ب ه

به نام خداوند بخشاینده مهربان

دانشگاه زنجان
دانشکده علوم - گروه ریاضی

پایان نامه کارشناسی ارشد

عنوان:

کدهای دوتایی ناشی از گراف‌های روی سه‌تایی‌ها

نگارش:

ایزاک صدیق پور

استاد راهنما:

دکتر مژگان امامی

تیر ۱۳۸۸

تقدیم به دو گنجینه‌ی معرفت و محبت:

پدر و مادر عزیزم

تشکر و قدردانی

آغاز کلام را با نام پروردگار یکتا مزیّن می‌کنم و سر تعظیم در برابر درگاهش فرود می‌آورم.

تهیهٔ این مجموعه و به سرانجام رسیدن آن را بعد از لطف و عنایت خدای بزرگ، مرهون تلاش‌ها و زحمات فراوان استاد راهنمایم، دکتر امامی می‌دانم که دلسوزانه در تمامی مراحل مرا یاری نمودند و همواره با صبر و خوش‌رویی، مشوق و راهنمای من بودند. به همین لحاظ صمیمانه سپاسگزار ایشان هستم.

از پدر و مادرم که همیشه و در همه حال یاور و پشتیبان من بودند و خالصانه هر آنچه در توان داشتند در حق من انجام دادند، از صمیم قلب تشکر و قدردانی می‌نمایم.

از جناب آقای دکتر نجفیان و جناب آقای دکتر ذاکر که داوری پایان نامه را بر عهده داشتند و ضمن مطالعهٔ دقیق رساله، راهکارهای ارزنده‌ای در هر چه بهتر شدن آن ارائه نمودند بسیار سپاسگزارم.

زحمات و پیگیری‌های خانم‌ها مصطفوی و احمدی از واحد تحصیلات تکمیلی را هیچ‌گاه فراموش نخواهم کرد و برای این دو بزرگوار آرزوی سلامتی و سعادت دارم. همچنین از خانم موسوی و خانم کریمی از گروه ریاضی به واسطهٔ مساعدت‌هایشان ممنون و متشکرم.

جا دارد از تمامی دوستان خوبم هم که بسیار نسبت به من لطف داشتند و در انجام هر کمکی که از دستشان بر می‌آمد کوتاهی نمی‌کردند، تشکر نمایم. در این میان لازم می‌دانم خصوصاً از آقایان سیّد جمال اخلاقی، مرتضی فکری و سعید زراعتی نام ببرم.

در پایان برای همهٔ عزیزانی که از آنها یاد شد و برای همهٔ آن‌هایی که به نوعی در زندگی و تحصیل مرا یاری نموده‌اند، سلامتی و توفیق روزافزون از خداوند متعال خواستارم.

ایزاک صدیق پور

تیر ماه ۱۳۸۸

چکیــده

فرض کنیم Ω مجموعه‌ای با اندازهٔ $n \geq ۷$ و $\Omega^{\{۳\}}$ مجموعهٔ تمام زیر مجموعه‌های ۳ عضوی Ω باشد. سه گراف $A_۰(n)$، $A_۱(n)$ و $A_۲(n)$ با مجموعه رئوس $\Omega^{\{۳\}}$ در نظر می‌گیریم به طوری که دو رأس، به عنوان مجموعهٔ ۳ عضوی، زمانی در $A_i(n)$، $i = ۰, ۱, ۲$، با هم مجاورند که در i نقطه اشتراک داشته باشند. ما به بررسی کدهای دوتایی و سه‌تایی حاصل از ماتریس مجاورت هر یک از این سه گراف می‌پردازیم و پارامترهای اصلی آن‌ها را به دست می‌آوریم. همچنین نشان خواهیم داد که روش کدگشایی به وسیلهٔ جایگشت‌ها برای برخی از این کدها قابل استفاده است.

