
بسم الله الرحمن الرحیم

دانشکده علوم ریاضی

رشته ریاضی کاربردی، گرایش گراف و ترکیبیات

پایان‌نامه کارشناسی ارشد

کدهای کامل و چندمجموعه‌ای روی کانال‌های جایگشتی و سادک‌های گسسته

نگارنده: آنسه اسلامی

استادان راهنما

دکتر صادق رحیمی شعرباف
دکتر عبدالله آل‌هوز

تیر ماه ۱۳۹۶

تقدیم به اولین معلّمان زندگیم
پدر و مادر عزیزم

پروردگارا...
نه می‌توانم مویشان را که در راه عزت من سفید شد، سیاه کنم و نه برای دست‌های پینه بسته‌شان که ثمره تلاش برای افتخار من است، مرهمی دارم. پس توفیقم ده که هر لحظه شکرگزارشان باشم و ثانیه‌های عمرم را در عصای دست بودنشان بگذارم.

از اساتید بزرگوارم جناب آقای دکتر آل‌هوز و جناب آقای دکتر رحیمی شعرباف بسیار سپاسگذارم، چرا که بدون راهنمایی‌های ایشان تأمین این پایان‌نامه بسیار مشکل می‌نمود.

آنسه اسلامی
تیر ماه ۱۳۹۶

تعهد نامه

اینجانب **آنسه اسلامی** دانشجوی کارشناسی ارشد رشته **ریاضی کاربردی** دانشکده **علوم ریاضی** دانشگاه صنعتی شاهرود، نویسنده پایان‌نامه با عنوان **کدهای کامل و چندمجموعه‌ای روی کانال‌های جایگشتی و سادک‌های گسسته** ، تحت راهنمایی **صادق رحیمی شعرباف** متعهد می‌شوم:

- تحقیقات در این پایان‌نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است.
- در استفاده از نتایج پژوهش‌های دیگر پژوهش‌گران، به مرجع مورد استفاده استناد شده است.
- مطالب این پایان‌نامه، تا کنون توسط خود، یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ‌جا ارایه نشده است.
- حقوق معنوی این اثر، به دانشگاه صنعتی شاهرود تعلق دارد، و مقالات مستخرج با نام " دانشگاه صنعتی شاهرود " یا " Shahrood University of Technology " به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به‌دست آوردن نتایج اصلی پایان‌نامه تاثیرگذار بوده‌اند، در مقالات مستخرج از پایان‌نامه رعایت می‌گردد.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که از موجود زنده (یا بافت‌های آنها) استفاده شده است، ضوابط و اصول اخلاقی رعایت شده است.
- در تمام مراحل انجام این پایان‌نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته (یا استفاده شده است)، اصل رازداری و اصول اخلاق انسانی رعایت شده است.

آنسه اسلامی
تیر ماه ۱۳۹۶

مالکیت نتایج و حق نشر

- تمام حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، کتاب، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) متعلق به دانشگاه صنعتی شاهرود می‌باشد. این مطلب باید به نحو مقتضی، در تولیدات علمی مربوطه ذکر شود.
- استفاده از اطلاعات و نتایج موجود در این پایان‌نامه بدون ذکر منبع مجاز نمی‌باشد.

چکیده

طراحی کدهای خوب از هر دو دیدگاه نظری و کاربردی مسأله‌ای بسیار مهم در نظریه کدگذاری است. از زمان پیدایش نظریه کدگذاری، پژوهشگران بسیاری در این راستا بسیار تلاش کرده و در جریان این تلاش‌ها گونه‌های جالب زیادی از این کدها را تولید کردند.

در این پایان‌نامه قصد بررسی وجود یا عدم وجود کدهای کامل در سادک‌های گسسته و همچنین کدهای چندمجموعه‌ای در کانال‌های جایگشتی را داریم. ابتدا مقدمه‌ای از نظریه کدگذاری و تعاریف لازم برای ادامه‌ی مطالب مطرح شده‌است. سپس کدهای کامل در سادک‌های گسسته در ابعاد مختلف بررسی شده‌است و به این نتیجه می‌رسیم که کدهای کامل در الفبای دودویی همیشه وجود دارند و در الفبای سه‌تایی در حالتی خاص وجود دارند. درواقع نشان می‌دهیم کدهای کامل در ۱ـسادک برای هر $\ell \geq ۲e+۱$ وجود دارند، همچنین کد کامل در ۲ـسادک وجود دارد، اگر و فقط اگر $\ell = ۳e+۱$ باشد. در حالی‌که کدهای کامل در سادک‌های با بعد بالاتر وجود ندارند. به عبارت دیگر، کدهای کامل فقط روی الفبای دودویی و سه‌تایی وجود دارند. سپس کدهای چندمجموعه‌ای در کانال‌های جایگشتی و خطاهایی همچون حذف، وارد کردن و جایگزینی در کانال‌های جایگشتی بررسی می‌شود. در آخر، وجود کدهای کامل در مشبکه‌های A_n و $\mathbb{Z}^n$ مورد بررسی قرار می‌گیرد.

کلمات کلیدی: کد کامل، سادک گسسته، کانال جایگشتی، کد چندمجموعه‌ای، مشبکه A_n، مشبکه $\mathbb{Z}^n$، وارد کردن، حذف، جایگزینی.

لیست مقالات مستخرج از پایان‌نامه

۱. آنسه اسلامی، ''بررسی کدهای کامل در مشبکه‌های $\mathbb{Z}^n$ و A_n''، **چهارمین کنفرانس ملی فناوری اطلاعات، کامپیوتر و مخابرات**، دانشگاه تربت حیدریه، ۲۲ تیرماه ۱۳۹۶.

فهرست مطالب

فهرست تصاویر

فصل ۱

تعاریف و مفاهیم اولیه

کدگذاری یکی از شاخه‌های بسیار جالب و کاربردی ریاضیات است که همواره کاربردهای بسیاری در حوزه‌های گوناگون داشته است. در زمان جنگ جهانی دوم ریاضیدانان بسیاری با به‌کارگیری روشهای کدگذاری پیچیده سعی در کد کردن داده‌های نظامی داشتند به‌گونه‌ای که طرف مقابل نتواند آنها را کدگشایی کند. نظریه کدگذاری در رابطه با انتقال موفّق اطلاعات در یک کانال پارازیت‌دار و تصحیح خطاها در پیام‌های مخدوش است. این نظریه برای بسیاری از کاربردها در علوم کامپیوتر و مهندسی اهمیتی ویژه دارد.

نظریه کدگذاری در سال ۱۹۴۸ توسط شانون پایه‌ریزی شد. وی پی برده بود هنگامی که رایانه از یک عمل رایج نسخه‌برداری می‌کند و با عمل دیگری شروع به کار می‌کند، هرگز نمی‌تواند به حالت اولیه بازگردد. نظریه کدگذاری مثال قابل توجهی از ریاضی محض در حل مسائل علمی است. اگر چه برخی از کدهای ساده دارای ساختاری هستند که نیاز زیادی به ریاضیات ندارند، با این حال ویژگی کدها از کشفیات ریاضیات است. مانند هسته ارسال خطی که اثبات فعالیتهای واقعی را ممکن می‌سازد و بدون این‌گونه برهان‌ها، کدها در حقیقت بدون استفاده می‌باشند. علاوه بر این، ریاضیات موجب ایجاد کدها در ابعاد دیگر می‌شود و با افزایش قابلیت تصحیح خطا، اثبات‌هایی را برای وجود یا عدم وجود کدها ارائه داده‌است.

۱.۱ مقدمه‌ای بر نظریه کدگذاری

در این قسمت، تعاریف مربوط به بخش گراف برگرفته از مرجع [۸] و تعاریف مربوط به بخش کدگذاری از مرجع [۳۸] می‌باشد.

تعریف ۱.۱.۱. گراف G یک سه‌تایی مرتب $(V(G), E(G), \psi_G)$ متشکل از مجموعه‌ی ناتهی $V(G)$ رأس‌ها و مجموعه‌ی $E(G)$ یال‌های مجزا از $V(G)$، و تابع وقوع ψ_G است که با هر یال G، یک جفت نامرتب (نه لزوماً مجزا) از رأس‌های G را همراه می‌کند.
اگر e یک یال و u و v رأس باشند، به قسمی که $\psi_G(e) = uv$ باشد، آنگاه می‌گویند e، u را به v وصل می‌کند، رأس‌های u و v را دو سر یال می‌نامند.

تعریف ۲.۱.۱. گراف مسیر گرافی است که رئوس آن را می‌توان به‌ترتیب $\{v_1, v_2, \ldots, v_n\}$ ذکر کرد، به‌طوری که یالهای آن به‌صورت $\{v_i, v_{i+1}\}$ می‌باشند، درحالی‌که $i = 1, 2, \ldots, n-1$.
به‌طور معادل، یعنی گرافی که دو رأس آویزان(رأس با درجه یک) دارد که رأس‌های میانی از درجه دو می‌باشند.

تعریف ۳.۱.۱. قطر گراف عبارت است از بزرگترین فاصله‌ی بین رئوس در گراف.

تعریف ۴.۱.۱. فرض کنید $\mathcal{A}$ یک مجموعه q عضوی بصورت $\{a_1, a_2, \ldots, a_q\}$ باشد، در این صورت مجموعه $\mathcal{A}$ را الفبای کد[۱] می‌نامیم و هریک از عناصر مجموعه $\mathcal{A}$ را سمبل (نماد) کد[۲] می‌گوییم.

تعریف ۵.۱.۱. یک کلمه q ـ‌آرایه‌ای با طول n روی مجموعه $\mathcal{A}$ در حقیقت دنباله‌ای است به شکل $w = w_1 w_2 \ldots w_n$. بطوری‌که برای هر $1 \leq i \leq n$ داریم $w_i \in \mathcal{A}$، همچنین می‌توان هر کلمه qـ‌آرایه‌ای را با طول n بصورت $(w_1, \ldots, w_n)$ نمایش داد.

تعریف ۶.۱.۱. کد بلوکی qـ‌آرایه‌ای[۳] با طول n روی مجموعه $\mathcal{A}$، مجموعه‌ای ناتهی مانند $\mathcal{C}$ از کلمات qـ‌آرایه‌ای می‌باشد که تمام کلمات دارای طول یکسان n می‌باشند و هر عنصر از مجموعه $\mathcal{C}$ را یک کدواژه[۴] می‌نامیم.

تعریف ۷.۱.۱. تعداد کدواژه‌های مجموعه $\mathcal{C}$ را اندازه کد می‌نامیم و با $|\mathcal{C}|$ نمایش می‌دهیم.

تعریف ۸.۱.۱. هر کد بلوکی از طول n و اندازه M را یک (n, M) ـ کد گویند.

---
[۱] Code alphabet
[۲] Code sambols
[۳] q-array block code
[۴] Code words

تعریف ۹.۱.۱. کانال ارتباطی[۵] بصورت کانالی تعریف می‌شود که متشکل از دو مجموعه می‌باشد که یکی از آنها مجموعه الفبای کد است و بصورت $\mathcal{A} = F_q = \{a_1, \ldots, a_q\}$ در نظر گرفته می‌شود و مجموعه دیگر مجموعه احتمال‌های کانال ارسال می‌باشد.

تعریف ۱۰.۱.۱. در یک کانال ارتباطی کدشده، فقط کدواژه‌ها ارسال می‌شوند. فرض کنید کلمه w دریافت شده است. اگر w یک کدواژه معتبر باشد می‌توان نتیجه گرفت که خطایی در انتقال وجود ندارد. از طرف دیگر، می‌دانیم چند خطا اتفاق افتاده است. در این مورد، به روشی برای پیدا کردن محتمل‌ترین کدواژه ارسال شده نیاز داریم. چنین روشی به روش کدگشایی معروف است.

تعریف ۱۱.۱.۱. اگر x و y دو n ـ تایی از ۰ و ۱ باشند، آنگاه فاصله همینگ[۶] آنها به‌صورت زیر تعریف می‌شود:

$$d_H(x, y) = |\{i; 1 \leq i \leq n, x_i \neq y_i\}|$$

تعریف ۱۲.۱.۱. مجموعه X که عناصرش نقاط می‌باشند، در صورتی یک فضای متریک است که برای هر دو نقطه p و q از X، عدد حقیقی $d(p, q)$، به نام فاصله از p تا q، داشته باشیم:

۱. $d(p, q) > 0$ هرگاه $p \neq q$ و $d(p, p) = 0$.

۲. $d(p, q) = d(q, p)$.

۳. به ازای هر $r \in X$، $d(p, q) \leq d(p, r) + d(r, p)$.

ملاحظه ۱.۱.۱. می‌توان به راحتی بررسی کرد که تعریف فوق از فاصله همینگ، تمام ویژگی‌های یک متر را دارا می‌باشد. یعنی اگر a و b و c کدواژه‌هایی از طول n در یک کد بلوکی باشند، همواره داریم :

۱. $0 \leq d_H(a, b) \leq n$.

۲. $d_H(a, b) = 0 \quad 1 \leq i \leq n, \quad a = b \Leftrightarrow \forall$.

۳. $d_H(a, b) = d_H(b, a)$.

۴. $d_H(a, c) \leq d_H(a, b) + d_H(b, c)$.

تعریف ۱۳.۱.۱. علاوه بر طول و اندازه کد، ویژگی مهم و مفید دیگر فاصله کد است. برای کد $\mathcal{C}$ که شامل حداقل دو کلمه می‌باشد، مینیمم فاصله $\mathcal{C}$ بصورت زیر تعریف می‌شود و با $d(\mathcal{C})$ نمایش می‌دهیم:

$$d(\mathcal{C}) = \min\{d_H(x, y); x, y \in \mathcal{C}, x \neq y\}$$

[۵] Communication channel

[۶] Hamming Distance

تعریف ۱.۱.۱۴. یک کد از طول n، اندازه M و فاصله d را (n, M, d) ـ کد می‌نامیم. اعداد n، M و d را پارامترهای کد می‌نامند.

مثال ۱.۱.۱. فرض کنید $\mathcal{C} = \{۰۰۰۰۰, ۰۰۱۱۱, ۱۱۱۱۱\}$، یک کد دودویی باشد، در این صورت $d(\mathcal{C}) = ۲$، زیرا:

$$d_H(۰۰۰۰۰, ۰۰۱۱۱) = ۳$$

$$d_H(۰۰۰۰۰, ۱۱۱۱۱) = ۵$$

$$d_H(۰۰۱۱۱, ۱۱۱۱۱) = ۲$$

از این‌رو $\mathcal{C}$ یک $(۵, ۳, ۲)$ ـ کد دودویی است.

تعریف ۱.۱.۱۵. کد خطی $\mathcal{C}$ از طول n روی F_q یک زیرفضا از F_q^n است.

مثال ۱.۱.۲. موارد زیر نمونه‌هایی از کدهای خطی می‌باشند:

۱. $\mathcal{C} = \{(\lambda, \lambda, \ldots, \lambda); \lambda \in F_q\}$ که کد تکرار نامیده می‌شود.

۲. $(q = ۲)$، $\mathcal{C} = \{۰۰۰, ۰۰۱, ۰۱۰, ۰۱۱\}$.

۳. $(q = ۳)$، $\mathcal{C} = \{۰۰۰۰, ۱۱۰۰, ۲۲۰۰, ۰۰۰۱, ۰۰۰۲, ۱۱۰۱, ۱۱۰۲, ۲۲۰۱, ۲۲۰۲\}$.

