دانشکده علوم ریاضی

گروه ریاضی کاربردی

پایان‌نامه

برای دریافت درجه کارشناسی ارشد در رشته
ریاضی کاربردی، گرایش گراف و ترکیبیات

عنوان

کدهای ضدجعل امن

استاد راهنما

دکتر میثم علیشاهی

استاد مشاور

آقای سیدرضا موسوی

پژوهشگر

زینب منتظری

شهریور ۱۳۹۲

نام خانوادگی دانشجو: منتظری نام: زینب

عنوان: کدهای ضدجعل امن

استاد راهنما: دکتر میثم علیشاهی
استاد مشاور: آقای سیدرضا موسوی

مقطع تحصیلی: کارشناسی ارشد رشته: ریاضی کاربردی گرایش: گراف و ترکیبیات

دانشگاه: دانشگاه صنعتی شاهرود دانشکده علوم ریاضی
تاریخ فارغ‌التحصیلی: شهریور ۱۳۹۲ تعداد صفحات: ۸۳

واژگان کلیدی: کد ضدجعل،کد ضدجعل امن

چکیده

در این پایان‌نامه ابتدا کدهای ضدجعل و کدهای ضدجعل امن را به‌عنوان مفاهیم اصلی تعریف کرده، سپس به دنبال روش‌هایی برای ساخت این کدها خواهیم بود. برای این منظور مجموعه‌های مختلفی از جمله خانواده‌های بدون پوشش، خانواده‌های آزاد، خانواده‌های درهم جداساز، خانواده‌های درهم‌ساز کامل و ... را ارائه می‌دهیم و چگونگی ساخت کدهای ضدجعل به کمک این خانواده‌ها را بیان می‌کنیم. هدف اصلی یافتن کدهای ضدجعل امن به بزرگی ممکن است. بنابراین تعدادی کران برای کدهای یادشده ارائه خواهیم داد. در پایان طرح‌های قابل ردیابی را که ارتباط بسیاری با کدهای ضدجعل دارند، معرفی می‌کنیم.

تقدیم به پدر و مادرم

که از نگاهشان، صلابت

از رفتارشان، محبت

و از صبرشان، ایستادگی را آموختم.

الهی...

اندیشه‌ام را در مسیری معنوی و روحانی قرار ده، تا روحم را با تو درآمیزم و لذت با تو بودن را در لحظه لحظه‌ی زندگی‌ام دریابم.

ای خالق بی‌مدد و ای واحد بی‌عدد، ای اول بی‌بدایت و ای آخر بی‌نهایت. ای ظاهر بی‌صورت و ای باطن بی‌سیرت، ای حی بی‌ذلت و ای بخشنده بی‌منت، ای داننده رازها، ای شنونده آوازها، ای رساننده گام‌ها، ای مطلع بر حقایق، ای مهربان بر خلایق، عذرهای ما بپذیر که تو غنی و ما فقیر و بر عیب‌های ما مگیر که تو قوی و ما حقیر، از بنده خطا آید و ذلت و از تو عطا آید و رحمت.

سپاس گزاری...

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت‌های او ندانند و کوشندگان، حق او را گزاردن نتوانند و سلام و درود بر پیامبر صدق و راستی، حضرت محمد(ص) و خاندان پاک ایشان.

اکنون که با لطف بی منتهای ایزد منان، مرحله ای دیگر از دوران تحصیل را به پایان می‌رسانم، فرصت را مغتنم شمرده و از خانواده مهربانم که موفقیت‌های خویش را وامدار فداکاری ایشان می‌دانم، سپاس‌گزاری می‌نمایم.

همچنین از استاد راهنمای گرامی و بزرگوارم جناب آقای دکتر علیشاهی که در تمام مراحل پایان‌نامه با دقت و ژرف نگری، متانت، صبر و شکیبایی راهنماییم نمودند خالصانه تشکر و قدردانی می‌نمایم. بی‌شک بدون راهنمایی‌های ارزشمند و حمایت ایشان، تکمیل این پایان‌نامه ممکن نبود.

در پایان، از جناب آقای موسوی و آقای دکتر جعفری راد و آقای دکتر شعبانی نیز کمال تشکر را دارم.

زینب منظری

شهریور ۱۳۹۲

پیشگفتار

در دنیای پیشرفته امروز، شاهد این هستیم که تولیدکنندگان محصولات مختلف، روی هر محصول بارکد منحصر به فردی را قرارداده‌اند. این برچسب‌ها در واقع شناسنامه‌ی محصول می‌باشند و بیان‌گر بسیاری از اطلاعات هستند که در نگاه اول به‌نظر نمی‌رسد. برای مثال یک شرکت معروف تولیدکننده‌ی گوشی تلفن همراه را بررسی می‌کنیم. محصولات این شرکت در عین حال که اختلافات بسیاری باهم دارند اما مشخصه‌های مشترکی نیز دارند. برای مثال ممکن است دکمه روشن و خاموش کردن همه‌ی این گوشی‌ها به‌صورت مشترک در قسمت فوقانی گوشی قرار گرفته باشد و یا شارژر همه‌ی گوشی‌های تولید شده توسط این شرکت یکسان باشد. اما ممکن است رنگ این محصولات بین چند رنگ خاص متفاوت باشد و شباهت‌ها و تفاوت‌هایی از این قبیل داشته باشند. حال فرض کنید یک شرکت متقلب سودجو قصد جعل محصولات شرکت مذکور را داشته باشد. یعنی گوشی تلفن همراه تولید کند و با نام تجاری شرکت قبلی در بازار ارائه کند. لذا با یک بررسی ساده، در می‌یابد که باید ویژگی‌های مربوط به شرکت اصلی را رعایت کند که با نگاه اولیه، خریدار به جعلی بودن محصول پی نبرد. همان‌طور که اشاره شد بارکد هر محصول به نوعی مشخصات محصول را دربر دارند. برای مثال اگر اولین عدد بارکد را رنگ دستگاه درنظر گرفته باشند و رنگ مشکی را با عدد ۰، سفید را با عدد ۱ و قرمز را با عدد ۲ مشخص کنند، در صورتی که همه تولیدات شرکت اصلی رنگ ثابت مشکی داشته باشند باید بارکد همه محصولات با عدد ۱ شروع شود و اگر از هر سه رنگ، محصول تولید می‌شود این عدد بین ۰، ۱ و ۲ متغیر است. با توجه به این توضیحات، از این پس فقط بارکدهای محصولات اصلی و جعلی را مدنظر قرار می‌دهیم. پس شرکت جاعل مجبور است برای محصولات جعلی خود بارکد جعلی تولید کند. لذا برای جلوگیری از جعل محصولات باید بارکدها به نحوی طراحی شوند که نتوانند آن‌ها را جعل کنند و یا در صورت جعل، به راحتی به جعلی بودن آن پی برده شود. همچنین مجموعه جاعلین شناخته شوند و قابل پی‌گیری باشند. برای این منظور کدهای ضدجعل و کدهای ضدجعل امن را معرفی می‌کنیم و از کدواژه‌های این کدها به عنوان بارکد برای محصولات استفاده میکنیم. ویژگی کدهای ضدجعل این‌گونه است که از روی تعداد مشخصی کدواژه، نمی‌توان یک کدواژه معتبر تولید کرد. به‌عبارت دیگر جعل یک کدواژه اصلی از روی تعداد (مشخص) دیگری کدواژه اصل، مقدور نیست. برای مثال اگر شرکت جاعل تعداد مشخصی از محصولات شرکت اصلی را تهیه کند و با حفظ ویژگی های مشترک اقدام به جعل محصول جدید کند، جعلی بودن آن محصول مشهود خواهد بود و همچنین جهت شناسایی محصولات اصلی که مورد سوء استفاده قرار گرفته‌اند نیز، می‌توان پیگیری‌هایی انجام داد. کدهای ضدجعل امن علاوه بر ویژگی فوق این امکان را به ما می‌دهد که برای پی‌گیری محصولات مورد سوء استفاده اقدامات بیشتری انجام

دهیم. فرض کنید بارکد هر محصول را به خریدار آن نسبت دهیم و به هر خریدار عنوان کاربر آن مجموعه را اطلاق کنیم. لذا کاربرانی که محصول خود را در خدمت جاعلان قرار می‌دهند، خیانت‌کار محسوب شده و برای ما اهمیت دارد که بتوانیم گروه خائنین را شناسایی کنیم. به همین جهت کدهای ضدجعل امن مطلوب‌تر هستند. از طرفی اندازه این کدها حائز اهمیت است و بدیهی است که به‌دنبال این کدها به بزرگی ممکن هستیم تا بتوانیم با گسترش تولیدات نیز از کدواژه‌های آن برای پوشش محصولات استفاده کنیم.

در فصل اول این پایان‌نامه ابتدا پیشینه تاریخی تحقیق پیش‌رو را ذکر می‌کنیم و سپس به معرفی کدهای ضدجعل و کدهای ضدجعل امن می‌پردازیم. نحوه‌ی عملکرد این کدها را شرح می‌دهیم و قابلیت ردیابی آن‌ها را مورد مطالعه قرار می‌دهیم.

در فصل دوم، تعاریف ترکیبی از کدهای ضدجعل و ضدجعل امن ارائه می‌دهیم. خانواده‌ها و مجموعه‌های جدیدی از قبیل خانواده‌های بدون پوشش، خانواده‌های آزاد، خانواده‌های درهم‌ساز کامل، خانواده‌های درهم جداساز، سیستم‌های جداساز، سیستم‌های منفصل و ... را شرح می‌دهیم و ارتباط آن‌ها را با کدهای مورد نظر بیان می‌کنیم.

در فصل سوم در صدد ساخت این کدها بر می‌آییم. انواع گوناگون کدهای ضدجعل و ضدجعل امن با پارامترهای مختلف را مورد بررسی قرار می‌دهیم و برای ساخت آن‌ها از مفاهیم ارئه شده در فصل دوم بهره می‌گیریم.

در فصل چهارم باتوجه به نحوه ساخت کدهای یادشده، اندازه آن‌ها (تعداد کدواژه‌هایشان) را بررسی می‌کنیم و کران بالا یا پایین آن‌ها را یافته و دقت هر کران را مورد ارزیابی قرار می‌دهیم.

در فصل پنجم مفهومی شبیه کدهای ضدجعل امن تحت عنوان طرح‌های قابل ردیابی ارائه می‌دهیم و ارتباط آن با کدهای ضدجعل را شرح می‌دهیم.

فهرست مطالب

فصل ۱
مقدمه و تاریخچه

کدهای ضدجعل[۱] اولین بار توسط بانه[۲] و شو[۳] در سال ۱۹۹۵ به عنوان یک روش از اثر انگشت دیجیتالی ارائه شد که نمی‌گذارد یک ائتلاف با حداکثر c عضو، کاربری خارج از ائتلاف خود را جعل کند. در سال ۱۹۹۸ استینسون[۴] و وی[۵] از روشهای ترکیبیاتی برای تحقیقات بیشتر روی کدهای ضدجعل استفاده کردند. ساختارهای متفاوتی از کدهای ضدجعل توسط بانه و شو در سال ۱۹۹۵ و چی[۶]درسال ۱۹۹۶ و استینسون و وی در سال ۱۹۹۸ ارائه شده است.

برای محافظت از محصولاتی از قبیل داده‌های دیجیتالی، نرم افزارهای کامپیوتری و... از کدهای ضدجعل استفاده می‌کنیم. به این صورت که توزیع کننده محصولات، هر محصول را توسط یکی از این کدواژه‌ها برچسب دهی می‌کند. این برچسب‌دهی برای توزیع کننده این امکان را فراهم می‌کند که بر چسب‌های غیر مجاز (و در نتیجه محصولات جعلی) را شناسایی کرده و کاربران جاعل را ردیابی کند. این امر کاربران را از انتشار یک کپی نامعتبر (جعلی) باز می‌دارد. اگرچه، یک ائتلاف ممکن است بتواند از روی مؤلفه‌های اعضایش، کدواژهای معتبری را بسازد و توزیع کننده نتواند کپی غیرقانونی را ردیابی کند. جهت محافظت در برابر چنین موضوعی تلاش می‌کنیم تا بتوانیم ساختار کدی (**کد ضدجعل امن**[۷]) را ارائه دهیم که در

[۱] frameproof codes
[۲] Boneh
[۳] Shaw
[۴] Stinson
[۵] Wei
[۶] Chee
[۷] secure frameproof code

آن بتوان برای یک کپی غیر قانونی داده شده، حداقل یکی از کاربران جاعل را پیدا کرد. در این تحقیق ما به‌دنبال یافتن کدهای مطلوب به بزرگی ممکن با خواص ذکر شده هستیم. برای این منظور احتیاج به معرفی مفاهیمی داریم که در ذیل به تعاریف آن‌ها می‌پردازیم.

۱.۱ کدهای ضدجعل

فرض کنید v و b اعداد صحیح مثبت باشند (b تعداد کاربران در این طرح را مشخص می‌کند). مجموعه‌ی $\Gamma = \{w^{(1)}, w^{(2)}, \cdots, w^{(b)}\} \subseteq \{0,1\}^v$ یک **(b و v)-کد** نام دارد و هر $w^{(i)}$ یک **کدواژه**[۸] است (برای هر $1 \leq i \leq b$، کدواژه‌ی $w^{(i)}$ مشخص کننده کاربر i-ام است). یک **v-تایی** دودویی $x \in \{0,1\}^v \backslash \Gamma$ را یک **کلمه ثبت نشده** [۹] می‌نامیم. برای کد Γ، **ماتریس وقوع**[۱۰] $M(\Gamma)$ یک ماتریس $b \times v$ خواهد بود که سطرهای آن کدواژه‌های Γ هستند.

فرض کنید Γ یک (b و v)-کد باشد. همچنین فرض کنید $C = \{w^{(u_1)}, \cdots, w^{(u_d)}\} \subseteq \Gamma$ است. مؤلفه i-ام ($i \in \{1, \ldots, v\}$) را برای C **غیر قابل کشف**[۱۱] گوییم، اگر:

$$w_i^{(u_1)} = w_i^{(u_2)} = \cdots = w_i^{(u_d)}.$$

فرض کنید $U(C)$ مجموعه‌ی مؤلفه‌های غیر قابل کشف C باشد، آن‌گاه:

$$F(C) = \{x \in \{0,1\}^v : x|_{U(C)} = w^{(u_i)}|_{U(C)} \quad \text{برای همه } w^{(u_i)} \in C \}$$

مجموعه شدنی[۱۲] C نام دارد. این مجموعه شامل تمام v-تایی های ممکن است که از ائتلاف C با مقایسه‌ی d کدواژه و ثابت نگه‌داشتن مؤلفه‌های مشترک به‌دست می‌آیند. واضح است که برای هر C، $C \subseteq F(C)$ است و اگر $|C| = 1$، آن‌گاه $F(C) = C$.

حال فرض کنید کدواژه $w^{(j)} \in F(C) \setminus C$ وجود داشته باشد، آن‌گاه اگر ائتلاف C، v-تایی $w^{(j)}$ را تولید کند، کاربر j-ام جعل شده است.

---

[۸] codeword
[۹] unregistered word
[۱۰] incidence matrix
[۱۱] undetectable
[۱۲] feasible set

تعریف ۱.۱. [۳۵] یک (v,b)-کد Γ یک c-کد ضدجعل نام دارد اگر برای هر $C \subseteq \Gamma$ به‌طوری‌که $|C| \leq c$، داشته باشیم $F(C) \cap \Gamma = C$. در این صورت به اختصار Γ را یک $c - FPC(v,b)$ می‌نامیم.

بنابراین در یک c-کد ضدجعل، کدواژه‌های درون مجموعه‌ی شدنی هر ائتلاف با حداکثر c عضو، فقط اعضای خود ائتلاف می‌باشد. از این‌رو هیچ ائتلافی با حداکثر c عضو، نمی‌تواند کاربر خارج از خودش را جعل کند.

مثال ۱.۱. [۸] برای هر عددصحیح مثبت b یک $b - FPC(b,b)$ وجود دارد که ماتریس وقوع آن ماتریس همانی $b \times b$ است.

در حالت کلی، ما به ساختن یک $c - FPC(v,b)$ با بزرگ‌ترین b ممکن (به‌عنوان تابعی از c و v) علاقه‌مندیم.

۲.۱ قابلیت ردیابی کدهای ضدجعل

فرض کنید Γ یک $c - FPC(c,v)$ باشد. برای هر $x \in \{0,1\}^v$، قرار دهید:

$$F^{-1}(x) = \{C \subseteq \Gamma : |C| \leq c \quad و \quad x \in F(C)\}.$$

واضح است که $F^{-1}(x)$ همه‌ی ائتلاف‌های حداکثر c عضوی که x را می‌سازند، شامل می‌شود.

فرض کنید $x \in \{0,1\}^v \setminus \Gamma$ (به این معنی که x یک کلمه ثبت نشده است). اگر $|F^{-1}(x)| = 1$، آن‌گاه $C \subseteq \Gamma$ چنان وجود دارد که $F^{-1}(x) = \{C\}$، لذا نتیجه می‌گیریم که C همان ائتلافی بوده که x را تولید کرده است. درحالت کلی‌تر، اگر $F^{-1}(x) \neq \emptyset$ و کدواژه‌ی $w^{(j)}$ وجود داشته باشد به‌طوری‌که برای هر $C \in F^{-1}(x)$ داشته باشیم $w^{(j)} \in C$، آن‌گاه حداقل می‌توانیم دریابیم که کاربر j-ام مجرم است. متأسفانه این اتفاق برای تعداد کاربر زیاد دست نیافتنی است که در قضیه زیر آن را نشان می‌دهیم.

قضیه ۱.۱. [۳۵] *فرض کنید Γ یک $c - FPC(v,b)$ و $b \geq 2c - 1$ باشد. فرض کنید $D \subseteq \Gamma$ و $|D| = 2c - 1$. آن‌گاه کلمه ثبت نشده $maj(D) \in \{0,1\}^v$ وجود دارد به‌طوری‌که برای هر $C \subseteq D$ که $|C| = c$، داریم $maj(D) \in F(C)$.*

برهان. قرار دهید $D = \{w^{(u_1)}, w^{(u_2)}, ..., w^{(u_{2c-1})}\}$. برای $1 \leq i \leq v$، تعریف کنید:

$$maj(D)_i = \begin{cases} 1 & |\{j : w_i^{(u_j)} = 1\}| \geq c, \\ 0 & |\{j : w_i^{(u_j)} = 0\}| \geq c. \end{cases}$$

به‌وضوح برای هر $C \subseteq D$ با شرط $|C| = c$ داریم، $maj(D) \in F(C)$. لذا کافی است نشان دهیم که $maj(D)$ یک کلمه ثبت نشده است. فرض کنید چنین نباشد، یعنی $maj(D)$ یک کلمه معتبر یا به عبارت دیگر یک کدواژه باشد. لذا u چنان وجود دارد که $maj(D) = w^{(u)}$. قرار دهید $C \subseteq D \setminus \{w^{(u)}\}$ که $|C| = c$. بنابراین $w^{(u)} \in F(C) \cap \Gamma$ و این با $c - FPC(v, b)$ بودن Γ تناقض دارد، لذا حکم برقرار است. □

قضیه بالا بیان می‌کند که در یک $c - FPC(v, b)$ ضمانتی برای پیدا کردن یک کاربر مجرم نیست. زیرا، اگر برای یک D با $|D| = 2c - 1$، $x = maj(D)$، آن‌گاه:

$$\bigcap_{C \in F^{-1}(x)} C = \emptyset.$$

بنابراین ما مجبوریم حالت محدودتری را در نظر بگیریم.

۳.۱ کدهای ضدجعل امن

تعریف ۲.۱. [۳۵] فرض کنید Γ یک (v, b)-کد باشد. می‌گوییم Γ یک c-کدضد جعل امن است، اگر برای هر $C_1, C_2 \subseteq \Gamma$ که $|C_1| \leq c$، $|C_2| \leq c$ و $C_1 \cap C_2 = \emptyset$، داشته‌باشیم $F(C_1) \cap F(C_2) = \emptyset$. در این صورت به‌اختصار Γ را $c - SFPC(v, b)$ می‌نامیم.

مثال ۲.۱. فرض کنید ماتریس زیر، ماتریس وقوع یک $(3, 4)$-کد باشد:

$$M(\Gamma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

نشان می‌دهیم که Γ یک $2 - SFPC(3, 4)$ است. برای این منظور $F(C)$ را برای هر $C \subseteq \Gamma$ که $|C| = 2$، محاسبه می‌کنیم.

$$F(\{w^{(1)}, w^{(2)}\}) = \{100, 010, 110, 000\},$$

$$F(\{w^{(۱)}, w^{(۳)}\}) = \{۱۰۰, ۰۰۱, ۱۰۱, ۰۰۰\},$$

$$F(\{w^{(۱)}, w^{(۴)}\}) = \{۱۰۰, ۱۱۱, ۱۰۱, ۱۱۰\},$$

$$F(\{w^{(۲)}, w^{(۳)}\}) = \{۰۱۰, ۰۰۱, ۰۰۰, ۰۱۱\},$$

$$F(\{w^{(۲)}, w^{(۴)}\}) = \{۰۱۰, ۱۱۱, ۰۱۱, ۱۱۰\}$$

و

$$F(\{w^{(۳)}, w^{(۴)}\}) = \{۰۰۱, ۱۱۱, ۰۱۱, ۱۰۱\}.$$

و با یک بررسی ساده می‌بینیم که:

$$F(\{w^{(۱)}, w^{(۲)}\}) \cap F(\{w^{(۳)}, w^{(۴)}\}) = \emptyset,$$

$$F(\{w^{(۱)}, w^{(۳)}\}) \cap F(\{w^{(۲)}, w^{(۴)}\}) = \emptyset$$

و

$$F(\{w^{(۱)}, w^{(۴)}\}) \cap F(\{w^{(۲)}, w^{(۳)}\}) = \emptyset.$$

لذا Γ یک $۲ - SFPC(۳, ۴)$ است.

قضیه ۲.۱. [۳۵] *هر $c - SFPC(v, b)$، یک $c - FPC(v, b)$ است.*

برهان. فرض کنید Γ یک $c - SFPC(v, b)$ باشد، اما یک $c - FPC(v, b)$ نباشد. بنابراین مجموعه‌ی $C \subseteq \Gamma$ و کدواژه‌ی $w^{(j)}$ وجود دارند، به‌طوری‌که $|C| \leq c$ و $w^{(j)} \in F(C) \setminus C$. قرار می‌دهیم $C_۱ = C$ و $C_۲ = \{w^{(j)}\}$. لذا خواهیم داشت:

$$|C_۱| \leq c \ , \ |C_۲| \leq c \ , \ C_۱ \cap C_۲ = \emptyset \text{ و } F(C_۱) \cap F(C_۲) = \{w^{(j)}\} \neq \emptyset.$$

که این با $c - SFPC(v, b)$ بودن Γ تناقض دارد. لذا حکم برقرار است. □

۴.۱ قابلیت ردیابی کدهای ضدجعل امن

یک $c - SFPC(v,b)$ اجازه‌ی ردیابی نمی‌دهد اما تا حدی امنیت ایجاد می‌کند به این صورت که:

- ائتلاف $C_۱$ با حداکثر c عضو، نمی‌تواند ادعا کند که، ائتلاف مجزای $C_۲$ با حداکثر c عضو، در ساخت یک کلمه ثبت نشده $x \in F(C_۱)$ شراکت داشته است.
- اگر x یک کلمه ثبت نشده باشد که توسط یک ائتلاف حداکثر c عضوی ساخته شده باشد، آن‌گاه هر $C \in F^{-۱}(x)$ شامل حداقل یک کاربر مجرم است.

اکنون $۲ - SFPC(v,b)$ را با جزئیات بیشتری بررسی می‌کنیم:

فرض کنید Γ یک $۲ - SFPC(v,b)$، x یک کلمه ثبت نشده و $C \in F^{-۱}(x)$ باشد. چون x یک کلمه ثبت نشده است، لذا داریم $|C| \neq ۱$. از طرفی چون Γیک $۲ - SFPC(v,b)$ است و با توجه به تعریف $F^{-۱}(x)$، داریم $|C| \leq ۲$، بنابراین $|C| = ۲$.

پس $F^{-۱}(x)$ مجموعه ای از زیرمجموعه‌های دو عضوی Γ است، لذا می‌توانیم آن رامجموعه‌ای از یال‌های یک گراف روی اعضای Γ (به‌عنوان رئوس گراف) در نظر بگیریم. چون Γ یک $۲ - SFPC(v,b)$ است، هر دو یال در $F^{-۱}(x)$ مجاور هستند. از این‌رو به راحتی در می‌یابیم که حتما یکی از دو حالت زیر رخ خواهد داد:

۱. $F^{-۱}(x)$ یک گراف ستاره‌ای است. (به این معنی که همه‌ی یال‌های آن در یک رأس مشترک می‌باشند).

۲. $F^{-۱}(x)$ همریخت با $K_۳$ است (یک گراف کامل ۳ رأسی است).

با توجه به صفات اختصاصی $F^{-۱}(x)$ در حالت $c = ۲$، به نتیجه‌ی زیر می‌رسیم:

قضیه ۳.۱. [۳۵] *فرض کنید Γ یک $۲ - SFPC(v,b)$ و x یک کلمه ثبت نشده، توسط یک ائتلاف حداکثر دوعضوی ساخته شده باشد. آن‌گاه یکی از دو حالت زیر حتما اتفاق می‌افتد:*

۱. *حداقل یک کاربر مجرم قابل شناسایی است.*

۲. *یک مجموعه سه عضوی شامل دو کاربر مجرم، قابل شناسایی است.*

۵.۱ فاصله همینگ در کدهای ضدجعل

تعریف ۳.۱. فرض کنید x و y دو کدواژه از کد C باشند. **فاصله همینگ**[۱۳] دو کدواژه x و y تعداد مکان‌های متمایز آن‌هاست و آن را با $d(x,y)$ مشخص می‌کنیم. به عبارت دیگر

$$d(x,y) = |\{i|x_i \neq y_i\}|.$$

ملاحظه ۱.۱. *برای دو کدواژه x و y به طول n،*

$$d(x,y) = d(x_۱,y_۱) + d(x_۲,y_۲) + \ldots + d(x_n,y_n).$$

لذا فاصله همینگ یک متر است و به آن متریک همینگ نیز می‌گویند.

