دانشگاه اصفهان
دانشکده علوم
گروه ریاضی

پایان نامه کارشناسی ارشد رشته رمز و کد

کدهای چرخشی دوگانه از طرح های شرکت پذیر کلاس دو

استاد راهنما:

دکتر جواد باقریان

استاد مشاور:

دکتر رضا سبحانی

پژوهشگر:

سعید اشعری

مرداد ماه ۱۴۰۰

تعهد نامه اصالت اثر

اینجانب دانشجوی مقطع دکتری □ کارشناسی ارشد □ رشته گرایش

متعهد می شوم که مطالب مندرج در این رساله/پایان نامه و بروندادهای منتشره در این رابطه حاصل کار پژوهشی اینجانب است و به دستاوردهای پژوهشی دیگران که در این پژوهش از آنها استفاده شده است، مطابق مقررات ارجاع و در فهرست منابع و ماخذ ذکر گردیده است. این رساله/پایان نامه قبلاً برای احراز هیچ مدرک هم سطح یا بالاتر ارائه نشده است. لذا در صورت اثبات تخلف (درهر زمان) دانشگاه اصفهان حق دارد مدرک تحصیلی صادر شده برای اینجانب را از اعتبار ساقط و ضمن درج عام موضوع در جراید کثیر الانتشار، کلیه امتیازات و حقوقی که به موجب آن در طی دوره تحصیل و مدت زمان بعد از فراغت از تحصیل تا اثبات تخلف به ذینفعان تعلق گرفته را مسترد گرداند.

کلیه حقوق مادی و معنوی این اثر متعلق به دانشگاه اصفهان می باشد.

نام و نام خانوادگی دانشجو: امضاء

تایید استاد(استادان) راهنما: نام و نام خانوادگی امضاء

چکیده

هدف ما در این پایان‌نامه،

فهرست مطالب

پیشگفتار

فصل ۱

مفاهیم مقدماتی

۱.۱ گراف

در این بخش برخی از تعاریف و خواص پایه‌ای گراف‌ها را ارائه می‌دهیم و خانواده‌هایی از گراف‌ها که در فصل‌های بعد استفاده می‌شوند را معرفی می‌کنیم.

تعریف ۱.۱.۱. ساختار وقوع متناهی $G = (\mathcal{V}, \mathcal{E}, \mathcal{I})$ یک گراف نامیده می‌شود اگر هر عضو از $\mathcal{E}$ دقیقاً بر دو عضو (نه لزوماً متمایز) از $\mathcal{V}$ واقع باشد. $\mathcal{V}$ یک مجموعه ناتهی از عناصر است که راس نامیده می‌شوند، $\mathcal{E}$ یک مجموعه متمایز از $\mathcal{V}$ است که اعضای آن یال نامیده می‌شوند و $\mathcal{I} \subseteq \mathcal{V} \times \mathcal{E}$ رابطه وقوع نامیده می‌شود.

تعریف ۱.۱.۲. اگر $e = \{u, v\} = uv$ یک یال از G باشد، آنگاه گوییم e به رئوس u و v متصل است و این رئوس را مجاور می‌گوییم. به عبارت دیگر، e روی u و v واقع است و v یک همسایه از u است. به طور مشابه، دو یال از G که روی راس‌های یکسانی واقع هستند را یال مجاور گوییم.

تعریف ۱.۱.۳. یک طوقه یالی است که یک راس را به خود متصل می‌کند، یعنی یالی که روی یک فقط روی یک راس واقع شده است طوقه نامیده می‌شود. دو یال یا بیش از دو یال که یک جفت یکسان از رئوس را به هم متصل می‌کنند یال چندگانه نامیده می‌شوند.

تعریف ۱.۱.۴. گراف بدون طوقه و بدون یال چندگانه گراف ساده نامیده می‌شود.

تبصره ۱.۱.۵. *در این پایان نامه همه گراف‌ها، گراف ساده هستند.*

تعریف ۱.۱.۶. مکمل گراف G را با $\overline{G}$ نمایش می‌دهیم. $\overline{G}$ گرافی است که مجموعه رئوس آن با مجموعه رئوس G یکسان است و در آن دو راس مجاور هستند اگر و تنها اگر در G مجاور نباشند.

تعریف ۱.۱.۷. گراف کامل یک گراف ساده است که هر دو راس آن با هم مجاور باشند. گراف کامل با n راس و $\frac{1}{2}n(n-1)$ یال با K_n نمایش داده می‌شود.

تعریف ۱.۱.۸. یک گراف دوبخشی گرافی است که مجموعه رئوس آن را بتوان به دو مجموعه افراز کرد به طوری که هر یال به یک راس از مجموعه اول و به یک راس از مجموعه دوم متصل باشد. گراف دوبخشی کامل یک گراف دوبخشی است که در آن هر راس در مجموعه اول با همه رئوس مجموعه دوم مجاور باشد. اگر دو مجموعه رئوس یک گراف دوبخشی کامل به ترتیب دارای n و m راس باشند، آنگاه این گراف را با $K_{m,n}$ نمایش می‌دهیم.

تعریف ۱.۱.۹. گراف $G = (\mathcal{V}, \mathcal{E}, \mathcal{I})$ با گراف $G = (\mathcal{V}', \mathcal{E}', \mathcal{I}')$ یکریخت است با نماد $G \cong G'$ نمایش داده می‌شود اگر و تنها اگر توابع دوسویی $f_V : \mathcal{V} \to \mathcal{V}'$ و $f_E : \mathcal{E} \to \mathcal{E}'$ وجود داشته باشند به طوری که حافظ وقوع باشند به این مفهوم که

$$(v, e) \in \mathcal{I} \Leftrightarrow (f_V(v), f_E(e)) \in \mathcal{I}', \quad \forall v \in \mathcal{V},\ \forall e \in \mathcal{E}.$$

جفت تابع (f_V, f_E) یک یکریختی از گراف‌های G و G' نامیده می‌شود. یک خودریختی از گراف G یک یکریختی از گراف G به خودش است. گروه تمام خودریختی‌های گراف G با $\mathrm{Aut}(G)$ نمایش داده می‌شود.

تعریف ۱.۱.۱۰. فرض کنیم $G = (\mathcal{V}, \mathcal{E}, \mathcal{I})$ یک گراف با مجموعه رئوس $\mathcal{V} = \{v_1, \ldots, v_n\}$ و مجموعه یال‌های $\mathcal{E} = \{e_1, \ldots, e_m\}$ باشد. ماتریس مجاورت G یک ماتریس $n \times n$ مانند $A = [a_{ij}]$ است به طوری که

$$a_{i,j} = \begin{cases} 1 & \text{اگر } v_i \text{ و } v_j \text{ مجاور باشند} \\ 0 & \text{در غیر این صورت} \end{cases}.$$

ماتریس وقوع G یک ماتریس $n \times m$ مانند $B = [b_{i,j}]$ است به طوری که

$$b_{i,j} = \begin{cases} 1 & \text{اگر } v_i \text{ واقع بر یال } e_j \text{ باشد} \\ 0 & \text{در غیر این صورت} \end{cases}.$$

تعریف ۱.۱.۱۱. فرض کنیم $v \in \mathcal{V}$ راسی از گراف G باشد. درجه (یا ظرفیت) v تعداد یال‌هایی است که بر v واقع شده‌اند.

تعریف ۱.۱.۱۲. گراف G را kـ منظم ($k \in \mathbb{N}_\circ$) می‌نامیم اگر تمام رئوس G دارای درجه یکسان k باشند.

تعریف ۱.۱.۱۳. فرض کنیم G یک گراف kـ منظم با v راس باشد. در این صورت G یک گراف قویاً منظم با پارامترهای (v, k, λ, μ) نامیده می‌شود اگر هر دو راس مجاور دارای λ همسایه مشترک و هر دو راس غیر مجاور دارای μ همسایه مشترک باشند. یک گراف قویاً منظم با پارامترهای (v, k, λ, μ) با $\mathrm{SRG}(v, k, \lambda, \mu)$ نمایش داده می‌شود.

قضیه ۱.۱.۱۴. *مکملِ یک گراف قویاً منظم با پارامترهای (v, k, λ, μ) مجدداً یک گراف قویاً منظم با پارامترهای $(v, v-k-۱, v-۲-۲k+\mu, v-۲k+\lambda)$ است.*

برهان. به قضیه ۲.۱ صفحه ۳۳۹ از [۴] مراجعه شود. □

پارامترهای یک گراف قویاً منظم، مستقل نیستند. رابطه آن‌ها در قضیه زیر آورده شده است.

قضیه ۱.۱.۱۵. *پارامترهای (v, k, λ, μ) از یک گراف قویاً منظم در معادله زیر صدق می‌کنند:*

$$k(k-\lambda-۱) = (v-k-۱)\mu.$$

برهان. به قضیه ۲.۲ صفحه ۳۳۹ از [۴] مراجعه شود. □

تعریف ۱.۱.۱۶. فرض کنیم $q \in \mathbb{N}$ و $n \in \mathbb{Z}$ به گونه‌ای باشند که $(n, q) = ۱$ ب‌م‌م. در این صورت n یک باقی‌مانده درجه دوم به پیمانه q نامیده می‌شود اگر و تنها اگر $n \overset{q}{\equiv} x^۲$ دارای جواب باشد. به طور مشابه، n یک ناباقی‌مانده درجه دوم به پیمانه q نامیده می‌شود اگر و تنها اگر $n \overset{q}{\equiv} x^۲$ جواب نداشته باشد.

تعریف ۱.۱.۱۷. فرض کنیم q توانی از یک عدد اول باشد به طوری که $q \overset{۴}{\equiv} ۱$ و فرض کنیم $(\mathbb{F}_q^*)^۲$ یک مجموعه از باقی‌مانده‌های درجه دوم ناصفر در $\mathbb{F}_q$ باشد. گراف پالی[1] از مرتبه q با نماد $P(q)$ نمایش داده

[1] Paley

می‌شود. مجموعه رئوس این گراف اعضای یک میدان متناهی از مرتبه q می‌باشد، یعنی $\mathcal{V} = \mathbb{F}_q$ و دو راس مجاور هستند اگر و تنها اگر تفاضل آن‌ها عضوی از $(\mathbb{F}_q^*)^۲$ باشد که این یعنی

$$\mathcal{E} = \{\{u, v\} \mid u - v \in (\mathbb{F}_q^*)^۲,\ u, v \in \mathbb{F}_q\}.$$

تبصره ۱.۱.۱۸. *گراف پالی $P(q)$ یک گراف قویاً منظم با پارامترهای $\left(q, \frac{q-۱}{۲}, \frac{q-۵}{۴}, \frac{q-۱}{۴}\right)$ می‌باشد. هم‌چنین گراف پالی، خود مکمل است؛ یعنی مکمل هر گراف پالی با خودش یکریخت است.*

لم ۱.۱.۱۹. *اگر G یک SRG باشد، داریم*

$$AA^T = A_۲ = kI + \lambda A + \mu\overline{A}.$$

برهان. به [۱۳] مراجعه شود. □

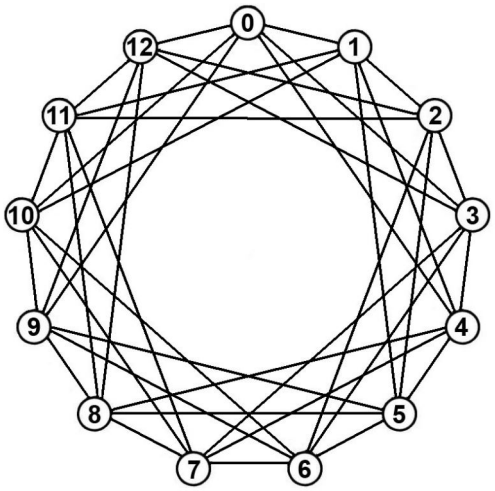
برهان. به [۱۷] مراجعه شود. □

مثال ۱.۱.۲۰. فرض کنیم $P(۱۳) = (\mathcal{V}, \mathcal{E})$ گراف پالی از مرتبه ۱۳ باشد. در این صورت داریم:

$$\mathcal{V} = \mathbb{Z}_{۱۳} = \{۰, ۱, ۲, ۳, ۴, ۵, ۶, ۷, ۸, ۹, ۱۰, ۱۱, ۱۲\},\ (\mathbb{Z}_{۱۳}^*)^۲ = \{۱, ۳, ۴, ۹, ۱۰, ۱۲\}.$$

هر راس $v \in \mathcal{V}$ با شش راس $v + i$ (به پیمانه ۱۳)، برای هر $i \in (\mathbb{Z}_{۱۳}^*)^۲$ مجاور است. بنابراین نتیجه می‌گیریم

$$\mathcal{E} = \{\{v, v + i(\text{به پیمانه}۱۳)\} \mid \forall v \in \mathbb{Z}_{۱۳},\ \forall i \in (\mathbb{Z}_{۱۳}^*)^۲\}.$$



شکل ۱.۱ : گراف پالی از مرتبه ۱۳

ماتریس مجاورت گراف پالی از مرتبه ۱۳ به صورت زیر است:

$$A = \begin{bmatrix} ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ \\ ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۱ \\ ۱ & ۰ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \end{bmatrix}$$

تعریف ۱.۱.۲. یک گشت در گراف $G = (\mathcal{V}, \mathcal{E}, \mathcal{I})$ یک دنباله نابدیهی متناهی از راس‌ها و یال‌ها مانند

$$W = v_۰ e_۱ v_۱ e_۲ v_۲ \dots e_k v_k$$

است که در آن $v_۰, \dots, v_k \in \mathcal{V}$ و $e_۱, \dots, e_k \in \mathcal{E}$، همچنین برای هر $i \in \{۱, \dots, k\}$، رئوس $v_{i-۱}$ و v_i توسط یال e_i با هم مجاور هستند. گشت W یک $(v_۰, v_k)$ـ گشت یا یک گشت از $v_۰$ به v_k نامیده می‌شود که $v_۰$ و v_k نقاط انتهایی گشت نام دارند.

طول یک گشت تعداد یال‌های گشت تعریف می‌شود. یک گشت را بسته نامیم اگر دارای طول مثبت باشد و نقاط انتهایی آن با هم یکسان باشند.

تعریف ۱.۱.۲۲. یک گشت که یال تکراری نداشته باشد را گذر می‌نامیم. یک گذر که تمام رئوس آن متمایز باشند مسیر نامیده می‌شود.

تعریف ۱.۱.۲۳. در گراف G دو راس u و v همبند نامیده می‌شوند اگر یک مسیر بین آن‌ها وجود داشته باشد. گرافی که هر دو راس آن همبند باشند، یک گراف همبند نام دارد.

تعریف ۱.۱.۲۴. فاصله دو راس u و v از یک گراف متناهی G با نماد $d(u,v)$ نشان داده می‌شود و برابر با کمترین طول (u,v)ـ مسیرهایی که آن دو را در G به هم وصل می‌کند تعریف می‌شود. اگر مسیری بین u و v وجود نداشته باشد، به عبارت دیگر اگر u و v در دو مؤلفه همبندی مختلف باشند، آنگاه فاصله آن‌ها ∞ تعریف می‌شود.

تعریف ۱.۱.۲۵. قطر گراف G با نماد $\mathrm{diam}(G)$ نمایش داده می‌شود و برابر با بیشترین فاصله هر دو راس در G تعریف می‌شود.

تعریف ۱.۱.۲۶. گذر بسته‌ای که تمام رئوس آن متمایز هستند (به جز راس اول و آخر آن که یکی هستند) یک دور نامیده می‌شود.

گرافی که حداقل دارای یک دور باشد، گراف دوری نام دارد و گرافی که هیچ دوری نداشته باشد گراف غیر دوری نامیده می‌شود.

تعریف ۱.۱.۲۷. طول کوتاه‌ترین دور در گراف G، کمر گراف G نامیده می‌شود. اگر G یک گراف غیر دوری باشد، آنگاه کمر آن ∞ تعریف می‌شود.

تعریف ۱.۱.۲۸. یک گراف با n راس $(n \geq ۳)$ $v_۰, v_۱, v_۲, \ldots, v_{n-۱}$ و n یال $v_۰v_۱, v_۱v_۲, \ldots, v_{n-۱}v_۰$ که به شکل یک دور از طول n باشد، یک گراف دور یا nـ دور نامیده می‌شود و با نماد C_n نشان داده می‌شود.

۲.۱ گراف‌های جهت‌دار

مسائل زیادی را می‌توان را با استفاده از گراف‌ها ارائه کرد ولی گاهی اوقات این کار پذیرفتنی نیست به این دلیل که در برخی از مسائل رابطه بین اشیا متقارن نیست. برای این گونه موارد به گراف جهت‌دار نیاز داریم.

در بخش قبل گراف غیر جهت‌دار معرفی شد. اگر به هر یال از گراف غیر جهت‌دار یک جهت اضافه کنیم، یک گراف جهت‌دار به دست می‌آوریم، این کار معمولاً با اضافه کردن یک فلش به یال انجام می‌شود.

در این بخش گراف‌های جهت‌دار بررسی می‌شوند و تورنمنت‌ها که در بحث ما مهم‌ترین مثال گراف‌های جهت‌دار هستند را معرفی می‌کنیم؛

تعریف ۱.۲.۱. گراف جهت‌دار $G_D = (\mathcal{V}_D, \mathcal{E}_D)$ یک گراف است که در آن یال‌ها دارای جهت هستند. این گراف از دو مجموعه متناهی تشکیل شده است، مجموعه ناتهی $\mathcal{V}_D$ از رئوس و مجموعه $\mathcal{E}_D \subseteq \mathcal{V}_D \times \mathcal{V}_D$ از یال‌های جهت‌دار یا کمان‌ها که در آن هر کمان به یک زوج مرتب از رئوس که نقاط انتهایی آن نامیده می‌شوند وابسته است.

تعریف ۲.۲.۱. اگر e یک یال از G_D با جفت رئوس (u, v) باشد، آنگاه e یک یال جهت‌دار از راس آغازین u به راس پایانی v نام دارد. در این حالت گوییم u مجاور با v می‌باشد یا u راس v را احاطه می‌کند و v یک همسایه خارجی u است. به طور مشابه، گوییم v مجاور از u است یا v توسط u احاطه شده است و u یک همسایه داخلی از v می‌باشد.