تعریف ۱.۱.۱۶. فرض کنید x یک کلمه در F_q^n باشد. وزن همینگ[۷] x، که با $wt(x)$ نمایش داده می‌شود، تعداد مؤلفه‌های ناصفر x تعریف می‌شود؛ به عبارت دیگر:

$$wt(x) = d(x, ۰)$$

که ۰، کلمه صفر است.

ملاحظه ۱.۱.۲. برای هر عضو $x \in F_q$ وزن همینگ را می‌توانیم بصورت زیر تعریف کنیم:

$$wt(x) = d(x, ۰) = \begin{cases} ۱ & x \neq ۰ \\ ۰ & x = ۰ \end{cases}$$

در این صورت با نوشتن $x \in F_q^n$ به شکل $x = (x_۱, x_۲, \ldots, x_n)$ ، وزن همینگ x می‌تواند بطور معادل بصورت زیر تعریف شود :

$$wt(x) = wt(x_۱) + wt(x_۲) + \cdots + wt(x_n)$$

ملاحظه ۱.۱.۳. موارد زیر دلایلی هستند که چرا ممکن است استفاده از کدهای خطی نسبت به کدهای غیرخطی مورد ترجیح باشد :

[۷] Hamming Weight

۱. از آنجا که یک کد خطی یک فضای برداری است، می تواند با استفاده از یک پایه بطور کامل توصیف شود.

۲. فاصله یک کد خطی با کمترین وزن کدواژه‌های ناصفر آن برابر است.

۳. روش‌های کدگذاری و کدگشایی برای یک کد خطی نسبت به کدهای غیرخطی دلخواه، سریع‌تر و آسان‌تر است.

تعریف ۱.۱.۱۷. فرض کنید v عدد صحیح مثبتی باشد. $\mathcal{C}$ را کد vـ تصحیح کننده خطا گوییم اگر به تصحیح v یا تعدادی کمتر خطا قادر باشد.

۱.۱.۱ کدهای کامل

مجموعه $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$ مجموعه اعداد صحیح نامنفی تعریف می‌شود. فرض کنید (S, d) فضای متریک متناهی با متر صحیح d باشد و $\mathcal{C} \subseteq S$ کد تصحیح کننده خطا است.

تعریف ۱.۱.۱۸. $\mathcal{C}$ را کد eـ کامل[۸] گوییم ($e \in \mathbb{Z}_+$) هرگاه گوی‌هایی با شعاع e و به مرکز کدواژه‌های متمایز، فضای کل را پوشش دهند:

$$\mathcal{B}(x, e) \cap \mathcal{B}(y, e) = \emptyset \qquad \forall x, y \in \mathcal{C}, \quad x \neq y, \tag{۱.۱}$$

$$\bigcup_{x \in \mathcal{C}} \mathcal{B}(x, e) = S, \tag{۲.۱}$$

که $\mathcal{B}(x, e) = \{w \in S : d(x, w) \leq e\}$ فضای کدگشایی کدواژه x تعریف می‌شود. باتوجه به خاصیت ذکرشده، هر عضو از S با فاصله‌ی کمتر یا مساوی e از دقیقاً یک کدواژه قرار دارد. همچنین هر مجموعه تک عضوی $\mathcal{C} = \{x\}$، $D-$کامل است که D قطر فضای S است و همچنین S خودش $0-$ کامل است، زیرا اگر $\mathcal{C} = S$ باشد آنگاه $e = 0$ است.

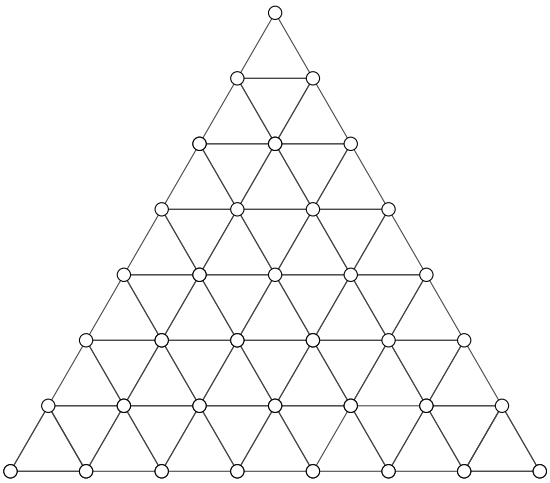
در این پایان‌نامه به بررسی نوعی کدخطی، یعنی کدهای کامل غیربدیهی که $|\mathcal{C}| \geq 2$ و $e \geq 1$ است، خواهیم پرداخت.

۲.۱.۱ سادک گسسته

تعریف ۱.۱.۱۹. فضای مدنظر در این پایان‌نامه nـ سادک گسسته[۹] است که بصورت زیر تعریف می‌شود و ℓ طول سادک موردنظر می‌باشد:

$$\Delta_\ell^n := \{(x_0, \dots, x_n); \quad x_i \in \mathbb{Z}_+, \sum_{i=0}^{n} x_i = \ell\}. \tag{۳.۱}$$

شکل زیر نمونه‌ای از یک سادک گسسته از طول ۷ می‌باشد.

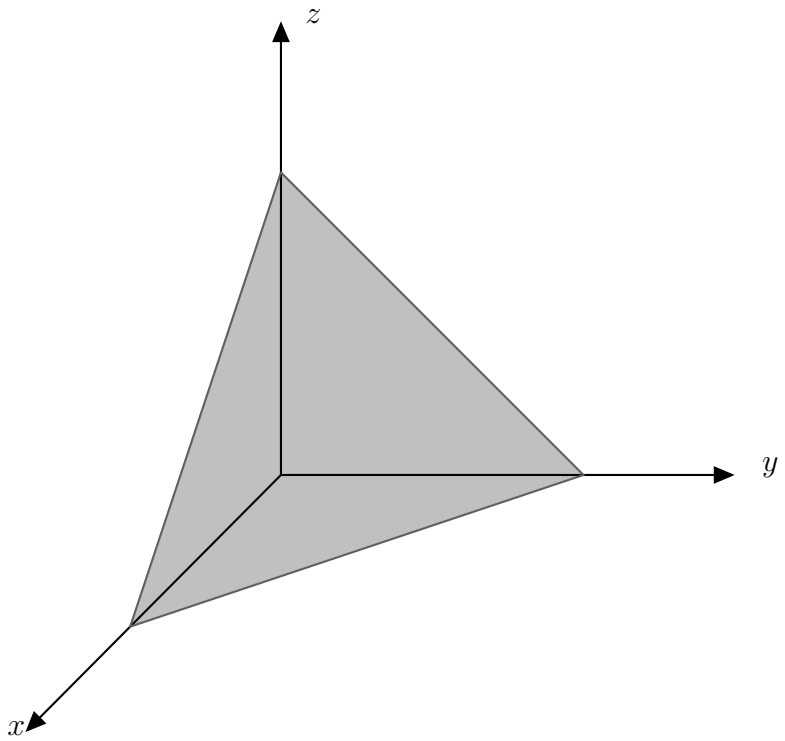


شکل ۱.۱: سادک گسسته از طول ۷

[۸] Perfect code

[۹] Discrete simplex

سادک گسسته در واقع صفحه‌ای در دستگاه مختصات سه‌بعدی می‌باشد که مختصات هر رأس روی سادک گسسته را می‌توان طبق مختصات نقاط روی صفحه نوشت.



شکل ۲.۱: صفحه سادک گسسته در دستگاه مختصات سه‌بعدی

در این پایان‌نامه از مترهای زیر استفاده می‌کنیم:

۱. متر منهتن[۱۰] ، فاصله دو نقطه است که مجموع قدرمطلق تفاضل طول و عرض آن دو نقطه می‌باشد:

$$d_1(p,q) = ||p-q||_1 = \sum_{i=1}^{n} |p_i - q_i|. \qquad (۴.۱)$$

۲. متر $d(x,y) = \frac{1}{2}\|x-y\|_1 = \frac{1}{2}\sum_{i=0}^{n}|x_i - y_i|$ می‌باشد، جایی‌که $x = (x_0,\ldots,x_n)$ و $y = (y_0,\ldots,y_n)$ رئوس روی سادک گسسته می‌باشند که مجموع درآیه‌های هر رأس باید برابر با طول سادک گسسته موردنظر باشد. همچنین می‌توانیم به‌طور معادل متر d را بصورت زیر درنظر بگیریم:

$$d(x,y) = \sum_{x_i > y_i} (x_i - y_i) = \sum_{x_i < y_i} (y_i - x_i) \qquad (۵.۱)$$

[۱۰] Manhattan metric

تعریف ۱.۱.۲۰. بردار $f_{i,j}$ که $i,j \in \{۱,۲,\dots\}$ را به این صورت تعریف می‌کنیم که در iـامین جایگاه یک و در jـامین جایگاه ۱− قرار می‌دهیم همچنین مابقی جایگاه‌ها صفر می‌باشند. برای مثال $f_{۱,۲} = (۱,-۱,۰)$.

تعریف ۱.۱.۲۱. $f_{i,j}$ و $f_{k,l}$ را متعامد گوییم اگر $\{i,j\} \cap \{k,l\} = \emptyset$ باشد، یعنی هیچ درآیه غیرصفری در جایگاه یکسان از هر دو بردار وجود نداشته باشد.

مثال ۱.۱.۳. دو بردار $f_{۱,۴} = (۱,۰,۰,-۱)$ و $f_{۲,۱} = (-۱,۱,۰,۰)$ متعامد نمی‌باشند، ولی بردارهای $f_{۱,۳} = (۱,۰,-۱,۰)$ و $f_{۲,۴} = (۰,۱,۰,-۱)$ متعامدند.

۳.۱.۱ کانال جایگشتی

تعریف ۱.۱.۲۲. فرض کنید $\mathcal{A} = \{۰,۱,\dots,n\}$ الفبایی متناهی باشد، بطوری‌که $n+۱ \geq ۲$ نماد دارد. کانال جایگشتی[۱۱] روی $\mathcal{A}$، کانالی ارتباطی است که دنباله‌ای از نمادهای $\mathcal{A}$ را به عنوان ورودی می‌گیرد و به ازای هر ورودی یک جایگشت تصادفی از آن دنباله را خارج می‌کند.

۴.۱.۱ چندمجموعه‌ای‌ها

تعریف ۱.۱.۲۳. چندمجموعه‌ای[۱۲] X، در واقع زوج مرتب $(\mathcal{A}, m_X)$ است که $\mathcal{A}$ مجموعه پایه[۱۳]، یعنی همان الفبای کانال در فضای مدنظر و همچنین $m_X : \mathcal{A} \to \mathbb{Z}_+$ تابع چندگانگی[۱۴] است که تعداد پیشامدهای عناصر $\mathcal{A}$ در X را نشان می‌دهد.

اعمال روی چندمجموعه‌ای‌ها بصورت زیر تعریف می‌شود:

$$m_{X\cup Y} = \max\{m_X, m_Y\}$$
$$m_{X\cap Y} = \min\{m_X, m_Y\}$$
$$m_{X\setminus Y} = \max\{۰, m_X - m_Y\}$$

درحالی‌که اندازه چندمجموعه‌ای برابر است با :

$$|X| = \sum_x m_X(x).$$

[۱۱] Permutation channel
[۱۲] Multi-set
[۱۳] Ground set
[۱۴] Multiplicity function

تعداد اعضای X، تعداد عناصری است که شامل آن می‌باشد و شامل تکرارها نیز است. در حقیقت یعنی $|X| = \sum_{i=0}^{n} x_i = \ell$. چندمجموعه‌ای‌ها می‌توانند توسط توابع چندگانگی‌شان تعریف شوند. مجموعه همه چندمجموعه‌ای‌ها با اندازه ℓ را بصورت زیر نشان می‌دهیم :

$$\{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}_+^{n+1}; \sum_{i=0}^{n} x_i = \ell\},$$

که دقیقاً سادک گسسته Δ_ℓ^n است.

فرض کنید $\mathcal{A}$ الفبای کانال و $P(\mathcal{A})$ مجموعه توانی $\mathcal{A}$؛ یعنی مجموعه تمام زیرمجموعه‌های $\mathcal{A}$ باشد و $P(\mathcal{A}, \ell)$ مجموعه همه زیرمجموعه‌های $\mathcal{A}$ با اندازه ℓ است.

تعریف ۲۴.۱.۱. کد زیرمجموعه[۱۵] روی $\mathcal{A}$ یک زیرمجموعه ناتهی از $P(\mathcal{A})$ است. اگر داشته باشیم $\mathcal{C} \subseteq P(\mathcal{A}, \ell)$، گوییم $\mathcal{C}$ کد اندازه‌ـ ثابت[۱۶] است.

تعریف ۲۵.۱.۱. تابع مشخصه [۱۷] مجموعه $X \subseteq A$ نگاشت $I_X(x) : A \to \{0, 1\}$ است که بصورت زیر تعریف می‌شود :

$$I_X(x) = \begin{cases} 1, & x \in X \\ 0, & x \notin X \end{cases} \tag{۶.۱}$$

مجموعه متناهی A را درنظر بگیرید. زیرمجموعه‌هایی از A که یکتا هستند، به‌وسیله توابع مشخصه تعیین می‌شوند.

اگر $A = \{1, \ldots, q\}$ باشد، آنگاه این توابع می‌توانند به‌وسیله دنباله‌های دودویی از طول q مشخص شوند، یعنی دنباله‌های $(I_X(1), \ldots, I_X(q))$. همه‌ی اعمال روی مجموعه (اجتماع، اشتراک، تفاضل و...) می‌توانند روی $P(A)$ در رابطه با توابع مشخصه متناظرش تعریف شوند. برای مثال :

$$I_{X\Delta Y} = I_X \oplus I_Y = |I_X - I_Y|, \tag{۷.۱}$$

جایی‌که $\oplus$ عمل جمع به پیمانه دو تعریف می‌شود. بنابراین اندازه مجموعه X بصورت زیر بیان می‌شود :

$$|X| = \sum_x I_X(x), \tag{۸.۱}$$

که همان وزن همینگ دنباله دودویی $(I_X(1), \ldots, I_X(q))$ است. از روابط بالا می‌توانیم بگوییم:

$$d(X, Y) = |X\Delta Y| = \sum_x |I_X(x) - I_X(x)|. \tag{۹.۱}$$

---

[۱۵] Subset code

[۱۶] Constant-cardinality

[۱۷] Characteristic function

یعنی فاصله بین مجموعه‌های X و Y برابر فاصله همینگ بین دنباله‌های دودویی مربوط به I_X و I_Y است.

فرض کنید $\mathcal{M}(\mathcal{A})$ مجموعه همه چندمجموعه‌ای‌های روی $\mathcal{A}$ تعریف شود و $\mathcal{M}(\mathcal{A},\ell)$ مجموعه همه چندمجموعه‌ای‌ها روی $\mathcal{A}$ از طول ℓ باشد، بطوری‌که $|\mathcal{A}| = \ell$. اعمال روی $\mathcal{M}(\mathcal{A})$ مانند اجتماع، اشتراک، تفاضل و ... مشابه اعمال روی مجموعه‌ها است. مثال ساده‌ای را در ادامه بیان می‌کنیم :

مثال ۱.۱.۴. فرض کنید $X = \{۱,۲,۲,۲,۳\}$ و $Y = \{۱,۲,۲,۳,۳,۴\}$ دو چندمجموعه‌ای روی $\mathcal{A} = \{۱,۲,۳,۴\}$ باشد، آنگاه:

$$X \cap Y = \{۱,۲,۲,۳\}$$
$$X \cup Y = \{۱,۲,۲,۲,۳,۳,۴\}$$
$$X \setminus Y = \{۲\}$$
$$Y \setminus X = \{۳,۴\}$$

و اندازه X و Y برابر ۵ و ۶ می‌باشد.

