بررسی و تعیین پیچیدگی بهینهٔ ساختارهای دسترسی دوبخشی

عباس چراغی چالشتری؛ دانشگاه اصفهان، دانشکده ریاضی و کامپیوتر خوانسار

چکیده

در یک طرح تقسیم راز دوبخشی، مجموعه سهامداران را به‌گونه‌ای به دو قسمت تقسیم می‌کنند که همهٔ سهامداران درون یک بخش، نقش یک‌سانی را بازی کنند. پادرو و سائز ساختارهای دسترسی ایده‌آل دو بخشی را به‌طور کامل دسته بندی کرده‌اند اما این‌که کدام ساختارهای دسترسی غیرایده‌آل پیچیدگی بهینه دارند همچنان نامعلوم است. از طرفی مشخص کردن پیچیدگی ساختارهای دسترسی در حالت کلی، یکی از بزرگ‌ترین مسائل حل نشده در بحث تقسیم راز است. به‌این منظور و در راستای بررسی پیچیدگی، ما خودمان را به ساختارهای دسترسی دوبخشی محدود می‌کنیم تا روش جدیدی برای محاسبه کران‌هایی روی پیچیدگی بهینه این گونه ساختارها به‌دست آوریم. در این مقاله با استفاده از ارتباط طرح‌های تقسیم راز و پلی‌ماتریدها، برای پیچیدگی هر ساختار دسترسی دوبخشی، از مسالهٔ برنامه‌ریزی خطی استفاده می‌کنیم تا کران پایینی روی پیچیدگی هر ساختار دسترسی ارائه دهیم. ساختارهای دسترسی که ما در این مقاله بررسی کرده‌ایم محدودیتی در تعداد سهامداران شرکت کننده در طرح ندارند. به‌علاوه در این مقاله نشان خواهیم داد که برخی از کران‌های پایین ارائه شده بر روی پیچیدگی این ساختارهای دسترسی دقیق هستند. در آخر طرح‌های بهینه جدیدی را بر روی ساختارهای دسترسی دوبخشی خاص ارائه خواهیم داد.

مقدمه

طرح تقسیم راز[۱] 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 کنند درحالی که زیرمجموعه‌های *غیرمجاز* نتوانند هیچ اطلاعاتی راجع به راز به‌دست آورند. خانواده Γ از زیرمجموعه‌های مجاز را *ساختار دسترسی* آن طرح می‌نامند. این دسته از طرح‌ها امنیت بدون شرط[۲] دارند. این طرح‌ها به قدرت و توانایی‌های دشمن وابسته نیستند.

بسیاری از پروتکل‌های رمزنگاری بر اساس ساختار طرح‌های تقسیم راز، پایه گذاری شده‌اند و کاربردهای بسیاری به‌صورت عملی ایجاب می‌کنند. بازده طرح‌های تقسیم راز به‌وسیلهٔ ارتباط اندازهٔ راز و اندازهٔ سهم‌ها، محک زده می‌شوند. حاصل تقسیم طول راز به‌طول بزرگ‌ترین سهم سهامداران را *نرخ اطلاعات*[۳] گویند [۱۵].

واژه های کلیدی: پیچیدگی، طرح تقسیم راز، ساختار دسترسی.
دریافت ۹۱/۷/۱۱ پذیرش ۹۲/۱۲/۱۲
*نویسنده مسئول cheraghi@sci.ui.ac.ir

۱. Secret sharing scheme ۲. Unconditionally secure ۳. Information rate

از آن‌جاکه طرح‌ها را به‌صورت امنیت بدون شرط درنظر می‌گیریم، از همین رو، در بهترین حالت اندازهٔ راز با اندازهٔ هریک از سهم‌ها برابر خواهد بود و در این حالت نرخ اطلاعات، برابر با ۱ است. در این صورت طرح و ساختار آن را *ایده‌آل*[۱] گویند [۶]. مشخص کردن ساختارهای دسترسی ایده‌آل هنوز مسئله‌ای حل نشده است و به‌دلیل تأثیر زیاد آن‌ها در بحث طرح‌های تقسیم راز، دسته‌بندی ساختارهای دسترسی ایده‌آل به‌عنوان یکی از با اهمیت‌ترین مسائل رمزنگاری شناخته شده است. همچنین تعیین نرخ اطلاعات بهینهٔ یک ساختار دسترسی در حالت کلی نیز از مسائل بزرگ رمزنگاری است. طرحی که نرخ اطلاعاتِ ساختار دسترسی آن بهترین حالت ممکن باشد را یک طرح *بهینه*[۲] می‌نامند.

ساختار *دسترسی یکنوا*[۳] ساختاری است که در آن هر ابرمجموعه[۴] یک مجموعه مجاز، خود مجموعه مجازی از سهام‌داران باشد. از این رو، ساختار دسترسی یکنوای Γ را می‌توان با استفاده از خانواده‌ای از مجموعه‌های مجاز مینیمال آن مشخص کرد که به آن پایه Γ گویند و آن را با Γ_0 نشان می‌دهند. در حالت کلی ساختارهای دسترسی را یکنوا در نظر می‌گیرند.

اهمیت ساختارهای دسترسی ایده‌آل، طرح‌های ایده‌آل و طرح‌های بهینه از نظر تحقیقاتی همانند بررسی نرخ اطلاعات ساختارهای دسترسی است و تا کنون مسائل پیچیده ریاضی را با خود به چالش کشیده است. در بررسی این گونه مسائل از مفاهیمی چون ماتریدها، پلی‌ماتریدها[۵] و گراف‌ها استفاده شده است. همچنین تاکنون از شاخه‌های مختلف ریاضیات مانند جبر، ترکیبیات و نظریه کدگذاری نیز برای حل این مسائل استفاده شده است.

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

شامیر [۱۸] و بلاکلی [۲] برای اولین بار در سال ۱۹۷۹ به‌طور مستقل، طرح تقسیم راز را مطرح کردند. طرح‌های ارائه شده در این مقاله‌ها ایده‌آل و آستانه‌ای بودند. طرح ارائه شده به‌وسیلهٔ شامیر بر اساس درونیابی لاگرانژ پایه ریزی شده است در حالی که طرح بلاکلی بر پایه ایده‌های هندسی مطرح می‌شود.

بریکل و داونپورت ثابت کردند که ساختارهای دسترسی ایده‌آل وابسته ماتریدی[۶] هستند [4]، به این معنی که برای هر ساختار دسترسی ایده‌آل، ماتریدی وجود دارد که در آن، مدارهای شامل یک نقطه ثابت، در تناظر یک به یک با زیرمجموعه‌های پایهٔ آن ساختار دسترسی هستند. اهمیت ایده آن‌ها در بررسی ایده‌آل بودن ساختارهای دسترسی و همچنین تولید طرح‌های ایده‌آل با استفاده از ماترید پورت‌ها[۷] است. نتایجی از ماترید پورت‌ها در [۱۱]، [۱۶] بیان شده و در مقاله [۱۲] این نتایج بهبود پیدا کرده است. در [۸] نشان داده شده که چگونه می‌توان با استفاده از آنتروپی‌های هر مجموعه از متغیرهای تصادفی، یک پلی‌ماترید ساخت. با استفاده از این روش در [۵] 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

۱. Ideal ۲. Optimal ۳. Monotone access structure ۴. superset
۵. Polymatroid ۶. Matroid related ۷. Matroid ports

می‌توان برای پیدا کردن کران‌های بالای میزان اطلاعات بهینه ساختارهای دسترسی استفاده کرد [۵]، [۱۲]. یکی دیگر از ارتباط‌های مهم بین طرح تقسیم راز و پلی‌ماتریدها که به‌تازگی پیدا شده است پلی‌ماتریدهای گسسته[۱] است [۹] که به‌کمک آن در [۶] مفاهیم ترکیبیاتی برای توصیف ساختارهای دسترسی سه‌بخشی ایده‌آل معرفی شده است.

