ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

ارائه کران بر روی نرخ اطلاعات طرح‌های تقسیم راز دوبخشی

عباس چراغی

اصفهان، دانشگاه اصفهان، دانشکده ریاضی و کامپیوتر خوانسار
cheraghi@sci.ui.ac.ir

چکیده

در یک طرح تقسیم راز دوبخشی، مجموعه سهام‌داران را به دو قسمت چنان تقسیم می‌کنند که همه سهام‌داران در یک بخش نقش یکسانی بازی کنند. پادرو و سائز ساختارهای دسترسی ایده‌آل دو بخشی را به طور کامل دسته‌بندی کرده‌اند. این در حالی است که مشخص کردن نرخ اطلاعات ساختارهای دسترسی در حالت کلی، یکی از بزرگترین مسائل حل نشده در بحث تقسیم راز است. در این مقاله با استفاده از ارتباط طرح‌های تقسیم راز و پلی‌ماتریدها، برای نرخ اطلاعات هر ساختار دسترسی دوبخشی یک کران بالا ارائه می‌دهیم. در این راستا از یک مساله برنامه‌ریزی خطی استفاده می‌کنیم.

واژه‌های کلیدی

نرخ اطلاعات، طرح تقسیم راز، ساختار دسترسی.

۱- مقدمه

یک *طرح تقسیم راز*[1] روشی است برای توزیع یک راز در بین یک مجموعه از سهام‌داران به‌طوری که هر سهام‌دار یک سهم از راز را دریافت کند و زیر مجموعه‌های *مجاز* از سهام‌داران بتوانند راز را بازسازی نمایند درحالی که زیرمجموعه‌های *غیرمجاز* نتوانند هیچ اطلاعاتی راجع به راز بدست آورند. خانواده Γ از زیرمجموعه‌های مجاز را *ساختار دسترسی* آن طرح می‌نامند. این دسته از طرح‌ها امنیت بدون شرط دارند لذا این طرح‌ها به قدرت و تواناییهای دشمن وابسته نمی‌باشند.

بسیاری از پروتکل‌های رمزنگاری بر اساس ساختار طرح‌های تقسیم راز، پایه گذاری شده‌اند و این طرح‌ها کاربردهای بسیاری به صورت عملی دارند. بازده طرح‌های تقسیم راز به وسیله ارتباط اندازه راز و اندازه سهم‌ها، محک زده می‌شوند. حاصل تقسیم طول راز به طول بزرگترین سهمِ سهام‌داران را *نرخ اطلاعات*[2] گویند. ازآنجائی که ما طرح‌ها را به صورت امنیت بدون شرط[3] درنظر می‌گیریم لذا در بهترین حالت اندازه راز با اندازه هریک از سهم‌ها برابر خواهد بود و در این حالت نرخ اطلاعات برابر ۱ می‌باشد. در این صورت طرح و ساختار آن را *ایده‌آل*[4] گویند. مشخص نمودن ساختارهای دسترسی ایده‌آل هنوز یک مساله حل نشده می‌باشد و به دلیل تاثیر زیاد آنها در بحث طرح‌های تقسیم راز، دسته بندی ساختارهای دسترسی ایده‌آل به عنوان یکی از با اهمیت‌ترین مسائل رمزنگاری شناخته شده است. همچنین تعیین نرخ اطلاعات بهینه یک ساختار دسترسی در حالت کلی نیز از مسائل بزرگ رمزنگاری می‌باشد. طرحی را که نرخ اطلاعاتِ ساختار دسترسی آن بهترین حالت ممکن باشد را یک طرح بهینه[5] می‌نامند. در مطالعه این گونه مسائل، مفاهیمی چون ماتریدها، پلی‌ماتریدها[6] و گراف‌ها به کار گرفته شده است. همچنین شاخه‌های مختلفی از ریاضیات مانند جبر، ترکیبیات و نظریه کدگذاری نیز ابزاری است که تاکنون برای حل این مسائل به کار گرفته شده است.

ساختار دسترسی یکنوا[7] ساختاری است که در آن هر مجموعهٔ مجموعهٔ شاملِ یک مجموعهٔ مجاز، خود مجموعه مجازی از سهام‌داران باشد. لذا ساختار دسترسی Γ را می‌توان با استفاده از خانواده‌ای از مجموعه‌های مجاز مینیمال آن مشخص نمود که به آن پایه Γ گویند و آن را با $min\ \Gamma$ نشان می‌دهند. یک *طرح*

[1] Secret sharing scheme
[2] Information rate
[3] Unconditionally secure
[4] Ideal
[5] Optimal
[6] Polymatroid
[7] Monotone access structure

آستانه‌ای طرحی است که در آن تعداد سهام‌داران یک مجموعه مجاز، از یک حد آستانه‌ای t بزرگتر است. همگی طرح‌های که در این مقاله معرفی شده است طرح‌های ایده‌آل و یکنوا می‌باشند.

شامیر و بلاکلی برای اولین بار در سال ۱۹۷۹ به طور مستقل، طرح تقسیم راز را مطرح نمودند. در [3] ثابت شده است که ساختارهای دسترسی ایده‌آل وابسته ماتریدی[1] هستند. به این معنی که برای هر ساختار دسترسی ایده‌آل, ماتریدی وجود دارد که در آن مدارها، شامل نقطه ثابتی هستند که در تناظر یک به یک با زیرمجموعه‌های پایه آن ساختار دسترسی می‌باشند. اهمیت ایدهٔ آنها در بررسی ایده‌آل بودن ساختارهای دسترسی و همچنین تولید طرح‌های ایده‌آل با استفاده از ماترید پورت‌ها[2] است. نتایجی از ماترید پورت‌ها در [9, 13] بیان شده و در مقاله [10] این نتایج بهبود پیدا کرده است. در [6] نشان داده شده که چگونه می‌توان با استفاده از آنتروپی‌های هر مجموعه از متغیرهای تصادفی، یک پلی‌ماترید ساخت. با استفاده از این روش در [4] ارتباط بین ماتریدها و طرح‌های ایده‌آل تعمیم داده شد. همچنین برای هر طرح تقسیم راز (نه لزوماً ایده‌آل) یک پلی ماترید وابسته به آن ارائه شده است. این رابطه را می‌توان برای پیدا کردن کران‌های بالای نرخ اطلاعات بهینهٔ ساختارهای دسترسی استفاده نمود [4,10]. یکی دیگر از ارتباط‌های مهم بین طرح تقسیم راز و پلی‌ماتریدها که به تازگی پیدا شده است پلی‌ماتریدهای گسسته[3] است [7] که به کمک آن در [5] مفاهیم ترکیبیاتی برای توصیف ساختارهای دسترسی سه‌بخشی ایده‌آل معرفی شده است.