کدهای روی $\mathcal{A}$ مشابه کدهای روی P هستند.

تعریف ۱.۱.۲۶. کد چندمجموعه‌ای A روی $\mathcal{A}$ زیرمجموعه‌ای ناتهی از $\mathcal{A}$ است که اگر $\mathcal{C} \subseteq \mathcal{M}(\mathcal{A},\ell)$ گوییم $\mathcal{C}$ کد اندازه‌ـ ثابت است.

توجه داشته باشید که $\mathcal{A}$ یک فضای نامتناهی می‌باشد. کدهای چندمجموعه‌ای هرچند که به صراحت بیان نشده، ولی همیشه متناهی درنظر گرفته شده‌است.

اگر الفبا برابر $\mathcal{A} = \{۰,۱,\ldots,q\}$ باشد، توابع چندگانه چندمجموعه‌ای X منحصربفرد و به وسیله دنباله $(m_X(۱),\ldots,m_X(q)) \in \mathbb{N}^q$ تعیین می‌شود. از این رو فضای $\mathcal{M}(\mathcal{A})$ معادل فضای $\mathbb{N}^q$ می‌باشد. بنابراین فاصله بین چندمجموعه‌ای‌ها برابر فاصله $\ell_۱$ (متر منهتن) بین دنباله‌های مربوطه است.

$$d(X,Y) = |X\Delta Y| = \sum_x |m_X(x) - m_Y(x)|.$$

بنابراین کدهای چندمجموعه‌ای فقط تعریف دیگری از کدها در $\mathbb{N}^q$ تحت متر منهتن هستند. کدهای اندازه‌ـ ثابت با کدهای روی فضای $\Delta_\ell^{q-۱}$ معادل‌اند.

$$\Delta_\ell^{q-۱} := \{(x_۱,\ldots,x_q); x_i \in \mathbb{N}, \sum_i x_i = \ell \in \mathbb{N}\},$$

که به عنوان سادک گسسته‌ی $q-۱$ تایی درنظر گرفته می‌شود.

تعریف ۱.۱.۲۷. مجموعه $\mathcal{L}$ را که تحت افزایش و کاهش بسته باشد، مشبکه[۱۸] گوییم.

تعریف ۱.۱.۲۸. مشبکه‌های A_n و $\mathbb{Z}^n$ بصورت زیر تعریف می‌شود:

$$\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$
$$A_n = \{(x_0, x_1, \ldots, x_n) : x_i \in \mathbb{Z}_+, \sum_{i=0}^{n} x_i = 0\}.$$

تعریف ۱.۱.۲۹. گوییم کد چندمجموعه‌ای $\mathcal{C} \subseteq \Delta_n^{q-1}$، خطی است اگر $\mathcal{C} = (\mathcal{L} + t) \cap \Delta_n^m$ باشد، برای مشبکه‌هایی که $\mathcal{L} \subseteq A_{q-1}$ و بردارهای $t \in \mathbb{Z}^q$ بطوری‌که $\sum_{i=1}^{q} t_i = n$. به عبارت دیگر $\mathcal{C}$ خطی می‌باشد اگر به وسیله انتقال یک کد خطی در A_{q-1} بدست آمده باشد و فقط مختصات نامنفی داشته باشد.

تعریف ۱.۱.۳۰. فرض کنیم S و T زیرمجموعه‌های ناتهی و متناهی از مشبکه $\mathbb{Z}^n$ باشند. S مجموعه‌ای است که می‌خواهیم با آن فضای کل را بپوشانیم و T مجموعه همه بردارهای انتقال می‌باشد. گوییم (S,T) یک بسته‌بندی[۱۹] در $\mathbb{Z}^n$ است اگر انتقال‌های S به‌وسیله بردارهای T مجزا باشند، یعنی:

$$(X + S) \cap (Y + S) = \emptyset \qquad \forall X, Y \in T, X \neq Y$$

جایی‌که $X + S = \{X + s; s \in S\}$ می‌باشد.

تعریف ۱.۱.۳۱. می‌خواهیم مجموعه T که بردارهای آن مجزا هستند و تمام مشبکه $\mathbb{Z}^n$ را فرش[۲۰] می‌کند پیدا کنیم، یعنی:

$$(X + S) \cap (Y + S) = \emptyset \qquad \forall X, Y \in T, X \neq Y$$

و

$$\bigcup_{X \in T} (X + S) = \mathbb{Z}^n.$$

درواقع فرش کردن، متراکم‌ترین بسته‌بندی ممکن است.

تعریف ۱.۱.۳۲. اگر $(S,\mathcal{L})$ یک بسته‌بندی مشبکه‌ای باشند، آنگاه گوییم $\mathcal{L}$ یک کد خطی است. اگر $(S,\mathcal{L})$ فرش کردن باشد، گوییم T کد کامل است.

---

[۱۸] Lattice
[۱۹] Packing
[۲۰] Tiling

فصل ۲

کدهای کامل در سادک‌های گسسته

مطالعه کدهای کامل ریشه قدیمی دارد و شاید یکی از جالب‌ترین موضوعات در نظریه کدگذاری باشد. بهترین موضوع مطالعه شده کدهای دقیق در فضای متریک همینگ[۱] می‌باشد [۶، ۱۱، ۱۷، ۳۰، ۳۶، ۳۹]، در حالی‌که در تاریخ، اولین کدهایی هستند که تعریف شده‌اند و بسیاری از آنها عملاً استفاده شده‌اند. مثال‌های گوناگون جالبی در مجلات وجود دارد، نمونه هایی مثل کدهای کامل تحت متر لی[۲] [۲، ۳، ۱۵، ۲۱، ۲۳، ۲۴، ۳۴]، متر لیوشتین[۳] [۹، ۲۹]، کدها در فضای تصویری [۱۸]، گراسمانیان[۴] [۱۰، ۳۱] و غیره. نظریه‌ی دیلزارت[۵] [۱۸] روی عدم وجود کدهای ثابت وزن [۶] کامل تحت متر جانسون [۷] نیز مورد توجه تعدادی از محققان قرار گرفته است و هنوز حل نشده باقی مانده‌اند [۱۳، ۱۴، ۱۶، ۲۲، ۳۳، ۳۴]. خیلی از این مسائل را می‌توان به‌عنوان مثال‌های خاص از نظریه اساسی کدهای کامل در فاصله‌ی متغیر گرافها در نظر گرفت [۷].

در این فصل کدهای کامل را روی سادک‌های گسسته تحت متر d بررسی می‌کنیم و می‌بینیم که این کدها در الفباهای متفاوت در این فضا وجود دارند یا خیر [۲۸]. درواقع

[۱] hamming codes
[۲] Lee metric
[۳] Levenshtein
[۴] Grassmanian
[۵] Delsarte
[۶] Constant weight
[۷] Johnson metric

هدف اصلی در این فصل، بررسی قضیه زیر می‌باشد :

قضیه ۲.۰.۱. فرض کنید $e \geq ۱$:

۱. کد $e-$کامل غیربدیهی در $(\Delta_\ell^۱, d)$ برای هر $\ell \geq ۲e+۱$ وجود دارد. هر کد، $\lceil \frac{\ell+۱}{۲e+۱} \rceil$ کدواژه دارد.

۲. کد $e-$کامل غیربدیهی در $(\Delta_\ell^۲, d)$ وجود دارد اگر و تنها اگر $\ell = ۳e+۱$ باشد. علاوه‌براین، دقیقاً دو کد در $\Delta_{۳e+۱}^۲$ وجود دارد، که هر کدام از اندازه سه می‌باشند.

۳. هیچ کد $e-$کامل غیربدیهی در (Δ_ℓ^n, d)، $n \geq ۳$؛ برای هر n و ℓ وجود ندارد.

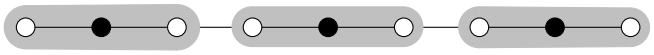
حال به بررسی و اثبات موارد بالا می‌پردازیم. برای این منظور از نمایش سادک Δ_ℓ^n برای فضای متریک (Δ_ℓ^n, d) به شکل گرافی با $\binom{n+\ell}{\ell}$ رأس که یالهای آن رئوس به فاصله یک از هم را متصل می‌کنند، استفاده می‌کنیم. همانطور که در بخش ۲.۱.۱ توجه کردید چنین نمایشی به ما اجازه می‌دهد که بتوانیم حداقل الفبای دودویی و سه‌تایی را در فضای مدنظرمان به تصویر بکشیم.

۱.۲ الفبای دودویی

حالت یک بعدی ($n = ۱$) را درنظر می‌گیریم. فضای :

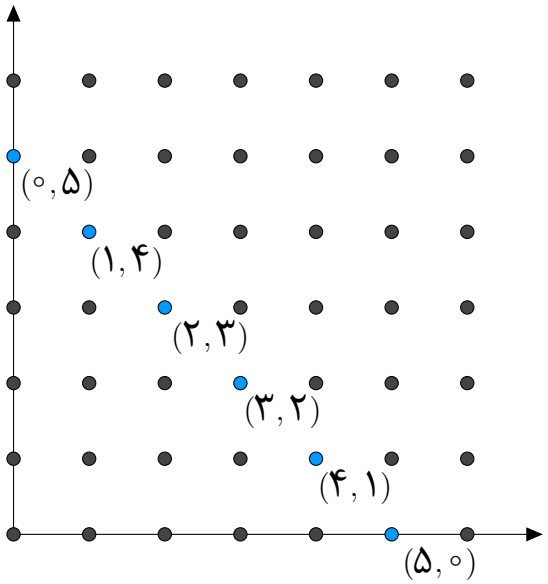
$$\Delta_\ell^۱ = \{(\ell - t, t) : t = ۰, \ldots, \ell\}, \tag{۱.۲}$$

را می‌توان بصورت مسیری با $|\Delta_\ell^۱| = \ell + ۱$ رأس نشان داد، برای مثال سمت چپ‌ترین رأس $(\ell, ۰)$ و سمت راست‌ترین آن $(۰, \ell)$ است، به شکل ۱.۲ توجه کنید.



شکل ۱.۲: کد ۱ ـ کامل در $\Delta_۸^۱$

همانطور که در شکل زیر پیداست ایده‌ی سادک گسسته از بعد یک، از محور زیر گرفته شده‌است. سادک گسسته از بعد یک و طول ℓ از سمت چپ $(۰, \ell)$ شروع می‌شود و به $(\ell, ۰)$ ختم می‌شود.



شکل ۲.۲: نمایش $\Delta_۵^۱$ در دستگاه مختصات

در حالت دودویی، گراف مسیر داریم و همچنین فاصله‌ی بین اولین و آخرین رأس ℓ می‌باشد در نتیجه قطر Δ_ℓ^1 برابر ℓ است و هر کدواژه از کد eـ کامل باید در فاصله‌ی بزرگتر یا مساوی $2e+1$ از یکدیگر قرار داشته باشد، در غیر اینصورت دو گوی در نقطه‌ای اشتراک پیدا می‌کنند که متناقض با تعریف است. به راحتی می‌توان نتیجه گرفت که برای هر مقدار ℓ، کد کامل وجود دارد. شکل ۱.۲ تصویری از یک کد کامل را نمایش می‌دهد و قضیه ۱.۱.۲ تمام کدهای کامل در Δ_ℓ^1 را بیان کرده است.

قضیه ۱.۱.۲. فرض کنید $\ell = q(2e+1)+r$ باشد که برای مقادیر $q \geq 1$ و $0 \leq r < 2e+1$ برقرار است، آنگاه دقیقاً $M = \min\{r+1, 2e+1-r\} > 0$ کد کامل در Δ_ℓ^1 وجود دارد که هر کدام $q+1 = \lceil \frac{\ell+1}{2e+1} \rceil$ کدواژه دارند. همچنین فرض کنید $s = \min\{r, e\}$ ، آنگاه همه‌ی کدهای کامل در Δ_ℓ^1 را می‌توان به‌فرم زیر نوشت :

$$\mathcal{C}_1^{(m)} = \{(\ell - s + m - 1 - i(2e+1), s - m + 1 + i(2e+1) : i = 0, \ldots, q\} \qquad (۲.۲)$$
$$\forall m = 1, \ldots, M.$$

برهان. قضیه را برای مقادیر ثابت j و برای i از صفر تا مقادیری بزرگ اثبات می‌کنیم. ابتدا چپ‌ترین کدواژه را $(\ell - j, j)$ فرض می‌کنیم. باتوجه به اینکه کدواژه‌های همسایه باید در فاصله‌ی $2e+1$ از یکدیگر باشند، کدواژه‌های دیگر را مشخص می‌کنیم. به عبارت دیگر می‌خواهیم مطمئن شویم که نواحی کدگشایی مجزا از هم هستند و تمام رئوس میانی پوشش داده می‌شوند. بنابراین برای اثبات کامل بودن $\mathcal{C}_1^{(m)}$، باید ثابت کنیم سراسر Δ_ℓ^1 پوشیده شده است. کافیست نشان دهیم نقاط پایانی $(\ell, 0)$ و $(0, \ell)$ پوشیده شده‌اند. فرض کنید $r \leq e$ باشد، در این حالت $s = r$ و همچنین داریم:

$$M = \min\{r+1, 2e+1-r\} = r+1$$

چون $s = r$ است، درنتیجه ادعا می‌کنیم $0 \leq s-m+1 \leq r \leq e$، آنگاه داریم $s-m+1 = r-m+1$ در صورتیکه m در ماکسیمم مقدارش باشد. یعنی $m = M$، آنگاه $s - m + 1 = 0$ است و در حالتی که m در مینیمم مقدارش باشد. یعنی $m = 1$، داریم $s - m + 1 = r$. از این رو رأس $(\ell, 0)$ در فاصله‌ی کمتر یا مساوی e از کدواژه $(\ell - s + m - 1, s - m + 1)$ قرار دارد. همچنین ادعا می‌کنیم $0 \leq r - s + m - 1 \leq r \leq e$ است. چون اگر m در مینیمم مقدارش باشد؛ یعنی، $m = 1$، آنگاه داریم $r - s + 1 - 1 = 0$. اگر m در ماکسیمم مقدارش باشد، یعنی $m = M$؛ آنگاه:

$$r - s + m - 1 = r + 1 - 1 = r \leq r \leq e$$

از این رو رأس $(\ell, 0)$ در فاصله‌ی کمتر یا مساوی e از کدواژه $(r - s + m - 1, \ell - r + s - m + 1)$ قرار دارد. تحلیل مشابهی برای $r > e$ بکار می‌رود. فرض کنید $r > e$باشد، لذا خواهیم داشت $M = 2e + 1 - r$ و $s = e$. در این صورت ادعا می‌کنیم $0 \leq s - m + 1 \leq e < r$ که رأس $(\ell, 0)$

در فاصله‌ی کمتر یا مساوی e از کدواژه $(\ell-s+m-۱,s-m+۱)$ قرار می‌گیرد. زیرا اگر m در حالت مینیمم مقدارش، یعنی $m=۱$ باشد، داریم:

$$s-m+۱=e-۱+۱=e\leq e,$$

و اگر در حالت ماکسیمم مقدارش، یعنی $m=۲e+۱-r$ باشد، آنگاه:

$$۰\leq s-m+۱=e-۲e-۱+r+۱=r-e\leq e,$$

از آنجایی‌که طبق فرض قضیه داریم $۰\leq r<۲e+۱$، لذا ماکسیمم مقدار r برابر $۲e$ می‌باشد و چون $r>e$، لذا $r-e>۰$ در نتیجه ماکسیمم مقدار $r-e$ برابر $۲e-e=e$ می‌باشد، بنابراین:

$$r-e\leq e<r,$$

بطور مشابه ادعا می‌کنیم $۰\leq r-s+m-۱\leq e<r$ است. چون برای حالت مینیمم مقدار m داریم :

$$r-s+m-۱=r-e+۱-۱=r-e\leq e<r,$$

و همچنین برای حالت ماکسیمم مقدارش داریم :

$$r-s+m-۱=r-e+۲e+۱-r-۱=e\leq e<r.$$

درنتیجه فاصله‌ی رأس $(۰,\ell)$ از کدواژه $(r-s+m-۱,\ell-r+s-m+۱)$ کمتر یا مساوی e می‌باشد.