تعریف ۳.۲.۱. به یک کمان طوقه گفته می‌شود اگر نقاط انتهایی آن برابر باشند، به عبارت دیگر اگر یک راس را مستقیماً به خودش وصل کند. کمان‌های چندگانه کمان‌هایی هستند که راس‌های آغازین و پایانی آن‌ها یکسان باشند.

تعریف ۴.۲.۱. گراف جهت‌دار ساده یک گراف جهت‌دار است که طوقه و یال چندگانه نداشته باشد.

تعریف ۵.۲.۱. کمان (u, v) وارون یافته کمان (v, u) نامیده می‌شود. یک جفت از کمان‌های وارون مانند (u, v) و (v, u) را یک جفت متقارن از کمان‌ها می‌نامند.

تعریف ۶.۲.۱. گراف جهت‌دار ساده‌ای که هر جفت از رئوس آن به وسیله یک جفت متقارن از کمان‌ها به هم متصل می‌شوند یک گراف جهت‌دار کامل نامیده می‌شود.

تعریف ۷.۲.۱. یک گراف جهت‌دار کامل با یک گراف کامل غیر جهت‌دار که یال‌هایش با جفت‌هایی از کمان‌های وارون تعویض شده است هم ارز می‌باشد.

تعریف ۸.۲.۱. گراف جهت‌داری که برای هر کمانش، کمان وارون یافته متناظر با آن نیز در گراف باشد یک گراف جهت‌دار متقارن نامیده می‌شود.

تعریف ۹.۲.۱. یک گراف جهت‌دار که هیچ یک از جفت رئوس آن با یک جفت از کمان‌های متقارن به هم متصل نباشند، گراف جهت‌دار نامتقارن نامیده می‌شود.

تبصره ۱۰.۲.۱. *در این پایان نامه، منظور از یک گراف جهت‌دار یک گراف جهت‌دار نامتقارن ساده است.*

تعریف ۱۱.۲.۱. فرض کنیم $G_D = (\mathcal{V}_D, \mathcal{E}_D)$ یک گراف جهت‌دار با مجموعه رئوس $\mathcal{V}_D = \{v_1, \ldots, v_n\}$ باشد. ماتریس مجاورت G_D یک ماتریس $n \times n$ مانند $A = [a_{i,j}]$ به طوری که

$$a_{i,j} = \begin{cases} ۱ & \text{اگر } (v_i, v_j) \in \mathcal{E}_D \\ ۰ & \text{در غیر این صورت} \end{cases}$$

تعریف ۱۲.۲.۱. فرض کنیم $v \in \mathcal{V}_D$ یک راس در گراف جهت‌دار G_D باشد. مجموعه همسایه‌های خارجی v را به صورت $N^+(v) = \{u \in \mathcal{V}_D \mid (v,u) \in \mathcal{E}_D\}$ تعریف می‌کنیم و درجه خارجی (یا ظرفیت خارجی یا امتیاز) راس v را با نماد $d^+(v)$ نمایش داده و برابر با تعداد رئوسی تعریف می‌کنیم که توسط v احاطه شده‌اند؛ یعنی $d^+(v) = |N^+(v)|$. هم‌چنین مجموعه همسایه‌های داخلی v را به صورت $N^-(v) = \{u \in \mathcal{V}_D \mid (u,v) \in \mathcal{E}_D\}$ تعریف می‌کنیم و درجه داخلی (یا ظرفیت داخلی یا هم‌ـامتیاز) راس v را با نماد $d^-(v)$ نمایش داده و برابر با تعداد رئوسی تعریف می‌کنیم که v را احاطه کرده‌اند؛ یعنی $d^-(v) = |N^-(v)|$.

تعریف ۱۳.۲.۱. راس v با $d^-(v) = ۰$ یک منبع نامیده می‌شود، زیرا مبداء هر یک از کمان‌های خروجی از آن است. به طور مشابه راس v با $d^+(v) = ۰$ یک مقصد نام دارد، چون پایان هر یک از کمان‌های ورودی به خود است. راسی که منبع و مقصد نباشد، راس داخلی نامیده می‌شود.

گزاره ۱۴.۲.۱. *فرض کنیم G_D یک گراف جهت‌دار باشد. در این صورت داریم:*

$$\sum_{v \in \mathcal{V}_d} d^+(v) = \sum_{v \in \mathcal{V}_d} d^-(v) = |\mathcal{E}_D|$$

که به آن فرمول مجموع درجات می‌گویند.

برهان. به گزاره ۱.۲.۱ از [۲] مراجعه شود. □

تعریف ۱۵.۲.۱. گراف جهت‌دار G_D یک گراف منظم از درجه k (یا kـ منظم) نامیده می‌شود اگر هر راس آن، k راس را احاطه کند و توسط k راس احاطه شده باشد. به عبارت دیگر G_D یک گراف جهت‌دار kـ منظم است اگر هر راس در G_D دارای درجه داخلی و درجه خارجی k باشد.

تعریف ۱۶.۲.۱. یک تورنمنت $T + (\mathcal{V}_T, \mathcal{E}_T)$ از درجه n یا nـ تورنمنت یک گراف جهت‌دار است که مجموعه رئوس $\mathcal{V}_T$ شامل n عضو باشد و مجموعه یال $\mathcal{E}_T \subset \mathcal{V}_T \times \mathcal{V}_T$ به گونه‌ای باشد که هر جفت از رئوس u و v دقیقاً به وسیله یکی از کمان‌های (u, v) یا (v, u) به هم متصل شده باشند.

تبصره ۱۷.۲.۱. *تورنمنت‌ها گراف‌هایی نامتقارن هستند که در واقع با انتخاب یک جهت برای هر یال در یک گراف کامل غیر جهت‌دار به دست می‌آیند.*

به لحاظ ماتریس مجاورت A، هر nـ تورنمنت یک گراف جهت‌دار است که خاصیت $A + A^T = J - I$ برای آن برقرار است. بنابراین $J - I$ ماتریس مجاورت یک گراف کامل روی n راس می‌باشد.

تبصره ۱۸.۲.۱. *فرض کنیم T یک تورنمنت kـ منظم با v راس باشد. اگر هر راس در $\mathcal{V}_T$ دارای درجه خارجی k باشد، آن‌گاه هر راس در $\mathcal{V}_T$ دارای درجه داخلی $v - k - ۱$ است. در نتیجه $k = v - k - ۱$؛ یعنی $v = ۲k + ۱$ و لذا v باید یک عدد فرد باشد.*

تعریف ۱۹.۲.۱. فرض کنیم T یک تورنمنت kـ منظم با v راس باشد. T را یک تورنمنت منظم دوگانه با پارامترهای (v, k, λ, μ) نامیده می‌شود اگر هر دو راس مجاور دارای λ همسایه خارجی مشترک باشند و هر یک از این دو راس دارای μ همسایه خارجی اضافی باشند که برای آن‌ها مشترک نباشند. یک تورنمنت منظم دوگانه با پارامترهای (v, k, λ, μ) با نماد $\mathrm{DRT}(v, k, \lambda, \mu)$ نمایش داده می‌شود.

رابطه میان پارامترها برای یک DRT در لم زیر آورده شده است:

لم ۲۰.۲.۱. *فرض کنیم T یک DRT با پارامترهای (v, k, λ, μ) باشد. در این صورت $v = ۴\lambda + ۳$، $k = ۲\lambda + ۱$ و $\mu = \lambda + ۱$.*

برهان. به لم ۳.۲ از [۱۳] مراجعه شود. □

تعریف ۱.۲.۱. فرض کنیم q توانی از یک عدد اول باشد که $q \overset{۴}{\equiv} ۳$ و فرض کنیم $(\mathbb{F}_q^*)^۲$ یک مجموعه از باقی‌مانده‌های درجه دوم ناصفر در $\mathbb{F}_q$ باشد. تورنمنت پالی از مرتبه q با نماد $P_T(q)$ نمایش داده می‌شود. مجموعه رئوس این گراف اعضای یک میدان متناهی از مرتبه q می‌باشد، یعنی $\mathcal{V}_T = \mathbb{F}_q$ و دو راس مجاور هستند اگر و تنها اگر تفاضل آن‌ها عضوی از $(\mathbb{F}_q^*)^۲$ باشد که این یعنی

$$\mathcal{E}_T = \{\{u, v\} \mid u - v \in (\mathbb{F}_q^*)^۲,\ u, v \in \mathbb{F}_q\}.$$

تبصره ۱.۲.۲. *گراف $P_T(q)$ یک تورنمنت منظم دوگانه با پارامترهای $(q, \frac{q-۱}{۲}, \frac{q-۳}{۴}, \frac{q+۱}{۴})$ است.*

برهان. به [۲۵] مراجعه شود. □

لم ۱.۲.۳. *اگر G یک DRT باشد، داریم*

$$AA^T = kI + (k - ۱ - \lambda)A + (k - \mu)\overline{A}.$$

برهان. به [۱۳] مراجعه شود. □

مثال ۱.۲.۴. فرض کنیم $P_T(۷) = (\mathcal{V}_T, \mathcal{E}_T)$ یک تورنمنت پالی از مرتبه ۷ باشد. در این صورت داریم

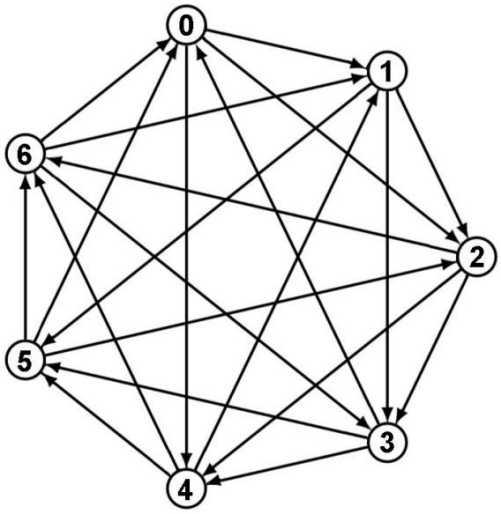
$$\mathcal{V}_T = \mathbb{Z}_۷ = \{۰, ۱, ۲, ۳, ۴, ۵, ۶\}, \quad (\mathbb{Z}_۷^*)^۲ = \{۱, ۲, ۴\}.$$

هر راس $v \in \mathcal{V}_T$ با سه راس $v + i$ (به پیمانه ۱۳)، به ازای هر $i \in (\mathbb{Z}_۷^*)^۲$ مجاور است. پس نتیجه می‌گیریم

$$\mathcal{E}_T = \{\{v, v + i(\text{به پیمانه}۷)\} \mid \forall v \in \mathbb{Z}_۷,\ \forall i \in (\mathbb{Z}_۷^*)^۲\}.$$

ماتریس مجاورت گراف پالی از مرتبه ۷ به صورت زیر است:

$$A = \begin{bmatrix} ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۰ & ۰ & ۱ \\ ۱ & ۱ & ۰ & ۱ & ۰ & ۰ & ۰ \end{bmatrix}.$$



شکل ۲.۱: گراف پالی از مرتبه ۷

۳.۱ کدها

در ادامه مفاهیم اساسی نظریه کدگذاری را بیان می‌کنیم.

تعریف ۱.۳.۱. فرض کنیم F_q یک مجموعه متناهی شامل q عضو باشد. در این صورت F_q الفبا نامیده می‌شود و اعضای آن نماد نامیده می‌شوند. کد qـ تایی C از طول n روی F_q یک زیرمجموعه C از مجموعه F_q^n متشکل از همه کلمات nـ حرفی از اجزای F_q است. عناصر موجود در C را کدکلمه می‌نامند. یک کد دوتایی نامیده می‌شود اگر $q = ۲$، به همین ترتیب سه‌تایی می‌نامند اگر $q = ۳$ و چهارتایی گویند اگر $q = ۴$ باشد.

کدهای خطی به دلیل ویژگی‌های جبری خود، بیشترین کدهایی هستند که از نظر ریاضی مطالعه شده‌اند. در این پایان نامه فقط با کدهای خطی کار خواهیم کرد.

تعریف ۲.۳.۱. فرض کنیم R یک حلقه جابه‌جایی (همراه همانی) باشد. فرض کنیم ϕ یک جایگشت از R باشد. یک کد به طول n روی R یک زیرمجموعه‌ای از R^n است و به کد خطی گفته می‌شود اگر R یک R زیرمدول از R^n باشد. می‌سازیم R^n با ضرب داخلی $x.y = \sum_{i=۱}^{n} x_i\phi(y_i)$، زمانی که ϕ همانی باشد ما آن را ضرب داخلی اقلیدسی می‌نامیم. در غیر این صورت ما آن را ضرب داخلی هرمیتین[۲] می‌نامیم.

[2] Hermitian

دوگان $c^{\perp}$ از کد c فهمیده می‌شود از رابطه ضرب داخلی اقلیدسی. یک کد خود دوگان نامیده می‌شود اگر با دوگان خودش معادل باشد و خود متعامد نامیده می‌شود اگر شامل دوگان باشد.

تعریف ۱.۳.۴. فاصله همینگ[۳] $d(x,y)$ بین دو بردار $x=(x_1,\ldots,x_n)$ و $y=(y_1,\ldots,y_n)$ برابر با تعداد مکان‌های مختصاتی است که x و y در آن‌ها متفاوت هستند، یعنی:

$$d(x,y)=|\{i \mid x_i \neq y_i,\ 1 \leq i \leq n\}|.$$

تعریف ۱.۳.۴. کمترین فاصله d از یک کد C، کوچکترین فاصله همینگ بین کلمات کدکلمه‌های متمایز از C تعریف می‌شود، یعنی:

$$d=\min\{d(x,y) \mid x,y \in C,\ x \neq y\}.$$

تعریف ۱.۳.۵. وزن همینگ $w(x)$ بردار $x \in \mathbb{F}_q^n$، تعداد مولفه‌های غیر صفر آن تعریف می‌شود، یعنی:

$$w(x)=|\{i \mid x_i \neq 0\}|.$$

تعریف ۱.۳.۶. اگر C یک کد باشد، آنگاه کمترین وزن را با نماد $w(C)$ نشان داده و برابر کوچکترین وزن تمام کدکلمه‌های ناصفر در C تعریف می‌شود، یعنی:

$$w(C)=\min\{w(x) \mid x \in C,\ x \neq 0\}.$$

به طور کلی یافتن کمترین فاصله یک کد مستلزم مقایسه هر جفت عنصر متمایز است. اما این کار برای یک کد خطی ضروری نیست. اگر کدکلمه‌های x و y متعلق به یک کد خطی C باشند، آنگاه $x-y$ نیز یک کدکلمه در C است. اکنون با توجه به تعاریف قبلی، گزاره زیر را نتیجه می‌گیریم [۲۷].

گزاره ۱.۳.۷. *کمترین فاصله یک کد خطی با کمترین وزنِ همه کدکلمه‌های ناصفر برابر است.*

ما از نماد $[n,k,d]$ برای کد خطی $[n,k]$ با کمترین فاصله، یا به طور معادل کمترین وزن d، استفاده می‌کنیم.

[3] Hamming

یک کد را می‌توان مجموعه‌ای از پیام‌هایی دانست که از طریق یک کانال ارتباطی در حال انتقال هستند. اگر کانال در معرض نویز باشد، ممکن است برخی از اجزای یک پیام $x = (x_1, \ldots, x_n) \in C$ خراب شده باشند. بنابراین، پیام دریافتی $y = (y_1, \ldots, y_n)$ ممکن است با x متفاوت باشد و فاصله $d(x, y)$ تعداد خطاها در y را شمارش می‌کند. فرآیند بازیابی پیام اصلی x از پیام دریافتی y را رمزگشایی می‌گویند.

نتیجه زیر اهمیت مفهوم کمترین فاصله را نشان می‌دهد و می‌توان آن را در [۱] یافت.

قضیه ۸.۳.۱. *یک کد خطی $[n, k, d]$ می‌تواند حداکثر $d - 1$ خطا را در یک کدکلمه شناسایی کند و حداکثر $t = \lfloor \frac{d-1}{2} \rfloor$ خطا را تصحیح کند.*

تعریف ۹.۳.۱. دو کد خطی معادل نامیده می‌شوند اگر بتوان یکی را از دیگری به وسیله جابجایی مکان‌های مختصاتی در همه کدکلمه‌ها و ضرب یک مختصات مشخص در عنصری ناصفر از یک میدان به دست آورد.

دو کد خطی یکریخت نامیده می‌شوند اگر جایگشتی از مکان‌های مختصاتی یک کد برای به دست آوردن کد دیگر کافی باشد.

هر یکریختی از کد C به خودش، یک خودریختی از C نامیده می‌شود. مجموعه تمام خودریختی‌های C را گروه خودریختی‌های C می‌نامند و با نماد $\mathrm{Aut}(C)$ نشان می‌دهند.

دو روش رایج برای ارائه یک کد خطی استفاده از ماتریس مولد یا ماتریس بررسی برابری می‌باشد.

تعریف ۱۰.۳.۱. یک ماتریس مولد G از یک کد $[n, k, d]$ خطی C، یک ماتریس $k \times n$ است که از هر k کدکلمه مستقل خطی C به دست می‌آید که پایه‌ای برای کد C تشکیل می‌دهد. یک ماتریس مولد به شکل $G = [I_k \mid A]$ که I_k ماتریس همانی از مرتبه k و A یک ماتریس $k \times (n - k)$ است که ماتریس مولد در شکل استاندارد نامیده می‌شود.