فهرست مندرجات

پیش گفتار

اهمیت نظریهٔ کدگذاری بر هیچ کس پوشیده نیست چرا که طیف وسیع کاربردهای آن در مخابرات، تبادل اطلاعات و ارتباطات، الکترونیک و صنایع مختلف، گویای جایگاه ویژه و ممتاز آن است. یکی از مهم‌ترین قسمت‌های این نظریه مربوط به یافتن کدهای جدید و بررسی ویژگی‌های آنها می‌باشد. در دهه‌های اخیر و در راستای همین امر، ارتباط بین کدها، گراف‌ها و طرح‌ها بسیار مورد توجه قرار گرفته است و مقالات و کتاب‌هایی در این زمینه تدوین شده است. به عنوان نمونه می‌توان کتاب اسموس [۱] و کی [۲] [۱] و کتاب کَمِرون [۳] و وَن لینت [۴] [۲] را برای مطالعه معرفی کرد.

در این میان ساختن کد (عموماً دو تایی) از روی ماتریس مجاورت گراف‌ها، خصوصاً گراف‌های قویاً منتظم، از مقوله‌هایی است که توسط افراد مختلفی بدان پرداخته شده است. در این ارتباط می‌توان از مقالهٔ هِمِرز[۵] و دیگران [۴] نام برد.

کی، موری[۶] و رُدریگِز[۷]، دسته‌هایی از گراف‌های منتظم را در نظر گرفتند و کدهای دوتایی ساخته شده از روی ماتریس مجاورت آنها را مورد مطالعه قرار دادند [۶]. این افراد سپس به بررسی کدهای سه تایی ناشی از این گراف‌ها پرداختند [۸] و پارامترهای اصلی این کدها و برخی دیگر از خواص آنها را به دست آوردند.

رسالهٔ حاضر نیز در همین راستا نگارش یافته و مبتنی بر پنج فصل است.

---

[۱] Assmus

[۲] Key

[۳] Cameron

[۴] van Lint

[۵] Haemers

[۶] Moori

[۷] Rodrigues

فصل اول به تعاریف مقدماتی و برخی از قضایایی که در فصل‌های بعدی مورد نیاز است، اختصاص دارد. در این فصل با مفاهیم کد، گراف و طرح آشنا می‌شویم.
در فصل دوم بعد از معرفی گراف‌های $A_0(n)$، $A_1(n)$ و $A_2(n)$، اقدام به ساختن کدهای دوتایی از روی ماتریس مجاورت این گراف‌ها نموده و سپس با استفاده از چندین لم و گزاره، پارامترهای اصلی این کدها و کدهای متعامد آنها را به دست می‌آوریم.
مطالب فصل سوم به بررسی کدهای سه تایی حاصل از گراف‌های روی ۳ تایی‌ها می‌پردازد.
درفصل چهارم، ما از ایدهٔ مشابهی استفاده کرده و کدهای دوتایی ناشی از گراف‌های روی ۴ تایی‌ها را مد نظر قرار می‌دهیم. در واقع بعد از تعریف چهار گراف $A_0(n)$، $A_1(n)$، $A_2(n)$ و $A_3(n)$، چهار دسته کد $C_0(n)$، $C_1(n)$، $C_2(n)$ و $C_3(n)$ را که متناظر با هر گراف ساخته می‌شوند، در نظر گرفته و سعی در پیدا کردن بعد آنها می‌کنیم.
سرانجام در فصل پنجم پس از آشنایی با مفهوم کدگشایی، روشی را جهت کدگشایی این کدها توسط جایگشت‌ها ارائه می‌نماییم.

فصل ۱

مقدمات و پیش نیازها

در این فصل به بیان تعاریف اولیه و قضیه‌های مورد نیاز از نظریهٔ کدگذاری، گراف و طرح‌های بلوکی پرداخته و به برخی از روابط بین آنها اشاراتی می‌کنیم.