خواص ماتریدها و پلی‌ماتریدهای که در طرح تقسیم راز به‌کار گرفته شده است در واقع نتیجه‌ای از نامساوی شانون متغیرهای تصادفی است [۱۹]. از طرفی با استفاده از نامساوی‌های غیر-شانون[۲] نتایج جدیدی در طرح تقسیم راز به‌دست آمده است [۱].

در ساختارهای *دسترسی چندبخشی*[۳] 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 [۳] معرفی شد. در مقاله [۱۴] برای میزان اطلاعات طرح‌های غیرایده‌آل 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 [۶]. 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 می‌دهیم. برای این منظور از ارتباط بین پلی‌ماتریدها و طرح‌های تقسیم راز و همچنین یک شیوه برنامه‌ریزی خطی استفاده شده است. این کران‌ها با به‌کار بردن نامساوی شانون بر روی آنتروپی مجموعه سهم سهام‌داران به‌دست آمده است. در [۲۱] نامساوی شانون در قالب مسئلهٔ برنامه‌ریزی خطی معرفی شده است. در این حالت، خواصی از طرح‌های دوبخشی باعث شده است تا این روش برنامه‌ریزی خطی به‌صورت ساده‌تری بهبود یابد. این روش بهبود یافته همچنین می‌تواند برای ساختارهای دسترسی چندبخشی با بیش از دو بخش نیز به‌کار رود. با استفاده از این روش برنامه‌ریزی خطی کران‌های بالایی برای میزان اطلاعات بهینه ساختارهای دسترسی غیرایده‌آل بیان شده است که نتایج در [۱۴] را بهبود داده است. همچنین در این مقاله ساختارهای بهینه معرفی شده در [۱۳] برای ساختارهای دسترسی دوبخشی با تعدادی دل‌خواه از سهام‌داران در هر بخش، تعمیم داده شده است. در [۷] طرح‌های تقسیم راز دوبخشی و پیچیدگی آن‌ها بررسی شده و با استفاده از دسته‌ای خاص از پلی‌ماتریدها کران‌های پایینی برای پیچیدگی ساختارهای دسترسی دوبخشی ارائه شده و برای خانواده‌ای خاص از آن‌ها، طرح تقسیم راز بهینه معرفی شده است. اما همچنان بهینه‌سازی طرح‌های تقسیم راز با ساختارهای دسترسی دوبخشی از مسائل حل نشده است. ما در این مقاله کران‌های جدیدی بر روی برخی دیگر از ساختارهای دسترسی دوبخشی ارائه می‌دهیم. به‌علاوه یک طرح تقسیم راز خطی بهینه با ساختار دسترسی دوبخشی را معرفی می‌کنیم. در [۱۵] کران‌های پایینی برای ساختارهای دسترسی با تنها ۵ سهام‌دار با استفاده از یک برنامه‌ریزی خطی ارائه

۱. Discrete polymatroids ۲. Non-Shannon inequality ۳. Multipartite access structure

شده است. کران‌های ارائه شده در [۱۵] در حالت کلی کران‌های دقیقی نیستند. ساختارهای دسترسی که در این مقاله بررسی کرده‌ایم محدودیتی در تعداد سهامداران شرکت کننده در طرح ندارند. به‌علاوه در این مقاله نشان خواهیم داد که برخی از کران‌های پایین ارائه شده بر روی پیچیدگی این ساختارهای دسترسی دقیق هستند.

در ادامه این مقاله و در بخش بعد ارتباط بین طرح‌های تقسیم راز با پلی‌ماتریدها بیان شده است. در بخش ۳ مروری بر نتایج به‌دست آمده روی پیچیدگی طرح‌های تقسیم راز و میزان اطلاعات ساختارهای دسترسی خواهیم داشت. در بخش ۴ مقاله با در نظر گرفتن Γ به‌عنوان یک ساختار دسترسی m-بخشی، نشان خواهیم داد که $\kappa(\Gamma)$ را می‌توان با کمک پلی‌ماتریدهای تقسیم راز m-بخشی نیز محاسبه کرد. در بخش ۵ روش جدیدی برای بررسی ساختارهای دسترسی دوبخشی ارائه شده است. در بخش ۶ شیوهٔ برنامه‌ریزی خطی برای یافتن مقدار $\kappa(\Gamma)$ بیان شده است، که در آن Γ به‌عنوان یک ساختار دسترسی دوبخشی روی مجموعه سهامدارن است. در ادامه و در بخش ۷ نتایج تجربی به‌دست آمده به‌کمک روش ارائه شده در بخش ۶ بیان شده است. در این قسمت نشان خواهیم داد که مقدار $\kappa(\Gamma)$ برای برخی ساختارهای دسترسی و به شیوهٔ برنامه‌ریزی خطی ارائه شده، به‌صورت دقیق قابل محاسبه است. سرانجام در بخش آخر با ارائه یک طرح تقسیم راز خطی و به‌کمک نتایج به‌دست آمده در بخش‌های قبلی مقدار دقیق $\sigma(\Gamma)$ برای یک ساختار دسترسی دوبخشی خاص محاسبه می‌شود.

طرح‌های تقسیم راز و پلی‌ماتریدها

طرح‌های تقسیم راز مطرح شده در این مقاله همگی امنیت کامل دارند. یعنی زیرمجموعه‌های مجاز می‌توانند راز را به‌دست آورند درحالی که زیرمجموعه‌های غیرمجاز با استفاده از سهم‌های‌شان با دیدگاه نظریه اطلاعات نمی‌توانند هیچ‌گونه اطلاعاتی از راز به‌دست آورند.

فرض کنید که Σ یک طرح تقسیم راز با مجموعه P از n سهامدار باشد. واسطه را سهامدار $p_0 \notin P$ و $Q = P \bigcup \{p_0\}$ در نظر بگیرید. در یک طرح، سهم p_0 را، راز در نظر می‌گیریم. s_i را سهم سهامدار $i \in Q$ فرض کنید. با توجه به همهٔ $(n+1)$-تایی‌های ممکن $(s_{p_0}, s_1, s_2, ..., s_n)$ از سهم‌ها، نگاشت $\pi_i : E \to E_i$ را برای یک مجموعه مشخص E چنان تعریف می‌کنیم که برای هر $e \in E$ اعضا $(\pi_i(e))_{i \in Q}$ سهم‌های از یک راز باشند. ما فقط نگاشت‌های پوشا را در نظر می‌گیریم، بنا بر این برای هر سهامدار $i \in Q$ مجموعه E_i همان مجموعه همه سهم‌های ممکن سهامدار i است. اگر یک توزیع احتمال در E را درنظر بگیریم آن‌گاه هر یک از نگاشت‌ها، یک توزیع احتمال در E_i القا می‌کنند. . بنا بر این می‌توان $H(E_i)$ را به‌عنوان آنتروپی شانون هر یک از متغییرهای تصادفی در نظر گرفت. برای هر زیرمجموعهٔ $A = \{i_1, ..., i_r\} \subset Q$ آنتروپی مشترک $H(E_{i_1}, ..., E_{i_r})$ را به‌صورت $H(A)$ می‌نویسیم و قرارداد مشابهی را برای آنتروپی شرطی قرار می‌دهیم، به‌طور مثال داریم $H(E_j \mid A) = H(E_j \mid E_{i_1}, ..., E_{i_r})$. مجموعه Γ را ساختار دسترسی Σ در نظر بگیرید. از آن‌جا که نگاشت‌های π_i طرح تقسیم راز کامل Σ را تعریف می‌کنند از همین رو، $H(E_{p_0}) > 0$ و داریم: $H(E_{p_0} \mid A) = 0$ اگر $A \in \Gamma$. در حالی که اگر $A \notin \Gamma$ داریم: $H(E_{p_0} \mid A) = H(E_{p_0})$.