خواص ماتریدها و پلی‌ماتریدهای که در طرح تقسیم راز به کار گرفته شده است در واقع نتیجه‌ای از نامساوی شانون متغیرهای تصادفی می‌باشد [14]. اخیراً با استفاده از نامساویهای غیر-شانون[4] شانون[4] نتایج جدیدی در طرح تقسیم راز بدست آمده است [1].

در *ساختارهای دسترسی چندبخشی*[5] مجموعه سهام‌داران به چند دسته مختلف چنان تقسیم میشوند که سهام‌داران هر بخش نقش یکسانی را در ساختار دسترسی ایفا می‌کنند. اولین طرح تقسیم راز چندبخشی در [2] معرفی شد. در مقاله [12] برای نرخ اطلاعات طرح‌های غیر ایده‌آل با ساختار دسترسی دوبخشی کران‌هایی بیان شده و ساختارهای دسترسی دوبخشی ایده‌آل مشخص شده است. با استفاده از پلی‌ماتریدهای گسسته می‌توان ساختارهای دسترسی سه‌بخشی را مشخص کرد [5]. اما هنوز پیدا کردن ساختارهای دسترسی ایده‌آل با بیش از سه بخش از مسائل حل نشده است.

در این مقاله کران جدیدی برای نرخ اطلاعات ساختارهای دسترسی دوبخشی ارائه شده است. برای این منظور از ارتباط بین پلی‌ماتریدها و طرح‌های تقسیم راز و همچنین یک شیوه برنامه‌ریزی خطی استفاده شده است. این کران‌ها با به کار بردن نامساوی شانون بر روی آنتروپی مجموعهٔ سهمِ سهام‌داران بدست آمده است. در [15] نامساوی شانون در قالب یک مساله برنامه‌ریزی خطی معرفی شده است. در این حالت، خواصی از طرح‌های دوبخشی باعث شده است تا این روش برنامه‌ریزی خطی به صورت ساده‌تری بهبود یابد. این روش بهبود یافته همچنین می‌تواند برای ساختارهای دسترسی چندبخشی با بیش از دو بخش نیز به کار رود. با استفاده از این روش برنامه‌ریزی خطی کران‌های بالایی برای نرخ اطلاعات بهینه ساختارهای دسترسی غیر ایده‌آل بیان شده است که نتایج در [12] را بهبود داده است. همچنین در این مقاله ساختارهای بهینه معرفی شده در [11] برای ساختارهای دسترسی دوبخشی با یک تعداد دلخواه از سهام‌داران در هر بخش، تعمیم داده شده است.

۲- طرح‌های تقسیم راز و پلی‌ماتریدها

طرح‌های تقسیم راز مطرح شده در این مقاله همگی کامل هستند. یعنی زیرمجموعه‌های مجاز می‌توانند راز را بدست آورند درحالی که زیرمجموعه‌های غیرمجاز نمی‌توانند هیچگونه اطلاعاتی از راز را با استفاده از سهم‌هایشان بدست آورند.

فرض کنید که Σ یک طرح تقسیم راز با مجموعهٔ P از n سهام‌دار باشد. واسطه را سهام‌دار $p_0 \notin P$ و $Q = P \cup \{p_0\}$ در نظر بگیرید. در یک طرح، سهمِ p_0 را، راز در نظر می‌گیریم. s_i را سهم سهام‌دار $i \in Q$ فرض کنید. با توجه به همه $(n+1)$-تایی‌های ممکن $(s_{p_0}, s_1, s_2, \ldots, s_n)$ از سهم‌ها، نگاشت $\pi_i : E \to E_i$ را برای یک مجموعه مشخص E چنان تعریف می‌کنیم که برای هر $e \in E$ اعضا $(\pi_i(e))_{i \in Q}$ سهم‌های از یک راز باشند. ما فقط نگاشت‌های پوشا را در نظر می‌گیریم، بنابراین برای هر سهام‌دار $i \in Q$ مجموعه E_i همان مجموعه همهٔ سهم‌های ممکنِ سهام‌دار i می‌باشد. اگر یک توزیع احتمال در E وجود داشته باشد آنگاه هر یک از نگاشتها یک توزیع احتمال در E_i القا می‌کنند. بنابر این می‌توان $H(E_i)$ را به عنوان آنتروپی شانون هر یک از متغییرهای تصادفی در نظر گرفت.

برای هر زیرمجموعه $A = \{i_1, \ldots, i_r\} \subset Q$ آنتروپی مشترک $H(E_{i_1}, \ldots, E_{i_r})$ را به صورت $H(A)$ می‌نویسیم و قرارداد مشابهی را برای آنتروپی شرطی قرار می‌دهیم، به طور مثال داریم $H(E_j \mid A) = H(E_j \mid E_{i_1}, \ldots, E_{i_r})$. Γ را ساختار دسترسی از Σ درنظر بگیرید. از آنجا که نگاشت‌های π_i طرح تقسیم راز کامل Σ را تعریف می‌کنند لذا $h(E_{p_0}) > 0$ و

[1] Matroid related
[2] Matroid ports
[3] Discrete polymatroids
[4] Non-Shannon inequality
[5] Multipartite access structure

داریم: $H(E_{p_0} \mid A) = 0$ اگر $A \in \Gamma$. در حالی که اگر $A \notin \Gamma$ داریم: $H(E_{p_0} \mid A) = H(E_{p_0})$.