۱–۱ کدهای خطی

این بخش به معرفی اجمالی نظریه کدگذاری می‌پردازد. در این نظریه ابتدا یک مجموعه مانند F شامل q نماد متفاوت اختیار می‌شود که الفبا نام دارد. در اکثر مواقع، $F = GF(q)$ انتخاب می‌شود که q توانی از یک عدد اول است. سپس مجموعه‌ای مانند C شامل دنباله‌های متناهی از عناصر F تشکیل می‌شود که هر دنباله یک کلمهٔ q تایی نامیده می‌شود. این کلمات را می‌توان به عنوان بردار تلقی نمود و چنانچه طول همگی آنها با هم برابر و مساوی n باشد آنگاه C را یک کد بلوکی q تایی به طول n روی F می‌نامیم. تعداد کلمات C، اندازهٔ C نامیده می‌شود و با $|C|$ مشخص می‌گردد. در همه جای این رساله، ما با کدهای خطی سر و کار خواهیم داشت که جزو کدهای بلوکی هستند. مطالب این بخش را می‌توان در مراجع [۵] و [۱۰] یافت.

تعریف ۱.۱ فرض کنیم F_q^n، فضای برداری شامل تمام بردارهای به طول n روی $GF(q)$ باشد. یک کد خطی q تایی مثل C روی $GF(q)$ عبارت است از یک زیرفضای F_q^n. به عبارت دیگر زیرمجموعهٔ C از F_q^n یک کد خطی است اگر و فقط اگر

۱) برای تمامی u و v های عضو C، $u+v$ نیز در C باشد.

۲) برای تمام u های عضو C و به ازای هر $a \in GF(q)$، au عضوی از C باشد.

به هر یک از اعضای C یک کلمهٔ کدی گفته می‌شود.

اگر کد خطی C یک زیرفضای k بعدی از F_q^n باشد آنگاه بعد C مساوی k تعریف می‌شود و آنرا با $dim(C)$ نشان می‌دهیم. معمولاً کد خطی C به طول n و بعد k روی $GF(q)$، یک $[n,k]$-کد q تایی نامیده می‌شود.

تعریف ۲.۱ فرض کنیم $\{g_1, g_2, \ldots, g_k\}$ یک پایه دلخواه برای کد خطی C با بعد k باشند. ماتریس $k \times n$

$$G = \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}$$

یک ماتریس مولد برای C نامیده می‌شود.

تعریف ۳.۱ فرض کنیم C یک $[n,k]$—کد q تایی باشد. کد دوآل (متعامد) C به صورت زیر تعریف می‌شود:

$$C^{\perp} = \{v \in F_q^n \mid v \cdot u = 0, \forall u \in C\}$$

قضیه ۴.۱ فرض کنیم C یک کد خطی به طول n روی $GF(q)$ باشد. آنگاه

۱) $|C| = q^{dim(C)}$؛

۲) $C^{\perp}$ یک کد خطی است و $dim(C) + dim(C^{\perp}) = n$؛

۳) $(C^{\perp})^{\perp} = C$.

در ادامه C را یک $[n,k]$-کد q تایی در نظر می‌گیریم.

تعریف ۵.۱ فرض کنیم $\{h_1, h_2, \dots, h_{n-k}\}$ یک پایه برای کد $C^{\perp}$ باشد. ماتریس $(n-k)\times n$

$$H = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_{n-k} \end{pmatrix}$$

یک ماتریس زوج آزمایی و یا یک ماتریس آزمون برای C نامیده می‌شود.

تعریف ۶.۱ هنگامی که ماتریس مولدی به شکل $G = (I_k \mid A)$، I_k ماتریس همانی $k\times k$ و A یک ماتریس $k\times(n-k)$ است، یا ماتریس آزمونی به فرم $H = (-B \mid I_{n-k})$ باشد آنگاه گفته می‌شود که این ماتریس‌ها به فرم استاندارد هستند.

اگر $G = (I_k \mid A)$ ماتریس مولد کد C باشد آنگاه می‌توان نشان داد که $H = (-A^T \mid I_{n-k})$ یک ماتریس آزمون برای C است. البته باید توجه داشت که لزومی ندارد هر کد خطی، ماتریس مولدی به فرم استاندارد داشته باشد.