به‌منظور اندازه‌گیری طول سهام هر طرح، از آنتروپی سهام آن طرح استفاده می‌شود. *پیچیدگی*[۱] طرح تقسیم راز Σ به‌صورت $\sigma(\Sigma)=\max_{i\in p} H(E_i)/H(E_{p.})$ تعریف می‌شود. مقدار $\rho(\Sigma)=1/\sigma(\Sigma)$ را *نرخ اطلاعات* طرح Σ گویند. هر دو مقدار σ و ρ را به‌عنوان ضریب تأثیر یک طرح به‌کار می‌برند. این پارامترها را می‌توان برای ارزیابی بهترین راندمان طرح‌های یک ساختار دسترسی مشخص استفاده کرد. *پیچیدگی بهینه*[۲] $\sigma(\Gamma)$ برای یک ساختار دسترسی Γ را اینفیمم پیچیدگی‌های $\sigma(\Sigma)$ روی تمامی طرح‌های Σ تعریف شده برای ساختار دسترسی Γ گویند. میزان اطلاعات بهینه ساختار دسترسی Γ نیز به‌صورت $\rho(\Gamma)=1/\sigma(\Gamma)$ تعریف می‌شود.

یک *طرح تقسیم راز خطی*[۳] 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 *برنامه‌های مولد یک‌نواخت*[۴] نیز گویند، بر پایهٔ خواص جبر خطی استوار است. بر اساس این ارتباط است که مؤثرترین طرح‌ها را خطی درنظر می‌گیرند. در حقیقت برای هر ساختار دسترسی یک طرح تقسیم راز خطی وجود دارد [۱۰]. بنا بر این $\lambda(\Gamma)$ را به‌عنوان اینفیمم پیچیدگی طرح‌های تقسیم راز خطی برای هر ساختار دسترسی Γ تعریف می‌کنیم. قضیه معروف زیر نتیجه مستقیمی از این تعریف است.

قضیه ۲-۱ [۱۵]. برای هر ساختار دسترسی Γ داریم $\sigma(\Gamma)\le\lambda(\Gamma)$.

اثبات: با توجه به آن‌که طرح‌های تقسیم راز خطی برای ساختار دسترسی Γ زیرمجموعه‌ای از تمامی طرح‌های Σ تعریف شده برای ساختار دسترسی دلخواه Γ هستند، از این رو، اینفیمم $\sigma(\Sigma)$ نیز کمتر یا مساوی اینفیمم $\lambda(\Gamma)$ است و این حکم را اثبات می‌کند.

بنا بر 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 $H(E_i)\ge H(E_{p.})$ و . بنا بر این $\sigma(\sum)\ge 1$. یک طرح تقسیم راز با $\sigma(\sum)=1$ را ایده‌آل گویند.

به‌طور مشابه ساختار دسترسی چنین طرحی را نیز ایده‌آل می‌نامند. ارتباط بین ماتریدها و ساختارهای دسترسی ایده‌آل توسط بریکل و داونپورت [۴] کشف شد. این ارتباط در بررسی چنین ساختارهای دسترسی نقش تعیین کننده‌ای را ایفا می‌کند. به‌علاوه در بررسی میزان اطلاعات، ارتباط بین پلی‌ماتریدها و طرح‌های تقسیم راز، اهمیت بسیاری دارد.

تعریف ۲-۲ [۸]: فرض کنید که Q یک مجموعه، $P(Q)$ مجموعه توانی آن و $h:P(Q)\to\Re$ یک تابع باشد، که در آن منظور از $\Re$ مجموعه اعداد حقیقی است. زوج $S=(Q,h)$ را یک پلی‌ماترید گویند اگر در شرایط زیر صدق کند:

۱. $h(\varphi)=0$ ،

۱. Complexity ۲. Optimal complexity ۳. Linear secret sharing scheme ۴. Monotone span programs

۲. تابع h صعودی یکنوا[۱] باشد، یعنی اگر $X \subset Y \subset Q$ ، آنگاه $h(X) \le h(Y)$ و

۳. تابع h خاصیت زیرمدولی[۲] داشته 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 به‌نام پلی‌ماتریدهای تقسیم راز استفاده شده است.

تعریف ۲-۳ [۱۲]: 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 $h(X \bigcup \{p\}) = h(X)+1$ یا $h(X \bigcup \{p\}) = h(X)$ را داشته باشیم، آنگاه S را یک *p-پلی‌ماترید تقسیم راز*[۳] گویند.

اگر Σ طرح تقسیم راز روی مجموعه $Q = P \bigcup \{p.\}$ باشد و مجموعه $\{E_i\}_{i \in Q}$ متغیرهای تصادفی وابسته به سهام باشد، نگاشت $h : P(Q) \to \Re$ را به‌صورت $h : X \to H(X) / H(E_{p.})$ تعریف می‌کنیم.

زوج (Q,h) را که به این شکل تعریف می‌شود یک *p-پلی‌ماترید تقسیم راز*[۴] و یا به اختصار *ss-p-* پلی‌ماترید گویند. بنا بر این هر طرح تقسیم راز Σ یک *ss-p-*پلی‌ماترید به‌صورت $S = S(\Sigma) = (Q,h)$ تعریف می‌کند. لازم به ذکر است که *ss-p-*پلی‌ماتریدهایی وجود دارند که وابسته به هیچ طرح تقسیم رازی نیستند. توجه کنید که اگر Σ کامل نباشد آنگاه $S(\Sigma)$ یک پلی‌ماترید تقسیم راز نیست.

این ارتباط را باید پذیرفت که، اصول طوری در تعریف یک *ss-p-*پلی‌ماترید، استفاده شده است تا خواص طرح‌های تقسیم راز به‌دست آید. در واقع این خواص دقیقا همان خواصی هستند که با به‌کار بردن نامساوی‌های شانون بر روی متغیرهای تصادفی $\{E_i\}_{i \in Q}$ به‌دست می‌آیند.

به‌طور عکس برای هر *ss-p-*پلی‌ماترید $S = (Q,h)$ می‌توان یک ساختار دسترسی وابسته به آن را به شکل زیر تعریف کرد: $\Gamma_{p.}(S) = \{A \subset P \mid h(A) = h(A \cup \{p.\})\}$.

مفهوم پیچیدگی بهینه طرح‌ها و ساختارهای دسترسی را می‌توان برای پلی‌ماتریدها بدین‌صورت 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 *ss-p-*پلی‌ماتریدهای S با $\Gamma = \Gamma_{p.}(S)$ گرفته شده است. این پارامترها برای مطالعه نرخ اطلاعات بهینه استفاده شده‌اند. مارتی و پادرو در [۱۲] با استفاده از *ss-p-*پلی‌ماترید، یک کران پایین روی پیچیدگی بهینهٔ هر ساختار دسترسی Γ ارائه دادند.

قضیه ۲- [۱۲]: پیچیدگی بهینه برای هر ساختار دسترسی Γ کرانی به‌صورت $\sigma(\Gamma) \ge \kappa(\Gamma)$ دارد.

اثبات: [۱۲].

بنا بر این با توجه به نامساوی‌های $\kappa(\Gamma) \le \sigma(\Gamma) \le \lambda(\Gamma)$ کران بالا و کران پایین $\sigma(\Gamma)$ به‌ترتیب به‌وسیلهٔ λ و κ به‌دست می‌آید. اولین کران با کمک جبر خطی و دومین کران به‌کمک ابزار ترکیباتی به‌دست آمده است.

نتایجی بر روی پیچیدگی بهینه ساختارهای دسترسی

در این بخش مروری بر مهم‌ترین نتایج به‌دست آمده روی پیچیدگی طرح‌های تقسیم راز و میزان اطلاعات ساختارهای دسترسی خواهیم داشت. به این منظور ابتدا یک ماترید را تعریف می‌کنیم.

۱. Monotone increasing ۲. Submodular ۳. p -secret sharing polymatroid
۴. p_0 -secret sharing polymatroid

یک *ماتروید*[۱] در واقع یک پلی ماتروید $S=(Q,h)$ است که در دو خاصیت زیر صدق کند:

- برای هر زیرمجموعه $X\subset Q$ داشته باشیم $h(X)\in Z$ و $0<h(X)\le|X|$.
- برای هر زیرمجموعه $Q\subset X$ و عضو $p\in Q$ داشته باشیم $h(X\cup\{p\})=h(X)$ یا $h(X\cup\{p\})=h(X)+1$.