حال کافی است نشان دهیم که تمام کدهای کامل در $\Delta_\ell^۱$ به فرم (۲.۲) می‌باشند. برای این منظور، فرض کنید $r\leq e$ باشد، در این حالت چپ‌ترین کدواژه از $\mathcal{C}_۱^{(m)}$ ، برابر $(\ell-r+m-۱,r-m+۱)$ است که $m=۱,\ldots,r+۱$. بنابراین $r+۱$ کد با چپ‌ترین کدواژه‌های $(\ell,۰),\ldots,(\ell-r,r)$ پیدا می‌کنیم. فرض کنید می‌خواهیم کد کامل دیگری به‌وسیله $(\ell-r-k,r+k)$ ، که $k\geq ۰$ است، بسازیم. در این صورت این چپ‌ترین کدواژه است. از آنجایی‌که نقطه پایانی $(\ell,۰)$ پوشیده شده‌است، پس برای اینکه فاصله $(\ell,۰)$ از $(\ell-r-k,r+k)$ کمتر از e باشد داریم $k\leq e-r$. از این رو می توان نتیجه گرفت $k\leq e$ می‌باشد. راست‌ترین کدواژه با جابجایی $i(۲e+۱)$ بدست می‌آید و برابر با $(۲e+۱-k,\ell-۲e-۱+k)$ یا $(-k,\ell+k)$ است. دومین حالت مختصات منفی دارد . درنتیجه غیرممکن است و اولین حالت، کد کامل نمی‌دهد چون نقطه $(۰,\ell)$ در ناحیه کدگشایی چنین کدواژه‌ای نیست، زیرا فاصله از راست‌ترین کدواژه $۲e+۱-k>e$ می‌باشد.

حال برای حالت $r>e$ هم بطور مشابه اثبات می‌شود. فرض کنید $r>e$ باشد، آنگاه داریم $m=۱,\ldots,۲e+۱-r$. چپ‌ترین کدواژه از $\mathcal{C}_۱^{(m)}$ برابر $(\ell-r-m+۲e+۱,r+m-۲e-۱)$ است. بنابراین $۲e+۱-r$ تا کد با چپ‌ترین کدواژه‌های $(\ell,۰),\ldots,(\ell-۲e+r,۲e-r)$ پیدا می‌کنیم. فرض کنید می‌خواهیم کد کامل دیگری به وسیله رأس $(\ell-۲e+r-k,۲e-r+k)$ که $k\geq ۰$ است، بسازیم؛ در این صورت این چپ‌ترین کدواژه می‌باشد. از آنجاییکه $(\ell,۰)$ پوشیده

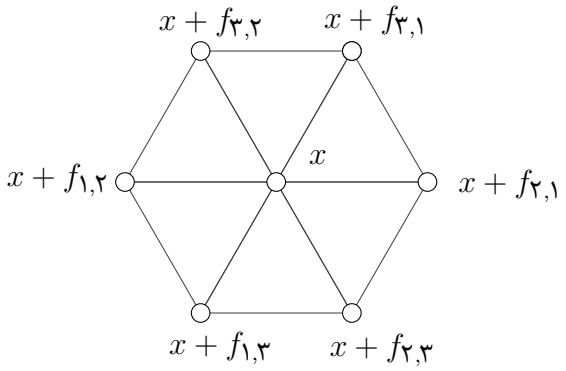
شده است پس فاصله‌ی $(\ell, \circ)$ و $(\ell - ۲e + r - k, ۲e - r + k)$ باید کمتر از e باشد، درنتیجه $k \leq r - e$ است، پس $k \leq r$. راست‌ترین کدواژه با جابجایی $i(۲e + ۱)$ بدست می‌آید و برابر با $(-k, \ell + k)$ یا $(-۱ - k, \ell + k + ۱)$ می‌باشد که در هر دو صورت مختصات منفی بدست آمده که ممکن نیست این کدواژه وجود داشته باشد.

□

۲.۲ الفبای سه‌تایی

حال سادک $\Delta^{۲}_{\ell}$ یعنی فضای دو بعدی را بررسی می‌کنیم. گراف متناظر با این فضا، گرافی مشبک و مثلثی می‌باشد که در شکل ۳.۲ نشان داده شده‌است. فرض کنید $(\ell,۰,۰)$ چپ‌ترین رأس و $(۰,\ell,۰)$ راست‌ترین رأس و $(۰,۰,\ell)$ رأس بالایی باشد. گوی‌های تحت متر d در این گراف شش ضلعی هستند. درحقیقت این فضا مثلثی بریده شده از شبکه شش ضلعی به‌نظر می‌رسد.

حال $x \in \Delta^{۲}_{\ell}$ را درنظر بگیرید. هر رأس $y \in \Delta^{۲}_{\ell}$ در یک مسیر از x به y در گراف متناظر قرار دارد. اولین رأس از این مسیر را x' می‌نامیم که مجاور x است و دومین رأس، مجاور x' است و ... . نقاط مجاور $x = (x_۰, x_۱, x_۲)$ یعنی نقاطی که در فاصله‌ی یک از آن قرار دارند. بهترین روش برای تعریف نقاط مجاور و مسیرها در $\Delta^{۲}_{\ell}$ استفاده از بردار است. از تعریف بردارها نتیجه می‌گیریم که $f_{i,j} = -f_{j,i}$ است و به عنوان قرارداد داریم $f_{i,i} = (۰,۰,۰)$.



شکل ۳.۲: همسایه‌های x در $\Delta^{۲}_{\ell}$

این بردارها تمام جهت‌های ممکن از هر رأس را تعریف می‌کنند و درنتیجه هر همسایه x' از x به‌وسیله بردار تعریف می‌شود. یعنی $x' = x + f_{i,j}$. بنابراین برای هر $y \in \Delta^{۲}_{\ell}$ و $\alpha_{i,j} \geq ۰$ رابطه زیر برقرار است:

$$y = x + \sum_{i,j} \alpha_{i,j} f_{i,j}.$$

اگر $d(x,y) = \delta$ باشد و چون $\frac{۱}{۲} \sum_{i,j} |f_{i,j}| = ۱$ است، آنگاه داریم $\sum_{i,j} \alpha_{i,j} = \delta$ در حقیقت می‌توانیم بنویسیم:

$$y = x + (s_۰, s_۱, s_۲).$$

درآیه‌های $f_{i,j}$ از ۱ و ۱− و صفر تشکیل شده است. درنتیجه مجموع درآیه‌های آن همیشه برابر صفر خواهد بود، یعنی داریم $\sum_i s_i = ۰$. همچنین:

$$y - x = (s_۰, s_۱, s_۲),$$

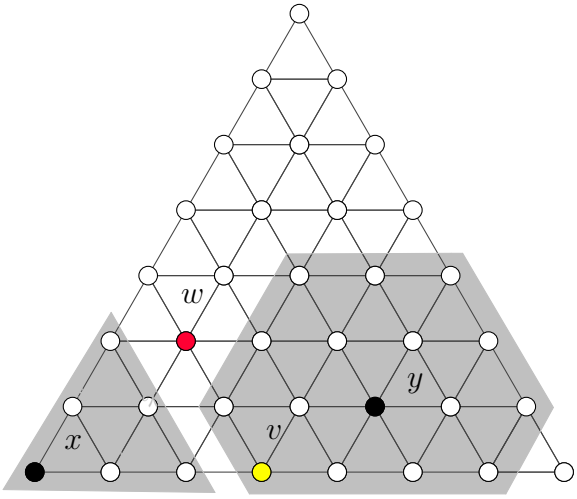
درنتیجه:

$$۲d(x,y) = \sum_i |s_i|,$$

از طرفی از قبل داشتیم :

$$d(x,y) = \delta = \frac{۱}{۲} \sum |s_i|,$$

بنابراین $\sum_i |s_i| = ۲\delta$ می‌باشد. لم زیر در اثبات قضایای بعدی استفاده خواهد شد.



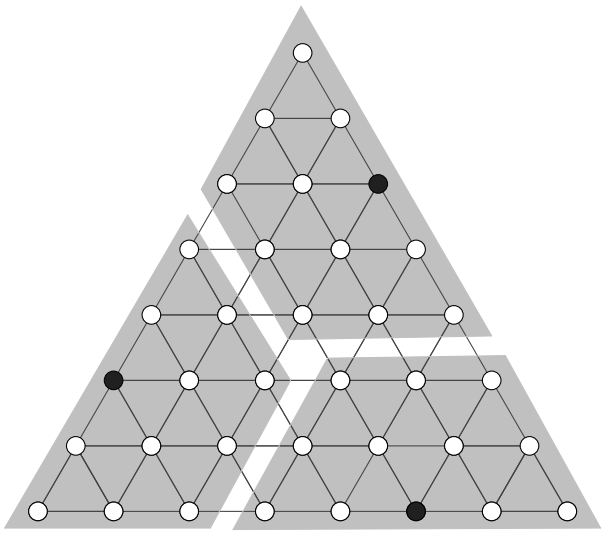
شکل ۴.۲: تصویر لم ۱.۲.۲

لم ۱.۲.۲. فرض کنید $x, y, z \in \Delta_\ell^۲$ باشد، بطوری‌که داشته باشیم $d(x,w) = d(y,w) = e+۱$، $d(x, w + f_{۱,۲}) = e$ و $d(y, w + f_{۲,۱}) = e$. آنگاه هیچ $z \in \Delta_\ell^۲$ نمی‌توان یافت که $w \in \mathcal{B}(z,e)$ و $\mathcal{B}(x,e) \cap \mathcal{B}(z,e) = \emptyset$ و $\mathcal{B}(y,e) \cap \mathcal{B}(z,e) = \emptyset$ برقرار باشد.

حال مفهوم این لم را شرح می‌دهیم. فرض کنید دو کدواژه‌ی x و y و یک رأس w که خارج از فضای کدگشایی آنها قرا دارد، داشته باشیم. می‌خواهیم کد کاملی بسازیم که w در فضای کدگشایی سومین کدواژه یعنی z باشد. این لم ادعا می‌کند که اگر w توسط $\mathcal{B}(y,e)$ و $\mathcal{B}(x,e)$ در بعضی جهت‌ها محدود شده‌باشد، در این صورت چنین کدواژه‌ای وجود ندارد، درنتیجه x و y نمی‌توانند کدواژه های کد کامل باشند.

حال به ادعای اصلی یعنی وجود یا عدم وجود کدهای کامل می‌پردازیم. اگر $\ell = ۳e + ۱$ باشد، آنگاه ارائه یک کد کامل کار چندان سختی نیست(مانند شکل ۵.۲). در حقیقت دقیقاً دو کد کامل در این فضا وجود دارد که عبارت است از:

$$\mathcal{C}_۲^{(۱)} = \{(۲e+۱, e, ۰), (۰, ۲e+۱, e), (e, ۰, ۲e+۱)\},$$
$$\mathcal{C}_۲^{(۲)} = \{(۲e+۱, ۰, e), (e, ۲e+۱, ۰), (۰, e, ۲e+۱)\}.$$



شکل ۵.۲: کد ۲ ـ کامل در $\Delta_۷^۲$

قضیه ۱.۲.۲. کدهای $\mathcal{C}_۲^{(۱)}$ و $\mathcal{C}_۲^{(۲)}$ در $\Delta_{۳e+۱}^۲$ کد eـ کامل هستند.

برهان. ابتدا ثابت می‌کنیم $\mathcal{C}_۲^{(۱)}$ کامل است. با توجه به تعریف کد کامل و خواص آن باید ثابت کنیم که هر دو کدواژه‌ی دلخواهی که از $\mathcal{C}_۲^{(۱)}$ درنظر بگیریم دارای فاصله‌ی $۲e+۱$ هستند و همچنین باید مجموع درآیه‌های هر کدواژه برابر با ℓ باشد. فرض کنید کدواژه‌ها بصورت زیر نامگذاری شوند :

$$\mathcal{C}_۲^{(۱)} = \{a = (۲e+۱, e, ۰), \quad b = (۰, ۲e+۱, e), \quad c = (e, ۰, ۲e+۱)\}$$

حال باتوجه به تعریف متری که تعریف شده فاصله‌ی بین کدواژه بصورت زیر بدست می‌آید :

$$d(a, b) = ۲e + ۱$$

$$d(b, c) = ۲e + ۱$$

$$d(a,c) = ۲e+۱$$

همچنین مجموع درآیه‌های کدواژه‌های a و b و c برابر با $۳e+۱$ می‌باشد که همان ℓ است.
برای اثبات کامل بودن $\mathcal{C}_۲^{(۲)}$ همین روند را تکرار می‌کنیم و خواهیم داشت :

$$\mathcal{C}_۲^{(۲)} = \{a' = (۲e+۱, ۰, e), \quad b' = (e, ۲e+۱, ۰), \quad c' = (۰, e, ۲e+۱)\}$$

آنگاه:

$$d(a', b') = ۲e+۱$$

$$d(b', c') = ۲e+۱$$

$$d(a', c') = ۲e+۱$$

همچنین مجموع درآیه‌های کدواژه‌های a' و b' و c' برابر با $۳e+۱$ می‌باشد، که همان ℓ است.
درنتیجه حکم ثابت شد.

□

در بخش بعدی حالت جامع‌تری از قضیه ۱.۲.۲ را اثبات می‌کنیم. یعنی وقتی $\ell = ۳e+۱$ باشد، فقط دو کد کامل وجود دارد و اگر $\ell \neq ۳e+۱$ باشد، هیچ کد کاملی وجود ندارد.
رأس $(\ell, ۰, ۰)$ را درنظر بگیرید. برای اینکه این رأس پوشیده شود باید کدواژه‌ای به فرم زیر وجود داشته باشد:

$$x = (\ell - t, x_۱, x_۲), \tag{۳.۲}$$

که $x_۱ + x_۲ = t \geq e$ است. فرض کنید رأس زیر را داشته باشیم:

$$v = (\ell - x_۱ - e - ۱, x_۱ + e + ۱), \tag{۴.۲}$$

در نتیجه داریم:

$$d(x,v) = \frac{۱}{۲}(e+۱-x_۲+e+۱+x_۲) = e+۱ \not< e.$$

پس v توسط گوی $\mathcal{B}(x,e)$ پوشیده نمی‌شود. برای اینکه v پوشیده شود به کدواژه دیگری مانند y نیاز است کهداشته باشیم $d(v,y) = e$ و $d(x,y) = ۲e+۱$.