تبصره ۱۱.۳.۱. *هر کد خطی معادل با یک کد با ماتریس مولد در شکل استاندارد است.*

تعریف ۱۲.۳.۱. حاصل‌ضرب داخلی بردارهای $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ به صورت زیر تعریف می‌شود:

$$x.y = \sum_{i=1}^{n} x_i y_i.$$

تعریف ۱.۳.۱۳. فرض کنیم کد $[n,k,d]$ خطی $C \subset \mathbb{F}_q^n$ داده شده باشد. کد دوگان $C^\perp \subset \mathbb{F}_q^n$ مجموعه همه کدکلمه‌هایی تعریف می‌شود که متعامد با هر کدکلمه در C هستند، یعنی:

$$C^\perp = \{x \in \mathbb{F}_q^n \mid x.y = 0, \forall y \in C\}.$$

یک کد C خود_متعامد نامیده می‌شود اگر $C \subseteq C^\perp$ و خود_دوگان می‌نامند اگر $C = C^\perp$

تبصره ۱.۳.۱۴. *اگر C یک کد $[n,k]$ خطی باشد، آنگاه C یک کد $[n,n-k]$ خطی است.*

گزاره ۱.۳.۱۵. *فرض کنید C یک کد خطی به طول n باشد. در این صورت:*

$$\dim(C) + \dim(C^\perp) = n.$$

طبق گزاره قبل که اثبات آن در [۱] آمده است، نتیجه می‌گیریم که طول n از یک کد خود_دوگان زوج است و بعد آن $n/2$ است.

نتیجه زیر نشان می‌دهد که با بررسی ماتریس مولد یک کد به راحتی می توانیم مشخص کنیم که چه زمانی آن کد خود_متعامد است.

لم ۱.۳.۱۶. *یک کد خطی C با ماتریس مولد G خود_متعامد است اگر و تنها اگر $GG^T = 0$.*

از این رو، برای اثبات این‌که یک کد $[n,k]$ خطی C با ماتریس مولد G خود_دوگان است، کافی است نشان دهیم که C دارای طول $n = 2k$ است و $GG^T = 0$. طبق این نکته لم زیر را به دست می‌آوریم:

لم ۱.۳.۱۷. *اگر C یک کد $[n,k]$ خود_دوگان روی یک میدان $\mathbb{F}_q$ با ماتریس مولد $G = [I_k \mid B]$ باشد، آنگاه $BB^T = -I_k$.*

اثبات دو لم قبلی را می‌توان در [۳۵] یافت.

تعریف ۱.۳.۱۸. فرض کنیم w_i نشان دهنده تعداد کدکلمه‌های از وزن i را در یک کد خطی C از طول n باشد. در این صورت وزن توزیعی C به صورت لیست $[w_i \mid 0 \leq i \leq n]$ می‌باشد.

تعریف ۱.۳.۱۹. کد C را زوج نامیم اگر وزن تمام کدکلمه‌های C زوج باشد.

تعریف ۲۰.۳.۱. کد C را خود-دوگان صوری نامیم اگر C و $C^{\perp}$ وزن توزیعی یکسانی داشته باشند.

در [۲۶] نشان داده شده است که کدهای $[۲n, n]$ خود-دوگان صوری زوج ممکن است بعضی از اوقات دارای کمترین وزن بزرگتر از هر کد $[۲n, n]$ خود-دوگان باشند.

تعریف ۲۱.۳.۱. یک ماتریس بررسی برابری H از یک کد خطی C یک ماتریس مولد از کد دوگان $C^{\perp}$ است.

اگر H یک ماتریس بررسی برابری برای یک کد خطی C باشد، آنگاه کدکلمه‌های C را می توان از H بازیابی کرد، زیرا آن‌ها باید با هر ردیف از H متعامد باشند. بنابراین، کد C ارائه شده توسط ماتریس بررسی برابری H به صورت زیر است:

$$C = \{x \in \mathbb{F}_q^n \mid H.x^T = ۰\}.$$

قضیه ۲۲.۳.۱. *فرض کنید H یک ماتریس بررسی برابری برای کد $[n, k]$ خطی C باشد. در این صورت هر مجموعه از $d - ۱$ ستون در H مستقل خطی است اگر و تنها اگر C دارای کمترین فاصله حداقل d باشد.*

از قضیه قبل که اثبات آن را می‌توان در [۱] یافت، نتیجه می‌شود که یک کد خطی C با ماتریس بررسی برابری H کمترین فاصله d را دارد اگر و فقط اگر هر مجموعه $d - ۱$ عضوی از ستون‌های H مستقل خطی باشد و تعدادی از مجموعه‌های d عضوی از ستون‌ها، وابسته خطی هستند. از این رو، قضیه قبل می‌تواند برای تعیین کمترین فاصله یک کد خطی، با توجه به ماتریس بررسی برابری استفاده شود.

هنگام کار با کدهای خطی اغلب اوقات مطلوب است که بتوان ماتریس مولد را به ماتریس بررسی برابری تبدیل کرد و برعکس. این کار به راحتی با استفاده از قضیه زیر قابل انجام است که اثبات را می‌توان در [۲۴] یافت.

قضیه ۲۳.۳.۱. *اگر $G = [I_k \mid A]$ یک ماتریس مولد در شکل استاندارد برای کد $[n, k]$ خطی C باشد، آنگاه $H = [-A^T \mid I_{n-k}]$ یک ماتریس بررسی برابری برای C است.*

مثال ۲۴.۳.۱. کدهای همینگ خانواده مهمی از کدهای خطی هستند که به راحتی رمزگذاری و رمزگشایی می‌شوند. یک کد همینگ دوتایی $\mathcal{H}_r$ به طول $n = ۲^r - ۱$ (که $r \geq ۲$) دارای ماتریس بررسی برابری H

است که ستون‌های آن از تمام بردارهای دوتایی ناصفر به طول r تشکیل شده‌اند که هر کدام یک‌بار استفاده شده است. $\mathcal{H}_r$ یک $[۲^r - ۱, ۲^r - r - ۱, ۳]$ کد می‌باشد. با افزودن یک مختصات بررسی برابری کلی به هر بردار ماتریس مولد آن (و بنابراین به هر کد کلمه از $\mathcal{H}_r$)، کد همینگ دوتایی تعمیم یافته $\hat{\mathcal{H}}_r$ به دست می‌آید که یک $[۲^r, ۲^r - r - ۱, ۴]$ کد است. برای مثال $\hat{\mathcal{H}}_۳$ یک $[۸, ۴, ۴]$ کد همینگ دوتایی با ماتریس مولد G و ماتریس بررسی برابری H می‌باشد که به صورت زیر هستند:

$$G = \left[\begin{array}{cccc|cccc} ۱ & ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۰ & ۱ & ۱ & ۰ & ۱ \\ ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ & ۰ \end{array}\right], \quad H = \left[\begin{array}{cccc|cccc} ۰ & ۱ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ \\ ۱ & ۰ & ۱ & ۱ & ۰ & ۱ & ۰ & ۰ \\ ۱ & ۱ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ \\ ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۰ & ۱ \end{array}\right]$$

به سادگی می‌توان نشان داد که $GG^T = ۰$، بنابراین این کد، خود-دوگان است.

قضیه زیر رابطه بین پارامترهای یک کد خطی را نشان می‌دهد که با نام کران سینگلتون[۴] شناخته می شود. اثبات این قضیه در [۲۷] ارائه شده است.

قضیه ۱.۳.۲۵. *اگر C یک کد $[n, k, d]$ خطی باشد، آنگاه* $d \leq nk + ۱$.

کران سینگلتون یکی از کران‌های بالای d برای پارامترهای داده شده n و k است. برای نمونه‌های بیشتری از کران‌های بالا برای کمترین فاصله به [۲۴] را ببینید.

تعریف ۱.۳.۲۶. یک کد $[n, k]$ خطی C بهینه نام دارد اگر کمترین وزن C یک کران بالا برای $[n, k]$ کدهای خطی باشد. C تقریباً بهینه است اگر کمترین وزن آن حداکثر یک واحد کمتر از بزرگترین مقدار ممکن باشد.

کد $[n, k]$ خطی C یک کد $[n, k]$ خطی C شناخته شده‌تر نامیده می‌شود اگر C دارای بالاترین مقدار کمترین وزن در میان همه کدهای $[n, k]$ خطی شناخته شده باشد.

فهرستی از کدهای شناخته شده در [۱۹] آورده شده است که ما آن‌ها را با حداقل وزن همه کدهای ساخته شده در این پایان نامه مقایسه می‌کنیم.

[4] Singleton bound

۴.۱ اسکیم‌های شرکت پذیر

تعریف ۱.۴.۱. فرض کنیم X یک مجموعه ناتهی باشد. فرض کنید $\{R_0, R_1, \ldots, R_d\}$ یک افراز از $X \times X$ باشند ($\forall i\ ,\ R_i \subseteq X \times X$). زوج $(X, \{R_i\}_{i=0}^{d})$ را یک اسکیم شرکت پذیر[5] روی X از کلاس d گویند هرگاه

۱. $R_0 = \{(x,x)\ :\ x \in X\}$، که به آن رابطه قطری گویند.

۲. به ازای هر رابطه R_i، رابطه R_j که $0 \leq j \leq d$ وجود داشته باشد به طوری که

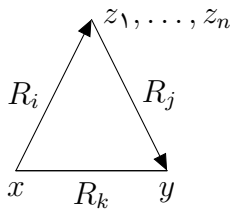
$$R_i^* = \{(y,x) \mid (x,y) \in R_i\} = R_j.$$

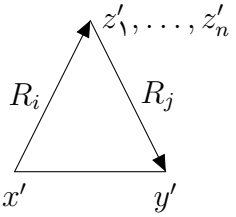
(در این حالت رابطه R_j را برابر $R_{i'}$ قرار می‌دهیم، یعنی $R_i^* = R_j = R_{i'}$.)

۳. به ازای هر $0 \leq i,j,k \leq d$ و $(x,y) \in R_k$، اندازه مجموعه

$$|\{z \in X \mid (x,z) \in R_i\ ,\ (z,y) \in R_j\}|$$

به انتخاب (x,y) در R_k بستگی نداشته باشد.





اندازه مجموعه فوق را با P_{ij}^k یا λ_{ij}^k نمایش می‌دهیم. در واقع

$$P_{ij}^k = |\{z \in X \mid (x,z) \in R_i\ ,\ (z,y) \in R_j\}|$$

به ازای یک $(x,y) \in R_k$ است. به مجموعه اعداد P_{ij}^k که اعداد صحیح نامنفی نیز هستند اعداد متقاطع[6] اسکیم گویند.

[5] asssociative scheme
[6] intersection numbers

در تعریف بالا، به $|X|$ درجه اسکیم و به d کلاس اسکیم گفته می‌شود.

تعریف ۱.۴.۲. اسکیم شرکت پذیر $(X, \{R_i\}_{i=0}^{d})$ را جابجایی[۷] گویند هرگاه

$$\forall i, j, k \ , \ P_{ij}^{k} = P_{ji}^{k}.$$

هم‌چنین اسکیم فوق را متقارن[۸] گویند هرگاه برای هر i داشته باشیم $R_{i'} = R_i$.

لم ۱.۴.۳. *اسکیم‌های متقارن، جابجایی هستند.*

برهان. به ازای هر i, j, k و $(x, y) \in R_k$ داریم $(y, x) \in R_k$ و

$$\begin{aligned} P_{ij}^{k} &= |\{z \in X \mid (x, z) \in R_i \ , \ (z, y) \in R_j\}| \\ &= |\{z \in X \mid (z, x) \in R_{i'} \ , \ (y, z) \in R_{j'}\}| \\ &= |\{z \in X \mid (z, x) \in R_i \ , \ (y, z) \in R_j\}| \\ &= |\{z \in X \mid (y, z) \in R_j \ , (z, x) \in R_i\}| = P_{ji}^{k}. \end{aligned}$$

□

مثال ۱.۴.۴. فرض کنید $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$. قرار دهید

$$\begin{aligned} R_0 =& \{(x_i, x_i) \ : \ x_i \in X\} \\ R_1 =& \{(x_1, x_2), (x_2, x_1), (x_3, x_5), (x_4, x_6), (x_5, x_3), (x_6, x_4)\} \\ R_2 =& \{(x_1, x_3), (x_1, x_4), (x_2, x_5), (x_2, x_6), (x_2, x_1), (x_3, x_4) \\ & , (x_4, x_1), (x_5, x_2), (x_5, x_6), (x_6, x_2), (x_6, x_5)\} \\ R_3 =& \{(x_1, x_5), (x_1, x_6), (x_2, x_3), (x_2, x_4), (x_3, x_2), (x_3, x_6) \\ & , (x_4, x_2), (x_4, x_5), (x_5, x_1), (x_5, x_4), (x_6, x_1), (x_6, x_3)\}. \end{aligned}$$

[7] commutative
[8] symmetric

در این صورت $(X, \{R_i\}_{i=۰}^{۳})$ یک اسکیم شرکت پذیر متقارن است، زیرا به وضوح $\bigcup_{i=۰}^{d} R_i = X \times X$ و $R_i \cap R_j = \emptyset$. همچنین $R_۰$ رابطه قطری است و برای هر i داریم $R_{i'} = R_i$. شرط (۳) اسکیم برقرار است، به عنوان نمونه اگر $(x_۱, x_۳) \in R_۲$ را در نظر بگیریم، آنگاه

$$P_{۳۱}^{۲} = |\{z \in X \mid (x_۱, z) \in R_۳ \ , \ (z, x_۳) \in R_۱\}| = ۱$$

یا مثلا $P_{۳۳}^{۳} = ۰$ و ... .

مثال ۵.۴.۱. فرض کنید X یک مجموعه ناتهی باشد. قرار دهید $R_۰ = \{(x, x) \mid x \in X\}$ و $R_۱ = X \times X \setminus R_۰$. در این صورت $X, \{R_۰, R - ۱\}$ یک اسکیم شرکت پذیر متقارن است که به آن اسکیم شرکت پذیر بدیهی روی X گویند. به وضوح $R_۰$ و $R_۱$ یک افراز از $X \times X$ هستند و شرایط (۱) و (۲) اسکیم برقرار هستند. برای بررسی شرط (۳)، به عنوان نمونه حالت‌های زیر را بررسی می‌کنیم:

۱. فرض کنیم $(x, x) \in R_۰$. در این صورت

$$|\{z \in X \mid (x, z) \in R_۱ \ , \ (z, x) \in R_۱\}| = |\{z \in X \mid (x, z) \in R_۱\}| = |X| - ۱.$$

بنابراین $P_{۱۱}^{۰} = |X| - ۱$.

۲. فرض کنیم $(x, y) \in R_۱$. در این صورت

$$|\{z \in X \mid (x, z) \in R_۱ \ , \ (z, y) \in R_۱\}| = |\{z \in X \mid (x, z) \in R_۱ \ , \ (y, z) \in R_۱\}| = |X| - ۲.$$

بنابراین $P_{۱۱}^{۱} = |X| - ۲$.

مشابهاً ثابت می‌شود که $P_{۰۱}^{۱} = P_{۱۰}^{۱} = P_{۰۰}^{۰} = ۱$ و $P_{۰۱}^{۰} + P_{۱۰}^{۰} = P_{۰۰}^{۱} = ۰$.

تعریف ۶.۴.۱. فرض کنید $(X, \{R_i\}_{i=۰}^{d})$ یک اسکیم شرکت پذیر باشد. همانطور که قبلاً گفتیم قرار می‌دهیم $R_i^* = R_{i'}$. در این صورت

$$P_{ii'}^{k} = |\{z \in X \mid (x, z) \in R_i \ , \ (z, x) \in R_i'\}| = |\{z \in X \mid (x, z) \in R_i\}| = k_i$$

به عدد فوق ظرفیت یا والنسی[۹] گفته می‌شود و معمولا آن را با k_i یا n_i نمایش می‌دهیم. به وضوح

$$k_۰ = P^k_{۰۰} = |\{z \in X \mid (x,z) \in R_۰\}| = |\{x\}| = ۱.$$

لم ۱.۴.۷. *در هر اسکیم* $(X, \{R_i\}_{i=۰}^d)$، *داریم:*

۱. $k_i|X| = |R_i|$.

۲. $k_i = k_{i'}$.

۳. $\sum_{i=۰}^d k_i = |X|$.

برهان. ۱. به ازای هر $x \in X$ قرار دهید $R_i(x) = \{y \in X \mid (x,y) \in R_i\}$. به وضوح $|R_i(x)| = k_i$.

چون

$$R_i = \bigcup_{x \in X} \{(x,y) \mid y \in R_i(x)\}$$

لذا

$$|R_i| = \sum_{x \in X} \{(x,y) \mid y \in R_i(x)\} = |X| k_i.$$

۲. چون به ازای هر i، $|R_i| = |R_{i'}|$، لذا طبق قسمت (۱) داریم $k_i|X| = |R_i| = |R_{i'}| = k_{i'}|X|$. در نتیجه $k_i = k_{i'}$.

۳. فرض کنید $x \in X$. در این صورت

$$\begin{aligned}
\sum_{i=۰}^d k_i &= \sum_{i=۰}^d |R_i(x)| \\
&= \sum_{i=۰}^d |\{z \in X \mid (x,z) \in R_i\}| = \left|\bigcup_{i=۰}^d \{z \in X \mid (x,z) \in R_i\}\right| \\
&= \left|\{z \in X \mid (x,z) \in \bigcup_{i=۰}^d R_i\}\right| = |\{z \in X \mid (x,z) \in X \times X\}| \\
&= |X|.
\end{aligned}$$

□

[9] valency

لم ۸.۴.۱. *در هر اسکیم شرکت پذیر* $(X, \{R_i\}_{i=0}^{d})$ *همواره داریم:*

۱. $P_{i0}^{k} = \delta_{ik}$.

۲. $P_{0j}^{k} = \delta_{jk}$.

۳. $P_{ij}^{0} = \delta_{ij'}k_i$.

۴. $P_{ij}^{k} = P_{j'i'}^{k'}$.

۵. $\sum_{j=0}^{d} P_{ij}^{k} = k_i$.