بریکل و داونپورت [۴] ثابت کردند که ساختارهای دسترسی ایده‌آل وابسته ماتریدی هستند. . بنا بر این اگر Σ یک طرح تقسیم راز ایده‌آل باشد آنگاه $S(\Sigma)$ یک ماتروید است. از همین رو، برای هر ماتروید S داریم $\kappa(S)=1$ ، . بنا بر این اگر Σ ایده‌آل باشد داریم $\kappa(S(\Sigma))=1$ ، از این رو می‌توان گفت که برای هر ساختار دسترسی ایده‌آل Γ داریم $\kappa(\Gamma)=1$.

اگر S یک ماتروید قابل نمایش[۲] باشد آنگاه ساختار دسترسی $\Gamma(S)$ ایده‌آل است. اگرچه ساختارهای دسترسی وابسته ماتریدی وجود دارند که ایده‌آل نیستند. این حالت‌ها در واقع ساختارهای دسترسی تعریف شده توسط واموس ماتریدها [۱۷] هستند، زیرا در این ساختارهای دسترسی $\sigma(\Gamma)$ اکیداً از $\kappa(\Gamma)$ بزرگ‌تر است [۱].

این نتایج با استفاده از نامساوی‌های غیر-شانون به‌دست آمده است و این نامساوی‌ها برای اولین بار در طرح-های تقسیم راز به‌کار گرفته شده است. بنا بر این این نتایج نشان می‌دهد که نامساوی‌های شانون برای بررسی پیچیدگی بهینه این طرح‌ها کافی نیست.

نتایج بریکل و داونپورت [۴] در مقاله [۱۲] به‌کمک قضیه زیر بر روی $\kappa(\Gamma)$ تعمیم داده شد.

قضیه ۳-۱ [۱۲]: هیچ ساختار دسترسی Γ با شرط $1<\kappa(\Gamma)<3/2$ وجود ندارد. همچنین یک ساختار دسترسی Γ وابسته ماتریدی است اگر و تنها اگر $\kappa(\Gamma)=1$.

متداول‌ترین ابزار در بررسی ساختارهای دسترسی غیرایده‌آل همان پلی ماتریدها هستند. سیرماز [۵] با استفاده از پلی ماتریدها، کران‌های پایینی بر روی طول سهام هر طرح با ساختار دسترسی مشخص ارائه داد. او همچنین این قضیه را ثابت کرد.

قضیه ۳-۲ [۵]: یک زیرمجموعه P از n سهام‌دار را درنظر بگیرید. هر ساختار دسترسی Γ در شرط $\kappa(\Gamma)\le n$ صدق می‌کند.

ساختار طرح‌های تقسیم راز، کران‌های بالا برای پیچیدگی بهینه آن‌ها ایجاب می‌کنند. در مقاله [۱۰] طرح تقسیم راز کلی ارائه شده است به‌طوری که برای هر ساختار دسترسی معتبر باشد. اما طرح آن‌ها یک طرح کارآمد نیست، چرا که پیچیدگی آن براساس تعداد سهام‌داران از مرتبه نمایی است. استینسون در مقاله [۲۰] روش خاصی برای ساخت طرح‌های کارآمد ارائه داد. ایده تجزیه‌ای آن برای ساختارهای دسترسی که به‌صورت گراف بیان شده‌اند مناسب است و بر پایهٔ یک تجزیه از ساختارهای دسترسی درون ساختارهای دسترسی طرح‌های کارآمد شناخته شده، بنا شده است.

۱. Matroid ۲. Representable matroid

مجموعه‌های چندبخشی

ساختارهای دسترسی که در این مقاله بررسی شده است همگی چندبخشی هستند. در این قسمت با استفاده از مقاله [6]، نتایجی کلی به‌دست 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 غیرتهی X با شرط $X = X_1 \cup \cdots \cup X_m$ است. فرض کنید $\Lambda \subset P(X)$ یک خانواده از زیرمجموعه‌های X باشد. برای هر جای‌گشت τ روی X تعریف می‌کنیم $\tau(\Lambda) = \{\tau(A) \mid A \in \Lambda\} \subset P(X)$. 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 $|A \cap X_i| = |B \cap X_i|$، 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 به‌صورت $\Pi_i(A) = |A \cap X_i|$ تعریف می‌کنیم. . بنا بر این برای هر افراز Π نگاشت $\Pi : P(X) \to Z_+^m$ را بدین‌صورت درنظر می‌گیریم:

$\Pi(A) = \big(\Pi_1(A),\dots,\Pi_m(A)\big)$. برای یک خانواده $\Lambda \subset P(X)$ درنظر بگیرید:

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

لم ۴-۱[۶]: فرض کنید Π یک افراز از مجموعه X و $\Lambda \subset P(X)$ یک خانواده Π-افراز باشد. آن‌گاه $A \in \Lambda$ اگر و تنها اگر $\Pi(A) \in \Pi(\Lambda)$ باشد.

این لم ایجاب می‌کند که Λ به‌وسیله مجموعه بردارهای $\Pi(\Lambda)$ به‌طور کامل مشخص می‌شود. این نماد گذاری مخصوصاً برای ساختارهای دسترسی چند بخشی مفید است که در واقع خانواده‌های از زیرمجموعه‌های مجموعه سهام‌داران در نظر گرفته شده باشند.

یک ساختار دسترسی Γ را یک m-بخشی گویند اگر یک m-افراز Π روی P وجود داشته باشد به‌طوری‌که Γ یک Π-بخشی باشد. در این حالت دو سهام‌دار در یک بخش نقش یکسانی را در طرح ایفا می‌کنند و بنا بر این غیرقابل تمایز هستند. در ادامه برای راحتی کار از نمادهای $\Pi(\Gamma)$ و $\Pi(\Gamma_0)$ استفاده می‌کنیم. مجموعه $\Pi(\Gamma_0)$ را مجموعه *نقاط مینیمال* گویند.

به‌منظور استفاده از نتایج روی پلی‌ماتریدها در طرح‌های تقسیم راز چندبخشی در ادامه تعریف پلی ماتریدهای تقسیم راز چند بخشی را بیان می‌کنیم.

تعریف ۴-۲[۶]: یک p-ss-پلی‌ماترید $S = (Q,h)$ را m-بخشی گویند اگر بتواند یک Π-بخشی، برای افراز $\Pi = (X_1,\dots X_m,\{p_0\})$ باشد به‌طوری‌که $X_1,\dots X_m \subset P$ 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

$$W = \{0,\ldots,|X_1|\} \times L \times \{0,\ldots|X_m|\} \times \{0,1\}$$

باشد. هر پلی‌ماترید Π-بخشی $S = (Q,h)$ به‌صورت یکتا با زوج (Ω,h') نمایش داده می‌شود که در آن $h': \Omega \to \Re$ بدین‌صورت تعریف می‌شود:

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

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

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

قضیه ۴-۳: فرض کنید Γ یک ساختار دسترسی m-بخشی روی مجموعه 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 پلی‌ماتریدهای تقسیم راز m-بخشی S گرفته شده است به‌طوری‌که $\Gamma = \Gamma_{p_0}(S)$.

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 $\omega(\Gamma) \geq \kappa(\Gamma)$.

از طرف دیگر مجموعه همهٔ 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 $\tilde{S} = (Q,\tilde{h})$ را با تابع $\tilde{h}$ زیر در نظر بگیرید:

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

توجه کنید که $\tilde{h}$ خوش تعریف است و $\tilde{S}$ یک p_0-ss-پلی‌ماترید m-بخشی با $\Gamma = \Gamma_{p_0}(\tilde{S})$ است. به‌علاوه با توجه به تعریف تابع $\tilde{h}$ داریم $\kappa(S) \geq \kappa(\tilde{S})$. بنا بر این $\omega(\Gamma) \leq \kappa(\Gamma)$. از این‌رو داریم $\omega(\Gamma) = \kappa(\Gamma)$ که به‌وضوح حکم را نتیجه می‌دهد.

پیچیدگی بهینه ساختارهای دسترسی دوبخشی

در این مقاله روشی جدید برای بررسی 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.