لم ۲.۲.۲. فرض کنید $x, v \in \Delta_\ell^۲$ به ترتیب از (۳.۲) و (۴.۲) داده شده است. در این صورت رأس $y \in \Delta_\ell^۲$ وجود دارد بطوری‌که $d(v,y) = e$ و $d(x,y) = ۲e+۱$. در این صورت y به فرم زیر است:

$$y = (\ell - x_۱ - ۲e - ۱, x_۱ + e + ۱ + u, e - u), \tag{۵.۲}$$

جایی‌که $۰ \leq u \leq e$. با این خاصیّت که:

$$x_۲ > ۰ \Rightarrow u = e. \tag{۶.۲}$$

برهان. فرض کنید برای هر $s \in \mathbb{Z}$ داشته باشیم $y = (\ell - x_۱ - ۲e - ۱ + s, y_۱, y_۲)$. اگر $s < ۰$ باشد، آنگاه:

$$d(v, y) \geq v_۰ - y_۰ = e - s > e$$

که تناقض با فرض قضیه است. در نتیجه $s > ۰$ می‌باشد. حال فرض کنید $x_۰ \leq y_۰$ باشد، آنگاه:

$$d(x, (\ell, ۰, ۰)) \leq e$$

و

$$d(y, (\ell, ۰, ۰)) \leq e$$

در اینصورت رأس $(\ell, ۰, ۰)$ هم توسط x و هم توسط y پوشیده می‌شود، در نتیجه داریم $x_۰ > y_۰$. حال فرض می‌کنیم $s \leq x_۱$ باشد، چون در غیر اینصورت خواهیم داشت:

$$x_۰ - y_۰ \leq ۲e - t.$$

همچنین مجموع مابقی x_iها برابر t می‌باشد. از آنجایی‌که x و y هردو کدواژه‌اند پس باید فاصله‌ی بین آنها $۲e + ۱$ باشد، در حالی که به تناقض رسیدیم.

$$\begin{aligned} d(x, y) &= \sum_{x_i > y_i} (x_i - y_i) = x_۰ - y_۰ + \sum_{i > ۰, x_i > y_i} (x_i - y_i) \\ &\leq x_۰ - y_۰ + \sum_{i > ۰} x_i \leq ۲e. \end{aligned} \tag{۷.۲}$$

در نتیجه فرض می‌کنیم $s > x_۱$ باشد:

$$\begin{aligned} x_۰ - y_۰ &= \ell - t - (\ell - x_۱ - ۲e - ۱ + s) \\ &= x_۱ + ۲e + ۱ - t - s \\ &= (۲e - t) + (x_۱ + ۱ - s) \\ &\leq ۲e - t \end{aligned} \tag{۸.۲}$$

حالت تساوی وقتی اتفاق می‌افتد که داشته باشیم $s = x_۱ + ۱$. همچنین داریم $v_۰ - y_۰ = e - s < e$ و $y_۲ \geq v_۲ = ۰$. حال برای اینکه تساوی $d(v, y) = e$ برقرار باشد، باید داشته باشیم :

$$\begin{aligned} &v_۱ - y_۱ = x_۱ + e + ۱ - y_۱ = s \\ &y_۱ = x_۱ - s + e + ۱ \geq e + ۱ > x_۱ \Longrightarrow x_۱ < e + ۱ \end{aligned} \tag{۹.۲}$$

از قبل داشتیم $y_۰ < x_۰$، همچنین از (۹.۲) داریم:

$$y_۱ - x_۱ = e + ۱ - s$$

برای اینکه رابطه $d(x,y)=۲e+۱$ برقرار باشد باید داشته باشیم $y_۲-x_۲=e+s$. امّا غیرممکن است، زیرا:

$$y_۲-x_۲\le y_۲=\ell-y_۰-y_۱=e<e+s$$

$$y_۲=\ell-y_۰-y_۱=\ell-(\ell-x_۱-۲e-۱+s)-(x_۱-s+e+۱)=e$$

بنابراین نتیجه می‌گیریم که s باید صفر باشد. دراین صورت داریم $v_۰-y_۰=e$ و $d(v,y)=e$. همچنین باید داشته باشیم:

$$y_۱\ge v_۱=x_۱+e+۱.$$

این رابطه نشان می‌دهد که y دقیقاً به فرم (۵.۲) است. برای اثبات قسمت آخر ادعا می‌توان دید که $y_۰<x_۰$ است و همچنین $y_۱-x_۱=e+۱+u$ و $d(x,y)=۲e+۱$ برقرار است، پس تساوی $y_۲-x_۲=e-u$ زمانی صحیح است که $u<e$ باشد ولی داریم $y_۲=e-u$. این در صورتی صحیح است که $x_۲=۰$ باشد. □

باتوجه به قضیه قبل فرض کنید دو کدواژه به فرم (۳.۲) و (۵.۲) داریم و فرض کنید رأس w به فرم زیر باشد:

$$w=(\ell-t-e-۱,x_۱+u,\max\{x_۲,y_۲\}+۱) \qquad (۱۰.۲)$$

بطوری‌که داشته باشیم $y_۲=e-u$. برای اینکه نشان دهیم $w\in\Delta_\ell^۲$ است، دو حالت را درنظر می‌گیریم:

۱. اگر $x_۲>۰$ باشد، آنگاه از (۶.۲) خواهیم داشت $y_۲=e-u=۰$ و $\max\{x_۲,y_۲\}=x_۲$ که $\sum_i w_i=\ell$ می‌باشد.

۲. اگر $x_۲=۰$ باشد، آنگاه $x_۱=t$ و $\max\{x_۲,y_۲\}=y_۲$. همچنین داریم $\sum_i w_i=\ell$. علاوه‌براین تساوی $d(x,w)=d(y,w)=e+۱$ برقرار است.

درنتیجه می‌توان گفت اگر $x_۲>۰$ باشد، آنگاه داریم $y_۲=e-u$ و درنتیجه:

$$y=(\ell-x_۱-۲e-۱,x_۱+۲e+۱,۰),$$

و

$$w=(\ell-t-e-۱,x_۱+e,x_۲+۱),$$

اگر $x_۲=۰$ باشد، آنگاه:

$$y=(\ell-t-۲e-۱,t+۲e+۱+u,e-u),$$

و

$$w=(\ell-t-e-۱,t+u,y_۲+۱).$$

لم ۳.۲.۲. فرض کنید $x,y,w\in\Delta_\ell^۲$ باشند، بطوری‌که

$$d(x,w)=d(y,w)=e+۱,$$

$$d(x,w+f_{m,\ell})=d(x,w+f_{k,\ell})=d(x,w+f_{k,m})=e.$$

درحقیقت w خارج از ناحیه‌ی کدگشایی x و y می‌باشد. امّا همسایه‌ها در امتداد سه جهت متوالی نیستند. آنگاه رأس z بطوری‌که $w\in\mathcal{B}(z,e)$ باشد و داشته باشیم $\mathcal{B}(z,e)\cap\mathcal{B}(x,e)=\mathcal{B}(y,e)\cap\mathcal{B}(z,e)=\emptyset$ روی جهت $f_{\ell,k}=-f_{k,\ell}$ وجود دارد، یعنی $z=w+ef_{\ell,k}$.

لم ۴.۲.۲. فرض کنید $x,y\in\Delta_\ell^۲$ به ترتیب از (۳.۲) و (۶.۲) داده شده باشد، بنابراین اگر $t<e$ یا $t=e$ درحالی‌که $۰<x_۱<e$، آنگاه x و y نمی‌توانند کد eـ کامل باشند.

برهان. ابتدا فرض کنید $x_۲>۰$ باشد. آنگاه باتوجه به نکات قبل $u=e$ است، در نتیجه:

$$y=(\ell-x_۱-۲e-۱,x_۱+۲e+۱,۰),$$

و طبق (۱۰.۲) w به‌فرم زیر می‌باشد:

$$w=(\ell-t-e-۱,x_۱+e,x_۲+۱),$$

بنابراین داریم:

$$w+f_{۱,۲}=(\ell-t-e,x_۱+e-۱,x_۲+۱),$$

و

$$w+f_{۲,۱}=(\ell-t-e-۲,x_۱+e+۱,x_۲+۱),$$

با استفاده از تعریف متر به این نتیجه می‌رسیم که $d(x,w)=d(y,w)=e+۱$ برقرار است و همچنین داریم $d(x,w+f_{۱,۲})=d(y,w+f_{۲,۱})=e$. برقراری رابطه دوم نیازمند دانستن این است که $t<e$ است یا $t=e$ می‌باشد در حالی‌که $x_۱>۰$ باشد. با استفاده از لم ۱.۲.۲ به این نتیجه می‌رسیم که کدواژه z که ناحیه کدگشایی‌اش شامل w و جدا از ناحیه کدگشایی x و y باشد، وجود ندارد.

حال فرض کنید $x_۲=۰$ باشد. اگر $u>۰$، آنگاه:

$$x=(\ell-x_۱,x_۱,۰),$$
$$y=(\ell-x_۱-۲e-۱,x_۱+e+u+۱,e-u),$$
$$w=(\ell-x_۱-e-۱,x_۱+u,e-u+۱),$$
$$w+f_{۱,۲}=(\ell-x_۱-e,x_۱+u-۱,e-u+۱),$$

درنتیجه روابط زیر را خواهیم داشت :

$$d(x,w)=d(y,w)=e+۱\quad,\quad d(x,w+f_{۱,۲})=d(y,w+f_{۲,۱})=e$$

و با استفاده از لم ۱.۲.۲ نتیجه به‌دست می‌آید.
در نهایت اگر داشته باشیم $x_۲ = ۰$ و $u = ۰$، آنگاه :

$$y = (\ell - x_۱ - ۲e - ۱, x_۱ + e + ۱, e),$$
$$w = (\ell - x_۱ - e - ۱, x_۱, e + ۱),$$
$$w + f_{۱,۳} = (\ell - x_۱ - e, x_۱, e),$$
$$w + f_{۲,۳} = (\ell - x_۱ - e - ۱, x_۱ + ۱, e),$$
$$w + f_{۲,۱} = (\ell - x_۱ - e - ۲, x_۱, e + ۱),$$

بنابراین خواهیم داشت:

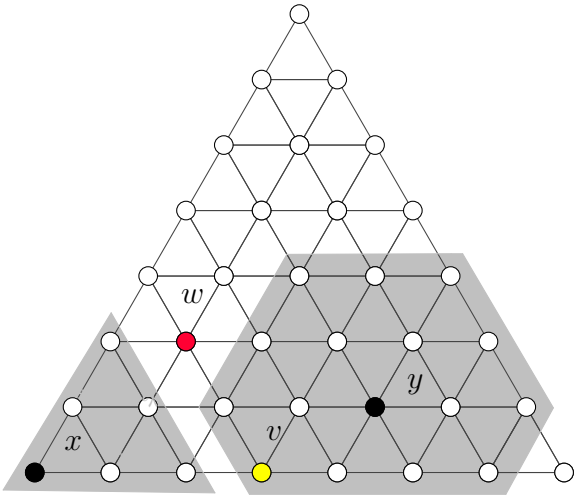
$$d(x, w) = d(y, w) = e + ۱,$$

$$d(x, w + f_{۱,۳}) = e \quad , \quad d(y, w + f_{۲,۳}) = d(y, w + f_{۲,۱}) = e.$$

با استفاده از لم ۳.۲.۲ به این نتیجه می‌رسیم که کدواژه z برای اینکه بتواند w را پوشش دهد باید به فرم زیر باشد :

$$z = w + ef_{۲,۳} = (\ell - x_۱ - e - ۱, x_۱ - e, ۲e + ۱),$$

اما این غیرممکن است زیرا فرض کرده بودیم که $x_۱ < e$ است در این صورت دومین درآیه z منفی خواهد شد و به تناقض می‌رسیم، درنتیجه حکم ثابت می‌شود.



شکل ۶.۲: تصویر لم۴.۲.۲

□

قضیه ۲.۲.۲. هیچ کد eـ کاملی در $\Delta_\ell^۲$ وقتی‌که $\ell \neq ۳e+۱$ باشد، وجود ندارد.

برهان. حالت خاصی از قضیه در شکل ۷.۲ نمایش داده شده‌است. در اینجا حالت کلی‌تر را اثبات می‌کنیم. با توجه به استدلال‌های قبلی می‌توانیم فرض کنیم که رأس $(\ell-e,۰,e)$ یک کدواژه است. حال رأس $v=(\ell-e-۱,e+۱,۰)$ را در نظر بگیرید. با استفاده از لم ۲.۲.۲ نتیجه می‌گیریم به جهت پوشیده شدن v، باید $y=(\ell-۲e-۱,۲e+۱,۰)$ را کدواژه درنظر بگیریم. همچنین باید $\ell \geq ۲e+۱$ باشد تا کد کامل داشته باشیم. حال $w=(\ell-۲e-۱,e,e+۱)$ را در نظر بگیرید. داریم $d(x,w)=d(y,w)=e+۱$. بنابراین باید کدواژه سومی مانند z وجود داشته باشد که w را پوشش دهد. همچنین توجه کنید که داریم:

$$d(y,w+f_{۲,۳})=d(x,w+f_{۱,۲})=d(x,w+f_{۱,۳})=e,$$

پس باتوجه به لم ۳.۲.۲ نتیجه می‌گیریم که کدواژه‌ای مانند z به فرم $w+ef_{۳,۱}$ وجود دارد. درحقیقت یعنی $z=(\ell-۳e-۱,e,۲e+۱)$، بنابراین برای داشتن کد کامل باید $\ell \geq ۳e+۱$ باشد. از قبل حالت $\ell=۳e+۱$ بررسی شده است، لذا فرض کنید $\ell > ۳e+۱$ باشد. حال رأس $u=(\ell-۳e-۲,۲e+۱,e+۱)$ را در نظر بگیرید. داریم $d(z,u)=d(y,u)=e+۱$ و $d(x,u)=۲e+۲$. بنابراین برای اینکه پوشیده شدن u به چهارمین کدواژه مانند q نیاز داریم. از آنجایی‌که داریم $d(z,u+f_{۱,۲})=d(z,u+f_{۳,۲})=d(y,u+f_{۱,۳})=e$، طبق لم ۳.۲.۲ نتیجه می‌گیریم که $q=(\ell-۴e-۲,۳e+۱,e+۱)$ است. درنتیجه باید $\ell \geq ۴e+۱$ باشد تا کد کامل داشته باشیم. درنهایت رأس $p=(\ell-۳e-۲,۳e+۲,۰)$ را درنظر بگیرید. فاصله‌ی کدواژه‌های x ، y ، z و q بیشتر از e است و در نتیجه به کدواژه‌ی دیگری برای پوشش آن نیاز داریم. ولی با توجه به اینکه داریم:

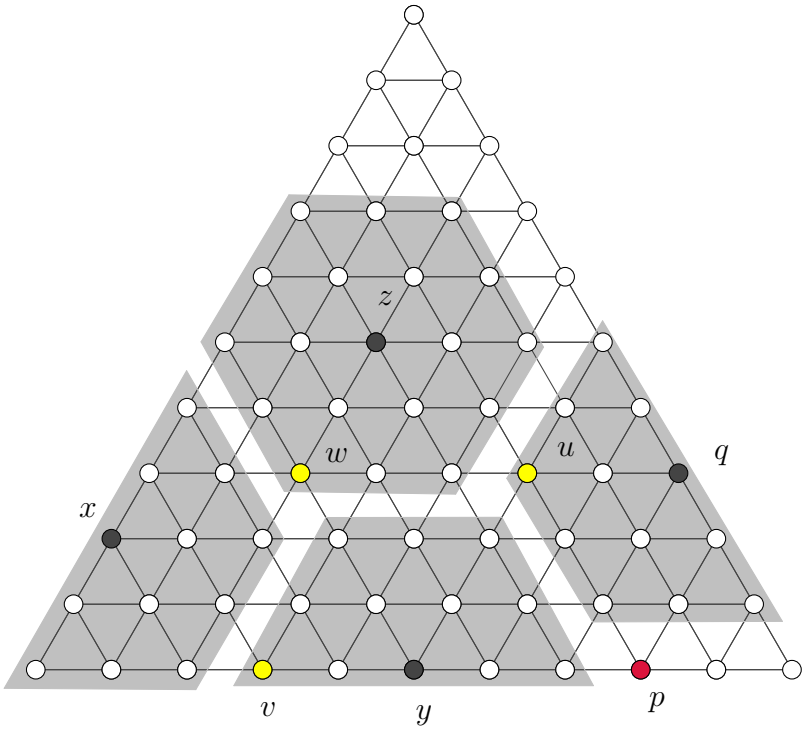
$$d(q,p)=d(y,p)=e+۱$$

و

$$d(q,p+f_{۳,۱})=d(q,p+f_{۳,۲})=d(y,p+f_{۱,۲})=e$$

این کدواژه را باید بصورت $p+ef_{۲,۳}=(l-۳e-۲,۴e+۲,-e)$ داشته باشیم که غیرممکن است چون درآیه منفی دارد.