بهترین راه برای اندازه‌گیری طول سهام هر طرح، استفاده از آنتروپی سهام آن طرح می‌باشد. پیچیدگی[1] طرح تقسیم راز Σ را به صورت $\sigma(\Sigma) = \max_{i \in p} H(E_i)/H(E_{p_0})$ تعریف می‌کنیم. مقدار $\rho(\Sigma) = 1/\sigma(\Sigma)$ را *نرخ اطلاعات* طرح Σ گویند. هر دو مقدار σ و ρ 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. پیچیدگی بهینه[2] $\sigma(\Gamma)$ برای یک ساختار دسترسی Γ را اینفیمم پیچیدگی‌های $\sigma(\Sigma)$ روی تمامی طرح‌های Σ تعریف شده برای ساختار دسترسی Γ گویند. نرخ اطلاعات بهینه ساختار دسترسی Γ نیز به صورت $\rho(\Gamma) = 1/\sigma(\Gamma)$ تعریف می‌شود. یک *طرح تقسیم راز خطی* طرحی است که در آن E و E_i فضاهای برداری روی یک میدان هستند، نگاشت π_i خطی است و توزیع احتمال روی E یکنواخت باشد. امنیت این طرح‌ها که به آنها طرح‌های هندسی و همچنین monotone span programs نیز گویند، بر پایه خواص جبر خطی استوار است. بر اساس این ارتباط است که موثرترین طرح‌ها را خطی درنظر می‌گیرند. در حقیقت برای هر ساختار دسترسی یک طرح خطی وجود دارد [8]. بنابراین $\lambda(\Gamma)$ را به عنوان اینفیمم پیچیدگی طرح‌های تقسیم راز خطی برای ساختار دسترسی Γ تعریف می‌کنیم. قضیه زیر نتیجه مستقیمی از این تعریف است.

قضیه ۲-۱: برای هر ساختار دسترسی Γ داریم $\sigma(\Gamma) \le \lambda(\Gamma)$.

بنابر این طرح‌های خطی هم از لحاظ کاربردهای عملی مورد توجه هستند و هم از لحاظ روشی برای یافتن یک کران بالا برای پیچیدگی بهینه ساختارهای دسترسی کلی. از آنجا که طرح‌های ما همگی کامل در نظر گرفته شده است، برای هر i داریم $H(E_i) \ge H(E_{p_0})$ و بنابر این $\sigma(\Sigma) \ge 1$. یک طرح تقسیم راز با $\sigma(\Sigma) = 1$ را ایده‌آل گویند. در مطالعه نرخ اطلاعات، ارتباط بین پلی‌ماتریدها و طرح‌های تقسیم راز، از اهمیت بسیاری برخوردار است.

تعریف ۲-۲: فرض کنید که Q یک مجموعه، $P(Q)$ مجموعه توانی آن و $h: P(Q) \to \Re$ یک تابع باشد، که در آن $\Re$ مجموعه اعداد حقیقی است. زوج $S = (Q,h)$ را یک پلی‌ماترید گویند اگر در شرایط زیر صدق کند:

۱. $h(\phi) = 0$،

۲. تابع h صعودی یکنوا باشد، یعنی اگر $X \subset Y \subset Q$، آنگاه $h(X) \le h(Y)$ و

۳. تابع h زیرمدولی باشد، یعنی اگر $X, Y \subset Q$، آنگاه $h(X \bigcup Y) + h(X \bigcap Y) \le h(X) + h(Y)$.

در این مقاله از یک نوع خاص پلی‌ماتریدها به نام پلی‌ماتریدهای تقسیم راز استفاده شده است.

تعریف ۲-۳: زوج $S = (Q,h)$ را یک پلی‌ماترید و p را یک عضو Q در نظر بگیرید. اگر برای هر $X \subset Q$ یکی از دو حالت $h(X \bigcup \{p\}) = h(X)$ یا $h(X \bigcup \{p\}) = h(X) + 1$ را داشته باشیم، آنگاه S را یک *p-پلی‌ماترید تقسیم راز*[3] گویند.

اگر Σ یک طرح تقسیم راز روی مجموعه $Q = P \bigcup \{p_0\}$ باشد و مجموعه $\{E_i\}_{i \in Q}$ متغیرهای تصادفی وابسته به سهام باشد، نگاشت $h: P(Q) \to \Re$ را به صورت زیر تعریف می‌کنیم:

$$h: X \to H(X)/H(E_{p_0})$$

زوج (Q,h) را که به این شکل تعریف می‌شود یک *p_0-پلی‌ماترید تقسیم راز*[4] و یا به اختصار *p_0-ss*-پلی‌ماترید گویند. بنابر این هر طرح تقسیم راز Σ یک *p_0-ss*-پلی‌ماترید به صورت $S = S(\Sigma) = (Q,h)$ تعریف می‌کند. لازم به ذکر است که *p_0-ss*-پلی‌ماتریدهایی وجود دارند که وابسته به هیچ طرح تقسیم رازی نمی‌باشند. توجه کنید که اگر Σ کامل نباشد آنگاه $S(\Sigma)$ یک پلی‌ماترید تقسیم راز نیست.

مفهوم پیچیدگی بهینه طرح‌ها و ساختارهای دسترسی را می‌توان برای پلی‌ماتریدها به صورت زیر تعمیم داد. برای هر پلی‌ماترید $S = (Q,h)$ تعریف می‌کنیم $\kappa(S) = \max\{h(x) \mid x \in Q\}$ و برای هر ساختار دسترسی Γ تعریف می‌کنیم $\kappa(\Gamma) = \inf\{\kappa(S)\}$ که در آن اینفیمم روی تمام *p_0-ss*-پلی‌ماتریدهای S با $\Gamma = \Gamma_{p_0}(S)$ گرفته شده است. این پارامتر برای مطالعه نرخ اطلاعات بهینه استفاده شده است.

قضیه ۲-۴ [10]: برای هر ساختار دسترسی Γ داریم $\sigma(\Gamma) \ge \kappa(\Gamma)$.