پادرو و سائز در [۱۴] بسیاری از ساختارهای دسترسی دوبخشی با پیچیدگی بهینه را ارائه داده‌اند. در آن مقاله یک دسته‌بندی از ساختارهای دوبخشی ایده‌آل ذکر شده است. در[۷] طرح‌های تقسیم راز دوبخشی و پیچیدگی

۱. Tight

آن‌ها بررسی شده است. در مقالهٔ [۷] با استفاده از دسته‌ای خاص از پلی‌ماتریدها کران‌های پایینی برای پیچیدگی ساختارهای دسترسی دوبخشی ارائه شده است. از آن‌جاکه می‌خواهیم کران‌های برای پیچیدگی بهینه در ارتباط با نقاط مینیمم ارائه دهیم از همی رو، این دسته‌بندی را در ارتباط با $\Gamma_{\cdot}$ بازنویسی می‌کنیم. یادآوری می‌کنیم که ساختار دسترسی یکنوای Γ را می‌توان با استفاده از خانواده‌ای از مجموعه‌های مجاز مینیمال آن مشخص کرد که به آن پایهٔ Γ گویند و آن را با $\Gamma_{\cdot}$ نشان می‌دهند.

قضیه ۵-۱ [۱۴]: یک ساختار دسترسی دوبخشی Γ ایده‌آل است اگر و تنها اگر $\Gamma_{\cdot} = \beta_{۱} \bigcup \beta_{۲}$، که در آن:

- برای یک $x, y > ۰$ داشته باشیم $\Pi(\beta_{۱}) \subset \{(۰, y), (x, ۰)\}$ و
- $\beta_{۲} = \varphi$ یا برای یک $x, y > m$ داشته باشیم $\Pi(\beta_{۲}) = \{(x-m, y-۱), \ldots, (x-۱, y-m)\}$

در مقاله [۶] ثابت شده است که همهٔ ماتریدهای سه بخشی نمایش پذیرند و تمامی ساختارهای دسترسی سه بخشی وابسته ماتریدی، ایده‌آل هستند. به‌عنوان نتیجه می‌توان گفت که تمامی ساختارهای دسترسی دوبخشی وابسته ماتریدی نیز، ایده‌آل هستنند. با استفاده از قضیه ۳-۱ این نتیجه حاصل می‌شود:

قضیه ۵-۲: اگر Γ یک ساختار دسترسی دوبخشی غیرایده‌آل باشد آن‌گاه $\sigma(\Gamma) \geq ۳/۲$.

در [۱۵] کران‌های پایینی برای ساختارهای دسترسی با تنها ۵ سهام‌دار با استفاده از یک برنامه ریزی خطی ارائه شده است. کران‌های ارائه شده در [۱۵] در حالت کلی کران‌های دقیقی نیستند.

در ادامه برای یافتن $\kappa(\Gamma)$، پلی ماتریدهای وابسته به ساختارهای دسترسی دوبخشی را بررسی می‌کنیم. به‌منظور بررسی پلی‌ماتریدهای بهینه از روش برنامه‌ریزی خطی استفاده شده است. در ابتدا با استفاده از یک تبدیل، پلی‌ماتریدها را به‌صورت بردار نمایش می‌دهیم و سپس با استفاده از یک روش بهینه‌سازی 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 $\Gamma = \Gamma_{p_{\cdot}}(S)$ صدق کنند، پیدا می‌کنیم.

چنان‌که ثابت کردیم برای این منظور کافیست که فقط پلی‌ماتریدهای دوبخشی را در نظر بگیریم. این روش باعث کاهش چشمگیری در تعداد تساوی‌ها خواهد شد. چرا که اندازه بردار در مسئله برنامه‌ریزی خطی ما با استفاده از زوج (Ω, h') از $۲^{|P_{۱}|+|P_{۲}|+۲}$ به $۲|P_{۱}|۰|P_{۲}|۰۲$ کاهش خواهد یافت، که تاثیر به‌سزایی در کاهش میزان محاسبات دارد.

شیوهٔ 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 $\Pi(\Gamma_{\cdot}) = \{(x_{۱}, y_{۱}), \ldots (x_{r}, y_{r})\}$. مقادیر $N_{۱} = |X|$ و $N_{۲} = |Y|$ و مجموعه $\Omega = \{۰,۱,\ldots,N_{۱}\} \times \{۰,۱,\ldots,N_{۲}\} \times \{۰,۱\}$ را در نظر بگیرید. برای هر پلی‌ماترید دوبخشی S، زوج (Ω, h) را به‌صورتی که در بالا تعریف شده است فرض کنید. h را *تابع رتبه*[۱] پلی‌ماترید دوبخشی S می‌نامیم.

۱. Rank function

مقدار $N = ۲(N_۱ + ۱)(N_۲ + ۰)$ و بردار $\vec{s} = \big(h(x,y,z)\big)_{(x,y,z)\in\Omega} \in \Re^N$ را که عناصر آن همهٔ مقادیر تابع رتبه h را نشان می‌دهند، در نظر بگیرید. هر درایه $\vec{s}$ به‌وسیلهٔ یک بردار $(x,y,z)\in\Omega$ مشخص و اندیس‌گذاری می‌شود.

با استفاده از قضیه ۴-۳ فقط کافیست آن پلی‌ماتریدهای تقسیم راز دوبخشی S را در نظر بگیریم که $\Gamma = \Gamma_{p.}(S)$. از آن‌جاکه در هر ساختار دسترسی دوبخشی تمامی عناصر در یک بخش، نقش یک‌سانی را ایفا می‌کنند کافیست برای یک نماینده از بخش X مقدار $h(۱,۰,۰)$ و برای نماینده بخش Y مقدار $h(۰,۱,۰)$ را درنظر گرفته و در نهایت بزرگ‌ترین مقدار به‌دست آمده بین این دو را به‌عنوان $\kappa(S)$ در نظر بگیریم یعنی $\kappa(S)$ برابر است با $\max\{h(۱,۰,۰), h(۰,۱,۰)\}$. برای هر $(x,y,z)\in\Omega$ بردار $\vec{e}_{(x,y,z)} \in \Re^N$ را برداری با مؤلفهٔ ۱ برای مکان متناظر (x,y,z) و صفر در مکان‌های دیگر، تعریف می‌کنیم. برای هر زوج از بردارهای $\vec{x}$ و $\vec{y}$ می‌گوییم $\vec{x} \le \vec{y}$ است، اگر به‌ازای مؤلفه‌های i-ام به‌ترتیب x_i و y_i آن‌ها داشته باشیم $x_i \le y_i$.

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 بدین‌صورت بازنویسی می‌کنیم:

۱. خاصیت $h(\varphi) = ۰$ معادل است با

$$\vec{e}_{(.,.,.)} \times \vec{s}^T = ۰ \qquad (۱)$$

(که در آن منظور، ضرب داخلی دو بردار است).