اکنون برخی از ویژگی‌های فاصله همینگ c-کدهای ضدجعل را مورد ارزیابی قرار می‌دهیم. ابتدا برای هر (v,b)-کد، d_{max} و d_{min} را به صورت زیر تعریف می‌کنیم.

$$d_{max} = \max\{d(w^{(i)},w^{(j)}) \ : \ w^{(i)},w^{(j)} \in \Gamma, i \neq j\},$$

$$d_{min} = \min\{d(w^{(i)},w^{(j)}) \ : \ w^{(i)},w^{(j)} \in \Gamma, i \neq j\}.$$

قضیه ۴.۱. [۳۶] *یک کد دودویی Γ، ۲-کد ضدجعل است اگر و تنها اگر برای هر $i \neq j \neq h \neq i$، داشته باشیم $d(w^{(i)},w^{(j)}) < d(w^{(i)},w^{(h)}) + d(w^{(h)},w^{(j)})$.*

برهان. فرض کنید Γ یک (v,b)-کد دودویی و $w^{(i)}$، $w^{(j)}$ و $w^{(h)}$ سه کدواژه دلخواه مجزا از Γ باشند. بدون از دست دادن کلیت فرض کنید $U(\{w^{(i)},w^{(j)}\}) = \{۱,۲,\ldots,r\}$. بنابراین r مؤلفه‌ی اول $w^{(i)}$ و $w^{(j)}$ باهم برابرند.

از طرفی $d(w^{(i)},w^{(j)}) = v - r$ و چون فاصله همینگ، متر است، داریم:

$$d(w^{(i)},w^{(h)}) + d(w^{(h)},w^{(j)}) \geq v - r.$$

[۱۳] Hamming distance

اما $d(w^{(i)}, w^{(h)}) + d(w^{(h)}, w^{(j)}) > d(w^{(i)}, w^{(j)})$ اگر و تنها اگر حداقل یک مؤلفه از r مؤلفه اول $w^{(h)}$ با مؤلفه نظیر آن در $w^{(i)}$ یا $w^{(j)}$ متفاوت باشد. زیرا $w^{(i)}$ و $w^{(j)}$ در $v-r$ مؤلفه آخر با هم متفاوتند پس $w^{(h)}$ در هر مؤلفه از این $v-r$ مؤلفه با یکی از این دو کدواژه موافق و با دیگری مخالف است. لذا در $v-r$ مؤلفه آخر مجموع فاصله‌های همینگ دقیقا همان $v-r$ خواهد بود. لذا زمانی نامساوی به صورت اکید خواهد بود که $w^{(h)}$ حداقل در یکی از r مؤلفه اول با یکی از این دو کدواژه تفاوت داشته باشد. لذا $w^{(h)}$ درون مجموعه شدنی $\{w^{(i)}, w^{(j)}\}$ قرار نمی‌گیرد. چون کدواژه‌ها به صورت دلخواه انتخاب شده بود، بنابراین برای هر $C \subseteq \Gamma$ که $|C| = ۲$، داریم $F(C) \cap C = C$. پس Γ یک $۲ - FPC$ می‌باشد. □

نتیجه زیر بی‌درنگ از قضیه قبل حاصل می‌شود.

نتیجه ۱.۱. [۳۶] *اگر در یک (v, b)-کد Γ، $d_{max} < ۲d_{min}$ آن‌گاه Γ یک $۲ - FPC$ است.*

اکنون یک مثال برای شرح کاربرد این نتیجه ذکر می‌کنیم. در [۱۰] یک ساختار واضح ساده برای یک $(q, (q^۲ - q)/۲)$-کد با $d_{max} < q/۲ + ۳\sqrt{q}/۲$ و $d_{min} > q/۲ - ۳\sqrt{q}/۲$ (برای هر q که توانی از یک عدد اول باشد)، آورده شده است. قابل مشاهده است که برای $q > ۸۱$، $d_{max} < ۲d_{min}$. همچنین این محاسبات طولانی توسط رایانه انجام شده است و این نتیجه را دربر داشته که برای اعداد فرد $۳۱ < q < ۷۹$ که توانی از یک عدد اول هستند نیز داریم $d_{max} < ۲d_{min}$. لذا با به کارگیری نتیجه ۱.۱، قضیه زیر حاصل می‌شود.

قضیه ۵.۱. [۳۶] *برای هر عدد فرد $q \geq ۳۱$ که توانی از یک عدد اول است یک $۲ - FPC(q, (q^۲ - q)/۲)$ وجود دارد.*

فصل ۲

تعاریف ترکیبی از کدهای ضدجعل و ضدجعل امن

۱.۲ مقدمه

در این بخش، چند تعریف ترکیبی از $c - SFPC(v, b)$ ارائه می‌دهیم. اولین تعریف که آن را **خانواده آزاد** [۱] می‌نامیم، از سیستم‌های مجموعه‌ای استفاده می‌کند که به ویژگی‌های اجتماع و اشتراک نیاز دارد. تعریف بعدی مربوط به **سیستم‌های جداساز**[۲] است که در [۲۵] توسط فرایدمن و سایرین تعریف شده‌است. سپس دو مفهوم **خانواده‌های بدون پوشش**[۳] و **سیستم‌های منفصل** [۴] که ارتباط نزدیکی با هم دارند، را مورد بررسی قرار می‌دهیم. در ادامه، تعاریف مورد نیاز برای ساخت کدهای ضدجعل و ضدجعل امن را بیان می‌کنیم.

۲.۲ خانواده‌های آزاد

ابتدا برخی اصطلاحات درباره‌ی سیستم‌های مجموعه‌ای بیان می‌کنیم. یک **سیستم مجموعه‌ای**[۵] یک زوج $(X, \mathscr{B})$ است که در آن X یک مجموعه است و عناصر آن را نقاط می‌نامیم و $\mathscr{B}$ یک مجموعه از زیرمجموعه‌های X است و هرعضو آن را یک **بلوک**[۶] می‌نامیم. یک سیستم مجموعه‌ای را می‌توان با یک ماتریس وقوع توصیف کرد.

[۱] sandwich-free family
[۲] separating systems
[۳] cover-free families
[۴] disjunct systems
[۵] set system
[۶] block

فرض کنید $(X,\mathscr{B})$ که $X=\{x_۱,x_۲,\dots,x_n\}$ و $\mathscr{B}=\{B_۱,B_۲,\dots,B_b\}$، یک سیستم مجموعه‌ای باشد. ماتریس وقوع $(X,\mathscr{B})$ یک ماتریس $b\times v$ است، با درایه‌های:

$$a_{ij}=\begin{cases}۱ & x_j\in B_i,\\ ۰ & x_j\notin B_i.\end{cases}$$

برعکس، اگر یک ماتریس وقوع داده شده باشد، به راحتی می‌توانیم سیستم مجموعه‌ای مربوط به آن را بیابیم.

حال اگر Γ یک (v,b)-کد باشد، آن‌گاه $M(\Gamma)$ یک $(۰,۱)$ **-ماتریس** است که می‌توان آن را ماتریس وقوع یک سیستم مجموعه‌ای درنظر گرفت. برای هر کدواژه $w\in\Gamma$، از B_wبرای مشخص کردن بلوک وابسته‌اش در سیستم مجموعه‌ای متناظر استفاده می‌کنیم.

لم ۱.۲. [۳۵] *فرض کنید* $C=\{w^{(۱)},w^{(۲)},\dots,w^{(d)}\}$ *و* $x_۰\in\{۰,۱\}^v$. *در این صورت* $x\in F(C)$ *اگر و تنها اگر:*

$$\bigcap_{i=۱}^{d}B_{w^{(i)}}\subseteq B_x\subseteq\bigcup_{i=۱}^{d}B_{w^{(i)}}.$$

برهان. ابتدا رابطه $B_x\subseteq\bigcap_{i=۱}^{d}B_{w^{(i)}}$ را درنظر بگیرید. واضح است که این رابطه برقرار است اگر و تنها اگر، زمانی‌که j-امین مؤلفه همه‌ی کدواژه‌های درون C، ۱ هستند، داشته باشیم $x_j=۱$. همچنین رابطه $B_x\subseteq\bigcup_{i=۱}^{d}B_{w^{(i)}}$ برقرار است اگر و تنها اگر، وقتی j-امین مؤلفه همه‌ی کدواژه‌های درونC، ۰ هستند، داشته باشیم $x_j=۰$. از طرفی واضح است که هر دوحالت فوق اتفاق می‌افتد، اگر و تنها اگر $x\in F(C)$. □

قضیه ۱.۲. [۳۶] *یک* $c-FPC(v,b)$ *وجود دارد اگر و تنها اگر یک سیستم مجموعه‌ای* $(X,\mathscr{B})$ *وجود داشته‌باشد که* $|X|=v$ *و* $|\mathscr{B}|=b$ *و برای هر زیرمجموعه با* $d\leq c$ *بلوک* $B_۱,B_۲,\cdots,B_d\in\mathscr{B}$، *بلوک* $B\in\mathscr{B}\setminus\{B_۱,B_۲,\cdots,B_d\}$ *با ویژگی* $\bigcap_{i=۱}^{d}B_i\subseteq B\subseteq\bigcup_{i=۱}^{d}B_i$، *وجود نداشته باشد.*

برهان. با توجه به لم ۱.۲ به‌وضوح برقرار است. □

حال می‌خواهیم یک توصیف مشابه برای کدهای ضدجعل امن ارائه دهیم. ابتدا نیاز داریم که یک مدل قطعی از سیستم‌های مجموعه‌ای تعریف کنیم.

تعریف ۱.۲. [۳۵] یک سیستم مجموعه‌ای $(X, \mathscr{B})$ یک (i,j)-**خانواده آزاد**[۷] است، درصورتی‌که برای هر دو زیرمجموعه مجزای C_1 و C_2 از $\mathscr{B}$ که $|C_1| \leq i$ و $|C_2| \leq j$، خاصیت زیر برقرار باشد:

$$\Big(\bigcap_{B\in C_1} B\Big) \cup \Big(\bigcap_{B\in C_2} B\Big) \nsubseteq \Big(\bigcup_{B\in C_1} B\Big) \cap \Big(\bigcup_{B\in C_2} B\Big).$$

یک (i,j)-خانواده آزاد $(X, \mathscr{B})$ با $|X| = v$ و $|\mathscr{B}| = b$ را به اختصار با $(i,j) - SFF(v,b)$ نمایش می‌دهیم.

قضیه ۲.۲. [۳۵] *یک $c - SFPC(v,b)$ وجود دارد اگر و تنها اگر یک $(c,c) - SFF(v,b)$ وجود داشته باشد.*

برهان. فرض کنید $(X, \mathscr{B})$ یک سیستم مجموعه‌ای باشد. بنا به تعریف، واضح است که $(X, \mathscr{B})$ یک $(c,c) - SFF$ نیست اگر وتنها اگر مجموعه $W \subseteq X$ وجود داشته باشد به‌طوری‌که:

$$\bigcap_{B\in C_1} B \subseteq W \subseteq \bigcup_{B\in C_1} B$$

و

$$\bigcap_{B\in C_2} B \subseteq W \subseteq \bigcup_{B\in C_2} B$$

که $|C_1| = |C_2| = c$. حال C_1 و C_2 را مجموعه‌هایی از کدواژه‌های (v,b)-کد وابسته به $(X, \mathscr{B})$ درنظر بگیرید. بنا به لم ۱.۲ دو حالت بالا معادل است با:

$$F(C_1) \cap F(C_2) \neq \emptyset.$$

و این یعنی (v,b)-کد وابسته به $(X, \mathscr{B})$ نمی‌تواند یک $c - SFPC$ باشد. لذا حکم برقرار است. □

مثال ۱.۲. $(۳,۴) - SFF(۲,۲)$ زیر، معادل $۲ - SFPC(۳,۴)$ ارائه شده در مثال ۲.۱ است.

$$X = \{۱,۲,۳\},$$

$$\mathscr{B} = \{\{۱\},\{۲\},\{۳\},\{۱,۲,۳\}\}.$$

[۷] (i,j)-sandwich-free family

در قضیه زیر که بی‌درنگ از قضیه۱.۲ نتیجه می‌شود، ارتباط کدهای ضدجعل و خانواده‌های آزاد را بیان می‌کنیم.

قضیه ۳.۲. [۳۵] *یک $c-FPC(v,b)$ وجود دارد اگر و تنها اگر یک $(1,c)-SFF(v,b)$ وجود داشته باشد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک سیستم مجموعه‌ای و Γ، (v,b)-کد متناظر با آن باشد. $w\in\Gamma$ و $C\subseteq\Gamma$ با $|C|\leq c$، را درنظر بگیرید. واضح است که $(X,\mathscr{B})$ یک $(1,c)-SFF(v,b)$ است، اگر و تنها اگر $w\notin F(C)$. و این یعنی $F(C)\cap\Gamma=C$. □

۳.۲ سیستم‌های جداساز

فرایدمن و سایرین در [۲۵] سیستم‌های جداساز را به‌صورت زیر تعریف کرده‌اند.

تعریف ۲.۲. [۲۵] به سیستم مجموعه‌ای $(X,\mathscr{B})$، یک (i,j)-**سیستم جداساز**[۸] گوییم، اگر برای هر $P,Q\subseteq X$ که $|P|\leq i$ و $|Q|\leq j$ و $P\cap Q=\emptyset$، یک $B\in\mathscr{B}$ وجود داشته باشد به‌طوری‌که $P\subseteq B$ و $Q\cap B=\emptyset$ یا $Q\subseteq B$ و $P\cap B=\emptyset$. یک (i,j)-سیستم جداساز $(X,\mathscr{B})$ را که $|X|=v$ و $|\mathscr{B}|=b$، به‌صورت $(i,j)-SS(v,b)$ می‌نویسیم.

خانواده‌های آزاد و سیستم‌های جداساز بسیار به هم مرتبط هستند. درواقع ساختار یکسانی دارند که در اثبات قضیه زیر به‌صورت مختصر و دقیق بیان می‌کنیم.

قضیه ۴.۲. [۳۵] *یک $(i,j)-SFF(v,b)$ وجود دارد اگر و تنها اگر یک $(i,j)-SS(b,v)$ وجود داشته باشد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $(i,j)-SFF(v,b)$ باشد. همچنین فرض کنید C_1 و C_2 دو زیرمجموعه از $\mathscr{B}$ باشند که $|C_1|=i$ و $|C_2|=j$ و $C_1\cap C_2=\emptyset$. لذا نقطه $x\in X$ موجود است به‌طوری‌که:

$$x\in\Big(\bigcap_{B\in C_1}B\Big)\cup\Big(\bigcap_{B\in C_2}B\Big)\quad\text{و}\quad x\notin\Big(\bigcup_{B\in C_1}B\Big)\cap\Big(\bigcup_{B\in C_2}B\Big)$$

[۸] (i,j)-separating system

و این یعنی

$$x \in \bigcap_{B\in C_1} B \quad \text{و} \quad x \notin \bigcup_{B\in C_2} B$$

یا

$$x \in \bigcap_{B\in C_2} B \quad \text{و} \quad x \notin \bigcup_{B\in C_1} B.$$

حال، واضح است که اگر A ماتریس وقوع $(X, \mathscr{B})$ باشد، آن‌گاه A^T ماتریس وقوع یک $(i,j) - SS(b,v)$ خواهد بود.

برعکس؛ اگر ماتریس $A_{v\times b}$، ماتریس وقوع یک $(i,j) - SS(b,v)$ باشد، آن‌گاه به‌راحتی خواهیم دید که A^T ماتریس وقوع یک $(i,j) - SFF(v,b)$ است. □

حال نتیجه زیر را از قضایای ۲.۲، ۳.۲و ۴.۲ داریم.

نتیجه ۱.۲. [۳۵] *یک $c - FPC(v,b)$ وجود دارد اگر و تنها اگر یک $(1,c) - SS(b,v)$ وجود داشته باشد و یک $c - SFPC(v,b)$ وجود دارد اگر و تنها اگر یک $(c,c) - SS(b,v)$ وجود داشته باشد.*

برهان. با توجه به قضیه ۳.۲ یک $c - FPC(v,b)$ وجود دارد اگر و تنها اگر یک $(1,c) - SFF(v,b)$ وجود داشته باشد. همچنین براساس قضیه ۴.۲، یک $(1,c) - SFF(v,b)$ موجود است اگر و تنها اگر یک $(1,c) - SS(b,v)$ موجود باشد. لذا یک $c - FPC(v,b)$ وجود دارد اگر و تنها اگر یک $(1,c) - SS(b,v)$ وجود داشته باشد.

همچنین با توجه به قضیه ۲.۲، $c - SFPC(v,b)$ وجود دارد اگر و تنها اگر یک $(c,c) - SFF(v,b)$ وجود داشته باشد. از طرفی بنا به قضیه ۴.۲، یک $(c,c) - SFF(v,b)$ موجود است اگر و تنها اگر یک $(c,c) - SS(b,v)$ وجود داشته باشد. □

مثال ۲.۲. $(2,2) - SS(۴,۳)$ زیر، معادل است با $۲ - SFF(۳,۴)$ مثال ۱.۲ و $۲ - SFPC(۳,۴)$ ارائه شده در مثال ۲.۱:

$$X = \{۱,۲,۳,۴\},$$

$$\mathscr{B} = \{\{۱, ۴\}, \{۲, ۴\}, \{۳, ۴\}\}.$$

۴.۲ خانواده‌های بدون پوشش و سیستم‌های منفصل

تعریف ۳.۲. [۳۵] یک سیستم مجموعه‌ای $(X, \mathscr{B})$ یک (i, j)-**خانواده بدون پوشش**[۹] ایجاد می‌کند اگر برای هر دو زیرمجموعه جدا از هم $C_۱$ و $C_۲$ از $\mathscr{B}$ با شرط $|C_۱| \leq i$ و $|C_۲| \leq j$، رابطه زیر برقرار باشد:

$$\bigcap_{B \in C_۱} B \nsubseteq \bigcup_{B \in C_۲} B.$$

زمانی که $|X| = v$ و $|\mathscr{B}| = b$، برای اختصار یک (i, j)-خانواده بدون پوشش $(X, \mathscr{B})$ را به‌صورت $(i, j) - CFF(v, b)$ می‌نویسیم.

ملاحظه ۱.۲. *تعریف ما حالت کلی از واژه "خانواده بدون پوشش" است که عموماً مورد استفاده قرار می‌گیرد (برای مثال:* [۲۲] *را ملاحظه کنید). تعریف استاندارد، مشابه حالت $i = ۱$ می‌باشد. مفهوم معادل دیگر "کدهای فاصله مضاعف شده"*[۱۰] *می‌باشد؛* [۱۸] *و* [۲۸] *را ببینید.*

تعریف ۴.۲. [۳۵] به سیستم مجموعه‌ای $(X, \mathscr{B})$ یک (i, j)-سیستم منفصل گوییم اگر برای هر $P, Q \subseteq X$ با شرط $|P| \leq i$، $|Q| \leq j$ و $P \cap Q = \emptyset$، یک $B \in \mathscr{B}$ وجود داشته باشد به‌طوری‌که $P \subseteq B$ و $Q \cap B = \emptyset$. وقتی $|X| = v$ و $|\mathscr{B}| = b$، (i, j)-سیستم منفصل $(X, \mathscr{B})$ را به اختصار با $(i, j) - DS(v, b)$ مشخص می‌کنیم.

ملاحظه ۲.۲. *تعریف ما حالت کلی از واژه "منفصل" است. این تعریف در* [۱۷] *مشابه است با حالت $i = ۱$ و در این صورت این ویژگی j-کامل شناخته شده است؛* [۹] *را مشاهده کنید.*

خانواده‌های بدون پوشش و سیستم‌های منفصل ساختارهای وقوع یکسان دارند. قضیه زیر به همان روش قضیه ۴.۲ اثبات می‌شود.

[۹] (i, j)-cover-free family
[۱۰] superimposed distance codes

قضیه ۵.۲. [۳۵] *یک $(i,j)-CFF(v,b)$ وجود دارد، اگر و تنها اگر یک $(i,j)-DS(b,v)$ وجود داشته باشد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $(i,j)-CFF(v,b)$ باشد و C_1و C_2 زیرمجموعه‌هایی از $\mathscr{B}$ باشند که $|C_1|\leq i$ ، $|C_2|\leq j$ و $C_1\cap C_2=\emptyset$. لذا $x\in X$ موجود است به‌طوری‌که:

$$x\in \bigcap_{B\in C_1} B \quad \text{و} \quad x\notin \bigcup_{B\in C_2} B$$

حال کافیست ماتریس وقوع آن، (A) رادر نظر بگیرید. به‌وضوح A^T ماتریس وقوع یک $DS(b,v)$ است. برای حالت عکس نیز به‌صورت مشابه می‌توان با در نظر گرفتن ماتریس وقوع یک $(i,j)-DS(b,v)$ و به‌دست آوردن ماتریس ترانهاده آن، به وجود یک $(i,j)-CFF(v,b)$ پی برد. □

دو لم زیر بی‌درنگ از تعاریف حاصل می‌شوند.

لم ۲.۲. [۳۵] *هر (i,j)-سیستم منفصل، یک (i,j)-سیستم جداساز می‌باشد.*

لم ۳.۲. [۳۵] *هر (i,j)-خانواده بدون پوشش، یک (i,j)-خانواده آزاد است.*

اکنون یک تفسیر ترکیبی از ماتریس وقوع یک سیستم منفصل ارائه می‌دهیم.

لم ۴.۲. *یک $(i,j)-DS(n,N)$ معادل است با یک $(0,1)$-ماتریس $N\times n$ ، به‌طوری‌که در هر دو مجموعه جدا از هم C_1 و C_2 از (به ترتیب) i و j ستون، حداقل یک سطر وجود دارد که درایه‌هایش روی ستون‌های C_1 همه "۱" و روی ستون‌های C_2 همه "۰" باشند.*

در بالا توضیح دادیم که سیستم‌های منفصل، سیستم‌های جداساز هستند و خانواده‌های بدون پوشش، خانواده‌های آزاد هستند. قضیه زیر به نوعی عکس این مطلب را بیان می‌کند.

قضیه ۶.۲. [۳۵] *اگر یک $(i,j)-SS(v,b)$ وجود داشته باشد، آن‌گاه یک $(i,j)-DS(v,2b)$ وجود دارد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $(i,j)-SS(v,b)$ باشد. قرار دهید:

$$\mathscr{C}=\mathscr{B}\cup\{X\setminus B : B\in\mathscr{B}\}.$$

توجه کنید که مجموعه $\mathscr{C}$ در واقع مکمل سطرها در ماتریس وقوع این $(i,j)-SS(v,b)$ می‌باشد که اگر آن‌ها را به ماتریس وقوع اضافه کنیم، به‌وضوح ماتریس حاصل بیان‌گر یک $(i,j)-SS(v,۲b)$ خواهد بود. اکنون برای هر $P,Q\subseteq X$ که $|P|\leq i$ ، $|Q|\leq j$ و $P\cap Q=\emptyset$، حتما $B\in\mathscr{B}$ وجود دارد که $P\subseteq B$ و $Q\cap B=\emptyset$. زیرا این شرط یا روی همان v سطر اولیه برقرار بوده و یا عکس آن برقرار بوده که اکنون خود شرط روی مکمل سطر مربوطه برقرار است. لذا ماتریس فوق، ماتریس وقوع یک $(i,j)-DS(v,۲b)$ می‌باشد. □

یک نسخه مشابه، از قضیه ۶.۲ در نتیجه زیر بیان شده است.

نتیجه ۲.۲. [۳۵] *اگر یک $(i,j)-SFF(v,b)$ وجود داشته باشد، آن‌گاه یک $(i,j)-CFF(۲v,b)$ وجود دارد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $(i,j)-SFF(v,b)$ باشد. بنا به قضیه ۴.۲ یک $(i,j)-SFF(v,b)$ موجود است اگر و تنها اگر یک $(i,j)-SS(b,v)$ وجود داشته باشد و با توجه به قضیه ۶.۲ یک $(i,j)-SS(b,v)$ نیز وجود دارد اگر و تنها اگر یک $(i,j)-DS(b,۲v)$ وجود داشته باشد و بنا به قضیه ۵.۲ یک $(i,j)-DS(b,۲v)$ وجود دارد اگر و تنها اگر یک $(i,j)-CFF(۲v,b)$ وجود داشته باشد. □

۵.۲ خانواده‌های درهم‌ساز کامل و خانواده‌های درهم جداساز

خانواده‌های درهم‌ساز کامل[۱۱] بیش از ۱۵ سال مورد مطالعه عمیق دانشمندان قرار گرفته‌اند. نتایج این تحقیقات در تعداد زیادی کتب درسی و مقاله‌های علمی یافت می‌شود [۳۳] که اخیراً چندین کاربرد آن در رمزنگاری یافت شده است [۲۴] . ما می‌خواهیم ساختارهایی که در [۳۶] داده شده است را تعدیل کنیم به‌طوری‌که بتوانند برای کدهای ضدجعل امن استفاده شوند. در ابتدا به تعریف خانواده‌های درهم‌ساز کامل می‌پردازیم.

تعریف ۵.۲. [۳۵] یک (n,m,w)-**خانواده درهم‌ساز کامل** ، یک مجموعه از توابع $(\mathscr{F})$ است به‌طوری‌که

[۱۱] perfect hash families

$|X| = m$ ، $|Y| = n$ ، برای هر $f \in \mathscr{F}$ ؛ $f : Y \to X$ و برای هر $C \subseteq \{۱, ۲, \ldots, n\}$ که $|C| = w$ ، حداقل یک $f \in \mathscr{F}$ وجود دارد به‌طوری‌که $f|_C$ یک به یک است. اگر $|\mathscr{F}| = N$، یک (n, m, w)-خانواده درهم‌ساز کامل را با $PHF(N; n, m, w)$ مشخص می‌کنیم.

ملاحظه ۳.۲. *یک $PHF(N; n, m, w)$ را می‌توانیم توسط یک ماتریس با ورودی‌های $\{۱, \ldots, m\}$ نمایش دهیم با این ویژگی که در هر w ستون، حداقل یک سطر وجود دارد که ورودی‌های آن در این w ستون باهم متمایزند.*

تعریف ۶.۲. [۳۵] یک $(n, m, \{w_۱, w_۲\})$-**خانواده درهم جداساز** مجموعه‌ای از توابع $(\mathscr{F})$ است به‌طوری‌که $|Y| = n$، $|X| = m$، برای هر $f \in \mathscr{F}$ ؛ $f : Y \to X$ و برای هر $C_۱, C_۲ \subseteq \{۱, ۲, \ldots, n\}$ که $|C_۱| = w_۱$، $|C_۲| = w_۲$ و $C_۱ \cap C_۲ = \emptyset$، حداقل یک $f \in \mathscr{F}$ وجود دارد که $\{f(y) : y \in C_۱\} \cap \{f(y) : y \in C_۲\} = \emptyset$.