□



شکل ۷.۲: تصویر قضیه ۲.۲.۲

۳.۲ کدهای کامل در سادک‌های گسسته با ابعاد بالاتر

در این بخش مراتب بالاتر را بررسی می‌کنیم. مانند دو بعد قبلی می‌توان گفت برای هر $x \in \Delta_\ell^n$ رأسی مانند $y \in \Delta_\ell^n$ وجود دارد که یک مسیر از x به y را می‌توان یافت. اینکار با استفاده از بردارهای $f_{i,j}$ که مشابه قبل در iـامین جایگاه ۱ و در jـامین جایگاه ۱− قرار می‌گیرد. به عنوان مثال :

$$f_{1,2} = (1, -1, 0, \ldots, 0).$$

یعنی برای هر $y \in \Delta_\ell^n$ می‌توان نوشت :

$$y = x + \sum_{i,j} \alpha_{i,j} f_{i,j}, \qquad (11.2)$$

که برای هر مقدار صحیح $\alpha_{i,j} \geq 0$ برقرار است. اگر $d(x,y) = \delta$ آنگاه y با این ویژگی ها وجود دارد بطوری‌که $\sum_{i,j} \alpha_{i,j} = \delta$ است.

ادعای بعدی ما همان لم ۱.۲.۲ است که به ابعاد بالاتر تعمیم داده شده‌است. فرض کنید دو کدواژه x و y در اختیار است که رأس w خارج از فضای کدگشایی آن دو قرار دارد. این لم ادعا می‌کند که اگر w توسط $\mathcal{B}(x,e)$ و $\mathcal{B}(y,e)$ از جهتی مانند $f_{1,2}$ محدود شده باشد، آنگاه کدواژه z که w را پوشش می‌دهد در زیرفضای متعامد $f_{1,2}$ قرار دارد. یعنی z باید به فرم زیر

باشد:

$$z = w + (۰, ۰, s_۲, \dots, s_n), \tag{۱۲.۲}$$

درحالی‌که $\sum_i s_i = ۰$ و $\sum_i |s_i| = ۲e$ می‌باشد.

لم ۱.۳.۲. فرض کنید $x, y, w \in \Delta_\ell^n$ باشد، بطوری‌که

$$d(x, w) = d(y, w) = e + ۱$$

$$d(x, w + f_{۱,۲}) = e$$

$$d(y, w + f_{۲,۱}) = e$$

برقرار باشد. آنگاه رأس z بطوری‌که $w \in \mathcal{B}(z, e)$ باشد و روابط $\mathcal{B}(x, e) \cap \mathcal{B}(z, e) = \emptyset$ و $\mathcal{B}(y, e) \cap \mathcal{B}(z, e) = \emptyset$ برقرار باشد، باید به فرم زیر باشد:

$$z = w + \sum_{i,j \notin \{۱,۲\}} \alpha_{i,j} f_{i,j}, \tag{۱۳.۲}$$

بطوری‌که $\alpha_{i,j} \geq ۰$ و $\sum_{i,j \notin \{۱,۲\}} \alpha_{i,j} = e$ می‌باشد.

برهان. رأس z در فاصله‌ی e از w قرار دارد، چون اگر فاصله بیشتر باشد آنگاه گوی $\mathcal{B}(z, e)$ شامل w نمی‌شود و اگر فاصله کمتر باشد آنگاه $\mathcal{B}(y, e)$ و $\mathcal{B}(x, e)$ تداخل پیدا می‌کنند. بنابراین می‌توان گفت:

$$z = w + \sum_{i,j} \alpha_{i,j} f_{i,j}, \tag{۱۴.۲}$$

درحالی‌که داریم $\alpha_{i,j} \geq ۰$ و $\sum_{i,j} \alpha_{i,j} = e$. باید نشان دهیم در چنین حالتی باید $\alpha_{i,j} = ۰$ باشد درصورتی‌که $i \in \{۱,۲\}$ یا $j \in \{۱,۲\}$ است. فرض کنید درست نباشد و برای مثال داشته باشیم $\alpha_{۱,۳} > ۰$. از آنجایی‌که می‌دانیم $f_{۱,۳} = f_{۱,۲} + f_{۲,۳}$ می‌توانیم بنویسیم :

$$\begin{aligned} z &= w + f_{۱,۲} + f_{۲,۳} + (\alpha_{۱,۳} - ۱)(f_{۱,۳}) + \sum_{(i,j) \neq (۱,۳)} \alpha_{i,j} f_{i,j} \\ &= w + f_{۱,۲} + \sum_{i,j} \beta_{i,j} f_{i,j}, \end{aligned} \tag{۱۵.۲}$$

جایی‌که $\beta_{i,j} \geq ۰$ و $\sum_{i,j} \beta_{i,j} = e$ باشد که یعنی $d(z, w + f_{۱,۲}) = e$، امّا در فرض داشتیم $d(x, w + f_{۱,۲}) = e$، به این معنی که $\mathcal{B}(x, e) \cap \mathcal{B}(z, e) = \emptyset$ می‌باشد که تناقض است. □

ملاحظه ۱.۳.۲. جهت‌های متعامد در سادک دو بعدی $\Delta_\ell^۲$ وجود ندارد، باتوجه به مفهوم لم قبلی اگر w بین $\mathcal{B}(x, e)$ و $\mathcal{B}(y, e)$ قرار گرفته باشد، آنگاه هیچ z ای با این خصوصیات وجود ندارد که $w \in \mathcal{B}(z, e)$ باشد و داشته باشیم $\mathcal{B}(z, e) \cap \mathcal{B}(x, e) = \emptyset$ و $\mathcal{B}(z, e) \cap \mathcal{B}(y, e) = \emptyset$. این دقیقاً همان حکم لم ۱.۲.۲ است.

در ادامه عدم وجود کدهای کامل را اثبات می‌کنیم. همانطور که در دو بخش قبلی داشتیم، با درنظر گرفتن رأس $(\ell, ۰, \dots, ۰)$ شروع می‌کنیم. برای اینکه این رأس پوشیده شود باید کدواژه‌ای به فرم زیر وجود داشته باشد :

$$x = (\ell - t, x_۱, \dots, x_n), \tag{۱۶.۲}$$

درحالی‌که $x_۱ + \dots + x_n = t \le e$ است. بدون از دست دادن کلیّت مسأله فرض می‌کنیم $x_۱ > ۰$ باشد، همچنین داشته باشیم $t > ۰$. حال رأس زیر را درنظر بگیرید :

$$v = (\ell - x_۱ - e - ۱, x_۱ + e + ۱, ۰, \dots, ۰), \tag{۱۷.۲}$$

داریم $d(x,v) = e + ۱$. بنابراین رأس v توسط $\mathcal{B}(x,e)$ پوشیده نمی‌شود، برای اینکه پوشیده شود به کدواژه دیگری مانند y نیاز است که $d(v,y) = e$ و $d(x,y) = ۲e + ۱$ باشد.

لم ۲.۳.۲. رأس y که در روابط $d(v,y) = e$ و $d(x,y) = ۲e + ۱$ صدق می‌کند به فرم زیر است:

$$y = (\ell - x_۱ - ۲e - ۱, x_۱ + e + ۱ + u, y_۲, \dots, y_n), \tag{۱۸.۲}$$

که $۰ \le u \le e$ و $y_۲ + \dots + y_n = e - u$ است و با این ویژگی که اگر:

$$x_i > ۰ \Rightarrow y_i = ۰, \quad i = ۲, \dots, n \tag{۱۹.۲}$$

برهان. فرض کنید $y = (\ell - x_۱ - ۲e - ۱ + s, y_۱, \dots, y_n)$ باشد بطوری‌که $s \in \mathbb{Z}$ است اگر $s < ۰$، آنگاه $d(v,y) \ge v_۰ - y_۰ = e - s > e$ می‌باشد که با یکی از فرض‌های لم در تناقض است. نشان داده می‌شود حالت $s > ۰$ همیشه غیرممکن است. فرض کنید $x_۰ > y_۰$ باشد، در غیراینصورت رأس $(\ell, ۰, \dots, ۰)$ توسط x و y پوشیده خواهد شد. فرض کنید $s \le x_۱$ ، درغیراینصورت خواهیم داشت $x_۰ - y_۰ \le ۲e - t$ و مجموع x_i های باقی‌مانده برابر t می‌شود، یعنی :

$$\begin{aligned} d(x,y) &= \sum_{x_i > y_i} (x_i - y_i) = x_۰ - y_۰ + \sum_{i>۰, x_i > y_i} (x_i - y_i) \\ &\le x_۰ - y_۰ + \sum_{i>۰} x_i \le ۲e, \end{aligned} \tag{۲۰.۲}$$

از آنجایی‌که $v_۰ - y_۰ = e - s < e$ و $\forall i \ge ۲, y_i \ge v_i = ۰$ است برای به‌دست آوردن $d(v,y) = e$ باید داشته باشیم $v_۱ - y_۱ = x_۱ + e + ۱ - y_۱ = s$ بنابراین :

$$y_۱ = x_۱ - s + e + ۱ \ge e + ۱ > x_۱, \tag{۲۱.۲}$$

که اولین تساوی از فرض $s \le x_۱$ به‌دست آمده است. از آنجایی‌که داریم $y_۰ < x_۰$ و همچنین $y_۱ - x_۱ = e + ۱ - s$، به منظور داشتن $d(x,y) = e + ۱$ باید داشته باشیم:

$$\sum i \ge ۲, y_i > x_i (y_i - x_i) = e + s.$$

امّا غیرممکن است، زیرا:

$$\sum_{i\geq ۲, y_i > x_i} (y_i - x_i) \leq \sum_{i\geq ۲} y_i = \ell - y_۰ - y_۱ = e < e + s \qquad (۲۲.۲)$$

که از (۲۱.۲) استفاده کردیم. بنابراین نتیجه می‌گیریم که s باید صفر باشد. در این حالت داریم $v_۰ - y_۰ = e$ و همچنین $d(v, y) = e$ و نیز باید داشته باشیم $y_۱ \geq v_۱ = x_۱ + e + ۱$. این نشان می‌دهد که y دقیقاً به فرم (۱۸.۲) است. برای اثبات قسمت آخر ادعا توجه کنید که $y_۰ < x_۰$ و $y_۱ - x_۱ = e + ۱ + u$ و $d(x, y) = ۲e + ۱$ بیانگر این است که:

$$\sum_{i\geq ۲, y_i > x_i} (y_i - x_i) = e - u,$$

امّا داریم $\sum_{i\geq ۲} y_i = e - u$، این فقط در صورتی می‌تواند درست باشد که $x_i = ۰$ شود هر زمان که برای $i \geq ۲$ داشته باشیم $y_i > ۰$. □

بنابراین فرض کنید دو کدواژه به فرم (۱۶.۲) و (۱۸.۲) داریم. رأس زیر را درنظر بگیرید :

$$w = (\ell - t - e - ۱, x_۱ + u, \max\{x_۲, y_۲\} + ۱, \max\{x_۳, y_۳\}, \ldots, \max\{x_n, y_n\}). \qquad (۲۳.۲)$$

با استفاده از (۱۹.۲) درمی‌یابیم که $w \in \Delta_\ell^n$ وجود دارد که $d(x, w) = d(y, w) = e+۱$ بنابراین به سومین کدواژه که بتواند w را پوشش دهد، نیاز داریم، امّا این کدواژه وجود ندارد چون فرض کنید $u > ۰$ باشد، آنگاه داریم $d(x, w + f_{۲,۱}) = e$ و $d(y, w + f_{۲,۱}) = e$. با توجه به لم ۱.۳.۲ می‌دانیم کدواژه z که w را پوشش دهد باید به فرم $z = w + (۰, ۰, s_۲, \ldots, s_n)$ باشد بطوری‌که $\sum_i s_i = ۰$ و $\sum_i |s_i| = ۲e$ است. برقراری دومین تساوی نیازمند این است که $d(z, w) = e$ باشد. بنابراین داریم:

$$z = (\ell - t - e - ۱, x_۱ + u, \max\{x_۲, y_۲\} + ۱ + s_۲, \max\{x_۳, y_۳\} + s_۳, \ldots$$
$$, \max\{x_n, y_n\} + s_n). \qquad (۲۴.۲)$$

همچنین $x_۰ - z_۰ = e+۱$ و $x_۱ < z_۱$ است. به‌منظور برقراری $d(x, z) = ۲e+۱$ باید داشته‌باشیم:

$$\sum_{i\geq ۲, x_i > z_i} (x_i - z_i) = e, \qquad (۲۵.۲)$$

بطور مشابه از $z_۰ > y_۰$ و $y_i - z_i = e + ۱$ نتیجه می‌گیریم که:

$$\sum_{i\geq ۲, y_i > z_i} (y_i - z_i) = e, \qquad (۲۶.۲)$$

امّا (۲۵.۲) و (۲۶.۲) باهم نمی‌توانند برقرار باشند زیرا طبق (۱۹.۲) x_i ها و y_i ها بطور همزمان مثبت نمی‌شوند. یعنی چون $\sum_{s_i<۰} |s_i| = e$ است حتّی اگر $d(y, z) = ۲e + ۱$ باشد هیچ s_i

منفی‌ای وجود ندارد که (۲۵.۲) برقرار باشد. لذا نتیجه می‌گیریم که امکان ندارد کدواژه‌ای مانند z تحت پوشش w پیدا کنیم و ناحیه کدگشایی جدا از کدواژه‌های xو y باشد.

حالت $u = ۰$ را درنظر می‌گیریم. در این حالت داریم:

$$y = (\ell - x_۱ - ۲e - ۱, x_۱ + e + ۱, y_۲, \dots, y_n) \tag{۲۷.۲}$$

توجه کنید که $y_۲ + \cdots + y_n = e$ و در نتیجه می‌توانیم فرض کنیم $y_۲ > ۰$، رأس زیر را در نظر بگیرید:

$$\begin{aligned} w' =& (\ell - t - e - ۱, x_۱ + ۱, y_۲ - ۱, \max\{x_۳, y_۳\} + ۱, \\ & \max\{x_۴, y_۴\}, \dots, \max\{x_n, y_n\}). \end{aligned} \tag{۲۸.۲}$$

در این صورت خواهیم داشت $d(x, w') = d(y, w') = e+۱$ و $d(x, w'+f_{۱,۲}) = d(y, w'+f_{۲,۱}) = e$. بنابراین، کدواژه‌ی z' تحت پوشش w' بصورت $z' = w' + (۰, ۰, r_۲, \dots, r_n)$ می‌باشد بطوری‌که $\sum_i r_i = ۰$ و $\sum_i |r_i| = e$ است. طبق استدلال بالا نتیجه می‌گیریم که نمی‌توان بطور همزمان $d(x, z') = ۲e + ۱$ و $d(y, z') = ۲e + ۱$ برقرار باشد و در نتیجه کدواژه‌ی z که تحت پوشش w' و جدا از ناحیه‌ی کدگشایی x و y باشد، وجود ندارد.