برهان. ۱. فرض کنید $(x, y) \in R_k$. در این صورت

$$\begin{aligned} P_{i0}^{k} &= |\{z \in X \mid (x,z) \in R_i \ , \ (z,y) \in R_0\}| \\ &= |\{z \in X \mid (x,y) \in R_i\}| \\ &= \begin{cases} 1 & i = k \\ 0 & i \neq k \end{cases} \\ &= \delta_{ik}. \end{aligned}$$

۲. فرض کنید $(x, y) \in R_k$. در این صورت

$$\begin{aligned} P_{0j}^{k} &= |\{z \in X \mid (x,z) \in R_0 \ , \ (z,y) \in R_j\}| \\ &= |\{z \in X \mid (x,y) \in R_j\}| \\ &= \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases} \\ &= \delta_{ik}. \end{aligned}$$

۳. فرض کنید $(x, x) \in R_0$. در این صورت

$$\begin{aligned} P_{ij}^{0} &= |\{z \in X \mid (x,z) \in R_i \ , \ (z,x) \in R_j\}| \\ &= \begin{cases} k_i & j = i' \\ 0 & j \neq i' \end{cases} \\ &= \delta_{ji'}k_i. \end{aligned}$$

۴. فرض کنید $(x,y) \in R_{k'}$. در این صورت $(y,x) \in R_k$ و داریم

$$\begin{aligned} P_{j'i'}^{k'} &= |\{z \in X \mid (x,z) \in R_{j'} \ , \ (z,y) \in R_{i'}\}| \\ &= |\{z \in X \mid (z,x) \in R_j \ , \ (y,z) \in R_i\}| \\ &= |\{z \in X \mid (y,z) \in R_i \ , \ (z,x) \in R_j\}| \\ &= P_{ij}^{k}. \end{aligned}$$

۵. فرض کنید $(x,y) \in R_k$. در این صورت

$$\begin{aligned} \sum_{i=0}^{d} P_{ij}^{k} &= \Big| \bigcup_{j=0}^{d} \{z \in X \mid (x,z) \in R_i \ , \ (z,y) \in R_j\} \Big| \\ &= \Big| \{z \in X \mid (x,z) \in R_i \ , \ (z,y) \in \bigcup_{j=0}^{d} R_j\} \Big| \\ &= |\{z \in X \mid (x,z) \in R_i\}| = |R_i(x)| = k_i. \end{aligned}$$

۶. برای اثبات، سه‌تایی‌های (x,y,z) را می‌شماریم که $(x,y) \in R_i$، $(y,z) \in R_j$ و $(x,z) \in R_t$.

ابتدا فرض کنید $(x,z) \in R_t$. در این صورت

$$|\{y \in X \mid (x,y) \in R_i \ , \ (y,z) \in R_j\}| = P_{ij}^{t}.$$

از طرفی تعداد $(x,z) \in R_t$ نیز برابر $|X|k_t$ است. پس اندازه مجموعه سه‌تایی‌های فوق برابر $|X|k_t P_{ij}^{t}$ است.

حال فرض کنید $(x,y) \in R_i$. در این صورت

$$|\{z \in X \mid (x,t) \in R_t \ , \ (z,y) \in R_{j'}\}| = P_{tj'}^{i}.$$

چون تعداد $(x,y) \in R_i$ نیز برابر $|X|k_i$ است. پس اندازه مجموعه سه‌تایی فوق برابر $|X|k_i P_{tj'}^{i}$ می‌باشد.

در نهایت، فرض کنید $(y,t) \in R_j$. در این صورت

$$|\{x \in X \mid (y,x) \in R_{i'} \ , \ (x,z) \in R_t\}| = P_{i't}^{j}.$$

از طرفی تعداد $(y,t) \in R_j$ نیز برابر $|X|k_j$ است. لذا اندازه مجموعه سه‌تایی فوق برابر $|X|k_j P^j_{i't}$ می‌باشد.

از تساوی‌های فوق داریم:

$$|X|k_t P^t_{ij} = |X|k_i P^i_{tj'} = |X|k_j P^j_{i't}.$$

در نتیجه $k_t P^t_{ij} = k_i P^i_{tj'} = k_j P^j_{i't}$. □

نکته ۹.۴.۱. در هر اسکیم شرکت پذیر شرط (۳) را می‌توان به صورت خلاصه بصورت زیر نوشت.

$$\begin{aligned} P^k_{ij} &= |\{z \in X \mid (x,z) \in R_i \ , \ (z,y) \in R_j\}| \\ &= |\{z \in X \mid z \in R_i(x) \ , \ z \in R_{j'}(y)\}| \\ &= |\{R_i(x) \cap R_{j'}(y)\}|. \end{aligned}$$

در این پایان نامه به دو کلاس از اسکیم‌های شرکت پذیر، یعنی در حالتی که $d = ۲$، علاقه‌مند هستیم. فرض کنید $A_۰ = I$، $A_۱$ و $A_۲$ ماتریس‌های مجاورت از اسکیم شرکت پذیر کلاس دو باشند. همان‌طور که در [۱۳] بیان شده است، دو حالت ممکن است رخ دهد: یا $A_۱^T = A_۱$ و $A_۲^T = A_۲$ که در این حالت گراف بدون جهت $(X, R_۱)$ یک گراف قویاً منظم با پارامترهای $(v, k := p^۰_{۱۱}, \lambda := p^۱_{۱۱}, \mu := p^۲_{۱۱})$ است، یا $A_۱^T = A_۲$ و $A_۲^T = A_۱$ که در این صورت گراف جهت‌دار $(X, R_۱)$ یک تورنمنت منظم دوگانه با پارامترهای $(v, k := p^۰_{۱۲}, \lambda := p^۱_{۱۱}, \mu := p^۲_{۱۱})$ می‌باشد. در هر دو حالت (SRGها و DRTها) داریم $A_۲ = J - I - A_۱$. فرض کنید $\overline{A}_۱ = A_۲$ و $A = A_۱$. در این صورت ماتریس A در $AJ = JA = kJ$ صدق می‌کند. در حالت اول، برای SRGها داریم:

$$A^۲ = kI + \lambda A + \mu(J - I - A)$$

و در حالت دوم، برای DRTها داریم

$$A^۲ = \lambda A + \mu(J - I - A).$$

فصل ۲

کدهای چرخشی دوگانه از اسکیم‌های شرکت پذیر کلاس دو

۱.۲ کدهای چرخشی دوگانه از درجه ۲

فرض کنید R یک حلقه جابه‌جایی شامل I و $r, s, t \in R$ ثابت‌های دلخواه باشند. به علاوه، فرض کنیم q توانی از یک عدد فرد و a یک نگاشت یک به یک از $\{\infty\} \cup \{۰, ۱, \ldots, q-۱\}$ به $GF(q) \cup \{\infty\}$ باشد به طوری که $a(۰) = ۰$، $a(۱) = ۱$ و $a(\infty) = \infty$. در این صورت نگاشت معکوس $a^{-۱}$ یک نگاشت یک به یک از $GF(q) \cup \{\infty\}$ به $\{\infty\} \cup \{۰, ۱, \ldots, q-۱\}$ است. اگر q اول باشد، اعضای $GF(q)$ می‌توانند به صورت اعداد صحیح نمایش داده شوند، یعنی

$$a(۰) = ۰,\ a(۱) = ۱,\ a(۲) = ۲,\ \ldots, a(q-۱) = q-۱$$

و لذا می‌توانیم فرض کنیم a نگاشت همانی است. حال ماتریس $Q(r, s, t) = [q_{i,j}]$ را یک ماتریس $q \times q$ روی R همراه با سطر و ستون‌های برچسب خورده با اعضای $GF(q)$:

$$a(۰) = ۰,\ a(۱) = ۱,\ a(۲) = ۲,\ \ldots, a(q-۱) = q-۱.$$

درایه‌های $q_{i,j}$ با استفاده از تابع مشخصه χ از باقی مانده درجه دوم $GF(q)$ تعریف می‌شود به طوری که

$$\chi(a_i) = \begin{cases} r & \text{اگر } a_i = a_۰ = ۰ \\ s & \text{اگر } a_i \text{ باقی‌مانده درجه دوم در } GF(q) \text{ نباشد} \\ t & \text{اگر } a_i \text{ باقی‌مانده درجه دوم در } GF(q) \text{ نباشد} \end{cases}$$

فرض می‌کنیم که $q_{i,j} = \chi(a_j - a_i)$. در این مورد زمانی که q اول باشد داریم

$$a(۰) = ۰,\ a(۱) = ۱,\ a(۲) = ۲,\ \ldots, a(q-۱) = q-۱$$

و این ما را به ماتریس چرخشی $Q_q(r,s,t)$. به علاوه تعریف می‌کنیم $Q = Q_q(۰,۱,۰)$ ماتریس باقی‌مانده درجه ۲ که شامل صفر نمی‌شود و $N = Q_q(۰,۰,۱)$ ماتریس غیر باقی‌مانده‌های درجه ۲ که شامل صفر نمی‌شود.

گابوریت کدهای چرخشی دوگانه را که از باقی‌مانده‌های درجه ۲ استفاده می‌کنند شناسایی و مطالعه کرده است و اسکیم‌های عمومی برای ساختار آن‌ها روی هر میدانی بدست آورد. کدهایی که از این ساختارها به دست می‌آیند، کدهای چرخشی دوگانه از باقی‌مانده درجه دوم یا QDC نامیده می‌شوند.

اکنون دو ساختار از کدهای چرخشی دوگانه (درجه ۲) روی R تعریف می‌کنیم. در ساختار اول یک کد توسط ماتریس مولد چرخشی دوگانه زیر به دست می‌آید:

$$P_q(r,s,t) = \left[I \mid Q_{q(r,s,t)} \right]$$

به این فرم، فرم محض چرخشی دوگانه گفته می‌شود.

در ساختار دوم برای هر $\alpha, \beta, \gamma \in R$ یک کد به وسیله ماتریس مولد چرخشی دوگانه زیر به دست می‌آید:

$$B_q(r,s,t) = \left[\begin{array}{c|c|c|c} ۱ & ۰ \ldots ۰ & \alpha & \beta \ldots \beta \\ \hline ۰ & & \gamma & \\ \vdots & I & \vdots & Q_q(r,s,t) \\ ۰ & & \gamma & \end{array}\right]$$

به این فرم، فرم محدود شده چرخشی دوگانه گفته می‌شود. در این حالت زمانی که $R = GF(p)$ برای p که یک عدد اول باشد دو کد $[۲q, q]$ و $[۲q+۲, q+۱]$ به ترتیب کدهای روی $GF(p)$ هستند.

در حالت‌های بالا زمانی که q اول نباشد، ماتریس $Q_q(r,s,t)$ چرخشی نخواهد بود.

۲.۲ ساختارهای عمومی

فرض کنیم A ماتریس مجاورت گراف G (نخستین گراف مجاورت از دو کلاس اسکیم شرکت پذیر) از v راس، درجه n، با پارامترهای λ و μ باشد.

ما باید دو حالت را در نظر بگیریم، حالت اول G یک SRG است که زمانی اتفاق می‌افتد که $A^T = A$ و حالت دوم G یک DRT باشد که زمانی است که $A^T = \overline{A}$.

لم ۱.۲.۲. *اگر G یک SRG باشد داریم*

$$AA^T = A^۲ = \kappa I + \lambda A + \mu\overline{A}. \tag{۱.۲}$$

اگر G یک DRT باشد داریم

$$AA^T = \kappa I + (\kappa - ۱ - \lambda)A + (\kappa - \mu)\overline{A}. \tag{۲.۲}$$

برهان. عبارت اول از مقدار شناخته شده $A^۲$ به دست می‌آید. عبارت دوم را نیز می‌توان با جای‌گذاری کردن $J - I - A$ به جای $A^T = \overline{A}$ و استفاده از مقدار شناخته شده AJ و $A^۲$ به دست آورد. □

برای یک DRT با پارامترهای $(v, \kappa, \lambda, \mu)$ داریم

$$AA^T = \kappa I + (\kappa - ۱ - \lambda)A + (\kappa - \mu)\overline{A}.$$

چون $\left(AA^T\right)^T = AA^T$ و $A^T = A$، پس $(\kappa - ۱ - \lambda) = (\kappa - \mu)$؛ یعنی $p^۱_{۱۲} = p^۲_{۱۲}$. بنابراین $\mu = \lambda + ۱$. در لم زیر روابط بین پارامترها را به طور خلاصه بیان کرده‌ایم.

لم ۲.۲.۲. *اگر G یک DRT با پارامترهای $(v, \kappa, \lambda, \mu)$ باشد، آن‌گاه $v = ۴\lambda + ۱$، $\kappa = ۲\lambda + ۱$ و $\mu = \lambda + ۱$.*

ساختارهای زیر را شرح می‌دهیم:

برای اسکالرهای دلخواه $r, s, t \in R$ فرض کنیم

$$Q_R(r, s, t) = \left(rI + sA + t\overline{A}\right). \tag{۳.۲}$$

ساختار محض عبارت است از

$$\mathcal{P}_R(r,s,t) = (I \mid Q_R(r,s,t))\,. \tag{۴.۲}$$

ساختار محدود شده عبارت است از

$$\mathcal{B}_R(r,s,t) = \left(\begin{array}{c|c|c|c} ۱ & ۰\ldots۰ & \alpha & \beta\ldots\beta \\ \hline ۰ & & \gamma & \\ \vdots & I & \vdots & Q_R(r,s,t) \\ ۰ & & \gamma & \end{array}\right) \tag{۵.۲}$$

که α، β و γ اسکالرهایی هستند که با توجه به حالت‌های خاص مشخص خواهند شد.

فرض می‌کنیم $P_R(r,s,t)$ پوشش سطری R از $\mathcal{P}_R(r,s,t)$ باشد و فرض کنیم $B_R(r,s,t)$ پوشش سطری R از $\mathcal{B}_R(r,s,t)$ باشد.

مثال بنیادی: اگر A ماتریس وقوع گراف پالی یا تورنمنت پالی باشد، آنگاه دو خانواده کدهای بالا، نخستین دو خانواده ذکر شده در [۱۵] هستند.

کد $P_R(r,s,t)$ یک کد به طول $۲v$ روی R و کد $B_R(r,s,t)$ یک کد به طول $۲v+۲$ روی R می‌باشد.

کد $P_R(r,s,t)$ یک کد آزاد روی هر حلقه R با $|R|^v$ عضو و کد $B_R(r,s,t)$ یک کد آزاد روی هر حلقه R با $|R|^{v+۱}$ عضو است. در نتیجه برای نشان دادن این‌که که آنها خودـ دوگان هستند، فقط باید نشان دهیم که آنها خودـ متعامد هستند. ابتدا با حالت محض شروع می‌کنیم.

برای این‌که کد $P_R(r,s,t)$ خودـ متعامد باشد به $Q_R(r,s,t)Q_R(r,s,t)^T = -I$ نیاز داریم.

لم ۳.۲.۲. *برای SRGها داریم*

$$\begin{aligned} Q_R(r,s,t)Q_R(r,s,t)^T &= \left(r^۲ + s^۲\kappa - t^۲ - t^۲\kappa + t^۲v\right) I \\ &+ \left(۲rs + s^۲\lambda - ۲st - ۲st\lambda + t^۲\lambda + ۲st\kappa + t^۲v - ۲t^۲\kappa\right) A \\ &+ \left(۲rt + s^۲\mu - ۲st\mu + t^۲\mu + ۲st\kappa + t^۲v - ۲t^۲ - ۲t^۲\kappa\right) \overline{A}. \end{aligned}$$

برای DRT ها داریم

$$\begin{aligned} Q_R(r,s,t)Q_R(r,s,t)^T &= \left(r^۲ + \left(s^۲+t^۲\right)\kappa\right) I \\ &+ \left(rt+sr+\left(s^۲+t^۲\right)(\kappa-۱-\lambda)+st\lambda+st\mu\right) A \\ &+ \left(rt+sr+\left(s^۲+t^۲\right)(\kappa-\mu)+st\mu+st\lambda\right)\overline{A}. \end{aligned}$$

برهان. با استفاده از لم ۱.۲.۲ ، معادله‌های ؟؟ و ؟؟ و یک محاسبه سرراست نتیجه می‌شود. □

وزن اقلیدسی هر یک از سطرهای $(I \mid Q_R(r,s,t))$ عبارت است $۱+r^۲+s^۲\kappa+t^۲(v-\kappa-۱)$. پس اگر یک $P_R(r,s,t)$ خودـدوگان برای یک کد روی $\mathbb{Z}_{۲m}$ دارای $۱+r^۲+s^۲\kappa+t^۲(v-\kappa-۱) \overset{۴m}{\equiv} ۰$ باشد، آنگاه $P_R(r,s,t)$ یک کد نوع II است. برای این‌که $B_R(r,s,t)$ خودـدوگان باشد به موارد زیر نیاز داریم:

$$۱+\alpha^۲+v\beta^۲ = ۰ \qquad (۶.۲)$$

$$\alpha\gamma+\beta(r+s\kappa+t(v-\kappa-۱)) = ۰ \qquad (۷.۲)$$

$$I+\gamma^۲J+Q_R(r,s,t)Q_R(r,s,t)^T = ۰. \qquad (۸.۲)$$

معادله اول حاصل ضرب داخلی سطر بالا با خودش می‌باشد. تساوی دوم حاصل ضرب داخلی سطر بالا با هر سطر دیگر است و رابطه سوم تضمین می‌کند که سایر سطرها با یکدیگر متعامد هستند.

معادله ۸.۲ ایجاب می‌کند که

$$Q_R(r,s,t)Q_R(r,s,t)^T = -\left(۱+\gamma^۲\right)I-\gamma^۲A-\gamma^۲\overline{A}.$$

زمانی که $R=\mathbb{Z}_{۲m}$ برای این‌که این کد نوع II باشد به نسبت‌های

$$۱+\alpha^۲+v\beta^۲ \overset{۴m}{\equiv} ۰$$

(حاصل ضرب داخلی سطر بالا با خودش) و

$$۱+\gamma^۲+r^۲+s^۲\kappa+t^۲(v-k-۱) \overset{۴m}{\equiv} ۰$$

(ضرب داخلی هر سطر دیگر با خودش) نیاز داریم. نتایج این بخش را در دو قضیه زیر خلاصه می‌کنیم.