از نماد $SHF(N; n, m, \{w_۱, w_۲\})$ برای مشخص کردن یک $(n, m, \{w_۱, w_۲\})$-خانواده درهم جداساز با $|\mathscr{F}| = N$ استفاده می‌کنیم.

ملاحظه ۴.۲. *یک $SHF(N; n, m, \{w_۱, w_۲\})$ را می‌توانیم توسط یک ماتریس $N \times n$ با ورودی‌های $\{۱, ۲, \ldots, m\}$ نمایش دهیم به‌طوری‌که در هر دو مجموعه جدا از هم $C_۱$ و $C_۲$ از (به‌ترتیب) $w_۱$ و $w_۲$ ستون، حداقل یک سطر وجود دارد که درایه‌ها در ستون‌های $C_۱$ از درایه‌ها در ستون‌های $C_۲$ مجزا هستند.*

فصل ۳

ساختارهایی از کدهای ضدجعل و ضدجعل امن

۱.۳ مقدمه

برای ساختن کدهای ضدجعل و ضدجعل امن می‌توان از روش‌های مختلفی استفاده کرد. ساده‌ترین راه، استفاده از روش‌های مستقیم و تولید ماتریس با ویژگی ماتریس وقوع این کدهاست. مشکلی که در این نوع ساختار وجود دارد محدودیت تعداد و یا افزایش طول کدواژه‌هاست. در ساختارهای وابسته، این مشکلات تا حدی رفع می‌شود. همچنین می‌توان کدهای مورد نظر را با روش‌های مستقیم و پارامترهای کوچک تولید نمود سپس با استفاده از مفاهیم ترکیبی فصل قبل و روش‌هایی که ذکر خواهیم کرد آن‌ها را بسط داد.

در این فصل ساختارهای روشنی از کدهای ضدجعل و ضدجعل امن به روش مستقیم و بازگشتی ارائه می‌شوند.

۲.۳ دو ساختار مستقیم (کدهای ضدجعل امن)

ابتدا با دو ساختار مستقیم از کدهای ضد جعل امن شروع می‌کنیم.

قضیه ۱.۳. [۳۵] *برای هر عددصحیح* $c \geq ۲$، *یک* $c - SFPC(\binom{۲c-۱}{c-۱}, ۲c)$ *وجود دارد.*

برهان. ماتریس وقوع $M(\Gamma)$ را به این صورت تعریف می‌کنیم. سطرهای $M(\Gamma)$ را توسط عناصر مجموعه‌ی $\{۱, ۲, \ldots, ۲c\}$ و ستون‌های آن را توسط زیرمجموعه‌های c تایی $\{۱, ۲, \ldots, ۲c\}$ که $۱ \in S \subseteq \{۱, ۲, \ldots, ۲c\}$،

شماره‌گذاری می‌کنیم. این زیرمجموعه‌ها را $S_۱, S_۲, \ldots, S_v$ می‌نامیم که $v = \binom{۲c-۱}{c-۱}$. حال ورودی سطر i-ام و ستون j-ام از $M(\Gamma)$ را به این صورت قرار می‌دهیم:

$$m_{ij} = \begin{cases} ۱ & i \in S_j, \\ ۰ & i \notin S_j. \end{cases}$$

نشان می‌دهیم که Γ یک $c - SFPC\left(\binom{۲c-۱}{c-۱}, ۲c\right)$ است.

کافیست بررسی کنیم که برای هر $C_۱, C_۲ \subseteq \Gamma$ با شرط $|C_۱| = |C_۲| = c$ و $C_۱ \cap C_۲ = \emptyset$ داریم $F(C_۱) \cap F(C_۲) = \emptyset$. از طرفی $b = ۲c$، لذا داریم: $C_۲ = \Gamma \setminus C_۱$. بدون از دست دادن کلیت فرض کنید $w^{(۱)} \in C_۱$. حال خواهیم دید که یک i واحد وجود دارد که برای هر $w^{(j)} \in C_۱$ ، $w_i^{(j)} = ۱$ و برای هر $w^{(j)} \in C_۲$، $w_i^{(j)} = ۰$. به‌عبارت دیگر در ماتریس $M(\Gamma)$ یک ستون یکتا وجود دارد که عناصر آن روی همه اعضای $C_۱$ برابر با ۱ و روی اعضای $C_۲$ برابر ۰ است. با توجه به چگونگی تعریف ماتریس $M(\Gamma)$ و نحوه انتخاب S_i ها، واضح است که چنین ستونی حتما وجود دارد. بنابراین برای هر x، اگر $x \in F(C_۱)$ آن‌گاه $x_i = ۱$ و اگر $x \in F(C_۲)$ آن‌گاه $x_i = ۰$. لذا $F(C_۱) \cap F(C_۲) = \emptyset$. پس Γ یک c-کد ضدجعل امن است. □

ملاحظه ۱.۳. *$c - SFPC$ ساخته شده در قضیه ۱.۳ ، دارای کوچکترین v ممکن و $b = ۲c$ است.*

مثال ۱.۳. اکنون یک $۳ - SFPC(۱۰, ۶)$ ساخته شده به روش قضیه ۱.۳ ارائه می‌دهیم. ماتریس وقوع $M(\Gamma)$ برابر است با:

$$\begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۰ & ۰ \\ ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ \end{pmatrix}.$$

قضیه ۲.۳. [۳۵] *برای هر عدد صحیح $c \geq ۲$، یک $c - SFPC(۲\binom{۲c-۱}{c-۱}, ۲c+۱)$ وجود دارد.*

برهان. فرض کنید ماتریس $M(\Gamma)$، $۲c \times \binom{۲c-۱}{c-۱}$ مانند قضیه ۱.۳ تعریف شده باشد. حال یک ماتریس $(۲c+۱) \times ۲\binom{۲c-۱}{c-۱}$ به‌صورت زیر می‌سازیم:

$$M = \begin{pmatrix} M(\Gamma) & M(\Gamma) \\ ۰ \cdots ۰ & ۱ \cdots ۱ \end{pmatrix}.$$

ثابت می‌کنیم که M ماتریس وقوع یک $c-SFPC(۲\binom{۲c-۱}{c-۱}, ۲c+۱)$ است.

دو زیرمجموعه مجزا $C_۱$ و $C_۲$ از سطرهای M را درنظر بگیرید که هر کدام شامل حداکثر c سطر از M باشند. واضح است که اگر هیچ یک از این دو زیرمجموعه، سطر آخر ماتریس را شامل نشوند، حکم برقرار است. لذا فرض کنید سطر آخر درون مجموعه $C_۱$ قرار گیرد. چون $M(\Gamma)$ ماتریس وقوع یک c-کد ضدجعل امن است، یک ستون وجود دارد که درایه‌هایش روی اعضای $C_۱$ برابر با ۰ و روی اعضای $C_۲$ برابر ۱ است و یا برعکس. اگر حالت اول رخ دهد این ستون را روی ماتریس $M(\Gamma)$ اول، واقع در M در نظر می‌گیریم و چون مؤلفه این ستون روی سطر آخر ماتریس، ۰ است همچنان داریم $F(C_۱) \cap F(C_۲) = \emptyset$. اما اگر حالت دوم رخ دهد، یعنی در ماتریس $M(\Gamma)$ ستونی وجود داشته باشد که عناصر آن روی اعضای $C_۱$ برابر با ۱ و روی اعضای $C_۲$ برابر ۰ باشند، این ستون را برای ماتریس M روی $\frac{۱}{۲}$ ستون آخر M واقع شده روی ماتریس $M(\Gamma)$ دوم، در نظر می‌گیریم. لذا در این حالت نیز داریم $F(C_۱) \cap F(C_۲) = \emptyset$. پس M ماتریس وقوع یک c-کد ضدجعل امن است. □

۳.۳ یک ساختار با استفاده از خانواده‌های درهم‌ساز کامل

نتایج بر روی خانواده‌های درهم‌ساز کامل در تعداد بسیاری کتاب درسی، رساله و مقاله قابل یافت است. مرجع [۳۳] منبع مناسبی است. ساختارهای جدید بیشتر را در مقاله‌های [۲] و [۵] می‌توان جستجو کرد.

در قضیه زیر چگونگی بسط دادن یک کد ضدجعل را با استفاده از یک خانواده درهم‌ساز کامل شرح می‌دهیم.

قضیه ۳.۳. [۳۶] *اگر یک $PHF(N; n, m, c+۱)$ و یک $c-FPC(v, m)$ وجود داشته باشد آن‌گاه یک $c-FPC(Nv, n)$ وجود دارد.*

برهان. فرض کنید $\Gamma = \{w^{(۱)}, w^{(۲)}, \ldots, w^{(m)}\}$ یک $c-FPC(v, m)$ و $\mathcal{F}$ یک $PHF(N; n, m, c+۱)$ باشد. همچنین فرض کنید Γ' یک (Nv, n)-کد، شامل n کدواژه $u^{(j)}$ به‌صورت زیر باشد.

$$\text{برای هر } ۱ \le j \le n : \quad u^{(j)} = \biguplus_{h \in \mathcal{F}} w^{h(j)}$$

که $\|$ الحاق رشته‌ها، در واقع کنار هم چیدن کدواژه‌هاست. نشان می‌دهیم که Γ' یک $c-FPC(Nv,n)$ است.

فرض کنید $W \subseteq \Gamma'$ و $W = \{u^{(i_1)}, u^{(i_2)}, \ldots\ldots, u^{(i_c)}\}$. به‌خاطر بیاورید که $U(W)$ مجموعه مؤلفه‌های غیر قابل کشف W می‌باشد. فرض کنید کدواژه‌ی $u^{(i_{c+1})} \in \Gamma' \setminus W$ چنان وجود داشته باشد که برای هر $1 \leq j \leq c$، $u^{(i_{c+1})}|_{U(W)} = u^{(i_j)}|_{U(W)}$. بنابراین برای هر $h \in \mathcal{F}$ ، $w^{(h(i_{c+1}))}$ در مجموعه شدنی $\{w^{(h(i_1)}, \ldots, w^{(h(i_c)}\}$ قرار می‌گیرد. ازطرفی چون $\mathcal{F}$ یک $PHF(N;n,m,c+1)$ است، یک تابع $f \in \mathcal{F}$ موجود است که $f|_C$، $(C = \{i_1, i_2, \ldots, i_{c+1}\})$ یک به یک است. لذا برای این تابع f می‌دانیم $f(i_1), \ldots, f(i_{c+1})$ اعداد متمایزی می‌باشند، پس کدواژه‌های $w^{f(i_j)} \in \Gamma$ $(1 \leq j \leq c+1)$ نیز متمایزند. اما $w^{f(i_{c+1})}$ در مجموعه شدنی $\{w^{(f(i_1))}, \ldots, w^{(f(i_c))}\}$ قرار دارد و این با $c-FPC$ بودن Γ تناقض دارد. لذا Γ' نیز یک $c-FPC$ است. □

قضیه ۴.۳. [۸] *اگر یک $c-FPC(v,q)$ داشته باشیم و (N,n)-کدی q-آرایه‌ای با مینیمم فاصله همینگ $d_{min} > N(1-1/c)$ وجود داشته باشد آن‌گاه یک $c-FPC(vN,n)$ وجود دارد.*

ساختار فوق در [۸] برای ساختن c-کدهای ضدجعل با استفاده از کدهای تصحیح کننده خطا داده شده است، که چون وارد مبحث کدهای تصحیح کننده خطا نمی‌شویم، به این ساختار نمی‌پردازیم. همچنین آلون در [۱] نیز یک ساختار برای خانواده‌های درهم‌ساز کامل با استفاده از کدهای تصحیح کننده خطا ارائه کرده است. مشاهده می‌شود که اگر از یک خانواده درهم‌ساز کامل ساخته شده به روش ارائه شده در [۱] برای به‌دست آوردن یک c-کد ضدجعل با به‌کارگیری قضیه ۳.۳ استفاده کنیم، آن‌گاه کد حاصل دقیقاً همان کد ساخته شده با استفاده از قضیه ۴.۳ می‌باشد. اگرچه امکان استفاده از ساختارهای دیگر خانواده‌های درهم‌ساز کامل برای به‌دست آوردن مثال‌های جدید از کدهای ضدجعل وجود دارد.

اگر یک $c-SFPC$ کوچک داشته باشیم، می‌توانیم به‌صورت بازگشتی یک $c-SFPC$ بزرگ، با استفاده از خانواده‌های درهم‌ساز کامل ساختارسازی نماییم. در قضیه زیر ساختارمان را ارائه می‌دهیم و از حالت عمومی‌تر خانواده‌های آزاد استفاده می‌کنیم.

قضیه ۵.۳. [۳۵] *اگر یک* $(i,j)-SFF(v,m)$ *و یک* $PHF(N;n,m,i+j)$ *وجود داشته باشد، آن‌گاه یک* $(i,j)-SFF(vN,n)$ *وجود دارد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $(i,j)-SFF(v,m)$ و $\mathscr{F}$ یک $PHF(N;n,m,i+j)$ باشد که برای هر $f\in\mathscr{F}$ ؛ $f:Y\to X$. قرار دهید $W=X\times\mathscr{F}$ و برای هر $y\in Y$، تعریف کنید:

$$A_y=\{(B_{f(y)},f):f\in\mathscr{F}\}.$$

فرض کنید $\mathscr{A}=\{A_y:y\in Y\}$. نشان می‌دهیم که سیستم مجموعه‌ای $(W,\mathscr{A})$ یک $(i,j)-SFF(vN,n)$ می‌باشد.

فرض کنید چنین نباشد. بنابراین دو زیرمجموعه جدا از هم $C_1,C_2\subseteq Y$ وجود دارند به‌طوری‌که $|C_1|=i,\ |C_2|=j$ و

$$\left(\bigcap_{y\in C_1}A_y\right)\cup\left(\bigcap_{y\in C_2}A_y\right)\subseteq\left(\bigcup_{y\in C_1}A_y\right)\cap\left(\bigcup_{y\in C_2}A_y\right).$$

آن‌گاه برای هر $f\in\mathscr{F}$، حالتی اتفاق خواهد افتاد که

$$\left(\bigcap_{y\in C_1}B_{f(y)}\right)\cup\left(\bigcap_{y\in C_2}B_{f(y)}\right)\subseteq\left(\bigcup_{y\in C_1}B_{f(y)}\right)\cap\left(\bigcup_{y\in C_2}B_{f(y)}\right). \qquad (۱.۳)$$

اکنون از آن‌جاییکه $\mathscr{F}$ یک خانواده درهم‌ساز کامل است، تابع $f\in\mathscr{F}$ وجود دارد که $f|_{C_1\cup C_2}$ یک به یک است. برای این f خاص، $f(C_1)$ و $f(C_2)$ دو زیرمجموعه مجزا از X می‌باشند. بنابراین رابطه (۱.۳) با $(i,j)-SFF(v,m)$ بودن $(X,\mathscr{B})$ تناقض دارد. □

ساختار بازگشتی زیر در به‌دست آوردن ساختارهای واضح برای مجموعه‌های نامتناهی از خانواده‌های درهم‌ساز کامل مفید است.

لم ۱.۳. [۵] *فرض کنید یک* $PHF(N_0;n_0,m,w)$ *وجود دارد که* $\gcd\left(n_0,\binom{w}{2}!\right)=1$. *آن‌گاه برای هر عددصحیح* $j\geq 0$، *یک* $PHF\Big(\left(\binom{w}{2}+1\right)^jN_0;n_0^{2^j},m,w\Big)$ *وجود دارد.*

اثبات لم فوق با استفاده از ارتباط ماتریس‌های تفاضلی[۱] با خانواده‌های درهم‌ساز کامل ممکن است، که

[۱] defference matrix

به علت عدم ارتباط مستقیم با کدهای ضدجعل امن، به آن نمی‌پردازیم.

حال، کاربرد قضیه ۵.۳ و لم ۱.۳ را برای به‌دست آوردن یک خانواده نامتناهی از ۲-کدهای ضدجعل امن نشان می‌دهیم.

مثال ۲.۳. [۵] یک $PHF(۷; ۷, ۴, ۴)$ بصورت زیر وجود دارد:

$$\begin{pmatrix} ۱ & ۲ & ۳ & ۴ & ۱ & ۲ & ۳ \\ ۱ & ۲ & ۳ & ۴ & ۲ & ۱ & ۴ \\ ۱ & ۲ & ۳ & ۴ & ۳ & ۴ & ۱ \\ ۱ & ۲ & ۳ & ۴ & ۴ & ۳ & ۲ \\ ۲ & ۳ & ۲ & ۳ & ۱ & ۱ & ۴ \\ ۲ & ۴ & ۱ & ۲ & ۳ & ۴ & ۳ \\ ۱ & ۱ & ۲ & ۲ & ۳ & ۴ & ۳ \end{pmatrix}$$

قضیه ۶.۳. [۳۵] *برای هر* $j \geq ۰$، *یک* $SFPC(۳ \cdot ۷^{j+۱}, ۷^{۲^j}) - ۲$ *وجود دارد.*

برهان. با توجه به مثال ۲.۳ یک $PHF(۷; ۷, ۴, ۴)$ داریم لذا با توجه به لم ۱.۳ برای هر $j \geq ۰$ یک $PHF(۷^{j+۱}; ۷^{۲^j}, ۴, ۴)$ داریم. از طرفی بنا به قضیه ۲.۲ و مثال ۲.۱ یک $SFF(۳, ۴) - (۲, ۲)$ داریم. با توجه به موارد فوق و قضیه ۵.۳ یک $SFF(۳ \cdot ۷^{j+۱}, ۷^{۲^j}) - (۲, ۲)$ حاصل می‌شود لذا بنا به قضیه ۲.۲ یک $SFPC(۳ \cdot ۷^{j+۱}, ۷^{۲^j}) - ۲$ وجود دارد. □

مثال ۳.۳. یک $PHF(۲; ۵, ۴, ۳)$ به‌صورت زیر وجود دارد.

$$\begin{matrix} ۱ & ۲ & ۳ & ۴ & ۳ \\ ۱ & ۱ & ۲ & ۱ & ۳ \end{matrix}$$

قضیه ۷.۳. [۳۶] *برای هر عدد صحیح* $j \geq ۱$ ، *یک* $FPC(۶ \times ۴^j, ۵^{۲^j}) - ۲$ *وجود دارد.*

برهان. با توجه به مثال ۳.۳ و به‌کارگیری لم ۱.۳ برای $j \geq ۰$ ، یک $PHF(۲ \times ۴^j, ۵^{۲^j}, ۴, ۳)$ به‌دست می‌آوریم. حال با ترکیب این خانواده درهم‌ساز کامل و $FPC(۳, ۴) - ۲$ داده شده در مثال ۲.۱ و به‌کارگیری قضیه ۳.۳ به یک $FPC(۶ \times ۴^j, ۵^{۲^j}) - ۲$ می‌رسیم. □

۴.۳ یک ساختار با استفاده از خانواده‌های درهم جداساز

اگر با دقت به اثبات قضیه ۵.۳ نگاه کنیم، به وجود یک تابع درهم‌ساز پی می‌بریم که روی مجموعه $C_1 \cup C_2$ از اندازه $i+j$ یک به یک است، که بیشتر از تقاضای ماست. درحقیقت کافیست که برای هر دو زیرمجموعه جدا از هم C_1 و C_2 در اندازه‌های (به‌ترتیب) i و j، یک تابع درهم‌ساز f با شرط $\{f(y) : y \in C_1\} \cap \{f(y) : y \in C_2\} = \emptyset$ ، موجود باشد. بدیهی است اگر $w_1 + w_2 = w$، هر $PHF(N; n, m, w)$ یک $SHF(N; n, m, \{w_1, w_2\})$ است و همچنین یک $SHF(N; n, m, \{1, 1\})$ معادل است با یک $PHF(N; n, m, 2)$. نتیجه زیر نیز به آسانی دریافت می‌شود که ما آن را به عنوان یک لم برای ارجاعات آینده ثبت می‌کنیم.

لم ۲.۳. *یک $SHF(N; n, 2, \{w_1, w_2\})$ برابر است با یک $(w_1, w_2) - SS(n, N)$.*

برهان. اگر توابع $f_1, f_2, \ldots, f_N$ در $SHF(N; n, 2, \{w_1, w_2\})$ را بلوک‌های سیستم مجموعه‌ای $(X, \mathscr{B})$ با $X = \{1, 2, \ldots, n\}$ در نظر بگیریم، به $(w_1, w_2) - SS(n, N)$ متناظر می‌رسیم. زیرا ماتریس وقوع هردو یکسان می‌باشد. □

قضیه ۸.۳. [۳۵] *اگر یک $(i, j) - SFF(v, m)$ و یک $SHF(N; n, m, \{i, j\})$ وجود داشته باشد، آن‌گاه یک $(i, j) - SFF(vN, n)$ وجود دارد.*

برهان. دقیقاً به روش اثبات قضیه ۵.۳ قابل اثبات است. □

حال یک ساختار بازگشتی برای خانواده‌های درهم جداساز مشابه لم ۱.۳ بیان می‌کنیم.

قضیه ۹.۳. [۵] *فرض کنید یک $SHF(N_0; n_0, m, \{w_1, w_2\})$ با $\gcd(n_0, (w_1 w_2)!) = 1$ وجود داشته باشند. آن‌گاه برای هر $j \geq 0$ یک $SHF((w_1 w_2 + 1)^j N_0; n_0^{2^j}, m, \{w_1, w_2\})$ وجود دارد.*

برهان. اثبات این قضیه دقیقاً همان اثبات لم ۱.۳ می‌باشد. □

مثال ۴.۳. یک $SHF(3; 7, 4, \{2, 2\})$ همانند زیر وجود دارد:

$$\begin{pmatrix} ۱ & ۱ & ۲ & ۲ & ۳ & ۳ & ۴ \\ ۲ & ۱ & ۱ & ۲ & ۴ & ۳ & ۳ \\ ۱ & ۲ & ۱ & ۲ & ۳ & ۴ & ۳ \end{pmatrix}$$

قضیه ۱۰.۳. [۳۵] *برای هر* $j \geq ۰$ *یک* $۲ - SFPC(۹ \cdot ۵^j; ۷^{۲^j})$ *وجود دارد.*

برهان. با توجه به مثال ۴.۳ و قضیه ۹.۳ برای هر $j \geq ۰$ یک $SHF(۳ \cdot ۵^j; ۷^{۲^j}, ۴, \{۲, ۲\})$ وجود دارد. از طرفی با توجه به $۲ - SFPC(۳, ۴)$ ارائه شده در مثال ۲.۱ و به‌کارگیری قضایای ۲.۲ و ۸.۳ حکم حاصل می‌شود. □

قضیه ۱۰.۳ یک خانواده نامتناهی از $۲ - SFPC(v, b)$ با $v = O((\log b)^{\log_۲ ۵})$ تولید می‌کند. این یک پیشرفت عمده در قضیه ۶.۳ که $v = O((\log b)^{\log_۲ ۷})$، بیان می‌کند.

قضیه ۱۱.۳. [۳۵] *اگر* $c \geq ۲$ *باشد، برای هر* $j \geq ۰$ *یک* $c - SFPC\left(۲\binom{۲d-۱}{d-۱} \cdot (c^۲+۱)^j, (۲d+۱)^{۲^j}\right)$ *وجود دارد که* $d > c$ *و* $\gcd(۲d+۱, (c^۲)!) = ۱$.

برهان. قضیه ۲.۳ نشان می‌دهد که یک $d - SFPC(۲\binom{۲d-۱}{d-۱}, ۲d+۱)$ وجود دارد. بنا به نتیجه ۱.۲، هر $d - SFPC(۲\binom{۲d-۱}{d-۱}, ۲d+۱)$ معادل است با یک $(d, d) - SS(۲d+۱, ۲\binom{۲d-۱}{d-۱})$. با به‌کارگیری لم ۲.۳ یک $(d, d) - SS(۲d+۱, ۲\binom{۲d-۱}{d-۱})$ معادل است با یک $SHF(۲\binom{۲d-۱}{d-۱}, ۲d+۱, ۲, \{d, d\})$. از طرفی چون $d > c$، این خانواده یک $SHF(۲\binom{۲d-۱}{d-۱}, ۲d+۱, ۲, \{c, c\})$ نیز هست. از طرفی $\gcd(۲d+۱, (c^۲)!) = ۱$، لذا می‌توانیم قضیه ۹.۳ را برای ساختن یک $SHF(۲\binom{۲d-۱}{d-۱})(c^۲+۱)^j, (۲d+۱)^{۲^j}, ۲, \{c, c\})$ برای هر $j \geq ۰$ اجرا کنیم. با توجه به لم ۲.۳ و نتیجه ۱.۲، SHF حاصل همان $c - SFPC$ مورد نظر ماست. □

نتیجه زیر بی‌درنگ از قضیه ۱۱.۳ استنباط می‌شود.

نتیجه ۱.۳. [۳۵] *به‌ازای هر* $c \geq ۲$ *یک ساختار واضح برای هر کلاس نامتناهی از* $c - SFPC(v, b)$ *وجود دارد به‌طوری‌که* $v = O((\log b)^{\log_۲(c^۲+۱)})$.

با توجه به قضایای ۲.۲ و ۴.۲، ساختارهای $c - SFPC(v, b)$ می‌توانند برای ساختن $(c, c) - SS(b, v)$ معادل سازی شوند. تا آنجا که می‌دانیم قضیه ۱۱.۳ اولین ساختارهای واضح مؤثر را به‌ازای c کلی برای

$(c,c)-SS(b,v)$ فراهم می‌کند. پیش از این در [۲۵] یک ساختار مشابه با قضیه ۱۰.۳ برای حالت $c=۲$ ارائه شده است.

۵.۳ دو ساختار مستقیم (کدهای ضدجعل)

ساختار ۱.[۶] فرض کنید $F=\{۰,۱,\dots,q-۱\}$. مجموعه C از همه کلمات به طول l و وزن ۱ (یعنی مجموعه همه اعضایی از F^l با دقیقا یک مؤلفه غیر صفر) یک c-کد ضدجعل با اندازه‌ی $l(q-۱)$ تشکیل می‌دهد.