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

$$[\vec{e}_{(x,y,z)} - \vec{e}_{(x',y',z')}] \times \vec{s}^T \le ۰.$$

حال ماتریس $A_۱$ را با سطرهای زیر در نظر بگیرید:

برای هر زوج $(x,y,z),(x',y',z') \in \Omega$ که $(x,y,z) \le (x',y',z')$ سطری از $A_۱$ را به‌صورت $\vec{e}_{(x,y,z)} - \vec{e}_{(x',y',z')}$ درنظر می‌گیریم. . بنا بر این خاصیت یکنوایی تابع رتبه h معادل است با نامساوی زیر:

$$A_۱ \times \vec{s}^T \le ۰ \qquad (۲)$$

۳. خاصیت زیرمدولی: برای هر $A, B \subset Q$ با $\Pi(A) = (x,y,z)$ و $\Pi(B) = (x',y',z')$ داریم $h(A) + h(B) \ge h(A \cup B) + h(A \cap B)$. در این حالت باید همهٔ مقادیر ممکن که $\Pi(A \cup B)$ و $\Pi(A \cap B)$ می‌توانند به‌خود بگیرند را در نظر بگیریم. اکنون برای هر زوج $(x,y,z),(x',y',z') \in \Omega$ این مقادیر را لحاظ کنید:

$l_x = \max\{۰, x + x' - N_۱\}$، $u_x = \min\{x, x'\}$، $l_y = \max\{۰, y + y' - N_۲\}$، $u_y = \min\{y, y'\}$،

$m_z = \min\{z, z'\}$ و $M_z = \max\{z, z'\}$. در نتیجه 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 $r_x \in \{l_x, l_x+۱, \ldots, u_x\}$ و $r_y \in \{l_y, l_y+1, \ldots, u_y\}$. توجه کنید که در این عملیات همه حالت‌های ممکن برای $\Pi(A \cup B)$ و $\Pi(A \cap B)$ در نظر گرفته شده است. اکنون ماتریس $A_۲$ را با در نظر گرفتن تمامی 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. از همین رو، خاصیت زیرمدولی تابع رتبه h معادل است با:

$$A_2\times\vec{s}^T\le 0. \qquad (۳)$$

۴. ساختار دسترسی: برای هر زیرمجموعه $A\subset Q$ تساوی $h(A\cup\{p_0\})=h(A)$ برقرار است، اگر A زیرمجموعه‌ای مجاز باشد و تساوی $h(A\cup\{p_0\})=h(A)+1$ برقرار است، اگر A یک زیر مجموعه غیرمجاز 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 $(a,b)\in\Pi(\Gamma_0)$ و

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

حال 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 آن‌جاکه این تفاضل، مقدار صفر یا ۱ را به خود می‌گیرد، ما یک بردار $\vec{b}$ را با مقدار صفر، به شرط $(x,y)\ge(a,b)$ به‌ازای $(a,b)\in\Pi(\Gamma_0)$ و ۱ در غیر این صورت بنا می‌کنیم. از این رو تساوی معادل، برابر است با:

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

همچنین به‌عنوان نتایجی از خواص (۱) تا (۴) شرط (۵) روی درایه‌های $\vec{s}$ به‌دست می‌آید.

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

از آن‌جاکه در یک پلی‌ماترید دوبخشی S داریم $\kappa(S)=\max\{h(1,0,0),h(0,1,0)\}$، بنا بر این برای نمایش مسئله به‌عنوان تابعی خطی در یک مسئله برنامه‌ریزی خطی، مسئله را به این دو بخش 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 به‌صورت جداگانه بررسی می‌کنیم. بدون کم شدن از کلیت مسئله فرض کنید که نامساوی اول برقرار باشد. از این رو، داریم $h(1,0,0)=\max\{h(1,0,0),h(0,1,0)\}$ بنا بر این این خاصیت را می‌توان به‌عنوان تابع خطی A_3 بدین‌صورت تبدیل کرد:

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

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 ماتریس A_3 به شکل متفاوتی به‌دست می‌آید.

خواص (۱) تا (۶)، ناحیهٔ محدب $U\subset\Re^N$ ایجاد می‌کند که آن را *ناحیهٔ شدنی*[1] بنامیم. بنا بر این هدف ما یافتن اینفیمم مقدار $\kappa(\Gamma)$ روی ناحیهٔ محدب U است که برای آن باید مقدار $h(1,0,0)=\vec{e}_{(1,0,0)}\times\vec{s}^T$ را، روی همهٔ $\vec{s}\in U$ کمینه[2] ساخت. ماتریس A از الحاق سطری ماتریس‌های A_2,A_1 و A_3 به‌دست می‌آید. $\vec{s}$ را برداری از متغیرها درنظر بگیرید. مسئلهٔ برنامه‌ریزی خطی که ما در نظر گرفته‌ایم بدین‌صورت است:

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

با شروط:

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

از آن‌جاکه ناحیه شدنی Uممکن است تهی باشد، از همین رو، یکی از دو حالت مسئلهٔ برنامه‌ریزی خطی داده شده با حالت‌های (الف) و (ب) ممکن است جواب نداشته باشد. اما این وضعیت نمی‌تواند به‌صورت همزمان برای هر دو حالت رخ دهد.

در حالتی که هر دو مسئلهٔ 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:

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

نتایج تجربی

برای پیاده‌سازی روش ارائه شده در قسمت قبل از نرم‌افزار بهینه‌سازی موزک[۳] در محیط متلب[۴] استفاده شده است. ورودی این برنامه دارای این سه پارامتر 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 ۷-۱: ساختار دسترسی Γ_s را روی مجموعه سهام‌داران $P = X \bigcup Y$ با نقاط مینیمال $\Pi(\Gamma_0) = \{(0, s), (1,1)\}$ و $1 \le N_1 = |X|$، $N_2 = |Y|$ 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 کردیم و خروجی زیر به‌دست آمد:

s	خروجی $\kappa(\Gamma_s)$
۳	۱/۵۰۰۰
۴	۱/۶۶۶۷
۵	۱/۷۵۰۰
۶	۱/۸۰۰۰
۷	۱/۸۳۳۳
۸	۱/۸۵۷۱
۹	۱/۸۷۵۰
۱۰	۱/۸۸۸۹
۱۱	۱/۹۰۰۰
۱۲	۱/۹۰۹۱
۱۳	۱/۹۱۶۷

که در آن ستون اول نمایش‌دهندهٔ مقدار s و ستون دوم نشان‌دهندهٔ مقادیر به‌دست آمده از اجرای برنامه در متلب® است. چنان‌که 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 [۱۳] در حالت خاص $N_1 = 1$ و $N_2 = s$ به‌دست آمده است. نتایج ما به‌دلیل به‌کار بردن مقادیر دیگر N_1 و N_2 کلی‌تر از نتایج به‌دست آمده تا کنون است. توجه کنید که مقادیر $\kappa(\Gamma_s)$ یک کران پایین روی پیچیدگی بهینه ساختارهای دسترسی به‌دست می‌دهد و داریم $\sigma(\Gamma_s) \ge \kappa(\Gamma_s) = \frac{2s-1}{s}$.

۱. Feasible region ۲. Minimize ۳. MOZEK® ۴. MATLAB®

مثال ۷-۲: در حالت کلی‌تر ساختار دسترسی $\Gamma^{۱}_{s,t}$ را روی مجموعه سهام‌داران $P = X \bigcup Y$ با نقاط مینیمال $\{(۰,s),(t,۱)\}$، $|X| = t$ و $|Y| = s$ را در نظر بگیرید. همچنین ساختار دسترسی $\Gamma^{۲}_{s,t}$ با نقاط مینیمال $\{(۱,s),(t,۱)\}$، $|X| = t$ و $|Y| = s$ مفروض است. تعدادی از خروجی‌های این ساختارهای دسترسی بدین‌صورت است:

s,t	خروجی $\kappa(\Gamma^{۲}_{s,t})$
۲،۳	۱/۵۰۰۰
۳،۳	۱/۵۰۰۰
۴،۳	۱/۶۶۶۷
۵،۳	۱/۷۵۰۰
۶،۳	۱/۸۰۰۰
۷،۳	۱/۸۳۳۳
۲،۴	۱/۶۶۶۷
۳،۴	۱/۶۶۶۷
۴،۴	۱/۶۶۶۷
۵،۴	۱/۷۵۰۰
۶،۴	۱/۸۰۰۰
۷،۴	۱/۸۳۳۳

s,t	خروجی $\kappa(\Gamma^{۱}_{s,t})$
۲،۳	۱/۵۰۰۰
۳،۳	۱/۵۰۰۰
۲،۴	۱/۶۶۶۷
۳،۴	۱/۶۶۶۷
۲،۵	۱/۷۵۰۰
۳،۵	۱/۷۵۰۰
۲،۶	۱/۸۰۰۰
۳،۶	۱/۸۰۰۰
۲،۷	۱/۸۳۳۳
۳،۷	۱/۸۳۳۳
۲،۸	۱/۸۵۷۱
۳،۸	۱/۸۵۷۱

توجه کنید که داریم $a = \max\{s, t-۱\} - ۱$. مقدار $\kappa(\Gamma^{۱}_{s,t})$ برای این مثال با تساوی $\kappa(\Gamma^{۱}_{s,t}) = \frac{۲a-۱}{a}$ به‌دست آمده است. از طرف دیگر مشاهده می‌کنید که ساختار دسترسی $\Gamma^{۲}_{s,t}$ مقادیر متفاوتی از κ برای ساختارهای دسترسی Γ_s و $\Gamma^{۱}_{s,t}$ به ما می‌دهد. حال اگر $a = \max\{s-۱, t-۱\}$ در نظر گرفته شود. مقدار $\kappa(\Gamma^{۲}_{s,t})$ برای این مثال از رابطه $\kappa(\Gamma^{۲}_{s,t}) = \frac{۲a-۱}{a}$ به‌دست می‌آید. توجه کنید که در این مثال ما فقط ساختارهایی با تعداد مینیمال از سهام‌داران را نسبت به نقاط مینیمال در هر بخش لحاظ کرده‌ایم.