تعریف ۷.۱ اگر $C \subseteq C^{\perp}$، C را خودمتعامد و اگر $C = C^{\perp}$ آن را خود دوآل می‌نامیم.

با توجه به این تعریف و قسمت دوم قضیهٔ ۴.۱ واضح است که اگر C خودمتعامد باشد آنگاه $k \leq \frac{n}{2}$ و اگر خود دوآل باشد آنگاه $k = \frac{n}{2}$ خواهد بود.

تعریف ۸.۱ فرض کنیم x و y دو کلمهٔ کدی از C باشند. فاصلهٔ همینگ[1] x و y را برابر تعداد مکان‌هایی که x و y با هم متفاوتند تعریف می‌کنیم و با $d(x,y)$ نمایش می‌دهیم.

مینیمم فاصلهٔ کد C به صورت زیر تعریف می‌شود:

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

[1] $Hamming$

مثال ۹.۱ فرض کنیم $C = \{۰۰۰۰, ۱۰۱۰, ۰۱۰۱, ۱۱۱۱\}$ یک [4,2] - کد دوتایی با ماتریس مولد

$$G = \begin{pmatrix} ۱ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۱ \end{pmatrix}$$

باشد. دو کلمهٔ ۰۰۰۰ و ۱۰۱۰ در مکان‌های اول و سوم با هم متفاوتند پس $d(۰۰۰۰, ۱۰۱۰) = ۲$. به طور مشابه

$$d(۰۰۰۰, ۰۱۰۱) = d(۱۱۱۱, ۱۰۱۰) = d(۱۱۱۱, ۰۱۰۱) = ۲$$

و

$$d(۰۰۰۰, ۱۱۱۱) = d(۱۰۱۰, ۰۱۰۱) = ۴$$

لذا $d(C) = \min\{۲, ۴\} = ۲$.

از این پس چنانچه علاوه بر میدان و طول و بعد یک کد، مینیمم فاصلهٔ آن نیز مشخص باشد آنگاه تمامی این اطلاعات را با $[n, k, d]_q$ نشان می‌دهیم و از آن به عنوان پارامترهای کد یاد می‌کنیم.

بردار تماماً یک، برداری است که تمامی درایه‌های آن ۱ باشد و با نماد $\jmath$ مشخص می‌گردد.

تعریف ۱۰.۱ فرض کنیم x یک کلمهٔ کدی به طول n باشد. تعداد درایه‌های غیر صفر x را وزن x می‌نامیم و آن را با $wt(x)$ نشان می‌دهیم. به طور معادل

$$wt(x) = d(x, \vec{۰}).$$

مجموعهٔ جایگاه‌های درایه‌های غیر صفر x را محمل x نامیده و آنرا با $supp\,(x)$ نمایش می‌دهیم. واضح است که $wt(x) = |\,supp\,(x)\,|$.

وزن کد C را به صورت زیر تعریف می‌کنیم:

$$wt(C) = \min\{wt(x) \mid x \in C, x \neq \vec{۰}\}$$

قضیه ۱۱.۱ فرض کنیم C یک کد خطی روی $GF(q)$ باشد، آنگاه $d(C) = wt(C)$.

برهان:

$$\begin{aligned} d(C) &= \min\{d(x,y) \mid x,y \in C, x \neq y\} \\ &= \min\{d(x-y,\vec{\circ}) \mid x,y \in C, x \neq y\} \\ &= \min\{wt(x-y) \mid x-y \in C, x-y \neq \vec{\circ}\} \\ &= \min\{wt(z) \mid z \in C, z \neq \vec{\circ}\} \\ &= wt(C). \end{aligned}$$

□

لم ۱۲.۱ فرض کنیم $x = (x_۱, x_۲, \ldots, x_n)$ و $y = (y_۱, y_۲, \ldots, y_n)$ دو بردار از $F_۲^n$ باشند. در این صورت

$$wt(x+y) = wt(x) + wt(y) - ۲wt(x \star y) \qquad (۱)$$

که در آن $x \star y = (x_۱y_۱, x_۲y_۲, \ldots, x_ny_n)$ تعریف می‌شود.