برهان. فرض کنید $x\in C$ برداری با وزن ۱ باشد که i-امین مؤلفه‌اش غیر صفر است. حال، هر مجموعه‌ی $P\subseteq C$ که $x\in F(P)$، باید شامل یک کدواژه y باشد که $x_i=y_i$ ، اما چون هر کدواژه با وزن ۱ منحصرا توسط مؤلفه‌ی غیر صفرش مشخص می‌شود لذا $x=y$. بنابراین برای هر c، C یک c-کد ضدجعل است. □

تعریف ۱.۳. فرض کنید f یک چندجمله‌ای برحسب x باشد. بزرگ‌ترین توان x را **درجه**[۲] f نامیم و آن را با نماد $\deg f$ مشخص می‌کنیم.

ساختار ۲.[۱۳] فرض کنید l و c اعداد صحیح مثبت بزرگ‌تر یا مساوی ۲ باشند و q توانی از یک عدد اول و $q\geq l$. همچنین فرض کنید F یک میدان متناهی با اندازه‌ی q باشد و $\alpha_۱,\alpha_۲,\dots,\alpha_l\in F$ مجزا باشند. کد C به طول l را روی میدان F به‌صورت زیر تعریف می‌کنیم:

$$C=\{(f(\alpha_۱),f(\alpha_۲),\dots,f(\alpha_l)) \ : \ f\in F[X] \ \text{ و } \ \deg f<\lceil l/c\rceil\}.$$

در این صورت C یک c-کد ضدجعل با اندازه‌ی $q^{\lceil l/c\rceil}$ است.

متذکر می‌شویم که اگر چندجمله‌ای f در بی‌نهایت تعریف شده باشد، محدودیت $q\geq l$ می‌تواند به‌صورت ضعیف‌تر $q+۱\geq l$ باشد. $f(\infty)$ را ضریب $X^{\lceil l/c\rceil-۱}$ در f تعریف می‌کنیم.

[۲] degree

برهان. برای چندجمله‌ای f از درجه‌ی کمتر از $\lceil l/c \rceil$، $q^{\lceil l/c \rceil}$ انتخاب وجود دارد زیرا برای هر ضریب آن، q انتخاب داریم. بنابراین $|C| = q^{\lceil l/c \rceil}$.

اگر $x, y \in C$ در $\lceil l/c \rceil$ مؤلفه با هم مشترک باشند آن‌گاه $x = y$ (زیرا در این صورت چندجمله‌ای‌های مربوط به این دو کدواژه یکسانند، لذا سایر مؤلفه‌ها نیز باهم برابرند). به طور ویژه، هر انتخاب مجزا برای چندجمله‌ای f یک کدواژه‌ی مجزا به ما می‌دهد و هر چندجمله‌ای f با تعیین کردن $f(\alpha)$ برای $\lceil l/c \rceil$ نقطه α، مشخص می‌شود. اکنون فرض کنید $x \in C \cap F(P)$ و $P \subseteq C$ دارای اندازه‌ی حداکثر c باشد. هر مؤلفه از x باید با مؤلفه‌ی متناظرش در حداقل یک کدواژه از P برابر باشد. لذا کدواژه‌ی $y \in P$ چنان وجود دارد که حداقل در $\lceil l/c \rceil$ مؤلفه با x برابر است. در نتیجه $x = y \in P$، بنابراین C یک c-کد ضدجعل است. □

۶.۳ کدهای ضدجعل و ضدجعل امن با پارامترهای مشخص

۱.۶.۳ کدهای ضدجعل با طول زوج

دو زیرکد مانند بخشی از ساختار اخیر تعریف می‌کنیم. فرض کنید l یک عدد صحیح زوج و $l \geq ۴$. همچنین فرض کنید m توانی از یک عدد اول، $m \geq l + ۱$ و قرار دهید $q = m^۲ + ۱$. میدان متناهی $\mathbb{F}_m$ از مرتبه m را در نظر بگیرید وقرار دهید $F = \{\infty\} \cup (\mathbb{F}_m)^۲$. $\beta_۰, \beta_۱, \alpha_۱, \alpha_۲, \ldots, \alpha_{l-۱}$ را عناصر مجزا از $\mathbb{F}_m$ در نظر بگیرید. برای چند جمله‌ای‌های $f, g \in \mathbb{F}_m[X]$، به‌جای $(f(\alpha_i), g(\alpha_i)) \in F$، از $(f, g)(\alpha_i)$، استفاده می‌کنیم و $C_۱ \subseteq F^l$ را به‌صورت زیر تعریف می‌کنیم:

$$C_۱ = \{(\infty, (f, g)(\alpha_۱), (f, g)(\alpha_۲), \ldots, (f, g)(\alpha_{l-۱}))\} \qquad (۲.۳)$$

که $f, g \in \mathbb{F}_m[X]$، $\deg f = (l/۲) - ۱$ و $\deg g \leq (l/۲) - ۱$. اکنون $C_۲ \subseteq F^l$ را به‌صورت زیر تعریف می‌کنیم:

$$C_۲ = \{((t(\beta_۰), t(\beta_۱)), (s, t)(\alpha_۱), (s, t)(\alpha_۲), \ldots, (s, t)(\alpha_{l-۱}))\} \qquad (۳.۳)$$

که $s, t \in \mathbb{F}_m[X]$، به‌طوری‌که $\deg s \leq (l/۲) - ۲$ و $\deg t \leq (l/۲)$.

ساختار ۳.[۶] فرض کنید l یک عدد صحیح زوج باشرط $l \geq ۴$ اباشد. همچنین فرض کنید m توانی از

یک عدد اول شرط $m \geq l+1$ باشد و قرار دهید $q = m^2+1$. مجموعه‌های C_1 و C_2 را به‌صورتی که در بالا ذکر شد، تعریف کنید. آن‌گاه $C = C_1 \cup C_2$ یک ۲-کد ضدجعل با اندازه $2(q-1)^{l/2}(1-1/(2\sqrt{q-1}))$ روی میدان F است.

برهان. با درنظر گرفتن مؤلفه‌های اول، واضح است که C_1 و C_2 مجزا هستند. یک چندجمله‌ای از درجه‌ی حداکثر $(l/2)-1$ توسط مقادیرش در $l/2$ نقطه‌ی مجزا مشخص می‌شود. به همین دلیل چندجمله‌ای‌های f و g در (۲.۳) به‌طور یکتا توسط یک کدواژه $x \in C_1$ مشخص می‌شوند. تعداد $m^{l/2} - m^{(l/2)-1}$ انتخاب برای چندجمله‌ای f و $m^{l/2}$ انتخاب برای چندجمله‌ای g وجود دارد. بنابراین $|C_1| = (m^2)^{l/2}(1-1/m)$. چندجمله‌ای s در (۳.۳) توسط $(l/2)$ مؤلفه از $l-1$ مؤلفه‌ی آخر یک کدواژه $x \in C_2$ مشخص می‌شود. به‌صورت مشابه چندجمله‌ای t توسط $(l/2)+1$ مؤلفه از یک کدواژه $x \in C_2$ تعیین می‌شود. از طرفی $|C_2|$ برابر است با تعداد انتخاب‌ها برای چندجمله‌ای‌های s و t ، لذا $|C_2| = m^{(l/2)-1}m^{(l/2)+1} = (m^2)^{l/2}$. از مجموع عبارت‌ها برای $|C_1|$ و $|C_2|$ و استفاده از این حقیقت که $m = \sqrt{q-1}$، به این نتیجه می‌رسیم که $|C| = 2(q-1)^{l/2}(1-1/2\sqrt{q-1}))$.

حال باید ثابت کنیم که C یک ۲-کد ضدجعل است. برای این منظور ابتدا ادعا می‌کنیم که کدواژه‌های $x \in C_1$ و $y \in C_2$ حداکثر در $(l/2)-1$ مؤلفه می‌توانند با هم برابر باشند.

مؤلفه‌های اول x و y هرگز برابر نیستند. اگر $(l/2)$ از مؤلفه های باقی‌مانده برابر باشند آن‌گاه بنا به تعریف C_1 و C_2 چندجمله‌ای f از درجه‌ی دقیقا $(l/2)-1$ و چندجمله‌ای s از درجه‌ی حداکثر $(l/2)-2$ در $l/2$ نقطه باهم برابرند و در این‌صورت باید f و s یکسان باشند که این غیرممکن است و لذا ادعای ما صحیح است.

فرض کنید $P \subseteq C$ با شرط $|P| = 2$ و $x \in F(P) \cap C$. باید نشان دهیم $x \in P$.

فرض کنید $x \in C_1$. به‌جز اولین مؤلفه، $l-1$ مؤلفه وجود دارد لذا x باید با برخی اعضای $y \in P$ (یک یا هردو عضو) در $l/2 = \lceil l/2 \rceil$ مکان غیر از اولین مؤلفه برابر باشد. چون x و y در بیشتر از $(l/2)-1$ مکان با هم برابرند لذا باید $y \in C_1$. از طرفی هر $l/2$ مؤلفه از $l-1$ مؤلفه‌ی آخر، یک کدواژه در C_1 را

تعیین می‌کند لذا $x = y$. بنابراین $x = y \in P$.

حال فرض کنید $x \in C_۲$. همچنین فرض کنید $y \in P$ که $x_۱ = y_۱$ (بنابراین $y \in C_۲$). اگر x و y در $۱ - (l/۲)$ یا بیشتر مؤلفه از $l - ۱$ مؤلفه‌ی آخر، باهم برابر باشند آن‌گاه مؤلفه‌های یکسان x و y شامل $۱ - (l/۲)$ مقدار از s و $۱ + (l/۲)$ مقدار از t می‌باشند. لذا چندجمله‌ای‌های تولید کننده این دو نقطه یکسان بوده و در نتیجه $x = y$. بنابراین، در این حالت هم $x = y \in P$.

حال فرض کنید x و y در کمتر از $۱ - (l/۲)$ مؤلفه از $l - ۱$ مؤلفه‌ی آخر با هم برابر باشند، اگر z را عضوی از P در نظر بگیریم که مخالف y است، آن‌گاه x و z حداقل در $۱ + (l/۲)$ مؤلفه باهم برابر خواهند بود. بنابراین $z \in C_۲$ و چون مؤلفه‌های یکسان x و z حداقل شامل $l/۲$ مقدار از s و $۱ + (l/۲)$ مقدار از t هستند لذا $x = z$. بنابراین در این حالت نیز $x = z \in P$ و در نتیجه C یک ۲-کد ضدجعل است. □

۲.۶.۳ یک ۳-کد ضدجعل به طول ۵

مجموعه های $X_۱$، $X_۲$، $X_۳$، $X_۴$ و $X_۵$ از کدواژه‌های به طول ۵ روی اعضای $\mathbb{F}_۳ \cup \{\infty\}$ را به‌صورت زیر تعریف می‌کنیم:

$$\begin{aligned}
X_۱ &= \{(\ \infty\ ,\ a\ ,\ a\ ,\ a\ ,\ a\ ) : a \in \mathbb{Z}_۳\},\\
X_۲ &= \{(\ a\ ,\ \infty\ ,\ a\ ,\ a+۱\ ,\ a+۲\ ) : a \in \mathbb{Z}_۳\},\\
X_۳ &= \{(\ a\ ,\ a\ ,\ \infty\ ,\ a+۲\ ,\ a+۱\ ) : a \in \mathbb{Z}_۳\},\\
X_۴ &= \{(\ a\ ,\ a+۱\ ,\ a+۲\ ,\ \infty\ ,\ a\ ) : a \in \mathbb{Z}_۳\},\\
X_۵ &= \{(\ a\ ,\ a+۲\ ,\ a+۱\ ,\ a\ ,\ \infty\ ) : a \in \mathbb{Z}_۳\}.
\end{aligned}$$

به‌وضوح X_i ها دو به دو مجزا و دارای اندازه ۳ هستند. همچنین واضح است که یک کدواژه از مجموعه‌ی $X_۱ \cup X_۲ \cup X_۳ \cup X_۴ \cup X_۵$ توسط دوتا از مؤلفه‌هایش به‌صورت یکتا مشخص خواهد شد.

فرض کنید m توانی از یک عدد اول با شرط $m \geq ۴$ باشد. $\alpha_۱$، $\alpha_۲$، $\alpha_۳$ و $\alpha_۴$ را عضوهای متمایز $\mathbb{F}_m$ درنظر بگیرید و مجموعه‌های $Y_۱$، $Y_۲$، $Y_۳$، $Y_۴$ و $Y_۵$ از کدواژه‌های به طول ۵ روی اعضای $\mathbb{F}_m \cup \{\infty\}$ را

به‌صورت زیر تعریف کنید:

$$Y_۱ = \{(\infty, f(\alpha_۱), f(\alpha_۲), f(\alpha_۳), f(\alpha_۴)) : f \in \mathbb{F}_m[X], \deg f \leq ۱\},$$

$$Y_۲ = \{(f(\alpha_۱), \infty, f(\alpha_۲), f(\alpha_۳), f(\alpha_۴)) : f \in \mathbb{F}_m[X], \deg f \leq ۱\},$$

$$Y_۳ = \{(f(\alpha_۱), f(\alpha_۲), \infty, f(\alpha_۳), f(\alpha_۴)) : f \in \mathbb{F}_m[X], \deg f \leq ۱\},$$

$$Y_۴ = \{(f(\alpha_۱), f(\alpha_۲), f(\alpha_۳), \infty, f(\alpha_۴)) : f \in \mathbb{F}_m[X], \deg f \leq ۱\},$$

$$Y_۵ = \{(f(\alpha_۱), f(\alpha_۲), f(\alpha_۳), f(\alpha_۴), \infty) : f \in \mathbb{F}_m[X], \deg f \leq ۱\}.$$

واضح است که Y_i ها مجزا و دارای اندازه $m^۲$ هستند. علاوه براین اگر دو عامل $x, y \in Y_i$ در دو مؤلفه (غیر از i-امین مؤلفه) با هم برابر باشند، آن‌گاه $x = y$. زیرا تابع f و f' که تعریف کننده (به ترتیب) x و y هستند در دونقطه برابرند و چون این توابع، ثابت یا از درجه‌ی یک هستند، هم ارز خواهند بود. لذا تمام مؤلفه‌های x و y با هم برابرند پس $x = y$. مجموعه کدهای $C_۱, C_۲, C_۳, C_۴, C_۵$ شامل کدواژه‌های به طول ۵ روی اعضای $(\mathbb{F}_۳ \times \mathbb{F}_m) \cup (\infty, \infty)$ را به‌صورت زیر تعریف کنید:

$$C_i = \{((x_۱, y_۱), (x_۲, y_۲), (x_۳, y_۳), (x_۴, y_۴), (x_۵, y_۵)) :$$

$$(x_۱, x_۲, x_۳, x_۴, x_۵) \in X_i \text{ و } (y_۱, y_۲, y_۳, y_۴, y_۵) \in Y_i\}$$

توجه کنید که $|C_i| = |X_i| \times |Y_i| = ۳m^۲$.

ساختار ۴.[۶] فرض کنید m توانی از یک عدد اول با شرط $m \geq ۴$ باشد. همچنین فرض کنید $q = ۳m + ۱$. مجموعه کدهای $C_۱$، $C_۲$، $C_۳$، $C_۴$، و $C_۵$ را روی میدان $F = (\mathbb{F}_۳ \times \mathbb{F}_m) \cup (\infty, \infty)$ به‌صورتی که گفته شد، تعریف کنید. آن‌گاه کد $C = C_۱ \cup C_۲ \cup C_۳ \cup C_۴ \cup C_۵$ یک ۳-کد ضدجعل به‌طول l و اندازه $\frac{۵}{۳}q^۲ - \frac{۱۰}{۳}q + \frac{۵}{۳}$ است.

برهان. واضح است که C_iها دو به دو مجزا هستند و برای هر $۱ \leq i \leq ۵$، $|C_i| = ۳m^۲ = \frac{۱}{۳}(q^۲ - ۲q + ۱)$. لذا $|C| = |C_۱| + |C_۲| + \ldots + |C_۵| = \frac{۵}{۳}(q^۲ - ۲q + ۱)$ می‌باشد. اکنون کافی است نشان دهیم که C یک ۳-کد ضدجعل است.

برای یک کدواژه $c \in C$، $\pi_1(c)$ را کلمه‌ای در $X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5$ درنظر بگیرد که از جابه‌جایی مؤلفه $(a,b) \in F$ از c با $a \in \mathbb{F}_3 \cup \{\infty\}$ به دست آمده است. توجه کنید که $\pi_1(c) \in X_i$ اگر و تنها اگر $c \in C_i$. به صورت مشابه $\pi_2(c)$ را کلمه‌ای در $Y_1 \cup Y_2 \cup Y_3 \cup Y_4 \cup Y_5$ درنظر بگیرید که از جابه‌جایی مؤلفه $(a,b) \in F$ از c با $b \in \mathbb{F}_m \cup \{\infty\}$ به‌دست آمده است.

فرض کنید $x \in C$ و $P \subseteq C$ به‌طوری‌که $|P| \leq 3$ و $x \in F(P)$. باید نشان دهیم $x \in P$. اکنون برای یک $j \in \{1,2,3,4,5\}$، $x \in C_j$. لذا j امین مؤلفه x، (∞,∞) و $\pi_1(x) \in X_j$. چون $|P| \leq 3$ و $l = 5$، لذا $y \in P$ چنان وجود دارد که با x در دومؤلفه یا بیشتر (به‌جز j-امین مؤلفه) یکسان است. می‌خواهیم نشان دهیم $x = y$. چون x و y در مؤلفه یا بیشتر یکسانند، $\pi_1(x)$ و $\pi_1(y)$ نیز در مؤلفه یا بیشتر باهم برابرند. با توجه به توضیحاتی که درباره اعضای $\bigcup_{i=1}^{5} X_i$ دادیم، $\pi_1(x) = \pi_1(y)$. از آن‌جایی که $\pi_1(x) = \pi_1(y) \in X_j$ پس $y \in C_j$.

چون $x, y \in C_j$ پس $\pi_2(x), \pi_2(y) \in Y_j$. علاوه براین، چون x و y در بیش از دو مؤلفه (به جز j-امین مؤلفه) باهم برابرند، $\pi_2(x)$ و $\pi_2(y)$ نیز در بیش از دو مؤلفه باهم برابرند و با توجه به ویژگی اعضای $\bigcup_{i=1}^{5} Y_i$، داریم $\pi_2(x) = \pi_2(y)$. حال بنا به تساوی‌های $\pi_1(x) = \pi_1(y)$ و $\pi_2(x) = \pi_2(y)$ نتیجه می‌گیریم $x = y \in P$. لذا C یک ۳-کد ضدجعل است. □

مذکر می‌شویم که اگر در تعریف مجموعه‌های Y_i ، قراردهیم $\alpha_4 = \infty$ باشد شرط $m \geq 4$ در شرح ساختار ۲ می‌تواند با حالت ضعیف‌تر $m \geq 3$ جایگزین شود (تذکر بعد از بیان ساختار ۲ را ملاحظه نمایید).

۳.۶.۳ $2 - FPC$

تعریف ۲.۳. [۳۱] اگر بردارهای یک **فضای برداری** [۳] را کدواژه در نظر بگیریم، یک **کد خطی** [۴] تشکیل داده‌ایم. یک کد خطی به طول n و بعد k روی میدان $\mathbb{Z}_p$ را با $\Lambda_p(n, p^k)$ نشان می‌دهیم.

تعریف ۳.۳. [۲۰] کدخطی Λ_p یک **کد متقاطع** [۵] است اگر پشتیبان (مجموعه مؤلفه‌های غیر صفر) هر دو

[۳] vector space
[۴] linear code
[۵] intersecting code

کدواژه غیرصفر باهم اشتراک ناتهی داشته باشند.

قضیه ۱۲.۳. [۱۴] *یک کد متقاطع، یک $FPC-۲$ است.*

برهان. فرض کنید Λ_p یک کد متقاطع باشد و a، b و c سه کدواژه متمایز آن باشند. چون Λ_p خطی است کدواژه‌های $c-a$ و $c-b$ نیز وجود دارند. اگر یکی از این دو کدواژه یا هردو صفر باشند آن‌گاه $c=a$ یا $c=b$ که با متمایز بودن آن‌ها تناقض دارد. لذا هردو غیر صفر هستند. از طرفی چون Λ_p یک کد متقاطع است، برای بعضی از مؤلفه‌های i می‌دانیم $c_i-a_i\neq ۰$ و $c_i-b_i\neq ۰$. لذا $c_i\notin\{a_i,b_i\}$. بنابراین c در مجموعه شدنی a و b قرار نمی‌گیرد و چون این سه کدواژه دلخواه بودند Λ_p یک $FPC-۲$ است. □

۴.۶.۳ $FPC-۳$

قضیه ۱۳.۳. [۲۰] *فرض کنید (n,m)-کد Γ یک کد دودویی با وزن ثابت $۲l$ باشد که فاصله همینگ هر دو کدواژه آن $۲l$ است. اگر برای بعضی اعداد صحیح مثبت $l_۱$، $l=۲l_۱+۱$ آن‌گاه Γ یک $FPC-۳$ است.*

برهان. فرض می‌کنیم (n,m)-کد Γ با وزن ثابت $۲(۲l_۱+۱)$، $FPC-۳$ نباشد. لذا چهار کدواژه وجود دارند که اگر آن‌ها را به صورت سطرهای یک ماتریس در نظر بگیریم، هیچ یک از دو ستون $(۱۰۰۰)^T$ و $(۰۰۰۱)^T$ به‌دست نمی‌آید. فرض کنید کدواژه‌های $c_۱$، $c_۲$، $c_۳$ و $c_۴$ به‌صورت سطرهای یک ماتریس نوشته شده باشند. بدون از دست دادن کلیت داریم:

$$c_۱=\overbrace{۱\ldots۱}^{l}\overbrace{۱\ldots۱}^{l}\overbrace{۰\ldots۰}^{l}\overbrace{۰\ldots۰}^{m}\overbrace{۰\ldots۰}^{n-۳l-m},$$

$$c_۲=\overbrace{۱\ldots۱}^{l}\overbrace{۰\ldots۰}^{l}\overbrace{۱\ldots۱}^{l}\overbrace{۰\ldots۰}^{m}\overbrace{۰\ldots۰}^{n-۳l-m},$$

$$c_۳=\overbrace{۱\ldots۱}^{m}\overbrace{۰\ldots۰}^{l-m}\overbrace{۱\ldots۱}^{l-m}\overbrace{۰\ldots۰}^{m}\overbrace{۱\ldots۱}^{l-m}\overbrace{۰\ldots۰}^{m}\overbrace{۱\ldots۱}^{m}\overbrace{۰\ldots۰}^{n-۳l-m},$$

$$c_۴=\overbrace{۱\ldots۱}^{\alpha_۱}\overbrace{۱\ldots۱}^{\beta}\overbrace{۰\ldots۰}^{l-\alpha_۱-\beta}\overbrace{۱.۱}^{x}\overbrace{۰\ldots۰}^{l-m-x}\overbrace{۱.۱}^{y}\overbrace{۰\ldots۰}^{m-y}\overbrace{۱.۱}^{z}\overbrace{۰\ldots۰}^{l-m-z}\overbrace{۱.۱}^{t}\overbrace{۰\ldots۰}^{m-t}\overbrace{۱\ldots۱}^{\gamma}\overbrace{۰\ldots۰}^{n-۳l-\gamma}.$$

$\alpha_۱=m$ زیرا در غیر این‌صورت یک ستون $(۱۰۰۰)^T$ به‌دست می‌آید و $\gamma\leq m$، زیرا در غیر آن یک ستون $(۰۰۰۱)^T$ به وجود می‌آید.

فرض کنید $e_۱$، $e_۲$ و $e_۳$ معادلاتی باشند که به‌ترتیب از $d(c_۱, c_۴) = ۲l$، $d(c_۲, c_۴) = ۲l$ و $d(c_۳, c_۴) = ۲l$ به‌دست آمده‌اند.

$$e_۱ : \quad l - m - \beta + l - x - y + z + t + \gamma = ۲l,$$

$$e_۲ : \quad l - m - \beta + x + y + l - z - t + \gamma = ۲l,$$

$$e_۳ : \quad \beta + l - m - x + y + l - m - z + t + m - \gamma = ۲l.$$

از مجموع معادلات $e_۱$ و $e_۲$، داریم $\gamma = m + \beta$. از طرفی $\gamma \leq m$، لذا نتیجه می‌گیریم $\beta = ۰$ و $\gamma = m$. با ساده کردن $e_۳$ و محاسبه $e_۱ - e_۲$ خواهیم داشت:

$$e_۱ - e_۲ = -۲x - ۲y + ۲z + ۲t = ۰ \quad \Longrightarrow \quad x + y = z + t,$$

$$e_۳ = -m - x + y - z + t - \gamma = ۰ \Longrightarrow y + t = ۲m + x + z.$$

از جمع دو رابطه بالا به $x + m = t$ می‌رسیم و چون $t \leq m$ نتیجه می‌گیریم $x = ۰$ و $t = m$. تفاضل روابط بالا یعنی $e_۱ - e_۲ - e_۳$ معادله $y = z + m$ را به ما می‌دهد. از طرفی $y \leq m$. لذا داریم $z = ۰$ و $y = m$. اکنون وزن کدواژه $c_۴$ را محاسبه می‌کنیم.

$$wt(c_۴) = \alpha_۱ + \beta + x + y + z + t + \gamma = ۴m.$$

اما این با فرض اولیه که وزن تمام کدواژه‌ها از مرتبه $۲(۲l_۱ + ۱)$ است تناقض دارد بنابراین Γ یک $FPC - ۳$ است. □

۵.۶.۳ دودویی با وزن ثابت $SFPC - ۲$

ملاحظه ۲.۳. *با توجه به تعریف کدهای ضدجعل امن، در یک $SFPC(v, b) - ۲$ دودویی، وقتی کدواژه‌ها را به عنوان سطرهای ماتریس وقوع درنظر بگیریم، برای هر چهارتایی مرتب شده از سطرها، حتما یک ستون $(۱۱۰۰)^T$ یا $(۰۰۱۱)^T$ وجود دارد. این ویژگی در* [۲۹] *تحت عنوان $(۲, ۲)$-انفصال مطالعه شده است.*

قضیه ۱۴.۳. [۱۹] *فرض کنید (n, M, d) یک کد دودویی با وزن ثابت d باشد. همچنین فرض کنید برای هر i و j، $c_i, c_j \in (n, M, d)$ در $\lfloor d/۲ \rfloor$ مکان باهم برابرند. اگر برای برخی اعداد صحیح مثبت l، داشته باشیم $n \leq ۴l - ۱$ و $d = ۲l$، آن‌گاه (n, M, d)-کد حاصل یک $SFPC - ۲$ است.*

برهان. فرض کنید $(۴l - ۱, M, ۲l)$-کد C، $SFPC - ۲$ نباشد. فرض کنید $c_۱, c_۲, c_۳, c_۴ \in C$ به عنوان سطرهای یک آرایه نوشته شده باشند. بدون از دست دادن کلیت داریم:

$$c_۱ = \overbrace{۱\ldots۱}^{l}\ \overbrace{۱\ldots۱}^{l}\ \ ۰\ldots۰\ \ ۰\ldots۰\ ۰\ldots۰,$$

$$c_۲ = \overbrace{۱\ldots۱}^{l}\ \overbrace{۰\ldots۰}^{l}\ \ \overbrace{۱\ldots۱}^{l}\ \ ۰\ldots۰\ ۰\ldots۰,$$

$$c_۳ = \overbrace{۰\ldots۰}^{m}\overbrace{۱\ldots۱}^{l-m}\ \overbrace{۱\ldots۱}^{m}\overbrace{۰\ldots۰}^{l-m}\ \overbrace{۱\ldots۱}^{m}\overbrace{۰\ldots۰}^{l-m}\ \overbrace{۱\ldots۱}^{l-m}\ ۰\ldots۰,$$

$$c_۴ = \overbrace{۱..۱}^{\alpha}\overbrace{۰..۰}^{m-\alpha}\overbrace{۱..۱}^{a}\overbrace{۰..۰}^{l-m-a}\ \overbrace{۱..۱}^{b}\overbrace{۰..۰}^{m-b}\overbrace{۱..۱}^{c}\overbrace{۰..۰}^{l-m-c}\ \overbrace{۱..۱}^{f}\overbrace{۰..۰}^{m-f}\overbrace{۱..۱}^{r}\overbrace{۰..۰}^{l-m-r}\ \overbrace{۱..۱}^{\beta}\overbrace{۰..۰}^{l-m-\beta}\overbrace{۱..۱}^{\gamma}.$$

اگر $\alpha < m$، در بین m ستون اول حداقل یک ستون $(۱۱۰۰)^T$ اتفاق می‌افتد و C، $SFPC - ۲$ خواهد بود. لذا $\alpha = m$.