قضیه ۴.۲.۲. *کد $P_R(r,s,t)$ تشکیل شده از یک SRG، اقلیدسی خودـ دوگان روی R است اگر و تنها اگر*

$$\begin{aligned}
\left(r^۲ + s^۲\kappa - t^۲ - t^۲\kappa + t^۲v\right) &= -۱ \\
\left(۲rs + s^۲\lambda - ۲st - ۲st\lambda + t^۲\lambda + ۲st\kappa + t^۲v - ۲t^۲\kappa\right) &= ۰ \\
\left(۲rt + s^۲\mu - ۲st\mu + t^۲\mu + ۲st\kappa + t^۲v - ۲t^۲ - ۲t^۲\kappa\right) &= ۰.
\end{aligned}$$

کد $P_R(r,s,t)$ تشکیل شده از یک DRT، اقلیدسی خودـ دوگان روی R است اگر و تنها اگر

$$\begin{aligned}
\left(r^۲ + \left(s^۲ + t^۲\right)\kappa\right) &= -۱ \\
\left(rt + sr + \left(s^۲ + t^۲\right)(\kappa - ۱ - \lambda) + st\lambda + st\mu\right) &= ۰ \\
\left(rt + sr + \left(s^۲ + t^۲\right)(\kappa - \mu) + st\mu + st\lambda\right) &= ۰.
\end{aligned}$$

قضیه ۵.۲.۲. *کد $B_R(r,s,t)$ تشکیل شده از یک SRG، اقلیدسی خودـ دوگان روی R است اگر و تنها اگر*

$$\begin{aligned}
\left(r^۲ + s^۲\kappa - t^۲ - t^۲\kappa + t^۲v\right) &= -\left(۱ + \gamma^۲\right) \\
\left(۲rs + s^۲\lambda - ۲st - ۲st\lambda + t^۲\lambda + ۲st\kappa + t^۲v - ۲t^۲\kappa\right) &= -\gamma^۲ \\
\left(۲rt + s^۲\mu - ۲st\mu + t^۲\mu + ۲st\kappa + t^۲v - ۲t^۲ - ۲t^۲\kappa\right) &= -\gamma^۲ \\
۱ + \alpha^۲ + v\beta^۲ &= ۰ \\
\alpha\gamma + \beta(r + s\kappa + t(v - \kappa - ۱)) &= ۰
\end{aligned}$$

کد $B_R(r,s,t)$ تشکیل شده از یک DRT، اقلیدسی خودـ دوگان روی R است اگر و تنها اگر

$$\begin{aligned}
\left(r^۲ + \left(s^۲ + t^۲\right)\kappa\right) &= -\left(۱ + \gamma^۲\right)\\
\left(rt + sr + \left(s^۲ + t^۲\right)(\kappa - ۱ - \lambda) + st\lambda + st\mu\right) &= -\gamma^۲\\
\left(rt + sr + \left(s^۲ + t^۲\right)(\kappa - \mu) + st\mu + st\lambda\right) &= -\gamma^۲\\
۱ + \alpha^۲ + v\beta^۲ &= ۰\\
\alpha\gamma + \beta(r + s\kappa + t(v - \kappa - ۱)) &= ۰.
\end{aligned}$$

به علاوه، این کد خودـ دوگان، نوع II روی $\mathbb{Z}_{۲m}$ است اگر و تنها اگر

$$۱ + \gamma^۲ + r^۲ + s^۲\kappa + t^۲(v - \kappa - ۱) \overset{۴m}{\equiv} ۰$$

و

$$۱ + \alpha^۲ + v\beta^۲ \overset{۴m}{\equiv} ۰.$$

۳.۲ شرایط خودـ دوگان به وسیله الفبا

در این بخش شرایط قبلی برای خودـ دوگان بودن را در مشخصه‌های ۲، ۳ و ۴ ساده می‌کنیم.

۱.۳.۲ $R = \mathbb{F}_۲$.

۱.۱.۳.۲ SRG ها

روی $\mathbb{F}_۲$ معادلات بیان شده در لم ۳.۲.۲ را برای SRG می‌توان به صورت زیر کاهش داد

$$\begin{aligned}
Q_{\mathbb{F}_۲}(r,s,t)Q_{\mathbb{F}_۲}(r,s,t)^T &= (r^۲ + s^۲\kappa + t^۲ + t^۲\kappa + t^۲v)I + (s^۲\lambda + t^۲\lambda + t^۲v)A\\
&+ (s^۲\mu + t^۲\mu + t^۲v)\overline{A}
\end{aligned}$$

و توجه داریم که برای هر a داریم $a^۲ = a$، پس خواهیم داشت

$$\begin{aligned}
Q_{\mathbb{F}_۲}(r,s,t)Q_{\mathbb{F}_۲}(r,s,t)^T &= (r + s\kappa + t + t\kappa + tv)I + (s\lambda + t\lambda + tv)A\\
&+ (s\mu + t\mu + tv)\overline{A}.
\end{aligned}$$

ما از این روابط برای بررسی زمانی که ساختارها، کدهای خودـدوگان را می‌دهند استفاده می‌کنیم. در جدول ۱.۲ و ۲.۲، همه تساوی‌ها در $F_۲$ و هم ارزی‌ها به پیمانه ۴ داده شده است. در ستون‌ها شرایط لازم برای نتایج را ارائه می‌دهیم. در سطرها نیز فقط شرایطی روی v، κ، λ، μ و γ ارائه می‌کنیم. به علاوه این شرایط باید در شرایط لازم ارائه شده برای α و β نیز صدق کنند.

r	s	t	خودـدوگان محض	محض نوع II	خودـدوگان محدود شده	محدود شده نوع II
۰	۰	۱	$\lambda = v = \mu = \kappa$	$v \equiv \kappa$	$\lambda = \mu = \kappa, \gamma = \kappa + v$	$v - \kappa + \gamma \equiv ۰$
۰	۱	۰	$\kappa = ۱, \lambda = \mu = ۰$	$\kappa \equiv ۳$	$\lambda = \mu = \gamma = \kappa + ۱$	$\gamma + \kappa \equiv ۳$
۰	۱	۱	$v = ۰$	$v \equiv ۰$	$v = \gamma$	$\gamma \equiv -v$
۱	۰	۰	همیشه	هیچ وقت	$\gamma = ۰$	هیچ وقت
۱	۰	۱	$\lambda = \mu = v = \kappa + ۱$	$v \equiv \kappa + ۳$	$\kappa + ۱ = v + \gamma = \lambda = \mu$	$\kappa + ۳ \equiv v + \gamma$
۱	۱	۰	$\lambda = \mu = \kappa = ۰$	$\kappa \equiv ۲$	$\kappa = \gamma = \lambda = \mu$	$\gamma + \kappa \equiv ۲$
۱	۱	۱	$v = ۱$	$v \equiv ۳$	هیچ وقت	هیچ وقت

جدول ۱.۲: کدهای خودـدوگان دوتایی SRG

۲.۱.۳.۲ DRT ها

روی $\mathbb{F}_۲$ معادلات برای DRT ها را نمی‌توان کاهش داد به جز زمانی که مربع هر عضو با خودش برابر باشد.

یادآوری می‌کنیم که بنا به لم ۲.۲.۲، پارامترهای یک DRT در روابط $v = ۴\lambda + ۳$، $\kappa = ۲\lambda + ۱$ و $\mu = \lambda + ۱$ صدق می‌کنند. بنابراین نتیجه می‌گیریم کدهای $P(۱, ۱, ۰)$ و $P(۱, ۰, ۱)$ هیچ وقت خودـدوگان نیستند، زیرا معادلات فوق نتیجه می‌دهند که κ باید برابر با صفر باشد که این با $\kappa = ۲\lambda + ۱$ تناقض دارد. هم‌چنین نتیجه می‌گیریم $B(۱, ۱, ۱)$ هیچ وقت خودـدوگان نیست، زیرا در این صورت خواهیم داشت $\mu = \lambda$ که مجددا یک تناقض است.

r	s	t	خودـدوگان محض	نوع II محض	خودـدوگان محدود شده	محدود شده نوع II
۰	۰	۱	$\lambda + ۱ = \kappa = ۱$	$v \equiv \kappa$	$\lambda = ۰, \kappa = \gamma + ۱$	$v - \kappa + \gamma \equiv ۰$
۰	۱	۰	$۱ = \kappa = \lambda + ۱$	$\kappa \equiv ۳$	$\lambda = ۰, \kappa = \gamma + ۱$	$\gamma + \kappa \equiv ۳$
۰	۱	۱	هیچ وقت	هیچ وقت	$\lambda + \mu = \gamma = ۱$	$\gamma + v \equiv ۰$
۱	۰	۰	همیشه	هیچ وقت	$\gamma = ۰$	هیچ وقت
۱	۰	۱	هیچ وقت	هیچ وقت	$\kappa = \gamma, \mu = ۱, \lambda = ۰$	$\kappa + ۳ \equiv v + \gamma$
۱	۱	۰	هیچ وقت	هیچ وقت	$\kappa = \gamma, \mu = ۱, \lambda = ۰$	$\gamma + \kappa \equiv ۲$
۱	۱	۱	$\kappa = \lambda$	$v \equiv ۳$	هیچ وقت	هیچ وقت

جدول ۲.۲: کدهای خودـدوگان دوتایی DRT

در حالتی که $r = ۰$ و $s = t = ۱$، نتیجه جالبی در حالت محض رخ می‌دهد. در ساخت این حالت، ماتریس $(I \mid JI)$ را به دست می‌آوریم که فقط در صورتی خود-دوگان خواهد بود که مرتبه ماتریس‌ها زوج باشد. با این حال، این نتیجه نشان می‌دهد که هیچ کد خود-دوگانی وجود ندارد که با استفاده از آن، نتیجه شناخته شده‌ای که بیان می‌کند در یک DRT باید داشته باشیم $v \overset{۲}{\equiv} ۱$ را بهبود می‌دهیم.

۲.۳.۲ $R = \mathbb{F}_۴$.

برای $\mathbb{F}_۴$ باید از ضرب داخلی هرمیتین استفاده کنیم. بنابراین برای این کار به محاسباتی مشابه لم ۳.۲.۲ داریم.

لم ۱.۳.۲. *روی $\mathbb{F}_۴$ با گستره ϕ، برای SRG ها داریم*

$$\begin{aligned} Q(r,s,t)\phi(Q(r,s,t)) = &\left(r^۳ + s^۳\kappa + t^۳ + t^۳\kappa + t^۳v\right) I \\ &+ \left(rs^۲ + sr^۲ + s^۳\lambda + ts^۲ + st^۲\right. \\ &\left. + t^۳\lambda + \left(ts^۲ + st^۲\right)\kappa + t^۳v\right) A \\ &+ \left(rt^۲ + tr^۲ + s^۳\mu + \left(ts^۲ + st^۲\right)\mu + t^۳\mu\right. \\ &\left. + \left(ts^۲ + st^۲\right)\kappa + t^۳v\right)\overline{A}. \end{aligned}$$

روی $\mathbb{F}_۴$ با گستره ϕ، برای DRT ها داریم

$$\begin{aligned} Q(r,s,t)\phi(Q(r,s,t)) = &\left(r^۳ + \left(s^۳ + t^۳\right)\kappa\right) I \\ &+ \left(rt^۲ + sr^۲ + \left(s^۳ + t^۳\right)(\kappa + ۱ + \lambda) + st^۲\lambda + ts^۲\mu\right) A \\ &+ \left(rs^۲ + tr^۲ + \left(s^۳ + t^۳\right)(\kappa + \mu) + st^۲\mu + ts^۲\lambda\right)\overline{A}. \end{aligned}$$

برهان. اگر گستره $\mathbb{F}_۴$ برابر با ϕ باشد، آنگاه داریم

$$\begin{aligned} Q(r,s,t)\phi(Q(r,s,t)) &= (rI + sA + t\overline{A})(\phi(r)\phi(I) + \phi(s)\phi(A) + \phi(t)\phi(\overline{A})) \\ &= (rI + sA + t\overline{A})(\phi(r)I + \phi(s)A + \phi(t)(\overline{A})). \end{aligned}$$

در این صورت توجه می‌کنیم که در $\mathbb{F}_۴$ داریم $\phi(a) = a^۲$ و لذا با استفاده از این نکته، مشخصه برابر ۲ است و درستی محاسبه بالا اثبات می‌شود. □

۱.۲.۳.۲ حالت محض

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از SRG ها در ساختار محض روی $\mathbb{F}_۴$ خودـ دوگان هستند. اگر s و t ناصفر باشند، آنگاه

$$r^۳ = v$$

$$\left(rt^۲ + sr^۲ + ts^۲ + st^۲\right) = \left(st^۲ + ts^۲\right)\kappa + v$$

$$\left(rt^۲ + tr^۲\right) = \left(st^۲ + ts^۲\right)(\mu + \kappa) + v.$$

اگر $s = ۰$ و $t \neq ۰$، آنگاه

$$r^۳ = \kappa + v$$

$$\lambda = v$$

$$\left(rt^۲ + tr^۲\right) = \mu + v.$$

اگر $s \neq ۰$ و $t = ۰$، آنگاه

$$r^۳ = \kappa + ۱$$

$$\left(rs^۲ + sr^۲\right) = \lambda$$

$$\mu = ۰.$$

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از DRT ها در ساختار محض روی $\mathbb{F}_۴$ خودـ دوگان هستند.

اگر s و t ناصفر باشند، آنگاه

$$rt^۲ + sr^۲ = st^۲\lambda + ts^۲\mu$$

$$rs^۲ + tr^۲ = st^۲\mu + ts^۲\lambda.$$

اگر یکی از s و t ناصفر باشد، آنگاه $r^۳ = ۱ + \kappa$. بنابراین r ناصفر است اگر و تنها اگر $\kappa \overset{۲}{\equiv} ۰$.

اگر $s = ۰$ و $t \neq ۰$، آنگاه

$$rt^۲ = \kappa + ۱ + \lambda$$

$$tr^۲ = \kappa + \mu.$$

اگر $s \neq ۰$ و $t = ۰$، آنگاه

$$sr^۲ = \kappa + ۱ + \lambda$$

$$rs^۲ = \kappa + \mu.$$

سپس با استفاده از این که $\mu = \lambda + ۱$ و $s \neq ۰$، داریم $r^۲ = rs$. بنابراین اگر r ناصفر باشد، آنگاه $r = s$.

۲.۲.۳.۲ حالت محدود شده

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از SRG ها در ساختار محدود شده روی $\mathbb{F}_۴$ خودـ دوگان هستند. اگر s و t ناصفر باشند، آنگاه

$$r^۳ + v = \gamma^۲$$

$$rs^۲ + sr^۲ + ts^۲ + st^۲ = \left(ts^۲ + st^۲\right)\kappa + v + \gamma^۲$$

$$rt^۲ + tr^۲ = \left(ts^۲ + st^۲\right)\mu + \left(ts^۲ + st^۲\right)\kappa + v + \gamma^۲.$$

اگر $s = ۰$ و $t \neq ۰$، آنگاه

$$r^۳ + \kappa + v = \gamma^۲$$

$$\lambda + v = \gamma^۲$$

$$\left(rt^۲ + tr^۲\right)\mu + v = \gamma^۲.$$

اگر $s \neq ۰$ و $t = ۰$، آنگاه

$$r^۳ + \kappa = ۱ + \gamma^۲$$

$$\left(rs^۲ + sr^۲\right) + \lambda = \gamma^۲$$

$$\mu = \gamma^۲.$$

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از DRT ها در ساختار محدود شده روی $\mathbb{F}_۴$ خودـ دوگان هستند.

اگر s و t ناصفر باشند، آنگاه

$$r^۳ = ۱ + \gamma^۲$$

$$rt^۲ + sr^۲ + st^۲\lambda + t^۲\mu = \gamma^۲$$

$$rs^۲ + tr^۲ + st^۲\mu + ts^۲\lambda = \gamma^۲.$$

اگر یکی از s و t ناصفر باشد، آنگاه $r^۳ = ۱ + \kappa$. بنابراین r ناصفر است اگر و تنها اگر $\kappa \overset{۲}{\equiv} ۰$.

اگر $s = ۰$ و $t \neq ۰$، آنگاه

$$r^۳ + \kappa = ۱ + \gamma^۲$$

$$rt^۲ + \kappa + ۱ + \lambda = \gamma^۲$$

$$tr^۲ + \kappa + \mu = \gamma^۲.$$

۳.۳.۲ $R = \mathbb{F}_3$.

مشاهده می‌کنیم که روی $\mathbb{F}_3$ حالت $s = t = 0$ را نمی‌توانیم داشته باشیم. معادلات جدول‌های ۳.۲، ۴.۲، ۵.۲ و ۶.۲ همه در میدان $\mathbb{F}_3$ هستند.

خود-دوگان محض	t	s	r
$rs = \lambda, \mu = 0, \kappa = 1$	0	$\neq 0$	$\neq 0$
$2 = v - \kappa, \kappa = \lambda + 2 = 2rt + \mu$	$\neq 0$	0	$\neq 0$
$\kappa = 2, \lambda = \mu = 0$	0	$\neq 0$	0
$v = \kappa = \lambda = \mu + 1$	$\neq 0$	0	0
$v = 0, \lambda - \kappa = st(1 + \lambda - \kappa), \mu - \kappa = st(\mu - \kappa)$	$\neq 0$	$\neq 0$	0

جدول ۳.۲: کدهای خود-دوگان سه‌تایی SRG: حالت محض

خود-دوگان محدود شده	t	s	r
$2rs + \lambda = \mu = 2 + \kappa, \gamma^2 = 1 + 2\kappa$	0	$\neq 0$	$\neq 0$
$\lambda = 1 + \kappa, 2rt + \mu = \kappa, \gamma^2 = 2 + 2v + \kappa$	$\neq 0$	0	$\neq 0$
$\lambda = 1 + \kappa = \mu, \gamma^2 = 2 + 2\kappa$	0	$\neq 0$	0
$\lambda = \kappa = \mu + 1, \gamma^2 = \kappa + 2v$	$\neq 0$	0	0
$v = -\gamma^2, \lambda - \kappa = st(1 + \lambda - \kappa), \mu - \kappa - 1 = st(\mu - \kappa)$	$\neq 0$	$\neq 0$	0

جدول ۴.۲: کدهای خود-دوگان سه‌تایی SRG: حالت محدود شده

خود-دوگان محض	t	s	r
$\lambda = rs, \kappa = 1$	0	$\neq 0$	$\neq 0$
$\lambda = rt, \kappa = 1$	$\neq 0$	0	$\neq 0$
$\lambda = 1, \kappa = 2$	0	$\neq 0$	0
$\lambda + 1 = \kappa = 2$	$\neq 0$	0	0
$\kappa = 1, (\kappa - 1 - \lambda) = st(\lambda + \mu)$	$\neq 0$	$\neq 0$	0

جدول ۵.۲: کدهای خود-دوگان سه‌تایی DRT: حالت محض

۴.۳.۲ $R = \mathbb{Z}_4$.