بنابر این با توجه به نامساوی‌های $\kappa(\Gamma) \le \sigma(\Gamma) \le \lambda(\Gamma)$ کران بالا و کران پایین $\sigma(\Gamma)$ به ترتیب به وسیله λ و κ بدست می‌آید. نتایج مقاله [3] در مقالهٔ [10] تعمیم داده شد.

قضیه ۲-۵ [10]: هیچ ساختار دسترسی Γ با شرط $1 < \kappa(\Gamma) < 3/2$ وجود ندارد. بعلاوه یک ساختار دسترسی Γ وابسته ماتریدی است اگر و تنها اگر $\kappa(\Gamma) = 1$.

[1] Complexity

[2] Optimal complexity

[3] p -secret sharing polymatroid

[4] p_0 -secret sharing polymatroid

۳- مجموعه‌های چندبخشی

ساختارهای دسترسی که در این مقاله بررسی شده است همگی چندبخشی هستند، در این قسمت نتایجی کلی بدست آمده روی این نوع ساختارها را بیان می‌کنیم.

یک m-افراز $\Pi=(X_1,\dots X_m)$ از مجموعه X، یک خانواده مجزا از m زیرمجموعه غیر تهی X با شرط $X=X_1\bigcup\cdots\bigcup X_m$ می‌باشد. فرض کنید $\Lambda\subset P(X)$ یک خانواده از زیرمجموعه‌های X باشد. برای هر جایگشت τ روی X تعریف می‌کنیم $\tau(\Gamma)=\{\tau(A)\mid A\in\Lambda\}\subset P(X)$. فرض کنید Ψ یک خانواده از جایگشت‌های τ باشد که برای هر $X_i\in\Pi$ در شرط $\tau(X_i)=X_i$ صدق کند. یک خانواده از زیرمجموعه‌های $\Lambda\subset P(X)$ را Π-بخشی گویند اگر برای هر جایگشت τ در Ψ داشته باشیم $\tau(\Lambda)=\Lambda$. یک خانواده $\Lambda\subset P(X)$ را m-بخشی گویند اگر برای یک m-افراز Π داشته باشیم Λ یک Π-بخشی است.

اگر A یک زیرمجموعه در Λ و B زیرمجموعه دیگری باشد که برای هر i داشته باشیم $|A\bigcap X_i|=|B\bigcap X_i|$، آنگاه B نیز یک زیرمجموعه در Λ است. از این خاصیت برای معرفی خانواده‌های چندبخشی استفاده می‌کنیم.

فرض کنید $\Pi=(X_1,\dots X_m)$ یک افراز از مجموعه X باشد. برای هر $A\subset X$ و $i\in\{1,\dots,m\}$ نگاشت $\Pi_i:P(X)\to Z$ را به صورت زیر تعریف می‌کنیم:

$$\Pi_i(A)=|A\bigcap X_i|.$$

بنابراین برای هر افراز Π نگاشت $\Pi:P(X)\to Z_+^m$ را به صورت زیر درنظر می‌گیریم:

$$\Pi(A)=\left(\Pi_1(A),\dots\Pi_m(A)\right).$$

برای یک خانواده $\Lambda\subset P(X)$ درنظر بگیرید:

$$\Pi(\Lambda)=\left\{\Pi(A)\mid A\subset X, A\in\Lambda\right\}\subset Z_+^m.$$

لم ۳-۱ [5]: فرض کنید Π یک افراز از مجموعه X و $\Lambda\subset P(X)$ یک Π-افراز باشد. آنگاه $A\in\Lambda$ اگر و تنها اگر $\Pi(A)\in\Pi(\Gamma)$ باشد.

این لم ایجاب می‌کند که Λ به وسیله مجموعه بردارهای $\Pi(\Lambda)$ به طور کامل مشخص می‌شود.

یک ساختار دسترسی Γ را یک m-بخشی گویند اگر یک m-افراز Π روی P وجود داشته باشد به طوری که Γ یک Π-بخشی باشد. در این حالت دو سهام‌دار در یک بخش نقش یکسانی را در طرح ایفا می‌کنند و بنابر این غیر قابل تمایز هستند. مجموعه $\Pi(\min\Gamma)$ را مجموعه نقاط مینیمال گویند.

به منظور استفاده از نتایج روی پلی‌ماتریدها در طرح‌های تقسیم راز چندبخشی تعریف زیر را می‌آوریم.

تعریف ۳-۲: یک ss-p_0-پلی‌ماترید $S=(Q,h)$ را یک m-بخشی گویند اگر یک Π-بخشی برای افراز $\Pi=(X_1,\dots X_m,\{p_0\})$ باشد به طوری که $X_1,\dots X_m\subset P$ و $h(A)=h(\tau(A))$ برای هر Π-جایگشت τ و برای هر $A\subset Q$.

فرض کنید Π یک افراز روی $Q=X_1\cup\cdots\cup X_m\cup\{p_0\}$ و $\Omega=\{0,\dots,|X_1|\}\times\cdots\times\{0,\dots|X_m|\}\times\{0,1\}$ باشد. هر پلی‌ماترید Π-بخشی $S=(Q,h)$ به صورت یکتا با زوج (Ω,h') نمایش داده می‌شود که در آن $h':\Omega\to\Re$ به صورت زیر تعریف می‌شود:

برای هر $A\in\Pi^{-1}(x_1,\dots x_{m+1})$ داریم $h'(x_1,\dots x_{m+1})=h(A)$.

همانند اینکه برای ساختارهای دسترسی Π-بخشی از نماد $\Pi(\Gamma)$ بجای نماد Γ استفاده نمودیم اکنون نیز از نماد (Ω,h') بجای $S=(Q,h)$ استفاده می‌نماییم. از این به بعد این نماد را برای پلی‌ماتریدهای تقسیم راز چند بخشی به کار خواهیم برد.