تعریف ۱۳.۱ هم‌ارزی کدها: فرض کنیم C و C' کدهایی به طول n روی $GF(q)$ باشند. این دو کد هم‌ارز نامیده می‌شوند هرگاه هر یک از آنها را بتوان از دیگری توسط ترکیبی از عمل‌های زیر به دست آورد:

الف) با جابجا کردن ستون‌های کلمات کدی؛

ب) با ضرب درایه‌های یک ستون در یک عدد غیر صفر.

چنانچه یک کد صرفاً با جابجا کردن ستون‌های کلمات کد دیگر حاصل شود آنگاه این دو کد را یکریخت می‌نامیم.

قضیه ۱۴.۱ هر کد خطی مانند C با یک کد خطی دیگر مانند C' که ماتریس مولد آن به فرم استاندارد است، هم‌ارز می‌باشد.

مثال ۱۵.۱ فرض کنیم $C = (۰۰۱۱۰, ۱۰۰۱۰, ۱۰۱۰۰, ۰۰۰۰۰)$ یک کد خطی دوتایی با ماتریس مولد زیر باشد

$$G = \begin{pmatrix} ۰ & ۰ & ۱ & ۱ & ۰ \\ ۱ & ۰ & ۰ & ۱ & ۰ \end{pmatrix}$$

اگر در هر یک از کلمات C (یا به طور معادل در G) ، ستون‌ها را به صورت ۳، ۱، ۲، ۴ و ۵ مرتب کنیم آنگاه کد خطی $C' = (۱۰۰۱۰, ۰۱۰۱۰, ۱۱۰۰۰, ۰۰۰۰۰)$ حاصل می‌شود که با C هم‌ارز است و ماتریس مولدی به شکل

$$G' = \begin{pmatrix} ۱ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۱ & ۰ & ۱ & ۰ \end{pmatrix}$$

دارد که به فرم استاندارد است.

تعریف ۱۶.۱ یک یکریختی از C به C را یک همریختی کد C می‌نامیم. گروه همریختی C را با $Aut(C)$ نمایش می‌دهیم.

۱—۲ گراف

مطالب این بخش از مرجع [۲] اقتباس شده است .

تعریف ۱۷.۱ گراف G یک دوتایی مرتب (V, E) است که تشکیل شده از یک مجموعهٔ ناتهی V از رأس‌ها و یک مجموعهٔ E از یال‌ها به طوری که هر یال، یک دوتایی نامرتب از رأس‌ها می‌باشد.
اگر $e = \{u, v\}$ یک یال باشد آنگاه رأس‌های u و v دو سر یال e نامیده می‌شوند. دو رأس متمایز u و v مجاور نامیده می‌شوند هرگاه دوتایی $\{u, v\}$ یک یال باشد.

یک یال با دو سر یکسان را طوقه می‌نامیم. گرافی را که طوقه نداشته باشد و بین هر دو رأس آن حداکثر یک یال وجود داشته باشد، ساده می‌نامیم.

گراف ساده‌ای که در آن هر دو رأس متمایز، با یک یال به یکدیگر متصل شده باشند، گراف کامل نامیده می‌شود. گراف کامل با n رأس را با K_n نمایش می‌دهیم. گراف بدون یال را گراف تهی می‌نامیم.

درجهٔ رأس v برابر است با تعداد یال‌هایی که v بر آنها واقع است. اگر درجهٔ تمام رئوس با هم برابر باشد، گراف منتظم نامیده می‌شود.