اگر $\beta > ۰$، آن‌گاه به‌صورت مشابه، C یک $SFPC - ۲$ خواهد بود زیرا حداقل یک ستون $(۰۰۱۱)^T$ به وجود می‌آید. بنابراین $\beta = ۰$ است. اکنون معادلات زیر را به‌دست می‌آوریم.

چون $wt(c_۴) = ۲l$ است، $\quad a + b + e + f + r + \gamma = ۲l - m$

چون $|c_۱ \cap c_۴| = l$ است، $\quad f + r + \gamma = l$

چون $|c_۲ \cap c_۴| = l$ است، $\quad f + r = l - m - a$

از دو معادله آخر داریم $a = \gamma - m$. پس $\gamma \geq m$. اما از طرفی می‌دانیم $n \leq ۴l - ۱$ و با توجه به تعداد مؤلفه‌های کدواژه‌های $c_۳$ و $c_۴$ به نامساوی $۴l - m + \gamma \leq ۴l - ۱$ می‌رسیم. یعنی $\gamma \leq m - ۱$، که با $\gamma \geq m$ به دست آمده، تناقض دارد لذا C یک $SFPC - ۲$ است. □

فصل ۴
کران‌هایی برای کدهای مورد نظر

۱.۴ مقدمه

کدهای ضدجعل و ضدجعل امن پارامترهای مختلفی دارند که روی هم تأثیر مستقیم دارند. برای افزایش اندازه این کدها ناگزیر باید تأثیرات آن‌ها روی پارامترهای دیگر مثل طول هر کدواژه و یا تعداد اعضای مجموعه‌ی مرجع (برای مثال میدان $\mathbb{Z}_۲$ برای کدهای دودویی) را پذیرفت. کران‌های متفاوتی وابسته به پارامترهای مختلف را مورد بررسی قرار می‌دهیم تا بتوان با توجه به امکانات و فضای نرم‌افزاری موجود از انواع آن بهره گرفت.

در این فصل با مفهوم گروه‌های متقارن مواجه خواهیم شد، لذا تعریف آن را در این‌جا ذکر می‌کنیم.

تعریف ۱.۴. فرض کنیم X یک مجموعه ناتهی باشد. مجموعه تمام توابع دوسویی روی X را با S_X نمایش می‌دهیم و به آن گروه متقارن می‌گوییم. اگر $X = \{۱, ۲, \ldots, n\}$، به جای S_X از نماد $Sym(n)$ استفاده می‌کنیم و هر عضو از آن را یک جایگشت می‌نامیم و داریم $|Sym(n)| = n!$.

همچنین **قضیه اسپرنر**[۱] به شرح زیر است:

قضیه ۱.۴. [۳۷] *خانواده $P = \{A_۱, A_۲, \ldots, A_p\}$ از زیرمجموعه‌های غیرتهی مجموعه $X = \{۱, ۲, \ldots, n\}$ را در نظر بگیرید. اگر برای هر $i \neq j$ داشته باشیم $A_i \not\subseteq A_j$ آن‌گاه $|P| \leq \binom{n}{\lfloor \frac{n}{۲} \rfloor}$.*

[۱] Sperner's Theorem

۲.۴ دو کران بالا

۱.۲.۴ کران بالا برای b، وابسته به v و c

فرض کنید $\Gamma = \{w^{(1)}, \dots, w^{(b)}\}$ یک $c - FPC(v, b)$ باشد. برای $1 \leq d \leq c$ قرار دهید:

$$t_d = \min\{|U(C)| \ : \ C \subseteq \Gamma \text{ و } |C| = d\}$$

که $U(C)$ همان مجموعه مؤلفه‌های غیر قابل کشف و $F(C)$ مجموعه شدنی $C \subseteq \Gamma$ می‌باشد.

لم ۱.۴. [۳۶] *فرض کنید $\Gamma = \{w^{(1)}, \dots, w^{(b)}\}$ یک $c - FPC(v, b)$ و $t_1, \dots, t_c$ همانند بالا تعریف شده باشند. در این صورت داریم:*

$$0 < t_c < t_{c-1} < \dots < t_1 = v.$$

برهان. فرض کنید برای یک d، $t_d = t_{d-1}$. همچنین فرض کنید $C = \{w^{(u_1)}, \dots, w^{(u_d)}\}$ به‌طوری‌که $|U(C)| = t_d$ و $C' = \{w^{(u_1)}, \dots, w^{(u_{d-1})}\}$. واضح است که $U(C) \subseteq U(C')$. از طرفی چون $t_d = t_{d-1}$ لذا داریم $U(C) = U(C')$. پس $C \subseteq F(C') \cap \Gamma$ که این با c-کد ضدجعل بودن Γ تناقض دارد. □

در قضیه زیر یک کران بالا برای b وابسته به t_{c-1} ارائه می‌دهیم.

قضیه ۲.۴. [۳۶] *فرض کنید $\Gamma = \{w^{(1)}, \dots, w^{(b)}\}$ یک $c - FPC(v, b)$ باشد و $t_1, \dots, t_c$ همانند بالا تعریف شده باشند. آن‌گاه داریم:*

$$b \leq c - 1 + \binom{t_{c-1}}{\lceil \frac{t_{c-1}}{2} \rceil}.$$

برهان. فرض کنید $W \subseteq \Gamma$ طوری انتخاب شده باشد که $|W| = c - 1$ و $|R| = t_{c-1}$ که $R = U(W)$. همچنین فرض کنید برای هر کدواژه $w^{(i)} \in \Gamma \setminus W$، $R_i = U(W \cup \{w^{(i)}\})$. واضح است که برای هر $w^{(i)} \in \Gamma \setminus W$، $R_i \subseteq R$ و برای هر $w^{(i)}, w^{(j)} \in \Gamma \setminus W$ که $i \neq j$، داریم $R_i \nsubseteq R_j$. زیرا اگر چنین نباشد آن‌گاه $w^{(j)} \in F(W \cup \{w^{(i)}\})$، که این با $c - FPC$ بودن Γ تناقض دارد. به‌عبارت دیگر زیرمجموعه‌های

R_i، تشکیل یک **خانواده اسپرنر** [۲] با مجموعه پایه R تشکیل می‌دهند. با توجه به قضیه اسپرنر داریم:

$$|\Gamma \setminus W| \leq \binom{t_{c-۱}}{\lceil \frac{t_{c-۱}}{۲} \rceil}.$$

وچون $|\Gamma \setminus W| = b - c + ۱$، بنابراین:

$$b \leq c - ۱ + \binom{t_{c-۱}}{\lceil \frac{t_{c-۱}}{۲} \rceil}.$$

□

نتیجه ۱.۴. [۳۶] *اگر Γ یک $c - FPC(v, b)$ باشد آن‌گاه:*

$$b \leq c - ۱ + \binom{v - c + ۲}{\lceil \frac{v-c+۲}{۲} \rceil}.$$

برهان. با توجه به لم ۱.۴ می‌دانیم:

$$t_c < t_{c-۱} < \ldots < t_۳ < t_۲ < t_۱ = v$$

$$\Rightarrow t_۳ < v - ۱$$

$$\Rightarrow t_۴ < v - ۲$$

$$\vdots$$

$$\Rightarrow t_{c-۱} < v - (c - ۳) = v - c + ۳$$

بنابراین $t_{c-۱} \leq v - c + ۲$. با جای‌گذاری در کران قضیه ۲.۴ به نتیجه مطلوب خواهیم رسید. □

به خاطر بیاورید که در مثال ۱.۱ یک $c - FPC(c, c)$ ارائه دادیم که به‌وضوح در کران بالا صدق می‌کند.

همچنین حالت تساوی کران بالا برای $۲ - FPC(۳, ۴)$ مثال ۲.۱ برقرار است.

۲.۲.۴ کران بالا وابسته به تعداد اعضای مجموعه‌ی مرجع

قضیه ۳.۴. [۶] *فرض کنید l ، q و c اعداد صحیح مثبت با شرط $l, c \geq ۲$ باشند. همچنین فرض کنید C یک c-کد ضدجعل q-**آرایه ای**[۳] به طول l و با اندازه‌ی $n > q$ باشد. باقیمانده تقسیم l بر c را*

[۲] Sperner family
[۳] q-array

$r \in \{۰, ۱, \dots, c-۱\}$ *قرار می‌دهیم. آن‌گاه:*

$$n \leq \max\left\{q^{\lceil l/c \rceil}, r\left(q^{\lceil l/c \rceil}-۱\right)+(c-r)\left(q^{\lfloor l/c \rfloor}-۱\right)\right\}. \qquad (۱.۴)$$

البته، ملاحظه می‌کنیم که تقریباً برای همه مجموعه‌ها، قسمت دوم نامساوی (۱.۴) بزرگ‌تر است.

برهان. فرض کنید C یک c-کد ضدجعل q-آرایه‌ای به طول l و اندازه n باشد. نشان می‌دهیم که کران (۱.۴) برقرار است. برای هر زیرمجموعه $S \subseteq \{۱, ۲, \dots, l\}$، U_S را به‌صورت زیر تعریف کنید:

$$U_S = \{x \in C : \nexists y \in C \;\; s.t. \;\; \forall i \in S \,; x_i = y_i\}.$$

بدیهی است که $|U_S| \leq q^{|S|}$ زیرا هر کدواژه‌ی $x \in U_S$ منحصرا توسط مؤلفه‌هایش $(x_i \;;\; i \in S)$ تعیین می‌شود. علاوه بر این اگر $n > q^{|S|}$، آن‌گاه $|U_S| \leq q^{|S|}-۱$. زیرا حداقل یک مؤلفه $(x_i \;;\; i \in S)$ در دو کدواژه از C یا بیشتر، باید یکسان باشند.

فرض کنید $S_۱, S_۲, \dots, S_c \subseteq \{۱, ۲, \dots, l\}$، زیرمجموعه‌های مجزای S باشند که برای هر $۱ \leq j \leq r$، $|S_j| = \lceil l/c \rceil$ و برای هر $r+۱ \leq j \leq c$، $|S_j| = \lfloor l/c \rfloor$. بنابراین $\cup_{j=۱}^{c} S_j = \{۱, ۲, \dots, l\}$. پس اگر نشان دهیم $C = \cup_{j=۱}^{c} U_{S_j}$ ، آن‌گاه کران (۱.۴) برقرار است.

فرض کنید چنین نباشد و $x \in C \setminus \cup_{j=۱}^{c} U_{S_j}$ وجود داشته باشد. بنابراین $x^۱, x^۲, \dots, x^c \in C \setminus \{x\}$ چنان وجود دارند که i-امین مؤلفه‌ی x و x^j برای هر $i \in S_j$ یکسان است. لذا $x \in F(\{x^۱, x^۲, \dots, x^c\})$ که با c-کد ضدجعل بودن C تناقض دارد. لذا $C = \cup_{j=۱}^{c} U_{S_j}$ و حکم برقرار است. □

نتیجه ۲.۴. [۶] *فرض کنید q، l و c اعداد صحیح مثبت باشند که $q \geq ۲$ و $۲ \leq l \leq c$. آن‌گاه بزرگ‌ترین c-کد ضدجعل q-آرایه‌ای به طول l، دارای اندازه‌ی $l(q-۱)$ است.*

برهان. چون $۲ \leq l \leq c$ لذا $\lceil \frac{l}{c} \rceil = ۱$ و باقیمانده تقسیم $\frac{l}{c}$ برابر با l می‌باشد. پس در این حالت کران بالای قضیه ۳.۴، $l(q-۱)$ خواهد بود. □

نتیجه ۳.۴. [۶] *یک c-کد ضدجعل q-آرایه‌ای به طول l ، حداکثر $tq^{\lceil l/c\rceil} + O(q^{\lceil l/c\rceil - ۱})$ کدواژه دارد به‌طوری‌که t عددصحیح یکتایی که $t \in \{۱, ۲, \ldots, c\}$ و $t = l \mod c$.*

برهان. توجه کنیدکه t همان r در قضیه ۳.۴ است با این تفاوت که برای $r = ۰$ داریم $t = c$. لذا اگر $t \neq c$، آن‌گاه $\lfloor l/c\rfloor = \lceil l/c\rceil - ۱$ و با جای‌گذاری در کران (۱.۴) به نتیجه مطلوب خواهیم رسید. □

نتیجه ۴.۴. [۶] *فرض کنید l و c اعداد صحیح ثابت بزرگ‌تر یا مساوی ۲ باشند. بزرگ‌ترین اندازه‌ی یک c-کد ضدجعل q-آرایه‌ای به طول l را $M_{c,l}(q)$ تعریف کنید. آن‌گاه:*

$$\lim_{q\to\infty} \log M_{c,l}(q) = \lceil l/c\rceil.$$

برهان. با توجه به نتیجه ۳.۴ داریم:

$$M_{c,l}(q) \leq tq^{\lceil l/c\rceil} + kq^{\lceil l/c\rceil - ۱} \leq (t+۱)q^{\lceil l/c\rceil},$$

بنابراین

$$\log_q M_{,l}(q) \leq \lceil l/c\rceil + \log_q(t+۱),$$

از طرفی می‌دانیم

$$\lim_{q\to\infty} \log_q(t+۱) = ۰,$$

لذا داریم:

$$\log M_{c,l}(q) \leq \lceil l/c\rceil + o(۱).$$

حال فرض کنید q' بزرگ‌ترین توانی از یک عدد اول باشد که $q' \leq q$. بنا به قضیه اعداد اول داریم: $q'/q = ۱ - o(۱)$. از آن‌جاییکه در ساختار ۲ (فصل قبل)، برای q' به اندازه‌ی کافی بزرگ ($q' \geq l$)، یک c-کد ضدجعل q' آرایه‌ای با اندازه‌ی $q'^{\lceil l/c\rceil}$ به‌دست آوردیم، لذا $\log_{q'} M_{c,l}(q') \geq \lceil l/c\rceil$. بنابراین

$$\log_q M_{c,l}(q) \geq \log_q M_{c,l}(q') \geq \log_{q'} M_{c,l}(q') - o(۱) \geq \lceil l/c\rceil - o(۱).$$

پس

$$\lceil l/c\rceil - o(۱) \leq \log_q M_{c,l}(q) \leq \lceil l/c\rceil + o(۱).$$

لذا $\lim_{q\to\infty} \log_q M_{c,l}(q)$ موجود و برابر با $\lceil l/c \rceil$ است. □

نتیجه ۵.۴. [۶] *فرض کنید l و c اعداد صحیح ثابت بزرگ‌تر یا مساوی ۲ باشند و $l = ۱ \mod c$. همچنین فرض کنید $M_{c,l}(q)$ همانند نتیجه ۴.۴ تعریف شده باشد. آن‌گاه:*

$$\lim_{q\to\infty} M_{c,l}(q)/q^{\lceil l/c \rceil} = ۱.$$

برهان. فرض کنید q' مانند قبل تعریف شده باشد. پس

$$\lim_{q\to\infty} \frac{q'^{\lceil l/c \rceil}}{q^{\lceil l/c \rceil}} = ۱.$$

از طرفی

$$q'^{\lceil l/c \rceil} \leq M_{c,l}(q') \leq M_{c,l}(q) \leq tq^{\lceil l/c \rceil} + O(q^{\lceil l/c \rceil - ۱}).$$

با تقسیم طرفین رابطه بالا بر $q^{\lceil l/c \rceil}$ و سپس حد گرفتن از آن‌ها به رابطه زیر خواهیم رسید

$$\lim_{q\to\infty} \frac{q'^{\lceil l/c \rceil}}{q^{\lceil l/c \rceil}} \leq \lim_{q\to\infty} \frac{M_{c,l}(q)}{q^{\lceil l/c \rceil}} \leq t$$

از طرفی با توجه به فرض $(l = ۱ \mod c)$، $t = ۱$. لذا خواهیم داشت:

$$\lim_{q\to\infty} M_{c,l}(q)/q^{\lceil l/c \rceil} = ۱.$$

□

نتیجه ۶.۴. [۶] *با توجه به نتیجه ۴.۴ داریم:*

$$\lim_{q\to\infty} M_{۲,l}(q)/q^{\lceil l/۲ \rceil} = ۱ \qquad \text{اگر } l \text{ فرد باشد:}$$

و

$$\lim_{q\to\infty} M_{۲,l}(q)/q^{\lceil l/۲ \rceil} = ۲ \qquad \text{اگر } l \text{ زوج باشد:}$$

برهان. قسمت اول بنا به نتیجه ۵.۴ بر قرار است. زیرا $c = ۲$ و $l = ۱ \pmod ۲$.

برای قسمت دوم، بنا به نتیجه ۳.۴ و همچنین با توجه به $|C|$ در ساختار ۳ (فصل قبل) داریم:

$$۲(q-۱)^{l/۲}(۱-۱/۲\sqrt{q-۱}) \leq M_{۲,l}(q) \leq tq^{\lceil l/۲ \rceil} + O(q^{\lceil l/۲ \rceil - ۱})$$

حال با تقسیم طرفین نامساوری بر $q^{\lceil l/۲ \rceil}$ و همچنین حد گرفتن از آن‌ها داریم:

$$۲ \leq \lim_{q\to\infty} \frac{M_{۲,l}(q)}{q^{\lceil l/۲ \rceil}} \leq t$$

همچنین با توجه به این‌که $l = ۲ \pmod ۲$، داریم $t = ۲$. بنابراین در حالت زوج بودن l داریم:

$$\lim_{q\to\infty} M_{۲,l}(q)/q^{\lceil l/۲ \rceil} = ۲.$$

□

۳.۴ یک کران بالای بهبود یافته

با توجه به نتایج ۲.۴ و ۶.۴ (در این نتایج کران قضیه ۳.۴ در حالت تساوی بر قرار است)، ممکن است حدس بزنید که کران قضیه ۳.۴ همیشه دقیق است، اگرچه این چنین نیست. این بخش، مشکل فراهم سازی کران بالای بهبود یافته را به یک مشکل در تئوری مجموعه حدی کاهش می‌دهد که این مشکل در بخش ۴.۴ بررسی خواهد شد.

فرض کنید l و k اعداد صحیح ثابت باشرط $۱ \leq k \leq l$ باشند. D را یک مجموعه و

$$(V_S \subseteq D : S \subseteq \{۱, ۲, \ldots, l\}, |S| = k)$$

را یک خانواده از زیرمجموعه‌های D که توسط زیرمجموعه‌های k عضوی از $\{۱, ۲ \ldots, l\}$ اندیس گذاری شده‌اند، در نظر بگیرید. به این خانواده یک $(k, l; b, t)$-**سیستم مجموعه‌ای کد ضدجعل** می‌گوییم، اگر برای هر زیرمجموعه‌ی k تایی S از $\{۱, ۲ \ldots, l\}$، $|V_S| \leq b$ و همچنین داشته باشیم:

$$V_{S_۱} \cup V_{S_۲} \cup \ldots \cup V_{S_t} = D, \qquad (۲.۴)$$

که $S_۱, S_۲, \ldots S_t$ زیرمجموعه‌های دو به دو مجزا از $\{۱, ۲ \ldots, l\}$ با اندازه k باشند. سپس این خانواده را با نماد $(k, l; b, t) - FPCSS$ مشخص می‌کنیم و اندازه آن را $|D|$ قرار می‌دهیم.

می‌خواهیم نشان دهیم از هر کد ضدجعل، یک $FPCSS$ به‌دست می‌آید پس اگر بتوانیم بیشترین اندازه یک $FPCSS$ را تعیین کنیم، آن‌گاه با استفاده از آن یک کران بالا برای اندازه یک کد ضدجعل فراهم خواهیم کرد.

لم ۲.۴. [۶] *فرض کنید q، c و l اعداد صحیح مثبت باشند که $l > c$. قرار دهید $t \in \{۱, ۲ \dots, c\}$ که $t = l \pmod c$ و $k = \lceil l/c \rceil$. اگر C یک c-کد ضدجعل q-آرایه‌ای به طول l و شامل n کدواژه باشد، آن‌گاه یک $(k, l; q^k, t) - FPCSS$ وجود دارد با اندازه حداقل*

$$n - \binom{l}{k-۱} q^{k-۱}.$$

برهان. مطابق بخش ۲.۲.۴ ، برای هر $S \subseteq \{۱, ۲, \dots, l\}$، U_S را مجموعه‌ای از کدواژه‌های $x \in C$ تعریف می‌کنیم که منحصراً توسط زیرمجموعه مرتب شده ($x_i : i \in S$) از مؤلفه‌هایشان مشخص می‌شوند به این معنی که مؤلفه‌های ($x_i : i \in S$) یکتا هستند و

$$U_S = \{x \in C \ , \ \nexists y \in C \setminus \{x\} \ \ s.t. \ \ \forall i \in S; \ \ x_i = y_i\}.$$

همانند اثبات قضیه۳.۴ ، می توانیم ثابت کنیم زمانی‌که $S_۱, S_۲, \dots, S_c$ زیرمجموعه‌هایی از $\{۱, ۲, \dots, l\}$ با ویژگی $S_۱ \cup S_۲ \cup \dots \cup S_c = \{۱, ۲, \dots, l\}$ ، هستند آن‌گاه

$$C = U_{S_۱} \cup U_{S_۲} \cup \dots \cup U_{S_c}.$$

اکنون یک $FPCSS$ به این صورت تعریف می‌کنیم. قرار دهید:

$$D = C \setminus \left(\bigcup_S U_S \right)$$

که S تمام زیرمجموعه‌های $k - ۱$ تایی از مجموعه $\{۱, ۲, \dots, l\}$ را شامل می‌شود. در اثبات قضیه ۳.۴ مشاهده کردیم که $|U_S| \leq q^{|S|}$. بنابراین داریم:

$$|D| \geq n - \binom{l}{k-۱} q^{k-۱}.$$

برای هر زیرمجموعه $S \subseteq \{۱, ۲, \dots, l\}$ که $|S| = k$، تعریف کنید $V_S = U_S \cap D$. واضح است که $|V_S| \leq |U_S| \leq q^k$.

حال باید نشان دهیم زیرمجموعه‌های V_S ، به درستی یک $(k,l;q^k,t)-FPCSS$ تشکیل می‌دهند. فرض کنید $S_۱,S_۲,\ldots,S_t$ مجموعه‌ای از زیرمجموعه‌های k تایی مجزا از $\{۱,۲,\ldots,l\}$ باشند. باید ثابت کنیم $V_{S_۱}\cup V_{S_۲}\cup\ldots\cup V_{S_t}=D$. تعداد عضوهای $\{۱,۲,\ldots,l\}$ که درون $S_۱\cup S_۲\cup\ldots\cup S_t$ قرار نمی‌گیرند، برابر است با $l-tk$. از طرفی می‌دانیم $t=l \pmod c$ و $k=\lceil l/c\rceil$، در نتیجه $l=(k-۱)c+t$ و لذا $l-tk=(c-t)(k-۱)$.

بنابراین، مجموعه‌های $S_{t+۱},S_{t+۲},\ldots,S_c$ با اندازه $k-۱$ وجود دارند که

$$S_۱\cup S_۲\cup\ldots\cup S_c=\{۱,۲,\ldots,l\}.$$

بنا به نحوه‌ی تعریف D می‌دانیم $U_{S_i}\cap D=\emptyset \quad ;\ \forall i\geq t+۱$، زیرا مجموعه D شامل زیرمجموعه‌های $k-۱$ تایی نمی‌شود. بنابراین داریم:

$$\begin{aligned}V_{S_۱}\cup V_{S_۲}\cup\ldots\cup V_{S_t}&=(U_{S_۱}\cup U_{S_۲}\cup\ldots\cup U_{S_t})\cap D\\&=(U_{S_۱}\cup U_{S_۲}\cup\ldots\cup U_{S_c})\cap D\\&=C\cap D\\&=D.\end{aligned}$$

لذا همان‌طور که ادعا کردیم مجموعه‌های مذکور یک $FPCSS$ با اندازه حداقل

$$n-\binom{l}{k-۱}q^{k-۱}$$

تشکیل می‌دهند. □

اکنون مشکل تئوری مجموعه حدی را که حائز اهمیت است، معرفی می‌کنیم.

تعریف ۲.۴. [۶] خانواده $\mathcal{S}$ از زیرمجموعه‌های یک مجموعه را t-**غیر مجزا**[۴] می‌گوییم، هرگاه دارای t زیرمجموعه دو به دو مجزا نباشند.

