The optimal information rates of the graph access structures on seven participants", Advanced Materials Research, 859, 596-601.
15. Song, Y. and Li, ZH. and Li, Y. and Xin, R. (2015), "The optimal information rate for graph access structures of nine participants", Frontiers of Computer Science, 9(5), 778-787.
16. Stinson, D.R. (1995), "Cryptography: Theory and Practice", 3rd ed, 481-515.