تعریف ۱۸.۱ فرض کنیم G یک گراف ساده با مجموعه رئوس $\{v_۱, v_۲, \dots, v_n\}$ باشد، ماتریس مجاورت $A(G)$ یک ماتریس $n \times n$ است که سطرها و ستون‌های نظیر به هم با رأس‌ها اندیس‌گذاری شده‌اند و به صورت زیر تعریف می‌شود

$$A(G) = (a_{ij}) = \begin{cases} ۱ & \text{اگر } v_i \text{ و } v_j \text{ مجاور باشند,} \\ ۰ & \text{در غیر این صورت.} \end{cases}$$

چون G یک گراف ساده است پس $a_{ii} = ۰$ است. همچنین اگر v_i با v_j مجاور باشد، v_j نیز با v_i مجاور است. بنابراین $A(G)$ یک ماتریس متقارن با درایه‌های صفر و یک است که همهٔ عناصر روی قطر اصلی آن صفرند.

فرض کنیم p یک عدد اول و A یک ماتریس $m \times n$ با درایه‌های صحیح باشد. منظور از $p\text{-}rank(A)$، رتبهٔ A روی F_p (میدان متناهی با p عضو) است. کد qتایی C_A ناشی از A را، زیرفضایی از F_q^n در نظر می‌گیریم که توسط سطرهای A و به پیمانهٔ q ساخته شده باشد. توجه داریم که $dim(C_A) = q\text{-}rank(A)$.

لم ۱۹.۱ اگر A یک ماتریس متقارن با درایه‌های صحیح و قطر صفر باشد آن‌گاه $۲\text{-}rank(A)$، زوج است.

برهان: به [۴] مراجعه شود. □

از این لم نتیجه می‌شود که اگر $A(G)$ ماتریس مجاورت گراف سادهٔ G باشد آن‌گاه بعد کد دوتایی $C_{A(G)}$ زوج خواهد بود.

۱—۳ طرح‌های بلوکی

تعریف ۲۰.۱ یک t-طرح با پارامترهای (v,k,λ) (و یا یک t-(v,k,λ) طرح) عبارت است از یک دوتایی $D=(P,B)$ که در آن P یک مجموعه v عضوی از نقاط و B گردایه‌ای از زیرمجموعه‌های k عضوی P است که بلوک‌ها نامیده می‌شوند و دارای این خاصیت است که هر t تایی از نقاط P دقیقاً در λ بلوک قرار دارند.

اگر تعداد بلوک‌ها و نقاط P با هم برابر باشند آنگاه آن طرح، متقارن نامیده می‌شود.

تعریف ۲۱.۱ ماتریس وقوع یک طرح، $M(D)=(m_{ij})$، یک ماتریس $|B|\times v$ است که سطرهای آن با بلوک‌ها و ستون‌های آن با نقاط اندیس‌گذاری شده باشد؛ $m_{ij}=۱$ است هرگاه نقطهٔ j-ام بر بلوک i-ام واقع باشد و در غیر این صورت $m_{ij}=۰$.

تعریف ۲۲.۱ فرض کنیم $D=(P,B)$ یک طرح و Z یک زیرمجموعه‌ی دلخواه از P باشد. بردار وقوع Z را با v^Z نمایش داده و به صورت زیر تعریف می‌کنیم :
v^Z برداری است به طول v که درایه j-ام آن ۱ است اگر نقطهٔ نظیر به ستون j-ام ماتریس $M(D)$ بر Z واقع باشد و در غیر این صورت ۰ است. لذا می‌توان نوشت:

$$v^Z=\sum_{x\in Z} v^{\{x\}}. \qquad (۲)$$

تعریف ۲۳.۱ کد C_F ساخته شده از طرح D روی میدان متناهی F عبارت است از فضای پدید آمده توسط بردارهای وقوعی بلوک‌ها(سطرهای ماتریس وقوع D) روی F. بنابراین

$$C_F=< v^b \,|\, b\in B >$$

زیر فضایی از F^v می‌باشد.

به ازای هر بردار $w\in F^v$ ، مختص w در نقطهٔ $p\in P$ را با $w(p)$ نشان می‌دهیم.