[۴] t-colliding

فرض کنید t، k و l اعداد صحیح مثبت باشرط $۱ \leq k \leq l$ باشند. بیشترین تعداد زیرمجموعه‌ها در یک خانواده t-غیر مجزای $\mathcal{S}$ از زیرمجموعه های k تایی $\{۱, ۲, \ldots, l\}$ را $m(t,k,l)$ می‌نامیم. بنابراین وقتی $tk > l$ ، داریم $m(t,k,l) = \binom{l}{k}$. زیرا در این حالت هر t زیرمجموعه k تایی بیش از l عضو خواهد داشت و این یعنی عضو تکراری وجود دارد پس نمی‌توانند مجزا باشند، لذا t-غیر مجزا هستند. بنابراین، در این حالت می‌توان تمام زیرمجموعه‌های k تایی را در نظر گرفت و در حالت‌های دیگر $m(t,k,l) < \binom{l}{k}$.

قضیه ۴.۴. [۶] *اگر t، k، l و b اعداد صحیح مثبت باشرط $tk \leq l$ باشند، آن‌گاه یک $(k,l;b,t) - FPCSS$ با اندازه حداکثر*

$$\left(\frac{۱}{۱ - m(t,k,l)/\binom{l}{k}}\right) b$$

وجود دارد.

ملاحظه می‌کنیم برای $tk > l$، شرط (۲.۴) برقرار است. بنابراین در این حالت هیچ کرانی روی اندازه یک $(k,l;b,t) - FPCSS$ وجود ندارد.

برهان. فرض کنید D یک مجموعه و (V_S) مجموعه‌ای شامل زیر مجموعه‌های D باشد که تشکیل یک $(k,l;b,t) - FPCSS$ می‌دهند.

کران بالا روی $|D|$ را با شمارش اعضای مجموعه‌ی

$$K = \{(x,S) : x \in V_S\} \tag{۳.۴}$$

که $S \subseteq \{۱, ۲, \ldots, l\}$، $|S| = k$ و $x \in D$، به دو روش محاسبه می‌کنیم. $\binom{l}{k}$ تا انتخاب برای زیرمجموعه‌ها (Sها) وجود دارد. فرض کنید ابتدا S انتخاب شده باشد، حداکثر b انتخاب برای x وجود دارد. زیرا بنا به تعریف $FPCSS$، $|V_S| \leq b$. بنابراین $|K| \leq \binom{l}{k} b$.

ادعا می‌کنیم که یک $x \in D$ برای حداقل $\binom{l}{k} - m(t,k,l)$ زیرمجموعه S با اندازه k در V_S وجود دارد. مجموعه $\mathcal{S}$ را به صورت زیر تعریف می‌کنیم.

$$\mathcal{S} = \{S \subseteq \{۱, ۲, \ldots, l\} : |S| = k \text{ و } x \notin V_S\}$$

اکنون $\mathcal{S}$، t-غیر مجزا است، زیرا اگر زیرمجموعه‌های دو به دو مجزای $S_1, S_2, \ldots, S_t$ وجود داشته باشند آن‌گاه $x \notin V_{S_1} \cup V_{S_2} \cup \ldots \cup V_{S_t}$، که این با ویژگی (۲.۴) برای $FPCSS$، تناقض دارد. از طرفی چون $\mathcal{S}$، t-غیر مجزا است $|\mathcal{S}| \leq m(t,k,l)$، لذا ادعای ما صحیح است.

$|D|$ انتخاب برای x در مجموعه (۳.۴) وجود دارد و ادعای ما بیان می‌کند که برای یک x ثابت، حداقل $\binom{l}{k} - m(t,k,l)$ انتخاب برای S که $(x,S) \in K$، وجود دارد. بنابراین $|K| \geq |D|\big(\binom{l}{k} - m(t,k,l)\big)$ می‌باشد. اکنون دایم:

$$|D|\big(\tbinom{l}{k} - m(t,k,l)\big) \leq |K| \leq \tbinom{l}{k} b.$$

بنابراین

$$\begin{aligned} |D| &\leq \frac{\binom{l}{k} b}{\binom{l}{k} - m(t,k,l)} \\ &= \Big(\frac{1}{1 - m(t,k,l)/\binom{l}{k}}\Big) b. \end{aligned}$$

□

در مثال زیر نشان می‌دهیم که کران قضیه ۴.۴ دقیق است.

فرض کنید t، k و l اعداد صحیح مثبت باشرط $tk \leq l$ باشند. $\mathcal{S}$ را یک خانواده t-غیر مجزا از زیرمجموعه‌های k تایی از $\{1,2,\ldots,l\}$ درنظر بگیرید که شامل $m(t,k,l)$ زیرمجموعه است. قرار دهید $D = Sym(l)$ که $Sym(l)$ گروه متقارن روی $\{1,2,\ldots,l\}$ ، شامل تمام جای‌گشت‌های ممکن روی این مجموعه است. برای هر زیرمجموعه $S \subseteq \{1,2,\ldots,l\}$ که $|S| = k$، قراردهید:

$$V_S = \{\pi \in D : \pi(S) \notin \mathcal{S}\}.$$

فرض کنید $S_1, S_2, \ldots, S_t$ زیرمجموعه‌های دو به دو مجزا از مجموعه‌ی $\{1,2,\ldots,l\}$ باشند که برای هر $1 \leq i \leq t$، $|S_i| = k$ است. همچنین فرض کنید $\pi \in D$ ولی $\pi \notin V_{S_1} \cup V_{S_2} \cup \ldots \cup V_{S_t}$. سپس با توجه به تعریف V_S، برای هر $i \in \{1,2,\ldots,t\}$، $\pi(S_i) \in \mathcal{S}$. ولی این بدان معنا است که $\pi(S_1), \pi(S_2), \ldots, \pi(S_t)$ یک مجموعه شامل زیرمجموعه‌های دو به دو مجزا از $\mathcal{S}$ تشکیل می‌دهند. که

این با t-غیر مجزا بودن $\mathcal{S}$ تناقض دارد. بنابراین برای هر $\pi \in D$، $\pi \in V_{S_1} \cup V_{S_2} \cup \ldots \cup V_{S_t}$. لذا شرط (۲.۴) برقرار است.

به‌وضوح $|D| = l!$ و برای هر S، $|V_S| = b = \left(\binom{l}{k} - m(t,k,l)\right)k!(l-k)!$. زیرا برای شمارش تعداد اعضای V_S ابتدا باید تعداد S هایی که $S \notin \mathcal{S}$ را محاسبه کرده و سپس تمام توابع π روی این مجموعه‌ها را شمارش کنیم. از طرفی داریم:

$$\begin{aligned}\frac{b}{1 - m(t,k,l)/\binom{l}{k}} &= \frac{\left(\binom{l}{k} - m(t,k,l)\right)k!(l-k)!}{\left(\binom{l}{k} - m(t,k,l)\right)/\binom{l}{k}} \\ &= \frac{\left(\binom{l}{k} - m(t,k,l)\right)\overbrace{k!(l-k)!\binom{l}{k}}^{l!}}{\binom{l}{k} - m(t,k,l)} \\ &= l! = |D|.\end{aligned}$$

بنابراین D یک $(k,l;b,t) - FPCSS$ است که در حالت تساوی کران قضیه ۴.۴ صدق می‌کند.

نتیجه ۷.۴. [۶] *فرض کنید c و l اعداد صحیح باشند که $l \geq 2$ و $c \geq 2$. $t \in \{1,2,\ldots,c\}$ را در نظر بگیرید که $t = l \pmod c$ باشد. فرض کنید C یک c-کد ضدجعل q-آرایه‌ای به طول l باشد. آن‌گاه برای c و l ثابت و q به اندازه کافی بزرگ $|C| \leq k'q^{\lceil l/c \rceil} + O(q^{\lceil l/c \rceil - 1})$ است. که ثابت k' به صورت زیر تعریف می‌شود*

$$k' = \frac{1}{1 - m(t, \lceil l/c \rceil, l)/\binom{l}{\lceil l/c \rceil}}.$$

برهان. فرض کنید D یک $(k,l;q^k,t) - FPCSS$ وابسته به C باشد. با توجه به $k = \lceil l/c \rceil$ و $t\lceil l/c \rceil \leq l$ و بنا به لم ۲.۴ و قضیه ۴.۴ داریم:

$$n - \binom{l}{k-1}q^{k-1} \leq |D| \leq \frac{b}{1 - m(t,k,l)/\binom{l}{k}},$$

که $|C| = n$. لذا

$$n \leq \frac{b}{1 - m(t,k,l)/\binom{l}{k}} + \binom{l}{k-1}q^{k-1}.$$

از طرفی $b = q^k$ و $k = \lceil l/c \rceil$، بنابراین

$$|C| \leq \frac{q^{\lceil l/c \rceil}}{۱ - m(t, \lceil l/c \rceil, l)/\binom{l}{\lceil l/c \rceil}} + \binom{l}{\lceil l/c \rceil - ۱} q^{\lceil l/c \rceil - ۱}.$$

لذا داریم:

$$|C| \leq k' q^{\lceil l/c \rceil} + O(q^{\lceil l/c \rceil - ۱}).$$

□

۴.۴ کران‌های وابسته

فرض کنید t، k و l اعداد صحیح مثبت باشرط $tk \leq l$ باشند. مانند قبل $m(t,k,l)$ را بیشترین اندازه یک خانواده t-غیر مجزای $\mathcal{S}$، از زیرمجموعه‌های مجموعه $\{۱, ۲, \ldots, l\}$ تعریف می‌کنیم، که برای هر $S \in \mathcal{S}$، $|S| = k$. در این بخش یک کران بالا برای $m(t,k,l)$ بیان می‌کنیم.

بدیهی است که در حالت $t = ۱$، هیچ خانواده از زیرمجموعه‌ها نمی‌توانند t-غیر مجزا باشند، لذا در این حالت $m(t,k,l) = ۰$. پس ما فرض می‌کنیم $t \geq ۲$. خانواده $\mathcal{M}$ را به‌صورت زیر تعریف می‌کنیم.

$$\mathcal{M} = \{S \subseteq \{۱, ۲, \ldots, l\} : \ |S| = k \quad و \quad S \cap \{۱, ۲, \ldots, t-۱\} \neq \emptyset\}$$

این خانواده t-غیر مجزا است، زیرا برای هر t زیرمجموعه $S_۱, S_۲, \ldots, S_t$ از مجموعه $\{۱, ۲, \ldots, l\}$ که برای $۱ \leq i \leq t$، $|S_i| = k$، می‌دانیم هرکدام حداقل شامل یک عضو از $\{۱, ۲, \ldots, t-۱\}$ می‌شوند. لذا بنا به اصل لانه کبوتری، حداقل دوتا از این زیرمجموعه‌ها عضو تکراری دارد. بنابراین $\mathcal{M}$، t-غیر مجزا و $|\mathcal{M}| = \binom{l}{k} - \binom{l-(t-۱)}{k}$. این خانواده یک کران پایین برای $m(t,k,l)$ بیان می‌کند که ما انتظار داریم دقیق باشد. در بسیاری از مقاله‌هایی که روی این مسئله تحقیق کرده‌اند، سعی شده است که نشان دهند وقتی که شرایط یادشده برای t، k و l برقرار باشد، $\mathcal{M}$ بهینه است (به این معنی که $m(t,k,l) = |\mathcal{M}|$). اردوش و سایرین در [۲۳] (همچنین [۴] را ملاحظه کنید) اظهار دارند که درحالت $t = ۲$، $\mathcal{M}$ بهینه است و $m(۲,k,l) = \binom{l-۱}{k-۱}$ می‌باشد. اردوش در [۲۱] برای این مسئله، ابتدا $t > ۲$ را درنظر گرفته بود. او اثبات

کرد که یک ثابت k وجود دارد که هرگاه $l > tk$، آن‌گاه $\mathcal{M}$ بهینه است. بولوباش و سایرین در [۷] نشان دادند که کافی است $l > ۲k^{۳}t$ باشد. در [۱۶] یک نتیجه از فرانکل آمده است که نشان می‌دهد، زمانی‌که برای برخی ثابت k'، $l > k'kt^{۲}$، آن‌گاه $\mathcal{M}$ بهینه است. دزا [۵] و فرانکل [۶] حدس می‌زنند که وقتی برای برخی ثابت k'' داشته باشیم $l > k''k't$، آن‌گاه $\mathcal{M}$ بهینه است.

علاوه بر اثبات $m(t,k,l) = \binom{l}{k} - \binom{l-(t-۱)}{k}$ برای مقادیر مشخص t، k و l، علاقه مندیم که یک کران بالا برای $m(t,k,l)$ به ازای هر مقداری از t، k و l پیدا کنیم. یک چنین کرانی را در قضیه ۵.۴ در ادامه خواهیم آورد. این کران از اثبات کتونا از قضیه اردوش-کو-رادو[۷] در [۲۷] نتیجه می‌شود که حالت خاصی از کران گرونا در [۲۶] است.

به منظور کامل کردن بحث اثبات آن را ذکر می‌کنیم. قبل از اثبات کران گرونا ابتدا یک حالت ساده‌تر را در نظر می‌گیریم. $\mathbb{Z}_l$ را در نظر بگیرید. برای $a \in \mathbb{Z}_l$، $T_l(a) \subseteq \mathbb{Z}_l$ را به‌صورت زیر تعریف کنید:

$$T_l(a) = \{a, a+۱, \ldots, a+(k-۱)\},$$

و قرار دهید:

$$\mathcal{T} = \{T_l(a) \,:\, a \in \mathbb{Z}_l\}.$$

لم ۳.۴. [۶] *فرض کنید t، k و l اعداد صحیح مثبت باشرط $l \geq tk$ باشند. مجموعه‌های $T_l(a)$ و خانواده $\mathcal{T}$ را به صورت بالا تعریف کنید. فرض کنید $\mathcal{S}$ در $\mathcal{T}$ قرار دارد و t-غیر مجزا است. آن‌گاه $|\mathcal{S}| \leq (t-۱)k$.*

دقت کنید که خانواده $\mathcal{S} = \{T_l(a) \,:\, ۰ \leq a \leq (t-۱)k-۱\}$، t-غیر مجزا است و در حالت تساوی کران بالا صدق می‌کند. زیرا هر t عضو از این خانواده را که در نظر بگیریم، غیر مجزا هستند. فرض کنید $T_l(a_۱), T_l(a_۲), \ldots, T_l(a_t) \in \mathcal{S}$ مجزا و $a_۱ < a_۲ < \ldots < a_t$. لذا بین هر a_i و $a_{i+۱}$ حداقل k اختلاف وجود دارد و این یعنی $a_t \geq tk$. بنابراین $T_l(a_t) \notin \mathcal{S}$. از این رو خانواده $\mathcal{S}$، t-غیر مجزاست و $|\mathcal{S}| = (t-۱)k$.

[۵] Deza
[۶] Frankle
[۷] Erdos-Ko-Rado

برهان. به استقراء روی l ثابت می‌کنیم. فرض کنید $l = tk$. در این حالت می‌توانیم $\mathcal{T}$ را به $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_k$ تقسیم‌بندی کنیم که برای هر i،

$$\mathcal{T}_i = \{T_l(i), T_l(i+k), T_l(i+2k), \ldots, T_l(i+(t-1)k)\}.$$

چون $\mathcal{T}_i$ ها شامل t مجموعه دو به دو مجزا هستند، لذا در $\mathcal{S}$ واقع نمی‌شوند پس $|\mathcal{T}_i \cap \mathcal{S}| \leq t-1$. بنابراین

$$\begin{aligned} |\mathcal{S}| &= |(\overbrace{\mathcal{T}_1 \cup \mathcal{T}_2 \cup \ldots \cup \mathcal{T}_K}^{\mathcal{T}}) \cap \mathcal{S}| \\ &= \sum_{i=t}^{k} |\mathcal{T}_i \cap \mathcal{S}| \\ &\leq (t-1)k. \end{aligned}$$

لذا برای حالت $t = lk$ ، لم برقرار است.

حال، $t > lk$ را درنظر بگیرید و فرض کنید برای تمام مقادیر کوچک‌تر از l ، حکم برقرار باشد. قطعاً $\mathcal{S} \neq \mathcal{T}$، لذا $c \in \mathbb{Z}_l$ وجود دارد که $\mathcal{T}_l(c) \notin \mathcal{S}$. خانواده $\bar{\mathcal{S}}$ از زیرمجموعه‌های $\mathbb{Z}_{l-1}$ را به‌صورت زیر تعریف می‌کنیم.

$$\begin{aligned} \bar{\mathcal{S}} =& \{T_{l-1}(a) : a \in \{0, 1, \ldots, c-1\}, T_l(a) \in S\} \\ & \cup \{T_{l-1}(a-1) : a \in \{c+1, c+2, \ldots, l-1\}, T_l(a) \in S\} \end{aligned}$$

به‌وضوح یک تناظر یک به یک بین زیر مجموعه‌های درون $\mathcal{S}$ و زیر مجموعه‌های درون $\bar{\mathcal{S}}$ وجود دارد. پس $|\mathcal{S}| = |\bar{\mathcal{S}}|$. علاوه براین اندازه اشتراک یک جفت از زیرمجموعه‌های درون $\bar{\mathcal{S}}$ ، حداقل به بزرگی اندازه اشتراک زیرمجموعه‌های متناظرشان در $\mathcal{S}$ است. بنابراین t-غیر مجزا بودن $\mathcal{S}$ موجب می‌شود که $\bar{\mathcal{S}}$ نیز t-غیر مجزا باشد.

بنا به فرض استقراء، $|\bar{\mathcal{S}}| \leq (t-1)k$. بنابراین $|\mathcal{S}| \leq (t-1)k$ و حکم برقرار است. □

قضیه ۵.۴. [۶] *فرض کنید t، k و l اعداد صحیح مثبت باشرط $tk \leq l$ باشند. همچنین فرض کنید $\mathcal{S}$ یک خانواده t-غیر مجزا از زیرمجموعه‌های k تایی $\{1, 2, \ldots, l\}$ باشد. آن‌گاه داریم:*

$$|\mathcal{S}| \leq \binom{l}{k} \frac{(t-1)k}{l}.$$

برهان. خانواده $\mathcal{T}$ را همانند قبل تعریف کنید. فرض کنید Q مجموعه‌ای از زوج مرتب‌های (α, S) باشد که $S \in \mathcal{S}$ و $\alpha(S) \in \mathcal{T}$ که $\alpha : \{۱, ۲, \ldots, l\} \to \mathbb{Z}_l$ یک نگاشت دوسویی باشد. حال عناصر مجموعه Q را به دو روش محاسبه می‌کنیم.

به تعداد $|\mathcal{S}|$، انتخاب برای $S \in \mathcal{S}$ وجود دارد و به‌ازای یک S ثابت، l انتخاب برای $\alpha(S) \in \mathcal{T}$ وجود دارد و $k!(l-k)!$ حالت برای یک نگاشت دوسویی مناسب α وجود دارد. بنابراین

$$|Q| = l|\mathcal{S}|k!(l-k)!.$$

حال تعداد عناصر Q را به روش دیگری محاسبه می‌کنیم. $l!$ انتخاب برای α وجود دارد. اکنون فرض کنید α ثابت باشد. تعداد حالت‌ها برای انتخاب S برابر با $|\mathcal{X}|$ است که

$$\mathcal{X} = \{S \in \mathcal{S} : \alpha(S) \in \mathcal{T}\}.$$

$\mathcal{X}$ یک زیرخانواده از خانواده t-غیر مجزا $\mathcal{S}$ است. لذا $\mathcal{X}$ نیز t-غیر مجزا است. پس زیرخانواده متناظر $\alpha(\mathcal{X})$ از $\mathcal{T}$ (که $\alpha(\mathcal{X}) = \{\alpha(S) : S \in \mathcal{X}\}$ است) نیز t-غیر مجزا می‌باشد. سپس با توجه به لم ۳.۴، $|\mathcal{X}| = |\alpha(\mathcal{X})| \leq (t-۱)k$. لذا داریم $|Q| \leq l!(t-۱)k$، بنابراین:

$$\begin{aligned}
|\mathcal{S}| &= |Q|/(k!(l-k)!l!) \\
&\leq l!(t-۱)k/(k!(l-k)!l!) \\
&= \binom{l}{k}\frac{(t-۱)k}{l}.
\end{aligned}$$

□

قضیه ۵.۴ بیان می‌کند که $m(t,k,l) \leq \binom{l}{k}\frac{(t-۱)k}{l}$. بدیهی است در حالت $t = ۱$ کران قضیه ۵.۴ بهترین حالت ممکن است، یعنی تساوی برقرار است زیرا در این حالت $|\mathcal{S}| = ۰$. همچنین برای حالت $t = ۲$ نیز این کران دقیق است. زیرا کافی است مجموعه $\mathcal{M}$ را که در ابتدای بخش تعریف کردیم درنظر

بگیریم. سپس داریم:

$$\begin{aligned}|\mathcal{M}| &= \binom{l}{k} - \binom{l-۱}{k} \\ &= \frac{l!}{k!(l-k)!} - \frac{(l-۱)!}{k!(l-k)!} \\ &= \frac{l! - (l-۱)!(l-k)}{k!(l-k)!} \\ &= \frac{(l-۱)!(l-l+k)}{k!(l-k)!} \\ &= \frac{(l-۱)!}{(k-۱)!(l-k)!} \\ &= \binom{l}{k}\frac{k}{l}.\end{aligned}$$

برای حالت $tk = l$ ، خانواده t-غیر مجزای

$$\mathcal{N} = \{S \subseteq \{۱, ۲, \ldots, l\} : |S| = k \text{ و } ۱ \notin S\}$$

شامل $\binom{l}{k}\frac{(t-۱)k}{l}$ مجموعه است. بنابراین کران قضیه ۵.۴ برای حالت $tk = l$ نیز دقیق است.

زمانی‌که t و k ثابت باشند و l به سمت بی‌نهایت میل کند کران قضیه ۵.۴ به شکل زیر خواهد بود:

$$m(t, k, l) \leq (t-۱)l^{k-۱}/(k-۱)! + O(l^{k-۲}).$$

ثابت می‌کنیم کران پایین $m(t, k, l)$ نیز به همین صورت خواهد بود. برای این منظور خانواده t-غیر مجزای $\mathcal{M}$ را که در ابتدای بخش تعریف کردیم، در نظر بگیرید. قبلا ثابت کردیم که $|\mathcal{M}| = \binom{l}{k} - \binom{l-(t-۱)}{k}$. در این محاسبه ابتدا همه زیرمجموعه‌های k تایی از $\{۱, ۲, \ldots, l\}$ شمارش شده و سپس زیرمجموعه‌هایی که هیچ اشتراکی با $\{۱, ۲, \ldots, t-۱\}$ ندارند، حذف شده است. می‌خواهیم $|\mathcal{M}|$ را به روش دیگری محاسبه کنیم. در این روش ابتدا تعداد زیرمجموعه‌های k تایی که یک عضو از $\{۱, ۲, \ldots, t-۱\}$ دارند را محاسبه می‌کنیم. سپس زیرمجموعه‌هایی که دو عضو از $\{۱, ۲, \ldots, t-۱\}$ دارند و به همین ترتیب ادامه می‌دهیم تا

در نهایت زیرمجموعه‌های k تایی که $t-۱$ عضو اولیه را دارند، شمارش می‌کنیم. بنابراین

$$\begin{aligned}|\mathcal{M}| &= \binom{t-۱}{۱}\binom{l-(t-۱)}{k-۱} \\ &+ \binom{t-۱}{۲}\binom{l-(t-۱)}{k-۲} \\ &+ \dots \\ &+ \binom{t-۱}{t-۱}\binom{l-(t-۱)}{k-(t-۱)} \\ &= \sum_{i=۱}^{t-۱}\binom{t-۱}{i}\binom{l-(t-۱)}{k-i}.\end{aligned}$$

اگر k و t را ثابت در نظر بگیریم و l به اندازه کافی بزرگ باشد به عبارت $(t-۱)l^{k-۱}/(k-۱)!+O(l^{k-۲})$ می‌رسیم.

پس در این حالت، نسبت بین کران بالا و کران پایین روی $m(t,k,l)$ به سمت ۱ میل می‌کند. بنابراین برای l به اندازه کافی بزرگ، کران قضیه ۵.۴ دقیق است و حالت تساوی آن رخ می‌دهد.

نتیجه ۸.۴. [۶] *فرض کنید c و l اعداد صحیح باشند که $c \geq ۲$ و $l \geq ۲$. $t \in \{۱,۲,\dots,c\}$ را درنظر بگیرید که $t = l \pmod c$. فرض کنید C یک c-کد ضدجعل به طول l باشد. آن‌گاه:*

$$|C| \leq \Big(\frac{l}{l-(t-۱)\lceil l/c\rceil}\Big)q^{\lceil l/c\rceil} + O(q^{\lceil l/c\rceil-۱}).$$

برهان. با توجه به نتیجه ۷.۴ می‌دانیم $|C| \leq kq^{\lceil l/c\rceil} + O(q^{\lceil l/c\rceil-۱})$، که ثابت k برابر است با:

$$k = \frac{۱}{۱ - m(t,\lceil l/c\rceil,l)/\binom{l}{\lceil l/c\rceil}},$$

و $t\lceil l/c\rceil \leq l$. از طرفی با توجه به قضیه ۵.۴ می‌دانیم

$$m(t,\lceil l/c\rceil,l) \leq \binom{l}{\lceil l/c\rceil}\frac{(t-۱)\lceil l/c\rceil}{l},$$

پس

$$\begin{aligned}۱ - m(t,\lceil l/c\rceil,l)\Big/\binom{l}{\lceil l/c\rceil} &\geq ۱ - \frac{(t-۱)\lceil l/c\rceil}{l} \\ &= \frac{l-(t-۱)\lceil l/c\rceil}{l}.\end{aligned}$$

از این‌رو

$$\frac{۱}{k} \geq \frac{l-(t-۱)\lceil l/c\rceil}{l}$$

و از آن‌جایی که ثابت k ، مثبت و $t\lceil l/c\rceil \leq l$، پس دوطرف نامساوی مثبت خواهد بود لذا

$$k \leq \frac{l}{l-(t-۱)\lceil l/c\rceil}.$$

بنابراین

$$|C| \leq \Big(\frac{l}{l-(t-۱)\lceil l/c\rceil}\Big)q^{\lceil l/c\rceil} + O(q^{\lceil l/c\rceil-۱}).$$

□

۵.۴ کران‌های بدون ساختار

کدهای ضدجعل بدون ساختار، اغلب با روش‌های احتمالی حاصل شده‌اند. برای بعضی از این کدها، کران‌هایی از این نوع نتیجه گرفته شده است. در این بخش یک روش برای به‌دست آوردن این کران‌ها ارائه می‌دهیم که اغلب به‌صورت مشابه اثبات شده‌اند. برای روشن ساختن تکنیک استفاده شده، با یک کران برای خانواده‌های درهم‌ساز کامل شروع می‌کنیم. این کران ابتدا در [۳۲] (همچنین [۳۳] را مشاهده کنید) ثابت شده بود.