توجه کنید که پلی‌ماتریدهای بدست آمده از طرح‌های تقسیم راز چندبخشی لزوما چندبخشی نیستند. به طور مثال ساختارهای وجود دارند که در آن اندازه سهام سهام‌داران یک بخش متفاوت است. ما علاقمند به مطالعه همه حالات ساختارهای دوبخشی نیستیم و توجه خود را بر روی بهترین ساختارها و کران‌های بالای دقیق[1] روی نرخ اطلاعات ساختارهای دسترسی معطوف میکنیم. قضیه بعدی نشان می‌دهد که چگونه برای رسیدن به هدف ما کافیست که آن پلی‌ماتریدهای تقسیم راز چندبخشی S را در نظر بگیریم به طوری که $\Gamma=\Gamma_{p_0}(S)$.

قضیه ۳-۳: فرض کنید Γ یک ساختار دسترسی m-بخشی روی مجموعهٔ سهام‌داران $P=Q\setminus\{p_0\}=X_1\cup\cdots\cup X_m$ باشد. آنگاه $\kappa(\Gamma)=\inf\{\kappa(S)\}$، که در آن اینفیمم روی همه پلی‌ماتریدهی تقسیم راز m-بخشی S گرفته شده است به طوری که $\Gamma=\Gamma_{p_0}(S)$.

[1] Tight

اثبات: مقدار $\omega(\Gamma)$ را اینفیمم $\kappa(S)$ روی همه پلی‌ماتریدهای تقسیم راز m-بخشی S بگیرید که $\Gamma = \Gamma_{p_0}(S)$. واضح است که $\omega(\Gamma) \geq \kappa(\Gamma)$.

مجموعه همه جایگشت‌های مانند Π را مجموعه Ψ در نظر بگیرید. برای هر پلی‌ماترید (نه لزوما چندبخشی) $S=(Q,h)$ با $\Gamma = \Gamma_{p_0}(S)$، پلی‌ماترید $\widetilde{S} = (Q, \widetilde{h})$ را با تابع $\widetilde{h}$ زیر در نظر بگیرید:

$$\widetilde{h}(A) = \frac{1}{|\Psi|}\sum_{\tau\in\Psi} h(\tau(A))$$

توجه کنید که $\widetilde{h}$ خوش تعریف است و $\widetilde{S}$ یک p_0-ss-پلی‌ماترید m-بخشی با $\Gamma = \Gamma_{p_0}(\widetilde{S})$ است. بعلاوه داریم $\kappa(S) \geq \kappa(\widetilde{S})$. بنابر این $\omega(\Gamma) \geq \kappa(\Gamma)$. ■

در این مقاله یک روش جدید برای مطالعه ساختارهای دسترسی دوبخشی ارائه شده است. ما مسائل طرح تقسیم راز را با استفاده از ساختار بیان شده در قسمت قبل به مسائلی در مبحث پلی‌ماتریدها تبدیل می‌کنیم.

در [12] بسیاری از ساختارهای دسترسی دوبخشی با پیچیدگی بهینه موجود می‌باشد. در این مقاله یک دسته‌بندی از ساختارهای دوبخشی ایده‌آل ذکر شده است. از آنجایی که می‌خواهیم کران‌های برای پیچیدگی بهینه در ارتباط با نقاط مینیمم ارائه دهیم لذا این دسته بندی را در ارتباط با $\min\Gamma$ بازنویسی می‌کنیم.

قضیه ۳-۴ [12]: یک ساختار دسترسی دوبخشی Γ ایده‌آل است اگر و تنها اگر $\Gamma_0 = \beta_1 \bigcup \beta_2$، که در آن:

- برای هر $x,y>0$ داشته باشیم $\Pi(\beta_1) \subset \{(0,y),(x,0)\}$ و
- $\beta_2 = \phi$ یا برای هر $x,y>m$ داشته باشیم $\Pi(\beta_2) = \{(x-m,y-1),\ldots,(x-1,y-m)\}$

با استفاده از قضیه ۲-۵ نتیجه زیر حاصل می‌شود.

قضیه ۳-۵: اگر Γ یک ساختار دسترسی دوبخشی غیر ایده‌آل باشد آنگاه $\sigma(\Gamma) \geq 3/2$.

به منظور بررسی پلی‌ماتریدهای بهینه از روش برنامه‌ریزی خطی استفاده شده است. در ابتدا با استفاده از یک تبدیل، پلی‌ماتریدها را به صورت بردار نمایش می‌دهیم و سپس با استفاده از یک روش بهینه سازی خطی مقدار $\kappa(\Gamma)$ را بعد از پیدا کردن بهترین پلی‌ماترید ممکن، محاسبه می‌کنیم. به این منظور برای هر $p\in P$ کمترین مقدار $h(p)$ را در بین تمامی پلی‌ماتریدهای دوبخشی $S=(Q,h)$ که در $\Gamma = \Gamma_{p_0}(S)$ صدق کنند، پیدا می‌کنیم.

همانطور که ثابت کردیم برای این منظور کافیست که فقط پلی‌ماتریدهای دوبخشی را در نظر بگیریم. این روش باعث کاهش تعداد تساویها خواهد شد. چون که اندازه بردار در مساله برنامه‌ریزی خطی ما با استفاده از زوج (Ω,h') از $2^{|P_1|+|P_2|+2}$ به $2\cdot|P_1|\cdot|P_2|$ کاهش خواهد یافت، که تاثیر چشمگیری در کاهش میزان محاسبات دارد.

۴- شیوه برنامه‌ریزی خطی

در این بخش برای پیدا کردن مقدار $\kappa(\Gamma)$ یک برنامه‌ریزی خطی را بیان می‌کنیم. فرض کنید که Γ یک ساختار دسترسی دوبخشی روی مجموعه سهام‌داران $P = X \bigcup Y$ باشد که در آن X و Y مجموعه‌های از هم جدا هستند و نقاط مینیمال آن برابر است با $\Pi(\min\Gamma) = \{(x_1,y_1),\ldots,(x_r,y_r)\}$. مقادیر $N_1 = |X|$ و $N_2 = |Y|$ و مجموعه $\Omega = \{0,1,\ldots,N_1\}\times\{0,1,\ldots,N_2\}\times\{0,1\}$ را در نظر بگیرید. برای هر پلی‌ماترید دوبخشی S، زوج (Ω,h) را به صورتی که در بالا تعریف شده است فرض کنید. h را *تابع رتبه*[1] S می‌نامیم. مقدار $N = 2(N_1+1)(N_2+1)$ و بردار $\vec{s} = \big(h(x,y,z)\big)_{(x,y,z)\in\Omega} \in \Re^N$ را که عناصر آن همهٔ مقادیرِ تابع رتبه را نشان می‌دهند، در نظر بگیرید. هر مولفهٔ $\vec{s}$ به وسیله یک بردار $(x,y,z)\in\Omega$ مشخص شده و اندیس گذاری می‌شود.