فصل ۳

کدهای چندمجموعه‌ای در کانال‌های جایگشتی

در این فصل وجود کدهای چندمجموعه‌ای کامل که اندازه‌ـ ثابت هستند، را بررسی می‌کنیم [۲۷]. ویژگی‌های کامل چنین کدهایی در حالت دودویی و سه‌تایی بدست آمده است. فضای تحت نظر ما مجموعه همه چندمجموعه‌ای‌های روی $\mathcal{A}$ با اندازه ℓ دارای متر d است که هم‌ارز با فضای Δ_ℓ^{q-1} تحت متر d می‌باشد.

۱.۳ الفبای دودویی

فضای (Δ_ℓ^1, d) را می‌توان به صورت یک گراف نمایش داد که مجموعه رئوس آن Δ_ℓ^1 بوده و یال‌های آن رئوس به فاصله یک از هم را متصل می‌کنند.

شکل ۱.۳: کد چندمجموعه‌ای ۱ـ کامل

قضیه ۱.۱.۳. کد چندمجموعه‌ای eـ کامل غیربدیهی در $\mathcal{M}(۲,\ell)$ برای هر $\ell \geq ۲e+۱$ وجود دارد. چنین کدی، $\lceil \frac{\ell+۱}{۲e+۱} \rceil$ کدواژه دارد.

برهان. توجه کنید که قطر $(\Delta_\ell^۱, d)$ برابر ℓ است. همچنین می‌دانیم که هر دو کدواژه از کد eـ کامل باید در فاصله بزرگتر یا مساوی $۲e+۱$ قرار گیرد. در صورتی کد کامل غیربدیهی وجود دارد که $\ell \geq ۲e+۱$ باشد. بنابراین فرض کنید $\ell = (۲e+۱)k + j$ برای هر $k \geq ۱$ و $۰ \leq j < ۲e+۱$. آنگاه داریم:

$$\mathcal{C}_۱ = \left\{ (\ell - \lfloor \frac{j}{۲} \rfloor - (۲e+۱)i, \lfloor \frac{j}{۲} \rfloor + (۲e+۱)i); i = ۰, \ldots, k \right\}. \qquad (۱.۳)$$

وجود مجموعه $\lfloor \frac{j}{۲} \rfloor$ برای جابجایی به اندازه یک رأس و وجود $(۲e+۱)i$ برای جابجایی به اندازه یک کدواژه می‌باشد. کد کامل موردنظر در $\Delta_\ell^۱$، دارای $|\mathcal{C}_۱| = k+۱ = \lceil \frac{\ell+۱}{۲e+۱} \rceil$ کدواژه می‌باشد. برای درستی رابطه اخیر باید نشان دهیم که گوی‌هایی با شعاع e به مرکز کدواژه‌ها وجود دارند که مجزا بوده و فضای کل $\Delta_\ell^۱$ را پوشش می‌دهند. توجه کنید که هر دو کدواژه به فرم زیر در فاصله $d(x,y) = ۲e+۱$ از هم قرار دارند :

$$x = \left(\ell - \lfloor \frac{j}{۲} \rfloor - (۲e+۱)i, \lfloor \frac{j}{۲} \rfloor + (۲e+۱)i \right),$$

$$y = \left(\ell - \lfloor \frac{j}{۲} \rfloor - (۲e+۱)(i+۱), \lfloor \frac{j}{۲} \rfloor + (۲e+۱)(i+۱) \right),$$

به این معنا که گوی‌هایی به شعاع e در اطراف آنها بصورت مجزا قرار دارند، یعنی همه رأس‌های بین کدواژه‌ها پوشیده شده اند. برای بررسی اینکه کل $\Delta_\ell^۱ = \{(\ell - t, t); t = ۰, \ldots, e\}$ پوشیده شده‌است، کافی است نشان دهیم رئوس پایانی پوشیده شده‌اند، که درواقع این مهم اتفاق می‌افتد، زیرا $(\ell, ۰)$ در فاصله $\lfloor \frac{j}{۲} \rfloor \leq e$ از کدواژه $(\ell - \lfloor \frac{j}{۲} \rfloor, \lfloor \frac{j}{۲} \rfloor)$ قرار دارد، پس $(\ell, ۰)$ پوشیده شده‌است. همچنین $(۰, \ell)$ در فاصله $\lceil \frac{j}{۲} \rceil \leq e$ از کدواژه $(\lceil \frac{j}{۲} \rceil, \ell - \lceil \frac{j}{۲} \rceil)$ قرار دارد (حالت $i = k$ در (۱.۳)). درنتیجه کل رئوس پوشیده شده‌اند و کد چندمجموعه‌ای eـ کامل غیربدیهی در $\mathcal{M}(۲,\ell)$ برای هر $\ell \geq ۲e+۱$ وجود دارد.

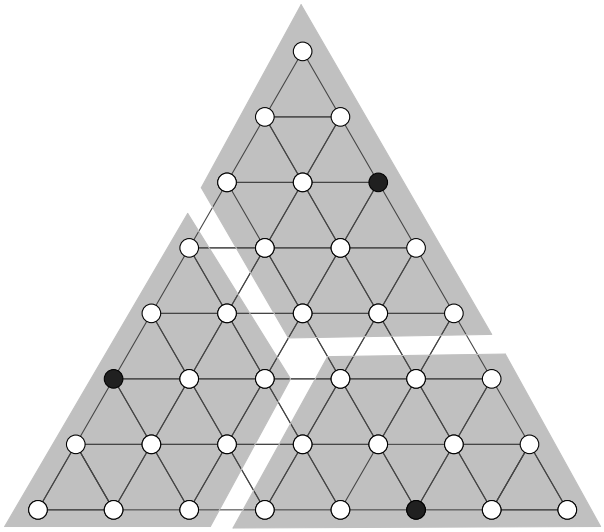
□

۲.۳ الفبای سه‌تایی

همانند حالت دودویی می‌توانیم سادک $\Delta_\ell^۲$ را به شکل گراف نمایش دهیم. اگر $\ell = ۳e+۱$ آنگاه به‌راحتی می‌توان دید که کد کامل وجود دارد. درواقع در این حالت دقیقاً دو کد به صورت زیر وجود دارد:

$$\mathcal{C}'_۲ = \{(\ell - e, e, ۰), (۰, \ell - e, e), (e, ۰, \ell - e)\}$$
$$\mathcal{C}''_۲ = \{(\ell - e, ۰, e), (e, \ell - e, ۰), (۰, e, \ell - e)\} \qquad (۲.۳)$$

به‌گونه‌ای که $\ell - e = ۲e + ۱$. در ادامه اثبات می‌کنیم که فقط دو کد کامل به فرم (۲.۳) در این حالت وجود دارد و اگر $\ell \neq ۳e + ۱$ باشد، آنگاه هیچ کد کاملی وجود نخواهد داشت.



شکل ۲.۳: کد چندمجموعه‌ای ۲ـ کامل

قضیه ۱.۲.۳. کد چندمجموعه‌ای eـ کامل غیربدیهی در $\mathcal{M}(۳, \ell)$ وجود دارد اگر و تنها اگر $\ell = ۳e + ۱$ باشد. بنابراین دقیقاً دو کد کامل در $\mathcal{M}(۳, ۳e + ۱)$ وجود دارد که هردوی آن‌ها از اندازه سه می‌باشند.

برهان. اثبات قضیه را به سه قسمت تقسیم کرده که هر کدام از آن‌ها شامل اثبات یک ادعا می‌باشد.

ادعا ۱. رئوس $(\ell, ۰, ۰)$، $(۰, \ell, ۰)$ و $(۰, ۰, \ell)$ نمی‌توانند کدواژه‌های کد کامل در $\Delta_\ell^۲$ باشند.

برهان. به خلف فرض کنید $x = (\ell, ۰, ۰)$ کدواژه باشد. رأس $y = (\ell - e - ۱, e + ۱, ۰)$ در فاصله $e + ۱$ از x قرار دارد. رأس y باید در فاصله کوچکتر یا مساوی e از هر کدواژه دیگری مانند z باشد تا فاصله x از کدواژه z برابر $e + ۱$ شود. درواقع این فاصله از z باید دقیقاً e باشد، چون در غیراینصورت گوی‌های به شعاع e اطراف x و z تداخل پیدا می‌کنند، زیرا داریم :

$$d(x, z) \leq d(x, y) + d(y, z) < ۲e + ۱.$$

می‌توان دید که فقط رئوس زیر به فاصله e از y و فاصله $۲e + ۱$ از x قرار دارند:

$$(\ell - (۲e + ۱), ۲e + ۱, ۰)$$

$$(\ell-(۲e+۱),۲e,۱)$$
$$\vdots$$
$$(\ell-(۲e+۱),e+۱,e)$$

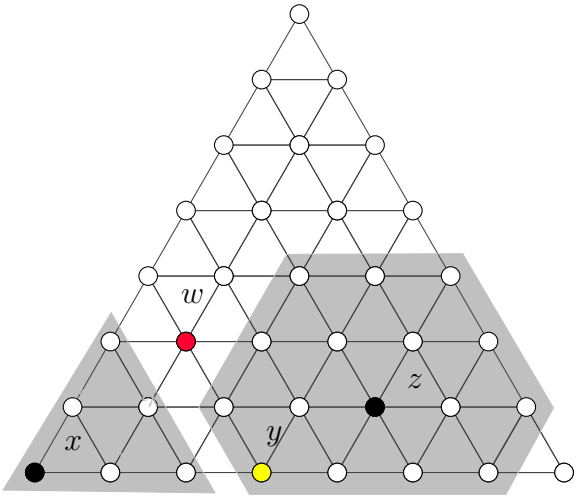
بنابراین می‌توانیم فرض کنیم که $z=(\ell-(۲e+۱),۲e+۱-i,i)$ به ازای هر $i\in\{۰,\dots,e\}$ کدواژه خواهد بود.
در شکل ۳.۳ رأس $w=(\ell-(e+۱),e-i,i+۱)$ را درنظر بگیرید. در این صورت، داریم:

$$d(x,w)=e+۱=d(z,w)$$

و لذا w به‌وسیله $\mathcal{B}(x,e)$ و $\mathcal{B}(z,e)$ پوشیده نمی‌شود. چون قصد ساخت کد کامل را داریم، w باید پوشیده شود؛ بنابراین باید کدواژه سومی مانند v وجود داشته باشد بطوری‌که روابط زیر برقرار باشد:

$$\mathcal{B}(v,e)\cap\mathcal{B}(x,e)=\emptyset\quad,\quad\mathcal{B}(v,e)\cap\mathcal{B}(z,e)=\emptyset.$$

امّا با توجه به شکل ۳.۳، چنین کدواژه‌ای وجود ندارد. درنتیجه حکم ثابت می‌شود.



شکل ۳.۳: اثبات ادعا ۱

□

از آنجایی‌که رأس $(\ell,۰,۰)$ باید پوشیده شود، پس می‌بایست کدواژه‌ای با فاصله کمتر یا مساوی e از آن قرار داشته باشد. رئوسی که در فاصله کمتر یا مساوی e از $(\ell,۰,۰)$ قرار دارند به فرم $(\ell-j,i,j-i)$ می‌باشند بطوری‌که $j\in\{۰,\dots,e\}$ و $i\in\{۰,\dots,j\}$.

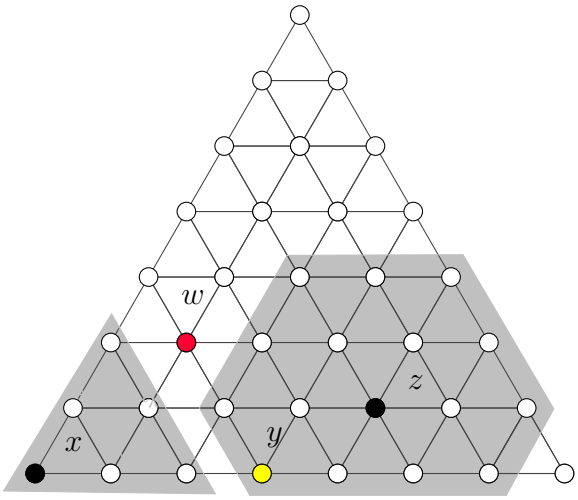
در ادامه اثبات می‌کنیم که هیچ یک از این رأس‌ها نمی‌توانند کدواژه‌های کد کامل باشند به غیر از $(\ell-e,\circ,e)$ و $(\ell-e,e,\circ)$.

ادعا ۲. رئوس $(\ell-j,i,j-i)$ که $\circ<j<e$ یا $\circ<i<j$ نمی‌توانند کدواژه‌های کد کامل در $\Delta_\ell^{\text{۲}}$ باشند.

برهان. این ادعا مشابه ادعای قبلی اثبات می‌شود.

فرض کنید $x=(\ell-j,i,j-i)$ به عنوان کدواژه انتخاب شده باشد، که $j=e$ یا $\circ<j<e$ امّا $\circ<i<e$. رأس $y=(\ell-i-e-\text{۱},i+e+\text{۱},\circ)$ را درنظر بگیرید. باید $z=(\ell-i-\text{۲}e-\text{۱},i+\text{۱},\circ)$ را در نظر بگیرید تا y پوشیده شود. حال $w=(\ell-j-e-\text{۱},i+e,j-i+\text{۱})$ را کدواژه قرار دهیم $(\text{۱},i+\text{۲}e+\text{۱},\circ)$ را در نظر بگیرید و نتیجه می‌گیریم که توسط هر گوی دیگری که مجزا از $\mathcal{B}(x,e)$ و $\mathcal{B}(z,e)$ است، نمی‌تواند پوشیده شود.

□



شکل ۴.۳: اثبات ادعا ۲

دو ادعای قبلی نشان می‌دهند که $(\ell-e,e,\circ)$ و یا $(\ell-e,\circ,e)$ می‌توانند کدواژه باشند اگر رأس $(\ell,\circ,\circ)$ پوشیده شود، همچنین برای دو رأس دیگر بطور مشابه برقرار است. این نشان می‌دهد که فقط کدهای اشاره شده در (۲.۳) کدهای کامل در $\Delta^{\text{۲}}_{\text{۳}e+\text{۱}}$ می‌باشند.

ادعا ۳. هیچ کد کاملی در $\Delta_\ell^{\text{۲}}$ برای $\ell\neq\text{۳}e+\text{۱}$ وجود ندارد.