فصل ۲

کدهای دوتایی ناشی از ۳ تایی‌ها

در این فصل، دسته‌ای از گراف‌های منتظم را در نظر گرفته و کدهای دوتایی ناشی از آنها را مدّ نظر قرار می‌دهیم؛ پارامترهای این کدها را به دست آورده و نشان خواهیم داد که گروه‌های اتومرفیسم آنها، S_n یا $S_{\binom{n}{3}}$ هستند.

فرض کنیم $n \geq ۷$ یک عدد صحیح و Ω مجموعه‌ای n عضوی باشد. مجموعهٔ تمام زیرمجموعه‌های ۳ عضوی Ω را با $\Omega^{\{۳\}}$ نشان می‌دهیم. سه گراف غیربدیهی با مجموعه رئوس $\mathcal{P} = \Omega^{\{۳\}}$ در نظر گرفته و آنها را $A_i(n)$، $i = ۰, ۱, ۲$، می‌نامیم. دو رأس در $A_i(n)$ مجاورند اگر زیرمجموعه‌های ۳ عضوی نظیر به آنها در i نقطه با هم مشترک باشند. کد دوتایی حاصل از ماتریس مجاورت گراف $A_i(n)$ را، $i = ۰, ۱, ۲$، با $C_i(n)$ نمایش می‌دهیم.
به ازای هر $i = ۰, ۱, ۲$ از روی $A_i(n)$ یک ۱- طرح $D_i(n)$ با مجموعه نقاط $\mathcal{P}$ چنان تعریف می‌کنیم که هر نقطهٔ $P = \{a, b, c\} \in \mathcal{P}$، مشخص کنندهٔ یک بلوک $\overline{\{a, b, c\}}_i$ به صورت

$$\overline{\{a, b, c\}}_i = \{\{x, y, z\} : |\{x, y, z\} \cap \{a, b, c\}| = i\}$$

باشد. به عبارتی $\overline{\{a, b, c\}}_i$، مجموعه رئوس مجاور به $\{a, b, c\}$ در گراف $A_i(n)$ است لذا ماتریس وقوع $D_i(n)$ با ماتریس مجاورت $A_i(n)$ مساوی خواهد بود.
مجموعهٔ بلوک‌های هر یک از طرح‌های $D_i(n)$ را با $B_i(n)$ نشان می‌دهیم. تعداد بلوک‌های هر طرح

برابر تعداد عناصر $\mathcal{P}$ و مساوی $\binom{n}{3}$ است، در نتیجه $D_i(n)$ ها متقارن هستند و طول بلوک‌های هر یک (درجهٔ رأس‌ها) به ترتیب برابر است با

- $\binom{n-3}{3}$ برای طرح $D_0(n)$،
- $3\binom{n-3}{2}$ برای طرح $D_1(n)$،
- $3(n-3)$ برای طرح $D_2(n)$.

بردار وقوع بلوک $\overline{\{a,b,c\}}_i$ به ازای $i = 0, 1, 2$ به صورت زیر خواهد بود:

$$v^{\overline{\{a,b,c\}}_0} = \sum_{x,y,z \in \Omega \setminus \{a,b,c\}} v^{\{x,y,z\}} \tag{1}$$

$$v^{\overline{\{a,b,c\}}_1} = \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{a,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{b,x,y\}} + \sum_{x,y \in \Omega \setminus \{a,b,c\}} v^{\{c,x,y\}} \tag{2}$$

$$v^{\overline{\{a,b,c\}}_2} = \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{a,b,x\}} + \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{a,c,x\}} + \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{b,c,x\}} \tag{3}$$

توجه داریم که چون نقاط ما به صورت سه‌تایی‌هایی از Ω هستند، صحیح‌تر آن است که بردار وقوع هر نقطه به صورت $v^{\{\{a,b,c\}\}}$ نوشته شود امّا برای سادگی آن را به صورت $v^{\{a,b,c\}}$ در نظر می‌گیریم. همچنین $C_i(n)$ ها می‌توانند به صورت زیر نیز نوشته شوند:

$$C_i(n) = < v^b \mid b \in B_i(n) > .$$

بلوک‌های $\overline{\{a,b,c\}}_i$، $i = 0, 1, 2$، با هم اشتراک ندارند در نتیجه بردارهای وقوع آنها در هیچ ستونی ۱ مشترک ندارند لذا به ازای هر نقطهٔ $P = \{a,b,c\}$ داریم

$$v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_1} + v^{\overline{\{a,b,c\}}_2} = \jmath . \tag{4}$$