همه کدهایی که روی $\mathbb{Z}_4$ خواهیم ساخت، آزاد هستند. چندین ساختار شناخته شده را بهبود می‌دهیم. حالت عمومی DRT در [۹، صفحه ۴۱] با استفاده از هم ارزی با ماتریس‌های هادامارد[1] بیان شده است. برای مثال معادله (۴۰) در [۹، صفحه ۴۱]، $B_{\mathbb{Z}_4}(0, 1, 3)$ می‌باشد. به طور مشابه ماتریس‌های در [۸، معادله

[1] Hadamard

خودـ دوگان محدود شده	t	s	r
$sr = \lambda, \gamma^۲ = ۱ + ۲\kappa$	۰	$\neq ۰$	$\neq ۰$
$rt = \lambda = ۰, \gamma^۲ = ۱ + ۲\kappa$	$\neq ۰$	۰	$\neq ۰$
$\lambda = ۱, \gamma^۲ = ۲ + ۲\kappa$	۰	$\neq ۰$	۰
$\lambda = ۱, \gamma^۲ = ۲ + ۲\kappa$	$\neq ۰$	۰	۰
$\kappa + ۲ = \gamma^۲, st(\lambda + \mu) = ۱ - \kappa - ۲(\kappa - ۱ - \lambda)$	$\neq ۰$	$\neq ۰$	۰

جدول ۶.۲: کدهای خودـ دوگان سه‌تایی DRT: حالت محدود شده

(۳.۱) و (۳.۲)] به ترتیب با حالت محدود شده $B_{\mathbb{Z}_۴}(b, b, ۰)$ و $B_{\mathbb{Z}_۴}(۱, ۳, ۲)$ ذکر شده ما، هم ارز (در حد سطر بالایی) هستند. $B_{\mathbb{Z}_۴}(۲, ۱, ۳)$ با $\alpha = ۲$، $\beta = ۱$ و $\gamma = ۳$، توسط چاپمن[۲] برای استخراج یک ساختار فارغ از رایانه از مشبکه لیچ[۳] استفاده شد.

۱.۴.۳.۲ حالت محض

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از SRG ها در ساختار محض روی $\mathbb{Z}_۴$ خودـ دوگان هستند. اگر s و t هر دو غیر یکه باشند، آنگاه $r^۳ = ۳$ یک معادله بدون جواب خواهد بود. پس فرض می‌کنیم حداقل یکی از s و t یکه باشد. اگر s یکه و t غیر یکه باشد، آنگاه داریم

$$r^۲ + v = \kappa$$

$$\lambda + v + ۲\kappa = ۰$$

$$۲(\mu + \kappa + ۱) + \mu + v = ۰.$$

اگر s غیر یکه و t یکه باشد، آنگاه

$$r^۲ + \kappa + ۱ = ۰$$

$$۲r + \lambda = ۰$$

$$\mu = ۰.$$

اگر s و t هر دو یکه باشند، آنگاه $r = v = ۰$.

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از DRT ها در ساختار محض روی $\mathbb{Z}_۴$ خودـ دوگان هستند. اگر s و t هر دو غیر یکه باشند، آنگاه $r^۳ = ۳$ یک معادله بدون جواب خواهد بود. پس فرض

[2] Chapman
[3] Leech

می‌کنیم حداقل یکی از s و t یکه باشد. اگر s یکه و t غیر یکه باشد، آنگاه داریم

$$r^۳ + \kappa = ۳$$

$$rt + sr + t^۲(\kappa - ۱ - \lambda) + st(\lambda + \mu) = ۰$$

$$rt + sr + t^۲(\kappa - \mu) + ts(\lambda + \mu) = ۰.$$

اگر s یکه و t غیر یکه باشد، آنگاه

$$r^۳ + \kappa = ۳$$

$$rt + sr + s^۲(\kappa - ۱ - \lambda) + st(\lambda + \mu) = ۰$$

$$rt + sr + s^۲(\kappa - \mu) + ts(\lambda + \mu) = ۰.$$

اگر s و t هر دو یکه باشند، آنگاه

$$r^۲ + ۲\kappa = ۳$$

$$rt + sr + ۲(\kappa - ۱ - \lambda) + st(\lambda + \mu) = ۰$$

$$rt + sr + ۲(\kappa - \mu) + ts(\lambda + \mu) = ۰.$$

۲.۴.۳.۲ حالت محدود شده

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از SRG ها در ساختار محدود شده روی $\mathbb{Z}_۴$ خودـ دوگان هستند.

اگر s و t غیر یکه باشند، آنگاه $r^۲ + \gamma^۲ = ۳$ یک معادله بدون جواب است.

اگر s غیر یکه و t یکه باشد، آنگاه

$$r^۲ + v = \kappa - \gamma^۲$$

$$\lambda + v + ۲\kappa = -\gamma^۲$$

$$۲(\mu + \kappa + ۱) + \mu + v = -\gamma^۲.$$

اگر s یکه و t غیر یکه باشد، آنگاه

$$r^۲ + \kappa = ۳ - \gamma^۲$$

$$۲r + \lambda = -\gamma^۲$$

$$\mu = -\gamma^۲.$$

اگر s و t هر دو یکه باشند، آنگاه

$$r^۲ = -\gamma^۲$$

$$v = ۰.$$

اکنون بررسی می‌کنیم که چه زمانی کدهای به دست آمده از DRT ها در ساختار محدود شده روی $\mathbb{Z}_۴$ خودـ دوگان هستند.

اگر s و t هر دو غیر یکه باشند، آنگاه $r^۲ + \gamma^۲ = ۳$ یک معادله بدون جواب است.

اگر s غیر یکه و t یکه باشد، آنگاه

$$r^۲ + \kappa = ۳ - \gamma^۲$$

$$rt + st + t^۲(\kappa - ۱ - \lambda) + st(\lambda + \mu) = -\gamma^۲$$

$$rt + sr + t^۲(\kappa - \mu) + ts(\lambda + \mu) = -\gamma^۲.$$

اگر s یکه و t غیر یکه باشد، آنگاه

$$r^۲ + \kappa = ۳ - \gamma^۲$$

$$rt + sr + s^۲(\kappa - ۱ - \lambda) + st(\lambda + \mu) = -\gamma^۲$$

$$rt + sr + s^۲(\kappa - \mu) + ts(\lambda + \mu) = ۰.$$

اگر s و t هر دو یکه باشند، آنگاه

$$r^۲ + ۲\kappa = ۳ - \gamma^۲$$

$$rt + sr + ۲(\kappa - ۱ - \lambda) + st(\lambda + \mu) = -\gamma^۲$$

$$rt + sr + ۲(\kappa - \mu) + ts(\lambda + \mu) = ۰.$$

۴.۲ خانواده‌هایی از SRGها

با بررسی ماتریس مولد، گزاره زیر به‌دست می‌آید.

گزاره ۱.۴.۲. *اگر $P(r,s,t)$ یک کد خودـ دوگان باشد، آنگاه $B(r,s,t)$ با پارامترهای $\gamma = \beta = ۰$ و $\alpha = \sqrt{-۱}$ یک کد خودـ دوگان است.*

اگر حالت فوق را داشته باشیم، نباید در حالت محدود شده این مورد را ثبت کنیم مگر این‌که کد نوع II باشد.

۱.۴.۲ گراف‌های خاص

گراف‌های زیر را می‌توان در [۶] یافت.

گراف پترسن[۴] با پارامترهای $(۱۰, ۳, ۰, ۱)$، که به وسیله ساختار محدود شده $(۴, ۳, ۰)$ با $\alpha = ۳$، $\beta = ۴$ و $\gamma = ۱$ به دست می‌آید یک $[۲۲, ۱۱, ۶]$ کد خود-دوگان روی $\mathbb{F}_۵$ با گروه خودریختی $S_۵$ می‌باشد.

گراف شریخنده[۵] با پارامترهای $(۱۶, ۶, ۲, ۲)$ که به وسیله ساختار محض $(۱, ۱, ۰)$ به دست می‌آید یک $[۳۲, ۱۶, ۸]$ کد اکسترمال نوع II است.

گراف سلبچ[۶] با پارامترهای $(۱۶, ۱۰, ۶, ۶)$ که به وسیله ساختار محض $(۱, ۰, ۱)$، یک $[۳۲, ۱۶, ۸]$ کد اکسترمال نوع II است.

سه **گراف چانگ**[۷] با پارامترهای $(۲۸, ۱۲, ۶, ۴)$ که به وسیله ساختار محض $(۱, ۰, ۰)$ به دست می‌آیند، هرسه $[۵۶, ۲۸, ۸]$ کد نوع II هستند.

گراف هافمن-سینگلتون[۸] با پارامترهای $(۵۰, ۷, ۰, ۱)$ که به وسیله ساختار محض $(۱, ۰, \omega)$ به دست می‌آید یک $[۱۰۰, ۵۰, ۱۴]$ کد خود-دوگان هرمیتین روی $\mathbb{F}_۴$ است.

گراف گویرتز[۹] با پارامترهای $(۵۶, ۱۰, ۰, ۲)$ که با استفاده از ساختار محض $(۱, ۱, ۰)$ به دست می‌آید یک $[۱۱۲, ۵۶, ۱۲]$ کد نوع II است.

۲.۴.۲ گراف خطی از گراف کامل

گراف $L(K_n)$ که هم ارز با اسکیم جانسون[۱۰] $J(n, ۲)$ [۲۷، فصل ۲۱] است، گراف مثلثی نیز نامیده می‌شود. طبق [۱۸، صفحه ۲۱۸] پارامترهای آن $(\binom{n}{۲}, ۲n - ۴, n - ۲, ۴)$ هستند.

- اگر $n \overset{۲}{\equiv} ۰$، آنگاه $P_{\mathbb{F}_۲}(۱, ۰, ۰)$ خود-دوگان است.

[4] Petersen
[5] Shrikhande
[6] Clebsch
[7] Chang
[8] Hoffman-Singleton
[9] Gewirtz
[10] Johnson

- اگر n زوج باشد، آنگاه $P_{\mathbb{F}_۲}(۱,۱,۰)$ یک کد خودـدوگان است.

مثال ۲.۴.۲. برای گراف $L(K_۶)$، کد $P_{\mathbb{F}_۲}(۱,۱,۰)$ یک $[۳۰,۱۵,۶]$ کد بهینه نوع I است. برای گراف $L(K_۸)$، کد $P_{\mathbb{F}_۲}(۰,۰,۱)$ یک $[۵۶,۲۸,۸]$ کد بهینه نوع II است.

- اگر $n \overset{۴}{\equiv} ۰$، آنگاه $P_{\mathbb{F}_۴}(۰,a,۰)P_{\mathbb{F}_۴}(۰,۰,a)$، و $P_{\mathbb{F}_۴}(۰,a,a)$ که در آن‌ها $a \neq ۰$، کدهایی خودـدوگان روی $\mathbb{F}_۴$ هستند.

- اگر $n \overset{۴}{\equiv} ۱$، آنگاه $P_{\mathbb{F}_۴}(۰,a,a)$ که در آن $a \neq ۰$، یک کد خودـدوگان روی $\mathbb{F}_۴$ است.

- اگر $n \overset{۴}{\equiv} ۲$، آنگاه $P_{\mathbb{F}_۴}(a,a,a)$ و $P_{\mathbb{F}_۴}(a,a,۰)$ که در آن‌ها $a \neq ۰$، کدهایی خودـدوگان روی $\mathbb{F}_۴$ هستند.

- اگر $n \overset{۴}{\equiv} ۳$، آنگاه $P_{\mathbb{F}_۴}\left(\omega,۰,\omega^۲\right)$ $P_{\mathbb{F}_۴}\left(\omega^۲,۰,\omega\right)$ و $P_{\mathbb{F}_۴}(a,a,۰)$ که در آن‌ها $a \neq ۰$، کدهایی خودـدوگان روی $\mathbb{F}_۴$ هستند.

مثال ۳.۴.۲. برای گراف $L(K_۳)$، کد $P_{\mathbb{F}_۴}\left(\omega,۰,\omega^۲\right)$ یک کد $[۶,۳,۲]$ نوع IV است. برای گراف $L(K_۷)$، کد $P_{\mathbb{F}_۴}\left(\omega,۰,\omega^۲\right)$ یک $[۴۲,۲۱,۸]$ کد نوع IV است.

۳.۴.۲ آرایه‌های متعامد

یک آرایه متعامد $OA(h,n)$ همان‌طور که در [۱۸، صفحه ۲۲۴] تعریف شده است، با استفاده از نماد گذاری [۲۷، فصل ۲۱]، یک کد از طول h، بعد ۲ روی یک الفبا از اندازه n و فاصله دوگان حداقل ۳ می‌باشد. دو کدکلمه را مجاور گوییم اگر فاصله همینگ آن‌ها $h-۱$ باشد. طبق [۱۸، قضیه ۱۰.۴.۲]، پارامترها عبارتند از $(n^۲, h(n-۱), n-۲+(h-۱)(h-۲), h(h-۱))$. به طور معادل یک $OA(h,n)$ دستگاهی از $h-۲$ مربع لاتین متعامد متقابل است. رئوس SRG، سلول‌های مربع‌ها هستند. دو سلول مجاور هستند اگر آن‌ها یک سطر یا ستون یا درایه‌ای مشترک در یکی از مربع‌ها داشته باشند.

- اگر هر دو h و n زوج باشند، آنگاه $P_{\mathbb{F}_۲}(۰,۰,۱)$ یک کد خودـدوگان است و اگر $h \overset{۴}{\equiv} ۰$، کد نوع II است.

- اگر هر دو h و n زوج باشند، آنگاه $P_{\mathbb{F}_۲}(۱, ۱, ۰)$ یک کد خودـدوگان است و اگر $h \overset{۴}{\equiv} ۲$، کد نوع II است.
- اگر h فرد و n زوج باشد، آنگاه $P_{\mathbb{F}_۲}(۰, ۱, ۰)$ یک کد خودـدوگان است و اگر $h \overset{۴}{\equiv} ۳$ و $n \overset{۴}{\equiv} ۲$ یا $h \overset{۴}{\equiv} ۱$ و $n \overset{۴}{\equiv} ۰$، آنگاه کد نوع II است.
- اگر h فرد و n زوج باشد، آنگاه $P_{\mathbb{F}_۲}(۱, ۰, ۱)$ یک کد خودـدوگان است و اگر $h \overset{۴}{\equiv} ۳$ و $n \overset{۴}{\equiv} ۰$ یا $h \overset{۴}{\equiv} ۱$ و $n \overset{۴}{\equiv} ۲$، آنگاه کد نوع II است.

۴.۴.۲ گراف‌های خطی از دستگاه‌های استینر

یک دستگاه سه‌تایی استینر[11] روی N نقاطی هستند که یک طراحی $(N, M, ۱) - ۲$ باشند. رئوس SRG بلوک‌ها هستند. دو بلوک را مجاور گوییم اگر آن‌ها حداقل در یک نقطه اشتراک داشته باشند. برای مثال از $M = ۳$ می‌توان یک SRG با پارامترهای $(N(N-۱)/۶, ۳(N-۳)/۲, (N+۳)/۲, ۹)$ به دست آورد. اگر $n \overset{۸}{\equiv} ۷$، آنگاه $P_{\mathbb{F}_۲}(۱, ۰, ۱)$ خودـدوگان است.

۵.۴.۲ پایگاه داده مگما

پارامترهای SRG ۴۳۴۴۲ را می‌توان در پایگاه داده مگما یافت که توسط برندان مک‌کی[12] [۳۱] پردازش شده‌اند.

پارامترهای $[(۳۶, ۱۵, ۶, ۶)]$.

با استفاده از ساختار محض $(۱, ۰, ۱)$، حداقل چهار $[۷۲, ۳۶, ۱۲]$ کد نوع I به دست می‌آوریم. طبق داده‌های صفحه شخصی گابوریت[13] [۱۶]، فقط دو گونه از این کدها تاکنون شناخته شده است. نتایج غیر هم ارزی از کدکلمه‌های با وزن ۱۲ به ترتیب عبارتند از $\{۴۹۰, ۵۲۶, ۶۳۴, ۶۸۲\}$.

با استفاده از ساختار محض $(۰, ۱, ۰)$، حداقل ۲۹ عدد $[۷۲, ۳۶, ۱۲]$ کد نوع II به دست می‌آوریم

[11] Steiner
[12] Brendan McKay
[13] Gaborit

که متمایز با ۳۲ کد ساخته شده در [۱۲] هستند. با استفاده از نماد گذاری [۱۲]، αهای

$$\{-۳۶۰۰, -۳۵۷۶, -۳۵۵۲, -۳۵۴۶, -۳۵۴۰, -۳۵۳۴, -۳۵۲۸, -۳۵۲۲,$$

$$-۳۵۱۰, -۳۵۰۴, -۳۴۹۸, -۳۴۹۲, -۳۴۸۰, -۳۴۶۸, -۳۴۶۲, -۳۴۵۶,$$

$$-۳۴۴۴, -۳۴۳۲, -۳۴۲۰, -۳۴۰۸, -۳۳۹۶, -۳۳۸۴, -۳۳۷۲,$$

$$-۳۳۴۸, -۳۳۳۶, -۳۳۰۰, -۳۲۲۸, -۳۲۰۴, -۲۳۱۶\}$$

نتایج غیر هم ارزی از کدکلمه‌های متمایز با وزن ۱۲ هستند. توجه داریم که این کدها متفاوت از از کدهای بیان شده در [۱۰] هستند، زیرا مرتبه گروه‌های خودریختی آن‌ها عضو مجموعه

$$\{۲, ۴, ۶, ۸, ۱۲, ۲۰, ۴۸, ۶۰, ۳۸۸۸\}$$

است و هیچ‌کدام از اعضای این مجموعه مضرب ۲۳ نیستند. همچنین توجه داریم که اخیراً بویوکلیو[۱۴] و سایرین در [۵]، مقادیر زیادی را از α ساختند که شامل بسیاری از موارد فوق می‌باشد. اما مقادیری α که در مجموعه $\{-۲۳۱۶, -۳۴۰۸, -۳۵۲۸, -۳۵۷۶, ۳۶۰۰\}$ می‌باشند شامل لیست داده شده در [۵] نیستند.