مثال ۷-۳: اکنون ساختار دسترسی $\Gamma^{۳}_{r,s,t}$ را روی مجموعه سهام‌داران $P = X \bigcup Y$ با نقاط مینیمال $\{(۰,r),(۱,s),(۲,t)\}$ (که در آن به‌وضوح $r > s > t$ است)، $|X| = ۲$ و $|Y| = r$ را در نظر بگیرید. تعدادی از خروجی‌های این ساختار دسترسی بدین‌صورت است:

r,s,t	خروجی $\kappa(\Gamma^{۳}_{r,s,t})$
۲ ،۱ ،۰	۱/۰۰۰۰
۳ ،۱ ،۰	۱/۵۰۰۰
۴ ،۱ ،۰	۱/۶۶۶۷
۵ ،۱ ،۰	۱/۷۵۰۰
۳ ،۲ ،۰	۱/۰۰۰۰
۴ ،۲ ،۰	۱/۵۰۰۰
۵ ،۲ ،۰	۱/۶۶۶۷
۴ ،۳ ،۰	۱/۰۰۰۰
۵ ،۳ ،۰	۱/۵۰۰۰
۵ ،۴ ،۰	۱/۰۰۰۰
۳ ،۲ ،۱	۱/۰۰۰۰
۴ ،۲ ،۱	۱/۵۰۰۰
۵ ،۲ ،۱	۱/۶۶۶۷
۴ ،۳ ،۱	۱/۵۰۰۰
۴ ،۳ ،۲	۱/۰۰۰۰

توجه کنید که داریم $a=\max\{r-s,s-t\}$. مقدار κ برای این مثال با تساوی $\kappa(\Gamma^{۳}_{r,s,t})=\frac{۲a-۱}{a}$ به‌دست آمده است.

مثال ۷-۴: نهایتاً ساختار دسترسی $\Gamma^{٤}_{r,s,t}$ را روی مجموعه سهام‌داران $P=X\bigcup Y$ با نقاط مینیمال $\{(۱,r),(۳,s),(٤,t)\}$ (که در آن به‌وضوح $r>s>t$ است)، $|X|=٤$ و $|Y|=r$ را در نظر بگیرید. تعدادی از خروجی‌های این ساختار دسترسی بدین‌صورت است:

r,s,t	خروجی $\kappa(\Gamma^{۳}_{r,s,t})$
۲، ۱، ۰	۱/۵۰۰۰
۳، ۱، ۰	۱/۵۰۰۰
۴، ۱، ۰	۱/٦٦٦٧
۵، ۱، ۰	۱/۷۵۰۰
۶، ۱، ۰	۱/۸۰۰۰
۷، ۲، ۱	۱/۸۰۰۰
۷، ۳، ۱	۱/۸۵۷۱
۷، ۴، ۱	۲/۰۰۰۰
۷، ۵، ۱	۱/۹۵٤۵
۷، ۶، ۱	۱/۸۰۰۰

یادآوری می‌کنیم که نقاط مینیمال در این طرح برابر $\{(۱,r),(۳,s),(٤,t)\}$، $|X|=٤$ و $|Y|=r$ هستند. در نظر بگیرید $a=\max\{٤-۳,۳-۱,r-s,s-t\}$. بنابراین مقدار κ برای این مثال با تساوی $\kappa(\Gamma^{٤}_{r,s,t})=\frac{۲a-۱}{a}$ به‌دست آمده است.

طرح‌های جدید

نتایج به‌دست آمده در بخش قبل، کران‌های پایینی بر روی پیچیدگی بهینه ساختارهای دسترسی‌شان ایجاد کرد. به‌عنوان نمونه در مثال ۷-۱ نشان دادیم که اگر Γ_s یک ساختار دسترسی دوبخشی با زیرمجموعه‌های مینیمال $\Pi(\Gamma_s)=\{(۱,۱),(۰,s)\}$ باشد، آنگاه داریم $\sigma(\Gamma_s)\geq\kappa(\Gamma_s)=\frac{۲s-۱}{s}$.

اگرچه ما برای ساختارهای دسترسی مشخصی، مقدار پیچیدگی بهینه را محاسبه کردیم، اما با توجه به تعریف پیچیدگی ساختارهای دسترسی، برای ارائه کران بالای روی پیچیدگی کافیست یک طرح تقسیم راز مناسب ارائه دهیم. در ادامه برای ساختار دسترسی Γ_s یک طرح خطی Σ چنان ارائه می‌دهیم که $\sigma(\Sigma)=\frac{۲s-۱}{s}$.

فرض کنید که Γ_s یک ساختار دسترسی با زیرمجموعه‌های مینیمال $\{(۱,۱),(۰,s)\}$ باشد. در مقاله [۱۳] با استفاده از ساختار دسترسی ملکه و سربازان طرحی ارائه شده که در آن تعداد سهام‌داران هر بخش به‌ترتیب برابر با ۱ و s است. ما به‌روشی مشابه یک طرح برای مجموعه سهام‌داران $\{q_۱,\ldots,q_{N_۱}\}\bigcup\{p_۱,\ldots,p_s\}$ ارائه می‌دهیم که در آن همه سهام‌داران q_i هم ارزش ملکه و p_j ها همان سربازان هستند. در واقع ساختار دسترسی این طرح بدین‌صورت است:

$$\Gamma_s=\{\{q_i,p_j\}\,|\,۱\leq i\leq N_۱,۱\leq j\leq s\}\bigcup\{p_۱,\ldots,p_s\}.$$

نتایج این پژوهش، به‌دلیل به‌کار بردن مقادیر دیگر $N_۱$ و $N_۲$ کلی‌تر از نتایج به‌دست آمده در مقاله [۱۳] است.

طرح Σ را با ترکیب دو طرح خطی Σ_1 و Σ_2 که در زیر تعریف شده است بیان می‌کنیم. از هیچ یک از این دو طرح به تنهایی پیچیدگی بهینه مطلوب به‌دست نمی‌آید، بلکه یک میانگین وزنی مناسبی از دو طرح Σ_1 و Σ_2، به طرح مطلوب می‌رسیم.

در هر دو طرح Σ_1 و Σ_2 راز k از میدان متناهی Z_q انتخاب شده است که در آن $q > s + N_1$. بدون کم شدن از کلیت مسئله فرض کنید که راز با یک توزیع یکنواخت انتخاب شده است. طرح Σ_1 را $(s, s+N_1)$-طرح آستانه‌ای شامیر با مقدار آستانه‌ای s در نظر بگیرید. مقادیر $x_1,\ldots,x_{s+N_1-1}$ را عناصر متمایز در Z_q و f را یک چند جمله‌ای از درجهٔ حداکثر $s-1$ درنظر بگیرید به‌طوری‌که $f(x_0)=k$ شود. در واقع تابع $f(x)$ همان چندجمله‌ای طرح آستانه‌ای شامیر است [۱۸]. هر سهام‌دار q_i در بخش اول سهم $(f(x_1),\ldots,f(x_{s-1}))$ و هر سرباز p_j در بخش دوم سهم $f(x_{j+s-1})$ را دریافت می‌کند. با ساختار مذکور ملاحظه می‌کنید که هرگاه از هر بخش حداقل یک عضو حاضر شوند آن‌ها قادر به بازسازی راز k خواهند بود. در واقع Σ_1 یک طرح تقسیم راز بر روی ساختار دسترسی Γ_s است. به‌راحتی می‌توان بررسی کرد که یک زیر مجموعه غیرمجاز از سهام‌داران با استفاده از Σ_1-سهم‌های خود هیچ اطلاعاتی راجع به راز k نخواهند یافت.