حال به ازای هر نقطهٔ $P = \{a,b,c\} \in \mathcal{P}$ و برای هر طرح به طور جداگانه، بردار زیر را تعریف می‌کنیم که در آن b_jها، بلوک‌های هر یک از طرح‌های $D_i(n)$ $(i = 0, 1, 2)$ هستند:

$$w_P = \sum_{P \in b_j} v^{b_j} \tag{5}$$

بنابراین w_P عبارت است از حاصل‌جمع تمام بردارهای وقوعی آن بلوک‌هایی از $D_i(n)$ که شامل P هستند.

به ازای هر نقطهٔ $Q \in \mathcal{P}$، $w_P(Q)$ (مختص w_P در مکان Qام) به تعداد نقاطی که P و Q اشتراک دارند(۰،۱،۲ یا۳ تا) بستگی دارد. این حالت‌ها در زیر بررسی می‌شوند:

الف) $i = ۰$

۱) $Q = P$ آن‌گاه $w_P(Q)$ برابر است با تعداد بلوک‌های شامل P که مساوی $\binom{n-۳}{۳}$ است.

۲) $|P \cap Q| = ۲$ و مثلاً $Q = \{a, b, d\}$ آن‌گاه $w_P(Q)$ برابر تعداد بلوک‌های شامل P و Q است که برابر تعداد سه تایی‌هایی است که شامل هیچ یک از نقاط a، b، c و d نباشند پس تعداد آنها مساوی $\binom{n-۴}{۳}$ است. تعداد نقاطی مانند Q که $|Q \cap P| = ۲$ برابر $۳(n - ۳)$ می‌باشد.

۳) $|P \cap Q| = ۱$ و مثلاً $Q = \{a, d, e\}$ آنگاه $w_P(Q)$ برابر تعداد سه تایی‌هایی است که شامل هیچ یک از عناصر a، b، c، d و e نباشند و تعداد آنها مساوی $\binom{n-۵}{۳}$ خواهد بود. $۳\binom{n-۳}{۲}$ نقطه مانند Q با شرط $|P \cap Q| = ۱$ وجود دارد.

۴) $|P \cap Q| = ۰$ و $Q = \{d, e, f\}$ آنگاه $w_P(Q)$ برابر است با تعداد سه‌تایی‌هایی که شامل هیچ کدام از عناصر P و Q نیستند لذا $w_P(Q) = \binom{n-۶}{۳}$ خواهد بود. $\binom{n-۳}{۳}$ نقطه مانند Q با این شرط موجود است.

ب) $i = ۱$

۱) $P = Q$ آنگاه $w_P(Q) = ۳\binom{n-۳}{۲}$.

۲) اگر $|P \cap Q| = ۲$ و به فرض $Q = \{a, b, d\}$ آنگاه $w_P(Q)$ برابر تعداد سه تایی‌هایی است که با $\{a, b, c, d\}$، فقط در a یا b و یا در $\{c, d\}$ اشتراک داشته باشند و مساوی $۲\binom{n-۴}{۲} + (n - ۴)$ است. تعداد Qها با شرط $|P \cap Q| = ۲$ برابر $۳(n - ۳)$ است.

۳) اگر $|P \cap Q| = ۱$ و $Q = \{a, d, e\}$ آنگاه $w_P(Q)$ برابر تعداد سه تایی‌هایی است که با $\{a, b, c, d, e\}$، فقط در a و یا در یکی از زوج‌های $\{b, d\}$، $\{b, e\}$، $\{c, d\}$ و $\{c, e\}$ اشتراک