گراف $G=(V,E)$ داده شده است. فرض کنید $P(G,m)$ **چندجمله‌ای رنگی** [۸] G باشد که به این صورت تعریف شده‌است: برای یک عددصحیح مثبت m، $P(G,m)$ تعداد m-رنگ آمیزی‌های مجاز G رامشخص می‌کند (یعنی تعداد روش‌ها برای رنگ کردن رئوس G با استفاده از m رنگ تعیین شده به‌طوری‌که هیچ دو رأس مجاور $v_۱, v_۲ \in V$ که توسط یال $e \in E$ به‌هم وصل شده‌اند، یک‌رنگ نباشند). واضح است که $P(G,m)$ یک چندجمله‌ای بر حسب m و از درجه $|V|$ می‌باشد. اگر رئوس G بطور مستقل و تصادفی با استفاده از m رنگ، رنگ آمیزی شده باشند، آن‌گاه احتمال اینکه نتیجه، یک m-رنگ آمیزی مجاز باشد برابر است با $P(G,m)/m^{|V|}$. اکنون ماتریس $N \times n$، A را درنظر بگیرید که ورودی‌های آن عناصر یک مجموعه ثابت S با اندازه m هستند و ستون‌های آن با اعداد $۱, ۲, \ldots n$ شماره گذاری شده‌اند. برای یک

[۸] chromatic polynomial

مجموعه C از w ستون A، تعریف کنید: $X_A(C) = ۰$، اگر یک سطر از A وجود داشته باشد که درایه‌هایش روی ستون‌های C متمایز باشند و در غیر آن قرار دهید $X_A(C) = ۱$. فرض کنید A یک ماتریس تصادفی $N \times n$ باشد (ورودی‌های A به‌صورت مستقل و تصادفی از مجموعه S انتخاب شوند) و $X(C)$ متغیر تصادفی باشد که توسط آن مشخص می‌شود. واضح است که مقادیر مورد انتظار از $X(C)$ برابر است با:

$$\begin{aligned} E[X(C)] &= \left(۱ - \frac{P(K_w, m)}{m^w} \right)^N \\ &= \left(۱ - \frac{m(m-۱)\cdots(m-w+۱)}{m^w} \right)^N. \end{aligned}$$

که این در واقع احتمال $X(C) = ۱$ است و با استفاده از محاسبه احتمال $X(C) = ۰$ به‌دست آمده است. $P(K_w, m)$ نیز چندجمله‌ای رنگی گراف کامل w رأسی است. زیرا برای متمایز بودن درایه‌ها روی w ستون مجموعه C، کافیست گراف کامل K_w را در نظر بگیریم. چون تمام رأس‌ها در این گراف به هم متصل هستند لذا واضح است که مجاز بودن یک m-رنگ آمیزی برای این گراف به معنی متمایز بودن درایه‌های این ستون‌ها می‌باشد. یعنی به تعداد رنگ آمیزی‌های مجاز برای این گراف، سطر در A وجود دارد که در این سطرها درایه‌های مربوط به ستون‌های C متمایزند. اگر متغیر تصادفی را به‌صورت زیر زیر تعریف کنیم

$$X = \sum_{\{C \subseteq \{۱,\dots,n\} : |C| = w\}} X(C),$$

آن‌گاه فرمول زیر حاصل می‌شود:

$$\begin{aligned} E[X] &= \binom{n}{w} \left(۱ - \frac{m(m-۱)\cdots(m-w+۱)}{m^w} \right)^N \\ &= \binom{n}{w} \left(۱ - \frac{w!\binom{m}{w}}{m^w} \right)^N \\ &= \binom{n}{w} \left(\frac{m^w - w!\binom{m}{w}}{m^w} \right)^N. \end{aligned}$$

واضح است که اگر $E[X] < ۱$ حداقل یک $X = ۰$ وجود دارد، لذا $\sum_{\{C \subseteq \{۱,\dots,n\} : |C| = w\}} X(C) = ۰$ و این یعنی یک ماتریس A وجود دارد که برای هر $C \subseteq \{۱, \dots, n\}$ با $|C| = w$، یک سطر موجود است که درایه‌های آن روی ستون‌های C متمایز است. لذا ماتریس A ماتریس وقوع یک $PHF(N; n, m, w)$ است.

قضیه ۶.۴. [۳۲] *اگر*

$$N > \frac{\log \binom{n}{w}}{\log(m^w) - \log\left(m^w - w!\binom{m}{w}\right)}$$

آن‌گاه یک $PHF(N; n, m, w)$ *وجود دارد.*

برهان. با توجه به توضیحات بالا فقط کافیست قرار دهیم $E[X] < ۱$:

$$\begin{aligned} E(X) &= \binom{n}{w}\left(\frac{m^w - w!\binom{m}{w}}{m^w}\right)^N < ۱ \\ \Rightarrow \quad & \log\binom{n}{w} + N\log\left(\frac{m^w - w!\binom{m}{w}}{m^w}\right) < ۰ \\ \Rightarrow \quad & \log\binom{n}{w} < -N\Big(\log\left(m^w - w!\binom{m}{w}\right) - \log\left(m^w\right)\Big) \end{aligned}$$

و سرانجام

$$N > \frac{\log \binom{n}{w}}{\log(m^w) - \log\left(m^w - w!\binom{m}{w}\right)}.$$

حال به روش بازگشتی به حکم می‌رسیم. □

ما می‌توانیم از روشی مشابه برای اثبات کران‌های خانواده‌های درهم جداساز استفاده کنیم. فرض کنید $|C_۱| = w_۱, |C_۲| = w_۲$ و $C_۱ \cap C_۲ = \emptyset$. قرار دهید $w = w_۱ + w_۲$. ماتریس $N \times n$، A را درنظر بگیرید، تعریف کنید $X_A(C_۱, C_۲) = ۰$، اگر یک سطر از A وجود داشته باشد که درایه‌هایش روی ستون‌های $C_۱$ با درایه‌ها روی ستون‌های $C_۲$ متمایزند و در غیر این صورت قرار دهید $X_A(C_۱, C_۲) = ۱$. بنابراین خواهیم داشت:

$$E[X(C_۱, C_۲)] = \left(۱ - \frac{P(K_{w_۱,w_۲}, m)}{m^w}\right)^N.$$

که در این‌جا $P(K_{w_۱,w_۲}, m)$ چندجمله‌ای رنگی گراف دوبخشی $K_{w_۱,w_۲}$ است که تمام یال‌های ممکن بین دو بخش آن وجود دارد ولی رأس‌های هر بخش به هم اتصالی ندارند. مجاز بودن رنگ آمیزی در این گراف به این معنی است که اعضای بخش اول یا بخش دوم می‌توانند با هم یک‌رنگ هم باشند اما رنگ‌های به‌کار

رفته در $w_۱$ رأس بخش اول نمی‌تواند در $w_۲$ رأس بخش دوم به‌کار رود و این دقیقا همان تعبیر خانواده‌های درهم جداساز است. لذا به تعداد رنگ آمیزی‌های مجاز برای این گراف، سطر در ماتریس A وجود دارد که درایه‌های این سطرها روی $w_۱$ ستون $C_۱$ با $w_۲$ ستون $C_۲$ متمایزند. برای سهولت قرار دهید:

$$p = ۱ - \frac{P(K_{w_۱,w_۲}, m)}{m^w},$$

و همچنین

$$X = \sum_{\substack{\{C_۱,C_۲\subseteq\{۱,۲,\cdots,n\}:\\ |C_۱|=w_۱,|C_۲|=w_۲\}}} X(C_۱, C_۲).$$

بنابراین داریم:

$$E[X] = \begin{cases} \binom{n}{w_۱}\binom{n-w_۱}{w_۲}p^N & w_۱ \neq w_۲, \\ \frac{۱}{۲}\binom{n}{w_۱}\binom{n-w_۱}{w_۱}p^N & w_۱ = w_۲. \end{cases}$$

همان‌طور که برای خانواده‌های درهم‌ساز کامل داشتیم، برای $E[X] < ۱$ ، یک $SHF(N; n, m, \{w_۱, w_۲\})$ وجود خواهد داشت. همچنین اگر $E[X] < n/۲$، یک $SHF(N; n/۲, m, \{w_۱, w_۲\})$ وجود دارد. از این بحث دو کران زیر را نتیجه می‌گیریم.

قضیه ۷.۴. [۳۵] *فرض کنید $w_۱, m, n$ و $w_۲$ اعداد صحیح مثبت باشند و p همانند بالا تعریف شده باشد. بنابراین حالت‌های زیر برقرار است:*

۱. *اگر*

$$N > \frac{(w_۱ + w_۲)\log n}{-\log p},$$

آن‌گاه یک $SHF(N; n, m, \{w_۱, w_۲\})$ وجود دارد.

۲. *اگر*

$$N > \frac{(w_۱ + w_۲ - ۱)\log(۲n)}{-\log p},$$

آن‌گاه یک $SHF(N; n/۲, m, \{w_۱, w_۲\})$ وجود دارد.

برهان. با توجه به توضیحات بالا کافیست برای قسمت اول $E(X) < ۱$ و برای قسمت دوم $E(X) < n/۲$ باشد. سپس مشابه اثبات قضیه ۶.۴ روند بازگشتی را برای اثبات دنبال می‌کنیم.

۱. می‌دانیم $\binom{n}{k} \leq n^k$ لذا

$$\binom{n}{w_۱}\binom{n-w_۱}{w_۲}p^N \leq n^{w_۱}n^{w_۲}p^N.$$

پس اگر عبارت سمت راست، کمتر از ۱ باشد $E(X)$ نیز کمتر از ۱ خواهد بود.

$$\begin{aligned} & n^{w_۱}n^{w_۲}p^N < ۱ \\ \Rightarrow \quad & w_۱ \log n + w_۲ \log n + N \log p < ۰ \\ \Rightarrow \quad & \frac{(w_۱ + w_۲)\log n}{-\log p} < N \end{aligned}$$

بنابراین به‌ازای $N > \frac{(w_۱ + w_۲)\log n}{-\log p}$، داریم $E(X) < ۱$ و یک $SHF(N; n, m, \{w_۱, w_۲\})$ موجود خواهد بود. همچنین برای حالت $w_۱ = w_۲$ نیز مشاهده می‌کنیم که مقدار $E(X)$ در این حالت از مقدار استفاده شده در محاسبات فوق کمتر است. لذا برای N به‌دست آمده، همچنان $E(X) < ۱$.

۲. با توجه به توضیحات قبلی، در این قسمت کافیست عبارت سمت راست نامساوی بالا کمتر از $n/۲$ باشد. لذا

$$\begin{aligned} & n^{w_۱}n^{w_۲}p^N < n/۲, \\ \Rightarrow \quad & ۲n^{w_۱+w_۲-۱}p^N < ۱. \end{aligned}$$

از طرفی می‌دانیم

$$۲n^{w_۱+w_۲-۱}p^N < (۲n)^{w_۱+w_۲-۱}p^N.$$

لذا اگر عبارت سمت راست این نامساوی کمتر از ۱ باشد آن‌گاه عبارت سمت چپ نیز کمتر از ۱ و

در نهایت $E(X)$ کمتر از $n/۲$ خواهد بود. بنابراین

$$(۲n)^{w_۱+w_۲-۱}p^N < ۱,$$

$$\Rightarrow \quad (w_۱ + w_۲ - ۱)\log(۲n) + N\log p < ۰,$$

$$\Rightarrow \quad \frac{(w_۱ + w_۲ - ۱)\log(۲n)}{-\log p} < N.$$

لذا برای N های به‌دست آمده $E(X) < n/۲$ و یک $SHF(N; n/۲, m, \{w_۱, w_۲\})$ وجود دارد.

□

۱.۵.۴ بحث و کاربردها

کاربرد قضیه ۷.۴ را با نتیجه گیری برخی کران‌های شناخته شده شرح می‌دهیم. قرار می‌دهیم $m = ۲$، زیرا در این حالت، سیستم‌های جداساز و کدهای دودویی ضدجعل امن به‌دست می‌آید. واضح است که

$$P(K_{w_۱,w_۲}, ۲) = ۲,$$

بنابراین وقتی $m = ۲$، داریم $p = ۱ - \frac{۱}{۲^{w_۱+w_۲-۱}}$.

در اینجا کاربردهایی از قضیه ۷.۴ را بیان می‌کنیم:

- فرض کنید $w_۱ = ۱$ و $w_۲ = ۲$. آن‌گاه $p = ۳/۴$ و $\frac{w_۱ + w_۲ - ۱}{-\log_۲ p} = \frac{۲}{۲ - \log_۲ ۳} \approx ۴/۸۱۹$. بنابراین یک $(۱, ۲)-SS(n, \approx ۴/۸۱۹\log_۲ n)$ با استفاده از قسمت دوم قضیه ۷.۴ وجود دارد. این نتیجه به‌طور مستقل در [۳]، [۲۹] و [۱۱] نشان داده شده است.

- فرض کنید $w_۱ = w_۲ = ۲$. آن‌گاه $p = ۷/۸$ و $\frac{w_۱ + w_۲ - ۱}{-\log_۲ p} = \frac{۳}{۳ - \log_۲ ۷} \approx ۱۵/۵۷۳$. بنابراین یک $(۲, ۲) - SS(n, \approx ۱۵/۵۷۳\log_۲ n)$ نیز با استفاده از قسمت دوم قضیه ۷.۴ وجود دارد. این نتیجه در [۳۰] نشان داده شده است. پیش از این در [۲۵] نشان داده شده که یک

$(۲,۲) - SS(n, \approx ۲۰/۷۴۶ \log_۲ n)$ وجود دارد. در حقیقت این نتیجه‌ای است که از قسمت اول قضیه ۷.۴ حاصل می‌شود.

- فرایدمن و سایرین در [۲۵] وجود یک $(w_۱, w_۲) - SS(n, \gamma \log_۲ n)$ را اثبات کردند که γ، مقدار داده شده در قسمت اول قضیه ۷.۴ است. البته با جایگزین کردن قسمت دوم همان قضیه، می‌توان خانواده مطلوب‌تری به‌دست آورد.

فصل ۵
طرح‌های قابل ردیابی

۱.۵ مقدمه

طرح‌های قابل ردیابی [۱] برای انتشار رمزگونه‌ی داده‌ها، توسط چور و سایرین در [۱۲] تعریف شد. اگرچه کدهای ضدجعل و طرح‌های قابل ردیابی برای اهداف متفاوتی طراحی شده‌اند اما شباهت زیادی به‌هم دارند. یکی از اهداف این فصل بررسی ارتباط بین کدهای ضدجعل و طرح‌های قابل ردیابی است. ابتدا تعریف ترکیبی طرح‌های قابل ردیابی را ارائه می‌دهیم سپس ثابت می‌کنیم که وجود یک c-طرح قابل ردیابی، وجود یک c-کد ضدجعل را نتیجه می‌دهد.

طرح‌های قابل ردیابی کاربردهای متفاوتی دارند برای مثال در برخی از کشورها شبکه‌های تلویزیونی وجود دارند که برنامه‌های خود را در ازاء پرداخت هزینه در اختیار بینندگان قرار می‌دهند لذا به کسانی که می‌توانند این برنامه‌ها را دریافت کنند کاربران مجاز می‌گوییم. برای ممانعت از دریافت این برنامه‌ها توسط کاربران غیرمجاز، تهیه کنندگان برنامه‌های خود را رمزدار می‌کنند و کلید رمزگشایی آن‌را در اختیار کاربران مجاز قرار می‌دهند. ممکن است گروهی از کاربران مجاز (که آن‌ها را خائن می‌نامیم) کلیدهای خود را در اختیار کاربران غیرمجاز (که آن‌ها را جاعل می‌نامیم) قرار دهند تا کلید جعلی تولید کنند. لذا کاربران جاعل می‌توانند برنامه‌ها را رمزگشایی کرده و دریافت کنند. درصورتی که حق آنان نیست و هزینه‌اش را پرداخت نکرده‌اند. برای جلوگیری از این عمل چور و سایرین در [۱۲] ، یک طرح برای ردیابی خائنین ارائه داده‌اند

[۱] traceability schemes

که به آن طرح قابل ردیابی می‌گوییم و در آن حداقل یک کاربر خائن از روی رمزگشای جعلی دستگیر شده قابل شناسایی است.

۲.۵ طرح‌های قابل ردیابی

فرض کنید اجتماعی از b کاربر وجود داشته باشد. تهیه‌کننده داده‌ها یک مجموعه پایه T از v کلید تولید می‌کند و به هر کاربر k کلید می‌دهد. مجموعه این k کلید، **کلید شخصی**[۲] کاربر را تشکیل می‌دهد که این مجموعه را برای کاربر U با $P(U)$ نمایش می‌دهیم و به آن کلید شخصی کاربر U می‌گوییم. یک پیام دریافتی شامل دو بخش **بلوک توانا سازی**[۳] و **بلوک رمزی** [۴] است. بلوک تواناسازی شامل داده‌هایی است که با استفاده از برخی یا همه v کلید مجموعه پایه، رمز شده است و با رمزگشایی آن، کلید خصوصی S حاصل می‌شود. بلوک رمزی شامل داده‌های متن اصلی یا همان داده‌های اصلی مورد نظر کاربران است که توسط کلید خصوصی S رمز شده است. هر کاربر مجاز باید بتواند با استفاده از کلید شخصی خود و بلوک تواناسازی، S را به‌دست آورد و سپس بلوک رمزی را با استفاده از S رمزگشایی کرده و داده‌های اولیه را به‌دست آورد.

ممکن است برخی خیانت کرده و به یک کاربر غیرمجاز یک مجموعه کلید جعلی F بدهند. این مجموعه کلید شامل k کلید انتخاب شده از مجموعه پایه T خواهد بود به‌طوری‌که $F \subseteq \bigcup_{U \in C} P(U)$ و C ائتلاف کاربران خائن است. این کاربر غیرمجاز ممکن است بتواند با استفاده از F، S را به‌دست آورد و داده یا برنامه اصلی را رمزگشایی کند. هدف تهیه‌کننده داده‌ها این است که کلیدها را به روشی بین کاربران خود توزیع کند که هرگاه یک کاربر مجرم دستگیر و مجموعه کلید جعلی کشف شد، بتوانند حداقل یک کاربر خائن را از بین ائتلاف C که حداکثر دارای c کاربر خائن است، شناسایی کنند. کشف خائنین با استفاده از محاسبه $|F \cap P(U)|$ برای هر کاربر U، صورت می‌گیرد. اگر برای هر $V \neq U$، $|F \cap P(U)| \geq |F \cap P(V)|$ آن‌گاه U به عنوان یک کاربر خائن افشا شده معرفی خواهد شد.

[۲] personal key
[۳] enabling block
[۴] cipher block

تعریف ۱.۵. [۳۶] یک طرح با توزیع کلید مشابه توضیحات بالا را در نظر بگیرید. فرض کنید هر کاربر افشا شده U یک عضو از ائتلاف حداکثر c عضوی C باشد که مجموعه کلید جعلی F توسط آن تولید شده است. آن‌گاه این طرح یک c-طرح قابل ردیابی است و آن را با نماد $c - TS(k, b, v)$ نمایش می‌دهیم.

طرح‌های قابل ردیابی با اندکی تفاوت در منابع علمی مختلف مورد مطالعه قرار گرفته‌اند. اکنون به‌طور خلاصه درمورد تفاوت‌های طرح ما و طرح ارائه شده در [۱۲] بحث می‌کنیم. در [۱۲] برای بعضی اعداد صحیح n، $v = nk$ و مجموعه پایه T به k زیرمجموعه S_i با اندازه n تقسیم می‌شود که برای هر $1 \leq i \leq k$، $S_i = \{s_{i,1}, s_{i,2}, \ldots, s_{i,n}\}$. هر کلید شخصی $P(U)$ یک تقاطع از $(S_1, \ldots, S_k)$ است (به این معنی که دقیقا شامل یک کلید از هر S_i است). فرض کنید کلید خصوصی S از یک گروه آبلی G انتخاب شده باشد. تهیه کننده داده‌ها برای پنهان کردن S ، آن را به k بخش $r_1, r_2, \ldots, r_k \in G$ که $\sum r_i = S$، تقسیم بندی می‌کند. آن‌گاه هر r_i، $1 \leq i \leq k$ را با n کلید درون S_i با محاسبه $t_{i,j} = r_i + s_{i,j}$ رمز می‌کند. nk مقدار حاصل برای $t_{i,j}$، بلوک تواناسازی را دربر دارد. هر کاربر مجاز، یک کلید از S_i را دارد پس او می‌تواند هر r_i را آشکار کند و سپس S را محاسبه کند.

در تعریف ما نیازی نیست که هر کلید شخصی یک تقاطع باشد. یک کلید شخصی می‌تواند هر انتخاب k تایی از مجموعه پایه T باشد (مانند طرح شمیر در [۳۴]).

تعریف ما یک کلیت از تعریف ارائه شده در [۱۲] است. اگرچه کلیت باید در روش تشکیل بلوک توانا سازی باشد و ارتباطی با ویژگی قابل ردیابی بودن طرح ندارد اما تعریف ما از ویژگی قابل ردیابی بودن، همانند تعریف [۱۲] است.

مثال ۱.۵. یک $۲ - TS(۵, ۲۱, ۲۱)$ به‌صورت زیر وجود دارد. مجموعه کلیدهای پایه $\mathbb{Z}_{۲۱}$ است و کلید شخصی برای هر کاربر $(۰ \leq i \leq ۲۰)$ برابر است با:

$$P(i) = \{۳ + i, ۶ + i, ۷ + i, ۱۲ + i, ۱۴ + i\}$$

که البته همه محاسبات در میدان $\mathbb{Z}_{۲۱}$ انجام می‌شود. (این یک کاربرد از ساختاریست که در قضیه ۱۰.۵ بیان خواهیم کرد). می‌توان نشان داد که هر دو کلید پایه در دقیقا یک کلید شخصی، با هم ظاهر می‌شوند. اکنون

فرض کنید که دو کاربر خائن U و V یک مجموعه کلید جعلی F تولید کنند. این مجموعه باید شامل حداقل ۳ کلید از کلیدهای $P(U)$ یا $P(V)$ باشد. از آن‌جاییکه برای هر کاربر $W \neq U, V$، $|F \cap P(W)| \leq ۲$، بنابراین هرگاه مجموعه کلید جعلی F بررسی شود کاربر U یا V افشا خواهد شد.

در ساختار کدهای ضدجعل و طرح‌های قابل ردیابی هدف اصلی تطبیق نمودن آن‌ها برای تعداد زیاد، تا حد ممکن است. به عبارت دیگر می‌خواهیم ساختاری پیدا کنیم که برای مقادیر معین (c و v در کدهای ضدجعل و k در طرح‌های قابل ردیابی)، b بزرگ‌ترین اندازه ممکن را داشته باشد. ولی در کل ما ساختارهای واضح را ترجیح می‌دهیم.

برای مثال بانه و شو در [۲۰] نتیجه جالب زیر را اثبات کرده‌اند.

قضیه ۱.۵. [۲۰] *برای هر دو عدد صحیح* $c, v > ۰$، *یک* $c - FPC(v, ۲^{v/(۱۶c^۲)})$ *وجود دارد.*

هرچند همان‌طور که در [۸] گفته شده، اثبات آن سودمند نیست لذا آن‌ها یک ساختار واضح برای یک $c - FPC(v, ۲^{\sqrt{v}/c})$ اثبات کردند.

مشابهاً، چور و سایرین در [۱۲] یک نتیجه جالب از وجود طرح‌های قابل ردیابی بدون ساختار به‌صورت زیر ارائه دادند.

قضیه ۲.۵. [۱۲] *برای هر دو عدد صحیح* $c, v > ۰$، *یک* $c - TS(v/(۲c^۲), ۲^{v/(۸c^۴)}, v)$ *وجود دارد.*

در این فصل چند ساختار واضح برای طرح‌های قابل ردیابی معرفی خواهیم کرد. اگرچه ساختارهای ما ممکن است به خوبی ساختارها در [۸] و [۱۲] نباشند اما اغلب برای مقادیر کوچک وابسته‌ی c و v بهتر خواهند بود (برای مثال در قضیه ۱.۵ برای به‌دست آوردن $b \geq ۲$ ضروریست که $v \geq ۱۶c^۲$ را اعمال کنیم. بنابراین این ساختار برای مقادیر کوچک v سودمند نخواهد بود.) ساختارهای ما به‌راحتی قابل اجرا، بسیار ساده و مؤثر و کاربردی هستند.

۳.۵ تعاریف ترکیبی

در این بخش تعریف ترکیبی c-طرح‌های قابل ردیابی را با استفاده از سیستم‌های مجموعه‌ای رائه می‌کنیم و از آن به سادگی درمی‌یابیم که وجود یک $c-TS(k,b,v)$ ، وجود یک $c-FPC(v,b)$ را نتیجه می‌دهد.

چون یک $c-TS(k,b,v)$ شامل b زیرمجموعه k تایی از یک مجموعه v تایی است می‌توانیم آن را به صورت یک سیستم مجموعه‌ای درنظر بگیریم که X مجموعه کلیدهای پایه و $\mathscr{B}$ مجموعه کلیدهای شخصی است.

قضیه ۳.۵. [۳۶] *یک $c-TS(k,b,v)$ وجود دارد اگر و تنها اگر یک سیستم مجموعه‌ای $(X,\mathscr{B})$ وجود داشته باشد که $|X|=v$، $|\mathscr{B}|=b$ و برای هر $B\in\mathscr{B}$، $|B|=k$ باشد و برای هر $d\leq c$ بلوک $B_1,B_2,\ldots,B_d\in\mathscr{B}$ و هر زیرمجموعه k تایی $F\subseteq\bigcup_{j=1}^{d}B_j$، بلوک $B\in\mathscr{B}\setminus\{B_1,B_2,\ldots,B_d\}$ که برای هر $1\leq j\leq d$، $|F\cap B_j|\leq|F\cap B|$، وجود نداشته باشد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $c-TS(k,b,v)$ باشد. برای هر مجموعه از $d\leq c$ کلید شخصی $B_1,B_2,\ldots,B_d$ و هر زیرمجموعه k تایی $F\subseteq\cup_{j=1}^{d}B_j$ (که F همان کلید جعلی است) و هر کلید شخصی دیگر B، یک B_j $(1\leq j\leq d)$ وجود دارد که $|F\cap B_j|>|F\cap B|$. بنابراین هیچ بلوک $B\in\mathscr{B}\setminus\{B_1,B_2,\ldots,B_d\}$ وجود ندارد که برای هر $1\leq j\leq d$، $|F\cap B_j|\leq|F\cap B|$.