با استفاده از قضیه ۳-۳ به راحتی می‌توان نشان داد که $\kappa(S)$ برابر است با $\max\{h(1,0,0),h(0,1,0)\}$. برای هر $(x,y,z)\in\Omega$ بردار $\vec{e}_{(x,y,z)} \in \Re^N$ را برداری با مولفه ۱ برای مکان متناظر (x,y,z) و صفر در غیر این صورت، تعریف می‌کنیم. برای هر زوج از بردارهای $\vec{x}$ و $\vec{y}$ می‌گوییم $\vec{x} \leq \vec{y}$ است، اگر به ازای مولفه‌های i-ام به ترتیب x_i و y_i آنها داشته باشیم $x_i \leq y_i$.

برای هر بردار $\vec{s}\in\Re^N$ که نمایش دهنده پلی‌ماترید $S=(\Omega,h)$ است، چهار خاصیت تعاریف ۲-۲ و ۲-۳ را به شکل یک تعداد نامساوی خطی به صورت زیر بازنویسی می‌کنیم:

[1] Rank function

۱. خاصیت $h(\phi)=0$ معادل است با

$$\vec{e}_{(0,0,0)}\cdot\vec{s}^{\,T}=0 \qquad (۱)$$

۲. **خاصیت یکنوایی**: برای هر $A\subset B\subset Q$ با $\Pi(A)=(x,y,z)$ و $\Pi(B)=(x',y',z')$ داریم $(x,y,z)\le(x',y',z')$. بنابر این نامساوی $h(A)\le h(B)$ معادل است با

$$[\vec{e}_{(x,y,z)}-\vec{e}_{(x',y',z')}]\cdot\vec{s}^{\,T}\le 0.$$

حال ماتریس A_1 را با سطرهای زیر در نظر بگیرید:

برای هر زوج $(x,y,z),(x',y',z')\in\Omega$ که $(x,y,z)\le(x',y',z')$ سطر $\vec{e}_{(x,y,z)}-\vec{e}_{(x',y',z')}$ را به ماتریس A_1 اضافه کنید. بنابراین خاصیت یکنوایی تابع رتبه h معادل است با نامساوی زیر:

$$A_1\cdot\vec{s}^{\,T}\le 0 \qquad (۲)$$

۳. **خاصیت زیرمدولی**: برای هر $A,B\subset Q$ با $\Pi(A)=(x,y,z)$ و $\Pi(B)=(x',y',z')$ داریم $h(A)+h(B)\ge h(A\bigcup B)+h(A\bigcap B)$. در این حالت بایستی کلیه مقادیر ممکن که $\Pi(A\bigcup B)$ و $\Pi(A\bigcap B)$ می‌توانند به خود بگیرند را در نظر بگیریم. حال برای هر زوج $(x,y,z),(x',y',z')\in\Omega$ مقادیر زیر را در نظر بگیرید:

$l_x=\max\{0,x+x'-N_1\}$، $u_x=\min\{x,x'\}$،
$l_y=\max\{0,y+y'-N_2\}$، $u_y=\min\{y,y'\}$،
$m_z=\min\{z,z'\}$ و $M_z=\max\{z,z'\}$. بنابراین خاصیت زیرمدولی معادل است با:

$$\vec{e}_{(x,y,z)}+\vec{e}_{(x',y',z')}\ge\vec{e}_{(x+x'-r_x,y+y'-r_y,M_z)}+\vec{e}_{(r_x,r_y,m_z)}$$

برای هر $r_x\in\{l_x,l_x+1,\ldots,u_x\}$ و $r_y\in\{l_y,l_y+1,\ldots,u_y\}$. توجه کنید که در این عملیات همه حالت‌های ممکن برای $\Pi(A\bigcup B)$ و $\Pi(A\bigcap B)$ در نظر گرفته شده است. اکنون ماتریس A_2 را با اضافه کردن سطرهای $\vec{e}_{(x+x'-r_x,y+y'-r_y,M_z)}+\vec{e}_{(r_x,r_y,m_z)}-\vec{e}_{(x,y,z)}-\vec{e}_{(x',y',z')}$ بنا می‌کنیم. بنابراین، خاصیت زیرمدولی تابع رتبه h معادل است با

$$A_2\cdot\vec{s}^{\,T}\le 0 \qquad (۳)$$

۴. **ساختار دسترسی**: برای هر زیرمجموعه $A\subset Q$ تساوی $h(A\bigcup\{p_0\})=h(A)$ برقرار است اگر A یک زیرمجموعه مجاز باشد و تساوی $h(A\bigcup\{p_0\})=h(A)+1$ برقرار است اگر A یک زیر مجموعه غیر مجاز باشد. در یک ساختار دسترسی دوبخشی این خاصیت‌ها معادل است با:

$\vec{e}_{(x,y,1)}-\vec{e}_{(x,y,0)}=0$ اگر $(x,y)\ge(a,b)$ به ازای یک $(a,b)\in\Pi(\min\Gamma)$ و

$\vec{e}_{(x,y,1)}-\vec{e}_{(x,y,0)}=1$ در غیر این صورت.