پارامترهای $[(۴۰, ۱۲, ۲, ۴)]$.

با استفاده از ساختار محض $(۱, ۰, ۰)$، ۹ عدد، $[۱۲, ۴۰, ۸۰]$ کد نوع II به دست می‌آوریم.

۶.۴.۲ رتبه سه گروه

از نظر تاریخی، مفهوم SRGها توسط عمل گروه‌های ساده متناوب روی گراف‌های معینی تعریف شد [۲۰]. با استفاده از جدول 10A1 در [۲۰]، برخی از کدهای خود-دوگان که تحت گروه‌های متناوب ثابت هستند (از ساختار محض) را می‌سازیم. پس بلافاصله نتیجه می‌گیریم که اگر ماتریس جایگشتی π روی A با ضابطه $\pi^T A\pi = A$ عمل کند، آنگاه π روی $\mathcal{P} = \mathcal{P}_{\mathbb{F}_۲}(r, s, t)$ با ضابطه $\pi^T\mathcal{P}(I_۲ \otimes \pi) = \mathcal{P}$ عمل می‌کند.

این ساختارها در جدول ۷.۲ خلاصه شده‌اند.

[14] Bouyukliev

نوع	(r,s,t)	μ	λ	κ	v	گروه
II	$(۰,۰,۱)$	۱۲	۱۴	۳۶	۱۰۰	HJ
I	$(۱,۱,۰)$	۱۲	۱۴	۳۶	۱۰۰	HJ
I	$(۰,۰,۱)$	۶	۰	۲۲	۱۰۰	HS
II	$(۱,۱,۰)$	۶	۰	۲۲	۱۰۰	HS
I	$(۰,۰,۱)$	۹۶	۱۰۰	۴۱۶	۱۷۸۲	Suz
I	$(۱,۱,۰)$	۹۶	۱۰۰	۴۱۶	۱۷۸۲	Suz
II	$(۰,۱,۰)$	۳۲۴	۳۷۸	۸۹۱	۲۳۰۰	Co2
I	$(۱,۰,۱)$	۳۲۴	۳۷۸	۸۹۱	۲۳۰۰	Co2
II	$(۰,۰,۱)$	۱۲۰۸	۱۳۲۸	۲۳۰۴	۴۰۶۰	Ru
I	$(۱,۱,۰)$	۱۲۰۸	۱۳۲۸	۲۳۰۴	۴۰۶۰	Ru
I	$(۰,۱,۰)$	۱۲۶	۱۸۰	۶۹۳	۳۵۱۰	Fi22
I	$(۱,۰,۱)$	۱۲۶	۱۸۰	۶۹۳	۳۵۱۰	Fi22
I	$(۱,۰,۱)$	۳۵۱	۶۹۳	۳۵۱۰	۳۱۶۷۱	Fi23
II	$(۰,۱,۰)$	۳۲۴۰	۳۵۱۰	۳۱۶۷۱	۳۰۶۹۳۶	Fi24
I	$(۱,۰,۱)$	۳۲۴۰	۳۵۱۰	۳۱۶۷۱	۳۰۶۹۳۶	Fi24
II	$(۰,۰,۱)$	۸۶۸۰	۸۴۰۸	۱۰۹۲۰	۱۴۰۸۰	Fi23
I	$(۱,۱,۰)$	۸۶۸۰	۸۴۰۸	۱۰۹۲۰	۱۴۰۸۰	Fi23
II	$(۰,۱,۰)$	۸۶۸۰۰	۸۶۶۰۰	۱۰۹۲۰۰	۱۳۷۶۳۲	Fi23
I	$(۱,۰,۱)$	۸۶۸۰۰	۸۶۶۰۰	۱۰۹۲۰۰	۱۳۷۶۳۲	Fi23

جدول ۷.۲: رتبه سه گروه: کدهای دوتایی

۵.۲ کدهای DRTها

در این بخش کدهای ساخته شده توسط DRTها را بررسی می‌کنیم. ابتدا با گزاره زیر شروع می‌کنیم.

گزاره ۱.۵.۲ ([۲۹]). *فرض کنیم $(X,R_۱)$ یک DRT با پارامترهای (v,κ,λ,μ) باشد. در حالت ساختار محض داریم $v \overset{۸}{\equiv} ۳$ اگر و تنها اگر $P_{\mathbb{F}_۲}(۰,۱,۰)$ و $P_{\mathbb{F}_۲}(۰,۰,۱)$ خودـ دوگان زوجـ منفرد باشند. به علاوه در حالت یک ساختار محدود شده، فرض کنیم $\alpha = ۰$ و $\beta = \gamma = ۱$. در این صورت $v \overset{۸}{\equiv} ۳$ اگر و تنها اگر $B_{\mathbb{F}_۲}(۱,۱,۰)$ و $B_{\mathbb{F}_۲}(۱,۰,۱)$ کدهای خودـ دوگان زوجـ دوگانه باشند.*

برهان. طبق لم ۲.۲.۲ داریم $AA^T = \kappa I + \lambda A + \lambda\overline{A}$ و $v \overset{۸}{\equiv} ۳$ اگر و تنها اگر $\lambda \overset{۲}{\equiv} ۰$. ابتدا ساختار محض را در نظر می‌گیریم. فرض کنیم $v \overset{۸}{\equiv} ۳$. در این صورت

$$Q_{\mathbb{F}_۲}(۰,۱,۰)Q_{\mathbb{F}_۲}(۰,۱,۰)^T = AA^T = \kappa I + \lambda A + \lambda\overline{A} \overset{۲}{\equiv} I.$$

بنابراین $P_{\mathbb{F}_۲}(۰,۱,۰)$ خودـ دوگان است و چون هر سطر از $\mathcal{P}_{\mathbb{F}_۲}(۰,۱,۰)$ دارای وزن $۲ \overset{۴}{\equiv} ۱+\kappa$ است،

$P_{\mathbb{F}_۲}(۰,۱,۰)$ زوج‌ـ منفرد است. به طور مشابه می‌توان نشان داد $P_{\mathbb{F}_۲}(۰,۰,۱)$ نیز خودـ دوگان زوج‌ـ منفرد است. برعکس، اگر $P_{\mathbb{F}_۲}(۰,۱,۰)$ خودـ دوگان باشد، آنگاه حاصل ضرب داخلی هر دو سطر متمایز از $Q_{\mathbb{F}_۲}(۰,۱,۰)$ برابر λ است که لزوماً باید زوج باشد، زیرا $P_{\mathbb{F}_۲}(۰,۱,۰)$ خودـ دوگان است. بنابراین $v \overset{۸}{\equiv} ۳$.

اکنون ساختار محدود شده را در نظر می‌گیریم. فقط $B_{\mathbb{F}_۲}(۱,۱,۰)$ را در نظر می‌گیریم، چون $B_{\mathbb{F}_۲}(۱,۰,۱)$ به طور مشابه اثبات می‌شود. داریم

$$\begin{aligned} Q_{\mathbb{F}_۲}(۱,۱,۰)Q_{\mathbb{F}_۲}(۱,۱,۰)^T &= (I+A)\left(I+A^T\right) = I + A + A^T + AA^T \\ &= J + AA^T = J + \kappa I + \lambda A + \lambda\overline{A} \\ &\overset{۲}{\equiv} I + J \end{aligned}$$

به عنوان $\lambda \overset{۲}{\equiv} ۰$.

به علاوه، سطر بالای $\mathcal{B}_{\mathbb{F}_۲}(۱,۱,۰)$ با سایر سطرهای باقی‌مانده $\mathcal{B}_{\mathbb{F}_۲}(۱,۱,۰)$ متعامد است. بنابراین $B_{\mathbb{F}_۲}(۱,۱,۰)$ خودـ دوگان است. توجه داریم با استفاده از شرط زوج بودن λ، وزن همه سطرهای $\mathcal{B}_{\mathbb{F}_۲}(۱,۱,۰)$ مضربی از ۴ است. بنابراین $B_{\mathbb{F}_۲}(۱,۱,۰)$ یک کد خودـ دوگان زوج‌ـ دوگانه است.

برعکس، فرض کنیم $B_{\mathbb{F}_۲}(۱,۱,۰)$ یک کد خودـ دوگان زوج‌ـ دوگانه باشد. در این صورت طبق محاسبه بالا داریم $Q_{\mathbb{F}_۲}(۱,۱,۰)Q_{\mathbb{F}_۲}(۱,۱,۰)^T = J + \kappa I + \lambda A + \lambda\overline{A}$. بنابراین حاصل ضرب داخلی هر دو سطر متمایز از $Q_{\mathbb{F}_۲}(۱,۱,۰)$ برابر با $\lambda + ۱$ است که باید فرد باشد، چون $B_{\mathbb{F}_۲}(۱,۱,۰)$ خودـ دوگان است. لذا λ .زوج است. در نتیجه $v \overset{۸}{\equiv} ۳$. □

۱.۵.۲ DRTهای از مرتبه ۳

می‌دانیم که یک DRT یکتا از مرتبه ۳ وجود دارد به طوری که متعلق به یک نوع پالی است.

- برای حالت دوتایی چون $n \overset{۸}{\equiv} ۳$، نتیجه می‌گیریم $P_{\mathbb{F}_۲}(۰,۱,۰)$ و $P_{\mathbb{F}_۲}(۰,۰,۱)$ هر دو $[۶,۳,۲]$ کدهایی خودـ دوگان هستند. هم‌چنین جالب است به این نکته نیز توجه کنیم که $B_{\mathbb{F}_۲}(۱,۱,۰)$ و $B_{\mathbb{F}_۲}(۱,۰,۱)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$، با کد همینگ یکتای توسعه یافته از طول ۸ هم ارز هستند.

- برای حالت سه‌تایی، چون $\lambda = ۰$، $\kappa = ۱$ و $\mu = ۱$، طبق جدول ۵.۲ و جدول ۶.۲ هیچ کد سه‌تایی از ساختار محض/محدود شده وجود ندارد.

- برای یک میدان از مرتبه ۴، $P_{\mathbb{F}_۴}(۱, \omega, \omega)$ همان هگزا کد $h_۶$[۳۴] است که $[۶, ۳, ۴]$ کد خود‌ـ دوگان هرمیتین یکتا روی $\mathbb{F}_۴$ است کد $B_{\mathbb{F}_۴}(۱, ۱, ۰)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$ همان $[۸, ۴, ۴]$ کد خود‌ـ دوگان یکتای هرمیتین روی $\mathbb{F}_۴$ است که ماتریس مولد آن از $[۸, ۴, ۴]$ کد همینگ دوتایی به دست می‌آید.

- برای حلقه $\mathbb{Z}_۴$، کد $B_{\mathbb{Z}_۴}(۲, ۱, ۳)$ با $\alpha = ۲$، $\beta = ۱$ و $\gamma = ۳$ طبق [۳۲، صفحه ۱۹۳]، همان اوکتاکد $o_۸$ است که این $\mathbb{Z}_۴$‌ـ کد نوع II یکتای از طول ۸ می‌باشد. به طور دقیق‌تر، دقیقاً ۲۴ کد از ساختار محدود شده وجود دارد به طوری که همه آن‌ها هم ارز با $o_۸$ هستند. کد $B_{\mathbb{Z}_۴}(۰, ۱, ۳)$ با $\alpha = ۰$، $\beta = ۱$ و $\gamma = ۳$ یک انتقال از کد همینگ توسعه یافته دوتایی از مرتبه ۸ است که با $\mathcal{E}_۸$ نمایش داده می‌شود ([۳۲، صفحه ۱۹۳] را ببینید). چون $o_۸$ و $\mathcal{E}_۸$ تنها کدهای با مینیمم وزن ۴ برای این طول هستند، ساختار محدود شده ما روی $\mathbb{Z}_۴$ با استفاده از DRT مرتبه ۳، هر دو کد را پیدا می‌کند.

۲.۵.۲ DRTهای از مرتبه ۷

طبق No.2 از [۲۲]، یک DRT یکتا از مرتبه ۷ وجود دارد.

- برای حالت دوتایی ساختار محض، $P_{\mathbb{F}_۲}(۱, ۰, ۰)$ یک $[۱۴, ۷, ۲]$ کد نوع I است. کد $B_{\mathbb{F}_۲}(۰, ۱, ۱)$ با $\alpha = ۰$ و $\gamma = \beta = ۱$ یک $[۱۶, ۸, ۴]$ کد نوع II است.

- برای حالت سه‌تایی، ۳۲ عدد $[۱۶, ۸, ۶]$ کد خود‌ـ دوگان اکسترمال روی $\mathbb{F}_۳$ از ساختار محدود شده با مقادیر مختلف α، β، γ، r، s و t وجود دارد. اما فقط یکی از این کدها را در حد هم ارزی به دست می‌آوریم. برای مثال $B_{\mathbb{F}_۳}(۱, ۱, ۰)$ با $\alpha = \beta = ۱$ و $\gamma = ۲$ با کد خود‌ـ دوگان سه‌تایی اکسترمال $f_۸^{۲+}$ (در نمادگذاری [۳۲]) هم ارز است.

- برای یک میدان از مرتبه ۴ داریم که $P_{\mathbb{F}_4}(1,\omega,\omega)$ یک $[14,7,4]$ کد نوع IV است و سایر ساختارهای محض، کدهای خود-دوگان روی $\mathbb{F}_4$ با $d=2$ یا $d=4$ را نتیجه می‌دهند. به طور مشابه، $B_{\mathbb{F}_4}(0,1,1)$ یا $\alpha=0$، $\beta=1$ و $\gamma=\omega^2$ یک $[16,8,4]$ کد نوع IV است.

- روی $\mathbb{Z}_4$ دو کد خود-دوگان غیر هم ارز از طول ۱۶ و بیشترین وزن همینگ ۴ می‌یابیم. اولین کد $B_{\mathbb{Z}_4}(0,1,3)$ با $\alpha=0$ و $\beta=\gamma=1$ است. این کد ۶۷۸ کدکلمه دارد با وزن همینگ ۸ دارد. این کد دارای بیشترین وزن لی ۶ و بیشترین وزن اقلیدسی ۸ است. همچنین این کد یک کد نوع II روی $\mathbb{Z}_4$ است (یعنی تمام وزن‌های اقلیدسی بر ۸ بخش‌پذیر هستند). کد دیگر $B_{\mathbb{Z}_4}(2,1,1)$ با $\alpha=2$، $\beta=1$ و $\gamma=2$ است. این کد نیز دارای حداکثر وزن لی ۶ و حداکثر وزن اقلیدسی ۸ است اما نوع II نیست. این کد ۴۲۲ کدکلمه از وزن همینگ ۸ دارد. برای وضعیت کنونی دسته‌بندی $\mathbb{Z}_4$-کدها، جدول ۹ از [۲۳] را ببینید.

۳.۵.۲ DRTهای از مرتبه ۱۱

می‌دانیم که یک DRT یکتا از مرتبه ۱۱ وجود دارد به طوری که متعلق به یک نوع پالی است.

- در حالت دوتایی از گزاره ۱.۵.۲ نتیجه می‌گیریم $P_{\mathbb{F}_2}(0,1,0)$ و $B_{\mathbb{F}_2}(1,1,0)$ با $\alpha=0$ و $\gamma=\beta=1$ به ترتیب کدهایی خود-دوگان با طول ۲۲ و ۲۴ هستند. همچنین کمترین فاصله آن‌ها به ترتیب عبارت است از ۶ و ۸. بنابراین $B_{\mathbb{F}_2}(1,1,0)$ با کد توسعه یافته گولای[15] از طول ۲۴ هم ارز است.

- برای حالت سه‌تایی، کد $B_{\mathbb{F}_3}(0,1,2)$ با $\alpha=0$، $\beta=1$ و $\gamma=2$ همان کد متقارن پلس[16] $S(24)$ است.

- برای یک میدان از مرتبه ۴ داریم که $P_{\mathbb{F}_4}(1,1,\omega)$ یک $[22,11,8]$ کد اکسترمال نوع IV روی $\mathbb{F}_4$ است که مرتبه گروه خودریختی آن $2^7\cdot 3^3\cdot 5\cdot 7\cdot 11$ می‌باشد. کد $B_{\mathbb{F}_4}(\omega,\omega,0)$ با $\alpha=0$ و

[15] Golay
[16] Pless Symmetry

$\beta = \gamma = ۱$ یک $[۲۴, ۱۲, ۸]$ کد نوع IV روی $\mathbb{F}_۴$ است که مرتبه گروه خودریختی‌های آن عبارت است از $۲^{۱۰} \cdot ۳^۴ \cdot ۵ \cdot ۷ \cdot ۱۱ \cdot ۲۳$.

- برای حلقه $\mathbb{Z}_۴$، هیچ $\mathbb{Z}_۴$ـکدی از ساختار محض وجود ندارد. از طرف دیگر، دقیقاً ۴۸ $\mathbb{Z}_۴$ـکد از ساختار محدود شده وجود دارد. برای مثال، $B_{\mathbb{Z}_۴}(۰, ۱, ۳)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$، دارای کمترین وزن همینگ ۴ و کمترین وزن لی ۸ است. در حالی که $B_{\mathbb{Z}_۴}(۱, ۱, ۲)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$، دارای کمترین وزن همینگ ۸ و کمترین وزن لی ۸ است. این دو کد، $\mathbb{Z}_۴$ـکد نیستند. کد $B_{\mathbb{Z}_۴}(۱, ۱, ۰)$ با $\alpha = ۲$ و $\beta = \gamma = ۱$ یک $\mathbb{Z}_۴$ـکد نوع II با کمترین وزن همینگ ۸، کمترین وزن لی ۸ و کمترین وزن اقلیدسی ۸ است. محاسبات انجام شده نشان می‌دهد $۲۴ \cdot ۲۲ = ۵۲۸$ کد کلمه از کمترین وزن اقلیدسی ۸ وجود دارد. بنابراین مشبکه تک‌مدولی زوج ۲۴ بعدی متناظر آن به وسیله ساختار A، همان مشبکه نیمیر[۱۷] با دستگاه ریشه‌ای $D_{۱۲}^۲$ است (جدول ۱۶.۱ از کانوی[۱۸] و اسلاون[۱۹] را ببینید).