طرح دوم Σ_2 با استفاده از یک $(2,2)$- طرح آستانه‌ای خطی و نیز یک (s,s)-طرح آستانه‌ای خطی بدین‌صورت ساخته می‌شود. در $(2,2)$- طرح آستانه‌ای، مقدار تصادفی $r \in Z_q$ را در بین تمامی سهام‌داران q_i بخش اول، و مقدار $k-r$ (به پیمانهٔ q) را در میان تمامی سربازان p_j بخش دوم توزیع می‌کنیم. در (s,s)-طرح آستانه‌ای تنها به سربازان بخش دوم سهم تعلق می‌گیرد. در حقیقت به $s-1$ سرباز اول، r_j مقدار تصادفی دلخواه به‌ازای $1 \le j \le s-1$ و به سرباز sام مقدار $k-\sum_{j=1}^{s-1} r_j$ (به پیمانهٔ q) اختصاص می‌یابد. در طرح Σ_2 سهم سهام‌داران q_i تنها از $(2,2)$- طرح آستانه‌ای به‌دست می‌آید. هر زیرمجموعه مجاز از Γ_s با کمک یکی از دو طرح آستانه‌ای خطی فوق قادر به بازسازی راز k خواهد بود. به‌راحتی می‌توان بررسی کرد که یک زیر مجموعه غیرمجاز در طرح Σ_2 هیچ اطلاعاتی راجع به راز k نخواهند یافت.

اکنون می‌توان طرح Σ را با ترکیب دو طرح Σ_1 و Σ_2 بیان کرد. فرض کنید تصمیم داریم sتا راز از Z_q را در بین سهام‌داران توزیع نماییم. به این منظور کافیست یکی از رازها را با طرح Σ_1 و $s-1$تا راز دیگر را با Σ_2 توزیع کنیم. قضیه بعدی نشان خواهد داد که Σ همان طرح خطی بهینه است.

قضیه ۸-۱: اگر Σ طرح تقسیم راز ارائه شده با روش فوق باشد آن‌گاه داریم: $\sigma(\Sigma) = \frac{2s-1}{s}$

اثبات: Σ- سهم q_i ها در طرح Σ_1 برابر $s-1$ سهم و در طرح Σ_2 نیز برابر است با $s-1$ سهم است از همین رو، در مجموع به هر یک از سهام‌داران q_i به تعداد $2s-2$ سهم تعلق می‌گیرد. این در حالی است که Σ- سهم p_j ها در طرح Σ_1 برابر ۱ سهم و در طرح Σ_2 برابر است با $2(s-1)$، از این رو در مجموع به هر یک از سهام‌داران p_j به تعداد $2s-1$ سهم تعلق می‌گیرد. برای توزیع sتا راز در بین مجموعه سهام‌داران $\{q_1,\ldots,q_{N_1}\} \cup \{p_1,\ldots,p_s\}$ حداکثر $2s-1$ سهم به سهام‌داران اختصاص داده خواهد شد و این حکم را ثابت می‌کند.

۱. Feasible region ۲. Minimize

با توجه به آنکه پیچیدگی بهینه Γ_s، اینفیمم پیچیدگی‌ها روی تمامی طرح‌های تعریف شده برای ساختار دسترسی Γ_s است لذا $\sigma(\Gamma_s) \le \sigma(\Sigma) = \frac{2s-1}{s}$ و با توجه به کران پایین ارائه شده در مثال ۷-۱ قضیه زیر به‌راحتی نتیجه می‌شود.

قضیه ۸-۲: اگر Γ_s یک ساختار دسترسی دوبخشی با زیرمجموعه‌های مینیمال $\Pi(\Gamma_s) = \{(1,1),(0,s)\}$ باشد، آنگاه داریم: $\sigma(\Gamma_s) = \frac{2s-1}{s}$.

نتیجه‌گیری

در این مقاله ارتباط بین $\sigma(\Gamma)$ یک ساختار دسترسی دوبخشی با پارامترهای $\kappa(\Gamma)$ و $\lambda(\Gamma)$ آن بررسی 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 کرد که تاکنون ناشناخته بوده است. به‌علاوه این روش را می‌توان برای بررسی ساختارهای دسترسی چند بخشی با بیش از دو بخش نیز تعمیم داد.

منابع

1. A. Beimel, N. Livne, C. Padro, "Matroids Can Be Far From Ideal Secret Sharing", Theory of Cryptography Conference, TCC 2008. Lecture Notes in Comput. Sci., 4948 (2008) 194-212.
2. G. R. Blakley, "Safeguarding cryptographic keys", AFIPS Conference Proceedings., 48 (1979) 313-317.
3. E. F. Brickell, "Some ideal secret sharing schemes", J. Combin. Math. and Combin. Comput, 9 (1989) 105-113.
4. E. F. Brickell, D. M. Davenport, "On the classification of ideal secret sharing schemes", J. Cryptology, 4(1991) 123-134.
5. L. Csirmaz, "The size of a share must be large", J. Cryptology, 10 (1997) 223-231.
6. O. Farras, J. Marti–Farre, C. Padro, "Ideal Multipartite Secret Sharing Schemes", Advances in Cryptology, EUROCRYPT 2007 LectureNotes in Comput. Sci., 4515 (2007) 448-465.
7. O. Farras, J. R. Metcalf-Burton, C. Padro, L. Vázquez, "On the optimization of bipartite secret sharing schemes", Des. Codes Cryptogr. 63(2012) 255-271.
8. S. Fujishige, “Polymatroidal Dependence Structure of a Set of Random Variables,” Information and Control, 39(1978) 55–72.

9. J. Herzog, T. Hibi, "Discrete polymatroids", J. Algebraic Combin., 16(2002) 239-268.
10. M. Ito, A. Saito, T. Nishizeki, "Secret sharing scheme realizing any access structure", Proc. IEEE Globecom' 87(1987) 99-102.
11. A. Lehman, "A solution of the Shannon switching game", J. Soc. Indust. Appl. Math., 12 (1964) 687-725.
12. J. Martı-Farre, C. Padro, "On Secret Sharing Schemes, Matroids and Polymatroids", Fourth IACR Theory of Cryptography Conference TCC 2007, Lecture Notes in Comput. Sci., 4392 (2007) 273-290.
13. J. R. Metcalf-Burton, "Information Rates of Minimal Non-Matroid-Related Access Structures", arxiv.org/pdf/0801.3642.
14. C. Padro, G. Saez, "Secret sharing schemes with bipartite access structure", IEEE Trans. Inform. Theory, 46 (2000) 2596-2604.
15. C. Padro, L. Vázquez, A. Yang, "Finding lower bounds on the complexity of secret sharing schemes by linear programming", Discrete Applied Mathematics, 161 (2013) 1072-1084.
16. P. D. Seymour, "A forbidden minor characterization of matroid ports", Quart. J. Math. Oxford Ser., 27 (1976) 407-413.
17. P. D. Seymour, "On secret- sharing matroids", J. Combin. Theory Ser. B, 56 (1992) 69-73.
18. A. Shamir, "How to share a secret", Commun. of the ACM, 22 (1979) 612-613.
19. C. E. Shannon, "A Mathematical Theory of Communication", Bell. Sys. Tech. Journal, 27 (1948).
20. D. R. Stinson, "Decomposition constructions for secret-sharing schemes", IEEE Transactions on Information Theory, 40 (1994) 118-125.
21. R. W. Yeung, "A framework for linear information inequalities", IEEE Trans. Inform. Theory, IT-41 (1995) 412-422.