اکنون ماتریس B را با سطرهای $\vec{e}_{(x,y,1)}-\vec{e}_{(x,y,0)}$ برای هر $(x,y,0),(x,y,1)\in\Omega$ در نظر بگیرید. از آنجایی که این تفاضل، مقدار صفر یا ۱ را به خود می‌گیرد، ما یک بردار $\vec{b}$ را با مقدار صفر اگر $(x,y)\ge(a,b)$ به ازای $(a,b)\in\Pi(\min\Gamma)$ و ۱ در غیر این صورت بنا می‌کنیم. لذا تساوی معادل، برابر است با:

$$B\cdot\vec{s}^{\,T}=\vec{b}\in\Re^{(N_1+1)(N_2+1)} \qquad (۴)$$

بعلاوه به عنوان نتایجی از خواص (۱) تا (۴) شرط زیر

$$\vec{s}\ge\vec{e}_{(0,0,1)}\in\Re^{N} \qquad (۵)$$

روی مولفه‌های $\vec{s}$ بدست می‌آید.

از آنجایی که در یک پلی‌ماترید دوبخشی S داریم $\kappa(S)=\max\{h(1,0,0),h(0,1,0)\}$، بنابراین برای نمایش مساله ما به عنوان یک تابع خطی در یک مساله برنامه‌ریزی خطی، مساله را به دو بخش زیر تقسیم می‌کنیم:

الف) $h(1,0,0)\ge h(0,1,0)$ و

ب) $h(1,0,0)\le h(0,1,0)$.

هر دو حالت را به صورت جداگانه بررسی می‌کنیم. بدون کم شدن از کلیت مساله فرض کنید که نامساوی اول برقرار باشد. لذا داریم $h(1,0,0)=\max\{h(1,0,0),h(0,1,0)\}$. بنابراین این خاصیت را می‌توان به عنوان تابع خطی A_3 به صورت زیر تبدیل کرد:

$$A_3\cdot\vec{s}^{\,T}\le 0 \qquad (۶)$$

که در آن $A_3=\vec{e}_{(0,1,0)}-\vec{e}_{(1,0,0)}$. توجه به این نکته ضروری است که اگر خاصیت (ب) برقرار باشد یک ماتریس A_3 متفاوت بدست می‌آید.

خواص (۱) تا (۶)، یک ناحیه محدب $U \subset \Re^N$ ایجاد می‌کند که ما آن را *ناحیه شدنی*[1] می‌نامیم. بنابراین هدف ما یافتن اینفیمم مقدار $\kappa(\Gamma)$ روی ناحیه محدب U می‌باشد که برای آن بایستی مقدار $h(1,0,0) = \vec{e}_{(1,0,0)} \cdot \vec{s}^T$ را، روی همه $\vec{s} \in U$ کمینه[2] ساخت. ماتریس A از الحاق سطری ماتریس‌های A_2, A_1 و A_3 بدست می‌آید. $\vec{s}$ را برداری از متغیرها درنظر بگیرید. مساله برنامه‌ریزی خطی که ما در نظر گرفته‌ایم به صورت زیر است.

کمینه کردن مقدار $\vec{e}_{(1,0,0)} \cdot \vec{s}^T$

با شرط:

$$A \cdot \vec{s}^T \le 0$$
$$B \cdot \vec{s}^T = \vec{b}$$
$$\vec{s} \ge \vec{e}_{(0,0,1)}$$

از آنجای که ناحیه شدنی U ممکن است تهی باشد، لذا یکی از دو حالت مساله برنامه‌ریزی خطی داده شده توسط حالت‌های (الف) و (ب) ممکن است جواب نداشته باشد. اما این وضعیت نمی‌تواند به صورت همزمان برای هر دو حالت رخ دهد.

در حالتی که هر دو مساله برنامه‌ریزی خطی دارای جواب باشند یعنی این که اگر $\vec{s}_I^{\,*}$ یک جواب بهینه در حالت (الف) و $\vec{s}_{II}^{\,*}$ یک جواب بهینه در حالت (ب) باشد آنگاه داریم

$$\kappa(\Gamma) = \min\{\vec{e}_{(1,0,0)} \cdot \vec{s}_I^{\,*T}, \vec{e}_{(0,1,0)} \cdot \vec{s}_{II}^{\,*T}\} \qquad (۷)$$

۵- نتایج تجربی

برای پیاده‌سازی طرح ارائه شده در قسمت قبل از نرم‌افزار بهینه‌سازی MOZEK® در محیط MATLAB® استفاده شده است. ورودی این برنامه دارای سه پارامتر زیر است:

نقاط مینیمال ساختار دسترسی را با $\{(x_1,y_1),\cdots,(x_m,y_m)\}$ و تعداد اعضای مجموعه‌های X و Y را به ترتیب با N_1 و N_2 نشان می‌دهیم.

مثال ۵-۱: ساختار دسترسی Γ_s را روی مجموعه سهام‌داران $P = X \cup Y$ با نقاط مینیمال $\Pi(\min\Gamma_s) = \{(0,s),(1,1)\}$ و $|X| = N_1 \ge 1$، $|Y| = N_2$ و $3 \le s \le N_2$ در نظر بگیرید. برای یک مقدار داده شده s، برنامه را با مقادیر $N_1 = 1,2,3,4$ و $N_2 = s, s+1, s+2, s+3$ اجرا نمودیم و خروجی زیر بدست آمد:

s	خروجی $\kappa(\Gamma_s)$
3	1.5000
4	1.6667
5	1.7500
6	1.8000
7	1.8333
8	1.8571
9	1.8750
10	1.8889
11	1.9000
12	1.9091
13	1.9167