حالت برعکس نیز واضح است. □

۴.۵ ارتباط طرح‌های قابل ردیابی با کدهای ضدجعل

قضیه زیر را در جهت بیان ارتباط بین طرح‌های قابل ردیابی و کدهای ضدجعل بیان می‌کنیم.

قضیه ۴.۵. [۳۶] *اگر یک $c-TS(k,b,v)$ وجود داشته باشد آن‌گاه یک $c-FPC(v,b)$ وجود دارد.*

برهان. فرض کنید $(X,\mathscr{B})$ سیستم مجموعه‌ای متناظر یک $c-TS(k,b,v)$ باشد. ثابت می‌کنیم $(X,\mathscr{B})$ یک $c-FPC(v,b)$ است. فرض کنید چنین نباشد. لذا بنا به قضیه ۱.۲، $d\leq c$ بلوک $B_1,B_2,\ldots,B_d\in\mathscr{B}$

و یک $B \in \mathscr{B} \setminus \{B_1, B_2, \ldots, B_d\}$ وجود دارد که $B \subseteq \bigcup_{i=1}^{d} B_i$. از طرفی برای هر $1 \leq i \leq d$، $|B \cap B_i| \leq |B \cap B|$. که این با قضیه ۳.۵ (برای $B = F$) تناقض دارد. □

همچنین لم زیر بی‌درنگ از اثبات قبل نتیجه می‌شود.

لم ۱.۵. [۱۲] *فرض کنید $(X, \mathscr{B})$ یک $c - TS(k, b, v)$ باشد. آن‌گاه برای هر زیرمجموعه از c $d \leq c$ بلوک $B_1, B_2, \ldots, B_d \in \mathscr{B}$، بلوک $B \in \mathscr{B} \setminus \{B_1, B_2, \ldots, B_d\}$ با شرط $B \subseteq \bigcup_{i=1}^{d} B_i$ وجود ندارد.*

۵.۵ ساختارهای ترکیبی

در این بخش چند ساختار ترکیبی از طرح‌های قابل ردیابی با استفاده از طرح‌های ترکیبی خاص ازجمله t-**طرح‌ها**[۵] ، **طرح‌های بسته بندی**[۶] و **آرایه‌های متعامد** [۷] ارائه می‌دهیم. همه نتایج نظریه طرح[۸] که ما به آن نیاز داریم در مراجع استاندارد مثل [۱۵] قابل یافت است.

۱.۵.۵ ساختارهایی با استفاده از t-طرح‌ها

ابتدا تعریف t-طرح را بیان می‌کنیم.

تعریف ۲.۵. [۳۶] یک $t - (v, k, \lambda)$ **طرح** ، یک سیستم مجموعه‌ای $(X, \mathscr{B})$ با $|X| = v$ و $|B| = k$ برای هر $B \in \mathscr{B}$ است که هر زیرمجموعه t تایی از X در دقیقا λ بلوک از $\mathscr{B}$ واقع می‌شود.

با شمارش تعداد اعضای مجموعه $S = \{(B, T) \mid B \in \mathscr{B} \ , \ T \subseteq X \ , \ T \subseteq B \ , \ |T| = t\}$ به دو روش، $|\mathscr{B}|$ در $t - (v, k, \lambda)$ طرح را محاسبه می‌کنیم. فرض کنید $|\mathscr{B}| = b$. $\binom{v}{t}$ حالت برای انتخاب T وجود دارد و چون هر T در λ بلوک واقع است لذا $|S| = \lambda\binom{v}{t}$. b انتخاب برای B وجود دارد و چون هر

[۵] t-designs
[۶] packing designs
[۷] orthogonal arrays
[۸] design theory

B، $\binom{k}{t}$ تا T را شامل می‌شود، لذا $|S| = b\binom{k}{t}$. بنابراین:

$$|S| = \lambda\binom{v}{t} = b\binom{k}{t}$$
$$\Rightarrow \quad b = \lambda\binom{v}{t}/\binom{k}{t}.$$

پس تعداد بلوک‌ها در یک $t-(v,k,\lambda)$ طرح برابر است با $b = \lambda\binom{v}{t}/\binom{k}{t}$. حال از $t-(v,k,۱)$ طرح برای ساختن کدهای ضدجعل و طرح‌های قابل ردیابی استفاده می‌کنیم که در قضایای زیر به شرح آن می‌پردازیم.

قضیه ۵.۵. [۳۶] *اگر یک $t-(v,k,۱)$ طرح وجود داشته باشد آن‌گاه یک $c-FPC(v,\binom{v}{t}/\binom{k}{t})$ با $c = \lfloor (k-۱)/(t-۱) \rfloor$ وجود دارد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $t-(v,k,۱)$ طرح باشد. قرار دهید $c = \lfloor (k-۱)/(t-۱) \rfloor$. فرض کنید $B_۱, B_۲, \ldots, B_d$ ($d \leq c$) بلوک‌های مجزا و $B \in \mathscr{B} \setminus \{B_۱, B_۲, \ldots, B_d\}$. اگر $B \subseteq \bigcup_{i=۱}^{d} B_i$ آن‌گاه یک B_i $(۱ \leq i \leq d)$ با $|B \cap B_i| \geq t$ وجود دارد . زیرا اگر برای هر $۱ \leq i \leq d$، $|B \cap B_i| < t$ آن‌گاه B با هر B_i حداکثر $t-۱$ اشتراک دارد و چون $d \leq c$ و $c = \lfloor (k-۱)/(t-۱) \rfloor$ لذا B حداکثر $k-۱$ عضوی خواهد بود که این تناقض است. از طرفی چون $(X,\mathscr{B})$ یک $t-(v,k,۱)$ طرح است لذا هر زیرمجموعه‌ی t تایی فقط در یک بلوک ظاهر می‌شود. پس باید $B = B_i$ باشد که تناقض است. بنابراین برای هر $B \in \mathscr{B} \setminus \{B_۱, B_۲, \ldots, B_d\}$ خواهیم داشت: $B \nsubseteq \bigcup_{i=۱}^{d} B_i$. لذا این t-طرح، یک سیستم مجموعه‌ای است که در شرایط قضیه ۱.۲ صدق می‌کند. پس $(X,\mathscr{B})$ یک $c-FPC(v,\binom{v}{t}/\binom{k}{t})$ است. □

به‌صورت مشابه می‌توانیم با استفاده از $t-(v,k,۱)$ طرح‌ها، طرح‌های قابل ردیابی بسازیم. اگرچه مقدار c به‌دست آمده برای آن‌ها کوچک‌تر خواهد بود.

قضیه ۶.۵. [۳۶] *اگر یک $t-(v,k,۱)$ طرح وجود داشته باشد آن‌گاه یک $c-TS(k,\binom{v}{t}/\binom{k}{t},v)$ با $c = \lfloor \sqrt{(k-۱)/(t-۱)} \rfloor$ وجود دارد.*

برهان. فرض کنید $(X,\mathscr{B})$ یک $t-(v,k,۱)$ طرح باشد. همچنین فرض کنید $B_۱, B_۲, \ldots, B_d$ $(d \leq c)$ بلوک‌های مجزا و $B \in \mathscr{B} \setminus \{B_۱, B_۲, \ldots, B_d\}$. اگر $F \subseteq \bigcup_{i=۱}^{d} B_i$ و $|F| = k$، آن‌گاه یک B_i

$(1 \leq i \leq d)$ وجود دارد که:

$$\begin{aligned} |F \cap B_i| &\geq \left\lceil \frac{k}{c} \right\rceil \\ &\geq k\sqrt{\frac{t-1}{k-1}} \\ &> \sqrt{(k-1)(t-1)}\,. \end{aligned}$$

از طرفی چون $(X, \mathscr{B})$ یک $t-(v,k,1)$ طرح است لذا برای هر $1 \leq i \leq d$، $|B \cap B_i| \leq t-1$. همچنین چون $F \subseteq \bigcup_{i=1}^{d} B_i$، لذا داریم: $(B \cap F) \subseteq (B \cap (\bigcup_{i=1}^{d} B_i))$. پس

$$\begin{aligned} |B \cap F| &\leq |B \cap (\cup_{i=1}^{d} B_i)| \\ &\leq |\cup_{i=1}^{d} (B \cap B_i)| \\ &\leq c|B \cap B_i| \\ &\leq c(t-1) \\ &\leq \sqrt{(k-1)(t-1)}. \end{aligned}$$

بنابراین $|F \cap B_i| > |F \cap B|$. لذا این t-طرح، یک سیستم مجموعه‌ای است که در شرایط قضیه ۳.۵ صدق می‌کند و لذا $c - TS(k, \binom{v}{t}/\binom{k}{t}, v)$ می‌باشد. □

نتایج معروف بسیاری برای وجود و ساختار $t-(v,k,1)$-طرح‌ها برای $t = 2, 3$ وجود دارد. از طرف دیگر هیچ $t-(v,k,1)$ طرحی با $v > k > t$ برای $t \geq 6$ یافت نشده است. البته کلاس‌های نامتناهی از $2, 3$ -طرح‌ها برخی کلاس‌های نامتناهی زیبا از کدهای ضدجعل و طرح‌های قابل ردیابی را فراهم می‌کند. برای روشن سازی، تعدادی از نمونه‌های شاخصی که می‌توان به‌دست آورد را ارائه می‌کنیم.

قضیه ۷.۵. [۱۵] *برای هر عددصحیح $3 \leq k \leq 5$، $2-(v,k,1)$ طرحی وجود دارد، اگر وتنها اگر $v \equiv 1$ یا $k \mod (k^2-k)$ باشد.*

بنابراین قضیه زیر را به‌دست می‌آوریم.

قضیه ۸.۵. [۳۶] *کدهای ضد جعلی به‌صورت زیر وجود دارند:*

۱. *برای هر* $v \equiv ۱, ۳ \mod ۶$ ، یک $FPC(v, v(v-۱)/۶) - ۲$ *وجود دارد.*

۲. *برای هر* $v \equiv ۱, ۴ \mod ۱۲$ ، یک $FPC(v, v(v-۱)/۱۲) - ۳$ *وجود دارد.*

۳. *برای هر* $v \equiv ۱, ۵ \mod ۲۰$ ، یک $FPC(v, v(v-۱)/۲۰) - ۴$ *وجود دارد.*

برهان. با جای‌گذاری $k = ۳, ۴, ۵$ در قضیه ۷.۵، برای هر k یک $(v, k, ۱) - ۲$ طرح به‌دست می‌آوریم و با جای‌گذاری پارامترهای مربوطه در قضیه ۵.۵ کدهای ضدجعل فوق به‌دست می‌آید. □

مشابهاً قضیه زیر درباره وجود ۲-طرح‌های قابل ردیابی وجود دارد (دقت کنید که در قضیه ۶.۵ هم برای به‌دست آوردن $c \geq ۲$ وقتی $t = ۲$، به $k \geq ۵$ نیاز داریم).

قضیه ۹.۵. [۳۶] *برای هر* $v \equiv ۱, ۵ \mod ۲۰$ یک $TS(v, v(v-۱)/۲۰, v) - ۲$ *وجود دارد.*

زمانی‌که q توانی از یک عدد اول باشد، یک $(q^۲+q+۱, q+۱, ۱) - ۲$ طرح را یک **صفحه تصویری**[۹] از مرتبه q می‌نامند [۱۵]. در یک صفحه تصویری $b = v$ است، پس کدهای ضدجعل به‌دست آمده از آن جالب به نظر نمی‌رسند (مثال۲.۱ مدل بهتری ارائه می‌کند). البته طرح‌های قابل ردیابی حاصل از آن مفید خواهند بود.

قضیه ۱۰.۵. [۱۵] *برای هر* q *که توانی از یک عدد اول است، یک* $TS(q+۱, q^۲+q+۱, q^۲+q+۱) - \lfloor \sqrt{q} \rfloor$ *وجود دارد.*

برهان. با توجه به قضیه ۶.۵ بدیهی است. □

مثال ۱.۵ در واقع از قضیه ۱۰.۵ برای حالت $q = ۴$ به‌دست آمده است.

[۹] projective plane

۲.۵.۵ ساختارهایی با استفاده از طرح‌های بسته بندی

نوع دیگری از طرح‌های ترکیبیاتی که می‌توانیم از آن‌ها برای ساخت کدهای ضدجعل و طرح‌های قابل ردیابی استفاده کنیم، طرح‌های بسته بندی هستند که به‌صورت زیر تعریف می‌شوند.

تعریف ۳.۵. [۳۶] یک $t-(k,v,\lambda)$ **طرح بسته بندی** ، یک سیستم مجموعه‌ای $(X,\mathscr{B})$ است که $|X|=v$ و برای هر $B\in\mathscr{B}$، $|B|=k$ و هر زیرمجموعه t تایی از X در حداکثر λ بلوک از $\mathscr{B}$ واقع شده است.

با استدلالی مشابه اثبات قضیه ۵.۵ ، ساختار زیر را برای کدهای ضدجعل داریم.

قضیه ۱۱.۵. [۳۶] *اگر یک $t-(k,v,1)$ طرح بسته بندی شامل b بلوک، وجود داشته باشد آن‌گاه یک $c-FPC(v,b)$ با $c=\left\lfloor (k-1)(t-1)\right\rfloor$ وجود دارد.*

همچنین با استدلالی شبیه اثبات قضیه ۶.۵ ، ساختار زیر را برای طرح‌های قابل ردیابی داریم.

قضیه ۱۲.۵. [۳۶] *اگر یک $t-(k,v,1)$ طرح بسته بندی شامل b بلوک، وجود داشته باشد آن‌گاه یک $c-TS(k,b,v)$ با $c=\left\lfloor \sqrt{(k-1)(t-1)}\right\rfloor$ وجود دارد.*

همان‌طور که پیش از این بیان کردیم، هیچ $t-(k,v,1)$ طرح برای $v>k>t\geq 6$ یافت نشده است، اما برای هر t ، کلاس‌های نامتناهی از طرح‌های بسته بندی با تعداد زیادی بلوک (حداکثر $\binom{v}{t}/\binom{k}{t}$ بلوک) وجود دارد. این طرح‌ها را می‌توان از طرح‌هایی معروف به آرایه‌های متعامد که در ادامه تعریف می‌کنیم به‌دست آورد.

تعریف ۴.۵. [۳۶] یک آرایه متعامد $OA(t,k,s)$ یک ماتریس $k\times s^t$ است که درایه‌های آن از یک مجموعه $s\geq 2$ نمادی انتخاب می‌شود به‌طوری‌که در هر t سطر، هر بردار $t\times 1$ فقط یک بار به عنوان ستون ظاهر شود.

همان‌طورکه در لم زیر نشان می‌دهیم، به‌راحتی از یک آرایه متعامد یک طرح بسته بندی به‌دست می‌آید.

لم ۲.۵. [۳۶] *اگر یک $OA(t,k,s)$ وجود داشته باشد، آن‌گاه یک $t-(ks,k,1)$-طرح بسته بندی با s^t بلوک وجود دارد.*

برهان. فرض کنید یک $OA(t,k,s)$ با درایه‌هایی از مجموعه $\{۰,۱,\dots,s-۱\}$ موجود باشد. مجموعه $X=\{(x,y)\,|\,۰\le x\le k-۱\ ,\ ۰\le y\le s-۱\}$ را تعریف می‌کنیم. برای هر ستون $(y_۰,y_۱,\dots,y_{k-۱})$ در آرایه متعامد فوق، بلوک $B=\{(۰,y_۰),(۱,y_۱),\dots,(k-۱,y_{k-۱})\}$ را تعریف می‌کنیم. فرض کنید $\mathscr{B}$ شامل s^t بلوک ساخته شده باشد. واضح است که $(X,\mathscr{B})$ یک $t-(ks,k,۱)$-طرح بسته بندی است. □

لم زیر برای هر عدد صحیح t، کلاس‌های نامتناهی از آرایه‌های متعامد فراهم می‌کند.

لم ۳.۵. [۱۵] *اگر q توانی از یک عدد اول و $t<q$ آن‌گاه یک $OA(t,q+۱,q)$ وجود دارد. بنابراین یک $t-(q^۲+q,q+۱,۱)$ طرح بسته بندی با q^t بلوک موجود است.*

با توجه به لم ۳.۵ و قضایای ۱۱.۵ و ۱۲.۵ ، قضیه زیر به‌راحتی نتیجه می‌شود.

قضیه ۱۳.۵. [۳۶] *برای هر q که توانی از یک عدد اول است و هر عدد صحیح t که $t<q$، یک $FPC(q^۲+q,q^t)$ و یک $TS(q+۱,q^t,q^۲+q)$ وجود دارد.*

مراجع

[1] N. Alon. Explicit construvtion of exponential sized family of k-independent sets. *Descrete Math.*, pages 191–193, 1986.

[2] N. Alon and M. Naor. *Derandomization , Witnesses for Boolean Matrix Multiplication and constructions of Perfect Hash Functions.* Weizmann Institute of Science, Israel.

[3] N. Alon and J. H. Spencer. *The Probabilistic Method.* Wiley, New York, 1992.

[4] I. Anderson. *Combinatorics of Finites Sets.* Oxford University Press, Oxford , UK, 1987.

[5] M. Atici, S. S. Magliveras, D. R. Stinson, and W. D. Wei. Some resursive construction for perfect hash families. *J. Combin. Designs*, pages 353–363, 1996.

[6] Simon R. Blackburn. Frameproof codes. *SIAM J. Discrete Math.*, 16(3):pages 499–510, 2003.

[7] B. Bollobas, D. E. Daykin, and P. Erdös. Sets of independent edges in a hypergraph. *Quart. J. Math. Oxford Ser. 2*, 27:pages 25–32, 1976.

[8] D. Boneh and J. Shaw. Collusion-secure fingerprinting for dijital data. *Advances in cryptology-Crypto '95*, pages 452–465, 1995.

[9] K. A. Bush, W. T. Federer, H. Pesotan, and D. Raghavarao. New combinatorial designs and their application to group testing. *J. Statist. Plann. Inference 10*, pages 335–343, 1984.

[10] M. Caragiu. On a class of constant weight codes. *Electronic J . Combin.*, 1996.

[11] Y. M. Chee. *Turán-type problems in group testing , coding theory and cryptography.* PhD thesis, University of Waterloo, 1996.

[12] B. Chor, A. Fiat, and M. Naor. Tracing traitors. *Advances in cryptology*, 839:pages 257–270, 1994.

[13] G. Cohen and S. Encheva. Efficient constructions of frameproof codes. *Electron. Lett.*, 36:pages 1840–1842, 2000.

[14] G. Cohen, S. Encheva, and G. Zémor. Copyright protection for digital data. *IEEE Comm. Lett.*, pages 158–160, 2000.

[15] C. J. Colbourn and J. H. Dinitz. *CRC Handbook of Combinatorial Designs.* CRC Press, 1996.

[16] M. Deza and P. Frankle. Erdös-ko-rado theorem-22 years later. *SIAM J. Algebraic Descete Methods*, 4:pages 419–431, 1983.

[17] D. Z. Du and F. K. Hwang. *Combinatorial Group Testing and Applications.* World Scientific, Singapore, 1993.

[18] A. G. Dyachkov, V. V. Rykov, and A. M. Rashad. Superimposed distance codes. *Problems Control Inform.*, pages 237–250, 1989.

[19] S. Encheva and G. Cohen. Some new p-ary two-secure frameproof codes. *Applied Mathematics Letters*, pages 177–182, 2001.

[20] S. Encheva and G. Cohen. Frameproof codes against limited coalitions of pirates. *Theoretical Computer Science*, pages 295–304, 2002.

[21] P. Erdös. A problem on independent r-tuples. *Ann. Univ. Sci. Budapest Eötvös Sect. Math.*, 8, 1965.

[22] P. Erdös, P. Frankle, and Z. Füredi. Families of finite sets in which no set is covered by the union of rothers. *Isreal J. Math. 51*, pages 75–89, 1985.

[23] P. Erdős, C. Ko, and R. Rado. Intersection theorems for systems of finite sets. *Quart. J. Math. Oxford Ser. 2*, 12:pages 313–320, 1961.

[24] A. Fiat and M. Naor. Broadcast encryption. *Advances in Cryptology-Crypto '93*, 773:pages 480–491, 1994.

[25] A. D. Friedman, R. L. Graham, and J. D. Ullman. Universal single transition time asynchronous state assignments. *IEEE Trans. Comput. C-18*, pages 541–547, 1969.

[26] H. D. O. F. Gronau. An extermal problem for set families. *Ann. Inst. Mat. Univ. Nac. Autonoma Mexico*, 25:pages 1–10, 1985.

[27] G. O. H. Katona. A simple proof of the erdős-ko-rado theorem. *J. Combin. Theory Ser. B*, 13:pages 183–184, 1972.

[28] W. H. Kautz and R. G. Singleton. Nonrandom binary superimposed codes. *IEEE Trans.*, pages 363–373, 1964.

[29] J. Körner. On the extremal combinatorics of the hamming space. *J. Combin.*, pages 112–126, 1995.

[30] J. Körner and G. Simonyi. Separating partition systems and locally diffrent sequences. *SIAM J. Discrete Math. 1*, pages 355–359, 1988.

[31] F. J. MacWilliams and N. J. A. Sloance. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[32] K. Mehlhorn. On the program size of perfect and universal hash functions. *In Proceedings of 23rd Annual IEEE Symposium on Fondations of Computer Science*, pages 170–175, 1982.

[33] K. Mehlhorn. *Data Structures and Algorithms*, volume 1. Springer, Berlin, 1984.

[34] A. Shamir. How to share a secret. *Comm . ACM*, pages 612–613, 1979.

[35] D. R. Stinson, Tran van Trung, and R. Wei. Secure frameproof codes , key distribution patterns , group testing algorithms and related structures. *Satistical Planning and Inference*, 23:pages 595–617, 1998.

[36] D. R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM J. Discrete Math. 11*, pages 41–53, 1998.

[37] J. H. Van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, Cambridge, 1992.

واژه‌نامه فارسی به انگلیسی

آرایه متعامد ..... orthogonal array

بلوک ..... block

بلوک تواناسازی ..... enabling block

بلوک رمزی ..... cipher block

چندجمله‌ای رنگی ..... chromatic polynomial

خانواده آزاد ..... sandwich-free family

خانواده بدون پوشش ..... cover-free family

خانواده درهم‌ساز کامل ..... perfect hash family

درجه ..... degree

سیستم جداساز ..... separating system

سیستم مجموعه‌ای ..... set system

سیستم منفصل ..... disjunct system

صفحه تصویری ..... projective plane

طرح ..... design

طرح بسته‌بندی ..... packing design

طرح قابل ردیابی ..... traceability scheme

فاصله همینگ ..... hamming distance

فضای برداری ..... vector space

کد خطی ..... linear code

کد ضدجعل ..... frameproof code

کد ضدجعل امن ..... secure frameproof code

کد متقاطع ..... intersecting code

کدواژه ..... codeword

کلمه ثبت نشده ..... unregistered word

کلید شخصی ..... personal key

ماتریس وقوع ..... incidence matrix

مجموعه شدنی ..... feasible set

غیر قابل کشف ..... undetectable

واژه‌نامه انگلیسی به فارسی

بلوک ..... block

چندجمله‌ای رنگی ..... chromatic polynomial

بلوک رمزی ..... cipher block

کدواژه ..... codeword

خانواده بدون پوشش ..... cover-free family

طرح ..... design

سیستم منفصل ..... disjunct system

بلوک تواناسازی ..... enabling block

مجموعه شدنی ..... feasible set

کد ضدجعل ..... frameproof code

فاصله همینگ ..... hamming distance

ماتریس وقوع ..... incidence matrix

کد متقاطع ..... intersecting code

کد خطی ..... linear code

آرایه متعامد ..... orthogonal array

طرح بسته‌بندی ..... packing design

خانواده درهم‌ساز کامل ..... perfect hash family

کلید شخصی ..... personal key

صفحه تصویری ..... projective plane

q-آرایه‌ای ..... q-array

خانواده آزاد ..... sandwich-free family

سیستم جداساز ..... separating system

کد ضدجعل امن ..... secure frameproof code

سیستم مجموعه‌ای ..... set system

طرح قابل ردیابی ..... traceability scheme

نایافتنی ..... undetectable

کلمه ثبت نشده ..... unregistered word

فضای برداری ..... vector space

نمایه

Surname: Montazeri Name: Zeinab

Title: Secure Frameproof Codes

Supervisor: Dr. Meysam Alishahi
Advisor: Mr. Seyed Reza Musawi

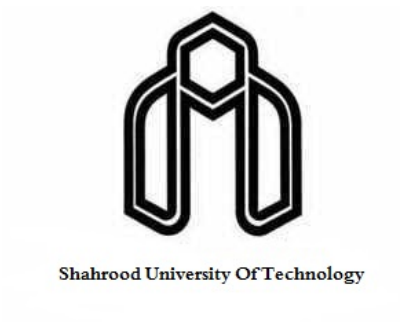
Degree: Master of Science Subject: Applied Mathematics
Field: Graph and Combinatorics

Shahrood University of Technology Faculty Of Mathematical Sciences
Date: September 2013 Number of pages: 83

Keywords: Secure Frameproof Code, Frameproof Code

Abstract

In this thesis, at the first, we present the definitions of frameproof codes and secure frameproof codes as the basic consepts; then, we will find some methods to construct these codes. Therefore, we present several families such as cover-free family, sandwich-free family, separataing hash family and perfect hash family. Next, it will be explained some methods to construct these codes. The main goal is finding secure frameproof codes as large as possible. Therefore, some bounds will be presented. At the end, we define traceability schemes which are relative to the frameproof codes.



Shahrood University of Technology
Faculty Of Mathematical Sciences

Dissertation Submitted in Partial
Fulfillment of The Requirements For The
Degree of Master of Science in
Applied Mathematics

Secure Frameproof Codes

Supervisor
Dr. Meysam Alishahi

Advisor
Mr. Seyed Reza Musawi

by
Zeinab Montazeri

September 2013