کدهای جالب دیگر از $B_{\mathbb{Z}_۴}(r, s, t)$ با

$$(\alpha, \beta, \gamma, r, s, t) = (۲, ۱, ۱, ۲, ۱, ۳), (۲, ۱, ۱, ۲, ۳, ۱), (۲, ۱, ۳, ۲, ۱, ۳), (۲, ۱, ۳, ۲, ۳, ۱),$$
$$(۲, ۳, ۱, ۲, ۱, ۳), (۲, ۳, ۱, ۲, ۳, ۱), (۲, ۳, ۳, ۲, ۱, ۳), (۲, ۳, ۳, ۲, ۳, ۱)$$

به دست می‌آید. با بررسی بیشتر، درمی‌یابیم که این کدها هم ارز هستند. به علاوه آن‌ها $\mathbb{Z}_۴$ـکدهایی با کمترین وزن همینگ ۴ و کمترین وزن لی ۸ هستند. بررسی‌های انجام شده نشان می‌دهد که ۶۶ کدکلمه از وزن همینگ ۴ و ۶۶ کدکلمه از وزن لی ۸ وجود دارد. این نشان می‌دهد که هیچ کدکلمه‌ای از وزن اقلیدسی ۸ وجود ندارد. بنابراین این کدها دارای کمترین وزن اقلیدسی ۱۶ هستند. متذکر می‌شویم که سه مورد از کدهای بالا کدهایی هستند که توسط چاپمن[۲۰] در [۷]، همان‌طور که در بخش ۴.۳.۲ هم بیان شد، تعریف شده‌اند.

[17] Niemeier
[18] Conway
[19] Sloane
[20] Chapman

۴.۵.۲ DRTهای از مرتبه ۱۵

فقط یک DRT از مرتبه ۱۵ وجود دارد [۲۱].

- برای حالت دوتایی، کد $B_{\mathbb{F}_2}(0,1,1)$ با $\alpha=0$ و $\beta=\gamma=1$ یک $[32,16,4]$ کد نوع II است.
- برای حالت سه‌تایی هیچ کد خود-دوگانی روی $GF(3)$ نه از ساختار محض و نه از ساختار محدود شده وجود ندارد.
- برای میدان از مرتبه ۴، کد $P_{\mathbb{F}_4}(1,\omega,\omega)$ یک $[30,15,4]$ کد نوع IV است و $P_{\mathbb{F}_4}(0,\omega,\omega)$ با $\alpha=0$ و $\beta=\gamma=1$ یک $[32,16,4]$ کد نوع IV است.

۵.۵.۲ DRTهای از مرتبه ۱۹

فقط یک DRT از مرتبه ۱۹ وجود دارد [۲۱].

- برای حالت دوتایی، از No.2 [۲۱]، نتیجه می‌گیریم $P_{\mathbb{F}_2}(0,1,0)$ یک $[38,19,6]$ کد نوع I است. به طور مشابه، با استفاده از No.3 [۲۱]، یک $[38,19,8]$ کد نوع I از $P_{\mathbb{F}_2}(0,1,0)$ به دست می‌آوریم. کد $B_{\mathbb{F}_2}(1,1,0)$ با $\alpha=0$ و $\beta=\gamma=1$، به ترتیب از هر DRT، دو $[40,20,8]$ کد نوع II اکسترمال غیر هم ارز هستند.
- برای حالت سه‌تایی، کد $B_{\mathbb{F}_2}(1,1,0)$ با $\alpha=1$، $\beta=2$ و $\gamma=1$ به ترتیب از هر DRT، دو $[40,20,8]$ کد نوع III اکسترمال غیر هم ارز نتیجه می‌دهد.
- برای یک میدان از مرتبه ۴، $[38,19,8]$ کدهای نوع IV و $[40,20,8]$ کدهای نوع IV از ساختارهای محض و محدود شده به دست می‌آوریم.

۶.۵.۲ DRTهای از مرتبه ۲۳

۱۹ DRT از مرتبه ۲۳ وجود دارد [۲۱].

- برای حالت دوتایی، $[۴۸, ۲۴, ۴]$ کدهای نوع II را از $B_{\mathbb{F}_۲}(۰, ۱, ۱)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$ به دست می‌آوریم.

- برای حالت سه‌تایی، هیچ کد خود-دوگانی روی $GF(۳)$ از ساختار محض وجود ندارد. همچنین فقط با استفاده از No.20 از [۲۱] می‌توان نشان داد دقیقاً ۸ عدد $[۴۸, ۲۴, ۱۵]$ کد نوع III اکسترمال از حالت محدود شده وجود دارد. کد $B_{\mathbb{F}_۳}(۰, ۱, ۲)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$ مثالی از این حالت می‌باشد. این کدها هم ارز با کد متقارن پلس $S(۴۸)$ هستند که در واقع همان $B_{\mathbb{F}_۳}(۰, ۱, ۲)$ با $\alpha = ۰$، $\beta = ۱$ و $\gamma = ۲$ است. ساختارهای محدود شده از DRTهای دیگر $[۴۸, ۲۴]$ کدهای روی $GF(۳)$ با کمترین فاصله حداکثر ۱۲ هستند.

۷.۵.۲ DRTهای از مرتبه ۲۷

۳۷۴ DRT از مرتبه ۲۷ وجود دارد [۲۱].

- برای حالت دوتایی، فقط No.378 از وب‌سایت [۲۱]، یک $[۵۴, ۲۷, ۱۰]$ کد نوع I اکسترمال از $P_{\mathbb{F}_۲}(۰, ۱, ۰)$ و یک $[۵۶, ۲۸, ۱۲]$ کد نوع II اکسترمال از $B_{\mathbb{F}_۲}(۱, ۱, ۰)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$ تولید می‌کند. بقیه DRTها کدهای نوع I با $d = ۶$ یا $d = ۸$ از ساختار محض و کدهای نوع II با $d = ۸$ از ساختار محدود شده با $\alpha = ۰$ و $\beta = \gamma = ۱$ ارائه می‌دهند.

۸.۵.۲ DRTهای از مرتبه ۳۱

حداقل ۶ ماتریس هادامارد اریب از مرتبه ۳۲ وجود دارد [۳۱]. بنابراین DRTهای از مرتبه ۳۱ وجود دارند [۲۴]. ما فقط ماتریس نوع پالی را در پایین در نظر می‌گیریم.

- برای حالت سه‌تایی، می‌توان دید که هیچ کد خود-دوگانی روی $GF(۳)$ از ساختار محض وجود ندارد. کد $B_{\mathbb{F}_۳}(۲, ۰, ۲)$ با $\alpha = \beta = \gamma = ۱$ یک $[۶۴, ۳۲, ۱۸]$ کد نوع III روی $\mathbb{F}_۳$ ارائه می‌دهد. هم‌چنین توجه داریم که $B_{\mathbb{F}_۳}(۱, ۲, ۳)$ با $\alpha = ۰$، $\beta = ۱$ و $\gamma = ۲$ یک کد بینکر[۲۱] است

[21] Beenker's code

[۳] که تنها کد شناخته شده برای این طول می‌باشد [۲۳]. بنابراین آشکار است که همه کدهای نوع III اکسترمال از ساختار محدود شده با استفاده از ماتریس نوع پالی مرتبه ۳۲، هم ارز هستند.

۹.۵.۲ DRTهای از مرتبه ۳۵

این نکته شناخته شده است که حداقل ۱۸ ماتریس هادامارد اریب از مرتبه ۳۶ وجود دارد [۳۰]. بنابراین DRTهای از مرتبه ۳۵ وجود دارند [۳۳].

- برای حالت دوتایی، دو $[۷۰, ۳۵, ۱۰]$ کد نوع I غیر هم ارز از $P_{\mathbb{F}_۲}(۰, ۱, ۰)$ به دست می‌آوریم و یک $[۷۲, ۳۶, ۱۲]$ کد نوع II از $B_{\mathbb{F}_۲}(۱, ۱, ۰)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$ با استفاده از ماتریس پانزدهم و شانزدهم هادامارد در [۳۰]، پس از نرمال‌سازی آن‌ها طبق [۳۳]، به دست می‌آوریم.
- برای حالت سه‌تایی، با استفاده از این ماتریس‌ها $[۷۲, ۳۶, ۱۵]$ کدهای خود-دوگان را از $B_{\mathbb{F}_۳}(۰, ۱, ۲)$ با $\alpha = ۰$، $\beta = ۱$ و $\gamma = ۲$ به دست می‌آوریم. همچنین کمترین فاصله آن‌ها ۳ است که کمتر از کد باقی‌مانده درجه دوم سه‌تایی می‌باشد که در واقع یک $[۷۲, ۳۶, ۱۸]$ کد نوع III اکسترمال است. این نکته یک انگیزه مضاعف برای مطالعه ساختار ماتریس‌های هادامارد کج از رتبه ۳۶ ارائه می‌دهد.

۱۰.۵.۲ DRTهای از مرتبه ۵۱

طبق [۳۰] می‌دانیم حداقل ۵۶۱ ماتریس هادامارد کج از مرتبه ۵۲ وجود دارد. بنابراین DRTهای از مرتبه ۵۱ وجود دارند.

- برای حالت دوتایی، با استفاده از این ماتریس‌ها، بسیاری از $P_{\mathbb{R}_۲}(۰, ۱, ۰)$، $[۱۰۲, ۵۱, ۱۲]$ کدهای نوع I را ارائه می‌دهند و بسیاری از $B_{\mathbb{F}_۲}(۱, ۱, ۰)$ با $\alpha = ۰$ و $\beta = \gamma = ۱$، $[۱۰۴, ۵۲, ۱۲]$ کدهای نوع II را ارائه می‌دهند. همچنین می‌دانیم که یک $[۱۰۴, ۵۲, ۲۰]$ کد QR نوع II اکسترمال وجود دارد.

۶.۲ کدهای چرخشی دوگانه درجه دوم

کدهای چرخشی دوگانه درجه دوم[۲۲] (QDC) به صورت زیر تعریف می‌شوند.

فرض کنیم q توانی از یک عدد اول فرد باشد. فرض کنیم χ نشان دهنده تابع نشانگر باقی‌مانده‌های درجه دوم $\mathbb{F}_q$ باشد. فرض کنیم Q و N نشان دهنده ماتریس‌های q در q با درایه‌های روی قطر اصلی صفر باشند و برای هر $j \neq i$، $Q_{i,j} = \frac{۱+\chi(j-i)}{۲}$ و $N_{i,j} = \frac{۱-\chi(j-i)}{۲}$. برای اسکالرهای r، s و t از R، ماتریس $Q_q(r,s,t) := rI + sQ + tN$ را تعریف می‌کنیم.

ماتریس Q در این ساختار همان ماتریس A در ساختار خودمان است و ماتریس N همان $\overline{A}$ است.

اگر $q = ۴\ell + ۱$، آنگاه A ماتریس مجاورت یک SRG به پارامترهای زیر است:

$$v = q, \kappa = ۲\ell, \lambda = \ell - ۱, \mu = \ell.$$

اگر $q = ۴\ell + ۳$، آنگاه A ماتریس مجاورت یک DRT با پارامترهای زیر است:

$$v = q, \kappa = ۲\ell + ۱, \lambda = \ell, \mu = \ell + ۱.$$

در این صورت ساختارهای محض و محدود شده داده شده در [۱۵]، متناظر با ساختارهای محض و محدود شده ما هستند. گابوریت $P_{\mathbb{F}_۲}(۰, ۱, ۰)$ زمانی که $q = ۸\ell + ۳$، $P_{\mathbb{F}_۴}\left(۱, \omega, \omega^۲\right)$ زمانی که $q = ۸\ell + ۱$، $P_{\mathbb{F}_۴}\left(۰, \omega, \omega^۲\right)$ زمانی که $q = ۸\ell + ۱$، $B_{\mathbb{F}_۴}\left(۰, \omega, \omega^۲\right), \alpha = ۰, \beta = ۱$ زمانی که $q = ۸\ell - ۱$ و $B_{\mathbb{F}_۴}\left(۱, \omega, \omega^۲\right), \alpha = ۰, \beta = ۱$ زمانی که $q = ۸\ell - ۱$ را همانند بسیاری از کدهای خود-دوگان روی $\mathbb{F}_۹\mathbb{F}_۵$ و $\mathbb{F}_۷$ ساخت.

[22] Quadratic Double Circulant

مراجع

[1] E. F. Assmus, J. D. Key, Designs and their Codes, Cambridge tracts in mathematics 103, Cambridge University Press, Cambridge (1992).

[2] J. Bang-Jensen, G. Z. Gutin, Digraphs: Theory, Algorithms and Applications, 2nd edition, Springer, London (2009).

[3] G. F. Beenker, A note on extended quadratic residue codes over $GF(9)$ and their ternary images, IEEE-IT, 30 (1984), 403–405.

[4] L. W. Beineke, R. J. Wilson, Selected Topics in Graph Theory, Academic Press, New York (1978).

[5] I. Bouyukliev, V. Fack and J. Winne, Hadamard matrices of order 36 and double-even self- dual $[72, 36, 12]$ codes. DMTCS proc, AE (2005), 93–98.

[6] A. E. Brouwer, A. M. Cohen and A. Neumaier, "Distance-regular graphs," Springer, New York (1985), EMG 18.

[7] R. J. Chapman, Double circulant constructions of the Leech lattice, J. Austral. Math. Soc. Ser. A, 69 (2000), 287–297.

[8] A. R. Calderbank, N. J, A. Sloane, Double circulant codes over Z4 and even unimodular lattices, J. of Algebraic Combinatorics, 6 (1997), 119–131.

[9] J. H. Conway, N. J, A. Sloane, Self-dual codes over the integers modulo 4, J. Combinatorial Th. A, 62 (1993), 30–45.

[10] R. Dontcheva, New binary self dual $[70, 35, 12]$ and binary $[72, 36, 12]$ self dual doubly even codes, Serdica Math. J., 27 (2001), 287–302.

[11] S. T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok, P. Sole, The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices, Int. J. Inf. Coding Theory 4 (2017), 116–128.

[12] S. T. Dougherty, T. A. Gulliver and M. Harada, Extremal Binary Self-dual codes, IEEE Trans. Inform. Theory, 43 (1997), 2036–2046.

[13] S. T. Dougherty, J.-L. Kim, P. Sole, Double Circulant Codes from Two Class Association Schemes, Adv. Math. Commun. 1 (2007), 45–64. " ii, iii, 3, 17, 28, 29, 32, 33, 49, 55.

[14] L. Euler, Solutio problematis ad geometriam situs pertinentis, Commentarii Academiae Scientiarum Imperialis Petropolitanae 8 (1741), 128–140.

[15] P. Gaborit, Quadratic double circulant codes over fields, Journal of Combinatorial Theory Series A, 97 (2002), 85–107.

[16] P. Gaborit, http://www.unilim.fr/pagesperso/philippe.gaborit/SD/

[17] C. D. Godsil, "Algebraic Combinatorics," Chapman and Hall, 1993.

[18] C. D. Godsil, G. Royle, "Algebraic Graph Theory," Springer, New York, 2001.

[19] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, http://www.codetables.de. Accessed: 2nd July 2020.

[20] R. L. Griess, jr "Twelve Sporadic Simple Groups," Springer SMM (1998).

[21] A. Hanaki, I. Miyamoto, http://kissme.shinshu-u.ac.jp/as/

[22] D. G. Higman, Coherent configuration, Geom. Dedicata, 4 (1975), 1–32.

[23] W. C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields and Their Applications, 11 (2005), 451–490.

[24] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge (2003).

[25] Y. J. Ionin, H. Kharaghani, Doubly regular digraphs and symmetric designs, J. Combinatorial Th. A, 101 (2003), 35-48.

[26] G. T. Kennedy, V. Pless, On designs and formally self-dual codes, Des. Codes Cryptogr. 4 (1994), 43-55.

[27] F. J. MacWilliams, N. J. A. Sloane, "The theory of error correcting codes," North Holland, 1981.

[28] J. L. Massey, Linear codes with complementary duals, Discrete Math. 106/107 (1992), 337–342.

[29] J. -L. Kim, Codes constructed from Non-Symmetric Association Schemes, preprint, 1997, www.math.louisville.edu/~jlkim/preprints.html

[30] C. Koukouvinos, http://www.math.ntua.gr/people/ckoukouv/hadamard.htm

[31] http://magma.maths.usyd.edu.au/magma/htmlhelp/text1394.htm#14180

[32] E. Rains, N. J. A. Sloane, Self-dual codes, in "Handbook of Coding Theory," V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam (1998), pp. 177-294.

[33] K. B. Reid, E. Brown, Doubly regular tournaments are equivalent to skew Hadamard matrices, J. Combinatorial Th. A, 1972, 332–338.

[34] C. E. Shannon, A Mathematical Theory of Communication, Bell System Tech. J. 27 (1948), 379–423, 623-656.

[35] S. A. Vanstone, P. C. van Oorschot, An Introduction to Error Correcting Codes with Applications, Springer, New York (1989).

واژه‌نامه فارسی به انگلیسی

واژه‌نامه انگلیسی به فارسی

فهرست اسامی

Abstract

This thesis is devoted to study the category of representations of a guiver.

Key Words. Auslander-Reiren theory, almost split sequences for complexes,...

University of Isfahan

Faculty of Science

Department of Mathematics

MsC. Thesis

Double Circulant Codes From Two Class Association Schemes

Supervisor:

Dr. Javad Bagherian

Advisor:

Dr. Reza Sobhani

By:

Saeed Ashari

September 2021