که در آن ستون اول نمایش دهنده مقدار s و ستون دوم نشان دهنده مقادیر بدست آمده از اجرای برنامه در MATLAB® می‌باشد. همانطور که مشاهده شد برای مقادیر N_1 و N_2 مقدار κ فقط به s وابسته است و داریم

$$\kappa(\Gamma_s) = \frac{2s-1}{s}.$$

این مقادیر همانهایی هستند که در [11] در حالت خاص $N_1 = 1$ و $N_2 = s$ بدست آمده است. نتایج ما به دلیل به کار بردن مقادیر دیگر N_1 و N_2 کلی‌تر از نتایج بدست آمده تا کنون است. توجه کنید که مقادیر $\kappa(\Gamma_s)$ یک کران پایین روی پیچیدگی بهینه ساختارهای دسترسی بدست می‌دهد و داریم

$$\sigma(\Gamma_s) \ge \kappa(\Gamma_s) = \frac{2s-1}{s}.$$

مثال ۵-۲: در حالت کلی‌تر ساختار دسترسی $\Gamma^1_{s,t}$ را روی مجموعه سهام‌داران $P = X \cup Y$ با نقاط مینیمال $\{(0,s),(t,1)\}$، $|X| = t$ و $|Y| = s$ را در نظر بگیرید. همچنین ساختار دسترسی $\Gamma^2_{s,t}$ با نقاط مینیمال $\{(1,s),(t,1)\}$، $|X| = t$ و $|Y| = s$ مفروض است. تعدادی از خروجی‌های این ساختارهای دسترسی به صورت زیر است:

[1] Feasible region

[2] Minimize

s,t	خروجی $\kappa(\Gamma^1_{s,t})$
3,2	1.5000
3,3	1.5000
4,2	1.6667
4,3	16667
5,2	1.7500
5,3	1.7500
6,2	1.8000
6,3	1.8000
7,2	1.8333
7,3	1.8333
8,2	1.8571
8,3	1.8571

s,t	خروجی $\kappa(\Gamma^2_{s,t})$
3,2	1.5000
3,3	1.5000
3,4	1.6667
3,5	1.7500
3,6	1.8000
3,7	1.8333
4,2	1.6667
4,3	1.6667
4,4	1.6667
4,5	1.7500
4,6	1.8000
4,7	1.8333

توجه کنید که داریم $a=\max\{s,t-1\}-1$. مقدار $\kappa(\Gamma^1_{s,t})$ برای این مثال به وسیله تساوی $\kappa(\Gamma^1_{s,t})=\frac{2a-1}{a}$ بدست آمده است. از طرف دیگر مشاهده می‌کنید که ساختار دسترسی $\kappa(\Gamma^2_{s,t})$ مقادیر متفاوتی از κ برای ساختارهای دسترسی Γ_s و $\Gamma^1_{s,t}$ به ما می‌دهد. حال اگر $a=\max\{s-1,t-1\}$ در نظر گرفته شود، مقدار $\kappa(\Gamma^2_{s,t})$ برای این مثال از رابطه $\kappa(\Gamma^2_{s,t})=\frac{2a-1}{a}$ بدست می‌آید. توجه کنید که در این مثال ما فقط ساختارهایی با تعداد مینیمال از سهام‌داران را به صورت نقاط مینیمال هر بخش لحاظ کرده‌ایم.

۶- نتیجه گیری

در این مقاله ارتباط بین $\sigma(\Gamma)$ یک ساختار دسترسی دوبخشی با پارامترهای $\kappa(\Gamma)$ و $\lambda(\Gamma)$ آن بررسی شد و نتایج جدیدی برای مقدار $\kappa(\Gamma)$ ساختارهای دسترسی دوبخشی ارائه شد. روش برنامه‌ریزی خطی ارائه شده در این مقاله مقادیری از $\kappa(\Gamma)$ را برای بعضی از ساختارهای دسترسی Γ مشخص نمود که تا کنون ناشناخته بوده است. بعلاوه این روش را می‌توان برای بررسی ساختارهای دسترسی چند بخشی با بیش از دو بخش نیز تعمیم داد.

۷- سپاسگذاری

از آقای دکتر Carles Padro Laimon بخاطر راهنمایی‌های ارزنده ایشان و خانم Leonor Vazquez به دلیل هم‌فکری در اجرای برنامه‌ریزی خطی این مقاله کمال تشکر را دارم.

مراجع

[1] A. Beimel and N. Livne and C. Padro, "Matroids Can Be Far From Ideal Secret Sharing," Theory of Cryptography Conference, TCC 2008. Lecture Notes in Comput. Sci., vol. 4948, 2008, pp. 194–212.

[2] E. F. Brickell, "Some ideal secret sharing schemes," J. Combin. Math. and Combin. Comput., vol. 9, 1989, pp. 105–113.

[3] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," J. Cryptology, vol. 4, 1991, pp. 123–134.

[4] L. Csirmaz, "The size of a share must be large," J. Cryptology, vol. 10, 1997, pp. 223–231.

[5] O. Farras and J. Marti–Farre and C. Padro, "Ideal Multipartite Secret Sharing Schemes," Advances in Cryptology, EUROCRYPT 2007 LectureNotes in Comput. Sci., 4515, 2007, pp. 448–465.

[6] S. Fujishige, "Polymatroidal Dependence Structure of a Set of Random Variables," Information and Control, vol. 39, 1978, pp. 55–72.

[7] J. Herzog and T. Hibi, "Discrete polymatroids," J. Algebraic Combin., vol. 16, 2002, pp. 239–268.

[8] M. Ito and A. Saito and T. Nishizeki, "Secret sharing scheme realizing any access structure," Proc. IEEE Globecom'87. 1987, pp. 99–102.

[9] A. Lehman, "A solution of the Shannon switching game," J. Soc. Indust. Appl. Math., vol. 12, 1964, pp. 687–725.

[10] J. Martı-Farre and C. Padro, "On Secret Sharing Schemes, Matroids and Polymatroids," Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Comput. Sci., vol. 4392, 2007, pp. 273–290.

[11] J. R. Metcalf-Burton, "Information Rates of Minimal Non-Matroid-Related Access Structures," arxiv.org/pdf/0801.3642

[12] C. Padro and G. Saez and "Secret sharing schemes with bipartite access structure," IEEE Trans. Inform. Theory, vol. 46, 2000, pp. 2596–2604.

[13] P. D. Seymour, "A forbidden minor characterization of matroid ports," Quart. J. Math. Oxford Ser., vol. 27, 1976, pp. 407–413.

[14] C. E. Shannon, "A Mathematical Theory of Communication," Bell. Sys. Tech. Journal, 27 , 1948.

[15] R. W. Yeung, "A framework for linear information inequalities," IEEE Trans. Inform. Theory, IT-41: pp. 412-422, 1995.