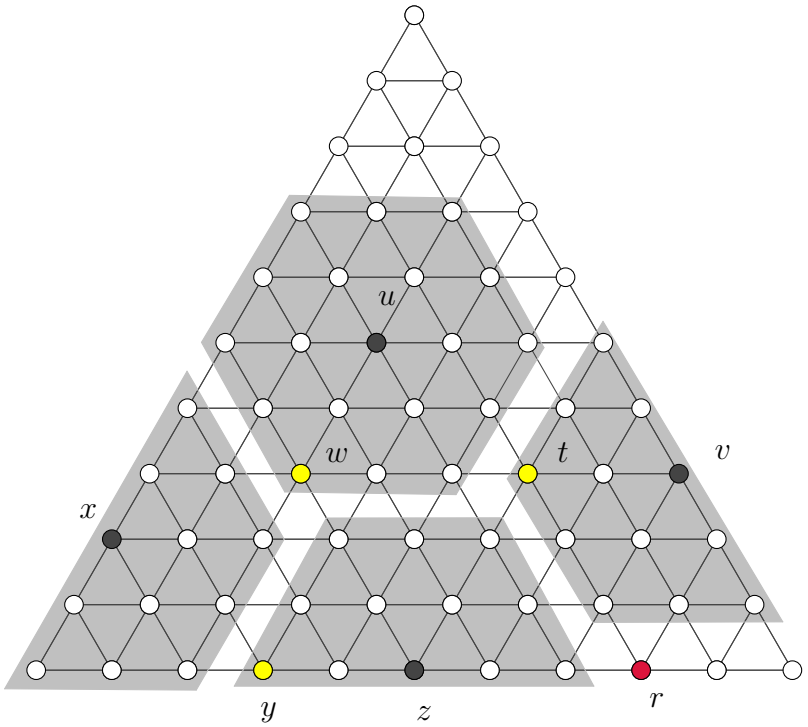
برهان. فرض کنید $x = (\ell - e, \circ, e)$ کدواژه باشد. رأس $y = (\ell - e - ۱, e + ۱, \circ)$ را درنظر بگیرید. همانطور که در اثبات ادعا ۲ داشتیم، می‌دانیم برای این منظور که y پوشیده شود باید رأس $z = (\ell - ۲e - ۱, ۲e + ۱, \circ)$ را کدواژه درنظر بگیریم. بنابراین باید داشته باشیم $\ell \geq ۲e + ۱$ تا کد مدنظر، غیربدیهی باشد. حال $w = (\ell - ۲e - ۱, e, e + ۱)$ را درنظر بگیرید. داریم :

$$d(x, w) = d(z, w) = e + ۱,$$

و بنابراین سومین کدواژه باید وجود داشته باشد تا w را پوشش دهد. در شکل ۵.۳ مشخص است که تنها حالت ممکن $u = (\ell - ۳e - ۱, e, ۲e + ۱)$ است و باید داشته باشیم $\ell \geq ۳e + ۱$ تا کد کامل وجود داشته باشد. بنابراین فرض کنید $\ell > ۳e + ۱$ و رأس $t = (\ell - ۳e - ۲, ۲e + ۱, e + ۱)$ را درنظر بگیرید. داریم:

$$d(z, t) = d(u, t) = e + ۱.$$

بنابراین برای اینکه t پوشیده شود به چهارمین کدواژه نیاز داریم که فقط برای یک حالت ممکن است، یعنی $v = (\ell - ۴e - ۲, ۳e + ۱, e + ۱)$. درنهایت رأس $r = (\ell - ۳e - ۲, ۳e + ۲, \circ)$ را درنظر بگیرید. به راحتی در شکل دیده می‌شود که r پوشیده نمی‌شود. درنتیجه، اثبات ادعا۳ کامل می‌شود و درنتیجه قضیه ثابت می‌شود.



شکل ۵.۳: اثبات ادعا ۳

□

با توجه به ادعای ۱ و ۲ و ۳ قضیه ۱.۲.۳ اثبات می‌شود. □

۳.۳ حذف، وارد کردن و جایگزینی در کانال‌های جایگشتی

در این بخش خصوصیات کلی از کانال‌های جایگشتی را شرح می‌دهیم و خطاهایی مانند حذف[۱]، جایگزینی[۲] و وارد کردن[۳] را روی کانال بررسی می‌کنیم [۲۹].

۱.۳.۳ مدل کانال

فرض کنید کانالی ارتباطی روی دنباله‌های انتقالی داریم که نمادهایش بطور تصادفی جایگشت داده شده اند و به شکل زیر نمایش داده می‌شود:

$$s_1 s_2 \dots s_n \rightsquigarrow s_{\pi(1)} s_{\pi(2)} \dots s_{\pi(n)} \qquad (۳.۳)$$

جایی‌که s_i ، $(1 \le i \le n)$ نمادهایی از الفبای ورودی $\mathcal{A} = \{a_1, \dots, a_q\}$ هستند و π به‌طور تصادفی از مجموعه تمام جایگشت‌های روی مجموعه$\{1, \dots, n\}$ انتخاب شده است. بنابراین فرض کنید این کانال انواع اختلال روی دنباله انتقالی را پیاده می‌کند؛ یعنی وارد کردن، حذف وجایگزینی و پاک شدن نمادها. وارد کردن یعنی در دنباله دریافتی نمادی از $\mathcal{A}$ وجود دارد که منتقل نشده‌بود. حذف یعنی نمادی که منتقل شده‌بود، در دنباله دریافتی ظاهر نشد. جایگزینی یعنی نمادی که منتقل شده با نماد دیگری تعویض شده است. پاک شدن، جابجایی نماد منتقل شده با نماد "?" است که $? \notin \mathcal{A}$.

۲.۳.۳ تصحیح خطا در کانال‌های جایگشتی

ابتدا روی حالتی که اختلال‌ها در کانال، جایگشت‌های تصادفی هستند، تمرکز می‌کنیم. کدواژه‌ها در این حالت به‌عنوان چندمجموعه‌ای روی الفبای کانال توصیف می‌شوند.

برای دنباله $S = (s_1, \dots, s_n) \in \mathcal{A}^n$ تعریف می‌کنیم $X^s = (x_1^s, \dots, x_q^s) \in \mathbb{Z}^q$. به این معنا که x_i^s تعداد پیشامدهای نماد $a_i \in \mathcal{A}$ در S می‌باشد. بطور واضح داریم $x_i^s \ge 0$ و همچنین $\sum_{i=1}^{q} x_i^s = n$ است. توجه داشته باشید که دو دنباله $S, \tilde{S} \in \mathcal{A}^n$ جایگشت‌هایی از یکدیگر هستند اگر و فقط اگر ترکیب مشابهی داشته باشند، یعنی اگر و تنها اگر $x^{\tilde{s}} = x^s$ باشد. بنابراین اگر دنباله منتقل شده با اطمینان در خروجی کانال جایگشتی بازیابی شود، آنگاه تنها یک دنباله با ترکیب نمادی خاص می‌تواند کدواژه معتبر باشد.

به این ترتیب نتیجه می‌گیریم؛ کدواژه‌ها برای این کانال به وسیله ترکیبشان بطور منحصربه‌فرد تعیین می‌شوند و می‌توانند به عنوان بردارهای صحیح $x = (x_1, \dots, x_q) \in \mathbb{Z}_+^q$ توصیف شوند که $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$ است. کدواژه‌ها را می‌توانیم چندمجموعه‌ای‌های $S = \{s_1, \dots, s_n\}$

---

[۱] Deletion
[۲] Substitution
[۳] Insertion

روی الفبای کانال در نظر بگیریم. چندگانه‌های عناصر $\mathcal{A}$ در S به‌وسیله بردارها به فرم $x^s = (x_1^s, \dots, x_q^s) \in \mathbb{Z}^q$ مشخص شده‌اند، بطوری‌که داشته باشیم $x_i^s \geq 0$ و $\sum_{i=1}^q x_i^s = n$. توجه داشته باشید که اگر کدواژه‌ها توسط بردارهای صحیح توصیف شوند، در واقع این بردارها نیستند که از طریق کانال جایگشتی ارسال می‌شوند، یعنی اگر $X = (x_1, \dots, x_q) \in \mathbb{Z}_+^q$ یک کدواژه باشد، آنگاه چیزی که در حال انتقال است x_1 نسخه‌ای از نماد a_1، x_2 نسخه‌ای از نماد a_2 و ... می‌باشند. بنابراین $\sum_{i=1}^q x_i$ را می‌توان به عنوان طول کدواژه X بیان کرد، چون این تعداد نمادها است که منتقل شده‌است. در ادامه با فضای زیر ادامه می‌دهیم:

$$\Delta_n^{q-1} = \{X \in \mathbb{Z}_+^q : \sum_{i=1}^q x_i = n\}. \tag{۴.۳}$$

مجموعه Δ_n^{q-1} سادک گسسته از طول n و با بعد $q-1$ و اندازه $|\Delta_n^{q-1}| = \binom{n+q-1}{q-1}$ می‌باشد.

ملاحظه ۱.۳.۳. کد چندمجموعه‌ای از طول n روی الفبای qـتایی، یک زیرمجموعه از Δ_n^{q-1} است که حداقل دو عضو دارد. لازم است هر کد، حداقل دو کدواژه داشته‌باشد. می‌توان این فضا را حالت محدود شده‌ی مشبکه A_{q-1} در نظر گرفت. بطوری‌که:

$$A_{q-1} = \{X \in \mathbb{Z}^q : \sum_{i=1}^q x_i = 0\}. \tag{۵.۳}$$

از این پس فرض می‌کنیم انواع خطا یعنی وارد کردن، حذف و جایگزینی در مدل کانال موجود است. می‌توانیم کانال مورد نظر را به‌صورت زیر تعریف کنیم:

ورودی‌های کانال، چندمجموعه‌ای‌های با اندازه n روی $\mathcal{A}$ می‌باشند و خروجی‌های کانال، چندمجموعه‌ای‌های با اندازه دلخواه روی $\mathcal{A}$ هستند و کانال روی چندمجموعه‌ای منتقل شده عمل می‌کند که امکان دارد تعدادی از نمادهایش حذف شده باشد یا اضافه شده باشد یا عنصری جای آن با عنصر دیگری از $\mathcal{A}$ تعویض شده باشد(جایگزینی).

فرض کنید $e_i \in \mathbb{Z}^q$ یک بردار واحد باشد به‌طوری‌که در iـامین جایگاهش عدد ۱ و در بقیه جایگاه‌ها عدد صفر قرار داشته‌باشد. اگر چندمجموعه‌ای دریافت شده‌ی $\tilde{S}$ به‌وسیله وارد کردن یک نماد a_i به S تولید شده باشد، آنگاه داریم $X^{\tilde{s}} = X^s + e_i$. بطور مشابه حذف a_i از S به معنی $X^{\tilde{s}} = X^s - e_i$ و جایگزینی a_i به‌وسیله a_j که یعنی $X^{\tilde{s}} = X^s - e_i + e_j$ است. گوییم یک کد می‌تواند h_{ins} وارد کردن و h_{del} حذف و h_{sub} جایگزینی را تصحیح کند اگر هر کدواژه بتواند به‌طور یکتا با یک الگوی دلخواه از تعداد کوچکتر یا مساوی h_{del} حذف، کوچکتر یا مساوی h_{ins} وارد کردن و کوچکتر یا مساوی h_{sub} جایگزینی بازیابی شود.

قضیه ۱.۳.۳. فرض کنید $\mathcal{C} \subseteq \Delta_n^{q-1}$ یک کد چندمجموعه‌ای باشد و h_{ins}، h_{del} و h_{sub} صحیح نامنفی باشند و داریم $h = h_{ins} + h_{del} + 2h_{sub}$. در اینصورت اگر $\mathcal{C}$ بتواند h_{ins} وارد کردن، h_{del} حذف و h_{sub} جایگزینی را صحیح کند، آنگاه $\mathcal{C}$ می‌تواند h حذف را صحیح کند.

برهان. توجه کنید از آنجایی‌که هر جایگزینی می‌تواند به عنوان ترکیبی از حذف و وارد کردن در نظر گرفته شود و برعکس، در این صورت قسمت اول هم‌ارز عبارت زیر است:
$\mathcal{C}$ می‌تواند $h_{ins}+h_{sub}$ وارد کردن و $h_{del}+h_{sub}$ حذف را تصحیح کند.
اثبات می‌کنیم که فرض کنید حکم برقرار نباشد. به این معنا که دو کدواژه متفاوت x و y وجود دارد بطوری‌که $x-f=y-g$ برای هر بردار f و g که $f_i,g_i\geq 0$ و $\sum_{i=1}^{q} f_i=$ $\sum_{i=1}^{q} g_i=h$ وجود دارند. f و g نشان‌دهنده h حذف از x و y می‌باشند. تعریف می‌کنیم $f=f^{del}+f^{ins}$ و $g=g^{del}+g^{ins}$. که f^{del} و f^{ins} و g^{del} و g^{ins} بردارهای دلخواه هستند بطوری‌که $f^{del},f^{ins},g^{del},g^{ins}\geq 0$ و همچنین داریم:

$$\sum_{i=1}^{q} f_i^{del}=\sum_{i=1}^{q} g_i^{del}=h_{sub}+h_{del},$$
$$\sum_{i=1}^{q} f_i^{ins}=\sum_{i=1}^{q} g_i^{ins}=h_{ins}+h_{sub}.$$

آنگاه $x-f^{del}+g^{ins}=y-g^{del}+f^{ins}$ که یعنی $\mathcal{C}$ نمی‌تواند $h_{ins}+h_{sub}$ وارد کردن و $h_{del}+h_{sub}$ حذف را تصحیح کند. درنتیجه فرض نمی‌تواند درست باشد.

□

از قضیه ۱.۳.۳ نتیجه می‌گیریم زمانی که بحث تصحیح خطا در کانال‌های جایگشتی مطرح است، باید فرض کنیم که حذفیات فقط نوعی از خطای افزایش در کانال هستند.
متری که روی Δ_n^{q-1} برای هدف ما مناسب باشد، فاصله ℓ_1 است:

$$d(x,y)=\frac{1}{2}\sum_{i=1}^{q}|x_i-y_i|.$$

می‌توان فضای متریک (Δ_n^{q-1},d) به عنوان گرافی با $|\Delta_n^{q-1}|=\binom{n+q-1}{q-1}$ رأس نمایش داد. فاصله $d(x,y)$ دقیقاً همان فاصله گراف بین رأس‌هایی مانند x و y است، یعنی کوتاهترین مسیر بین آنها. مینیمم فاصله کد $\mathcal{C}\subseteq\Delta_n^{q-1}$ با رابطه $d(.,.)$ را به‌وسیله $\delta(\mathcal{C})$ نمایش می‌دهیم.

قضیه ۲.۳.۳. کد چندمجموعه‌ای $\mathcal{C}\subseteq\Delta_n^{q-1}$، تعداد h حذف را تصحیح می‌کند اگر و تنها اگر مینیمم فاصله آن h باشد، یعنی $\delta(\mathcal{C})>h$.

برهان. فرض کنید x و y دو کدواژه با فاصله $\delta(\mathcal{C})$ باشند، آنگاه $f=y-x$ به‌طوری‌که $\sum_{i=1}^{q} f_i=0$ و $\sum_{i=1}^{q}|f_i|=2\delta(\mathcal{C})$ است. فرض کنید $f^+=\max(f,0)$ و $f^-=\max(-f,0)$ قسمت مثبت و منفی f هستند. بنابراین $f=f^+-f^-$. آنگاه:

$$y-f^+=x-f^-$$

از آنجایی‌که $f_i^+ \geq 0$ و $\sum_{i=0}^{q} f_i^+ = \delta(\mathcal{C})$ و $f_i^- \geq 0$ و $\sum_{i=1}^{q} f_i^- = \delta(\mathcal{C})$ درنتیجه هردو f^+ و f^- می‌توانند به عنوان الگوهای توصیف رئوس خطا از $\delta(\mathcal{C})$ حذف از y و x در نظر گرفته شود. به این معناست که $\mathcal{C}$ نمی‌تواند $\delta(\mathcal{C})$ حذف را تصحیح کند. عکس این استدلال نشان می‌دهد که $\mathcal{C}$ همیشه کمتر از $\delta(\mathcal{C})$ حذف را می‌تواند تصحیح کند. زیرا در غیراینصورت دو کلمه در فاصله‌ی کمتر از $\delta(\mathcal{C})$ قرار می‌گیرند که تناقض است. □

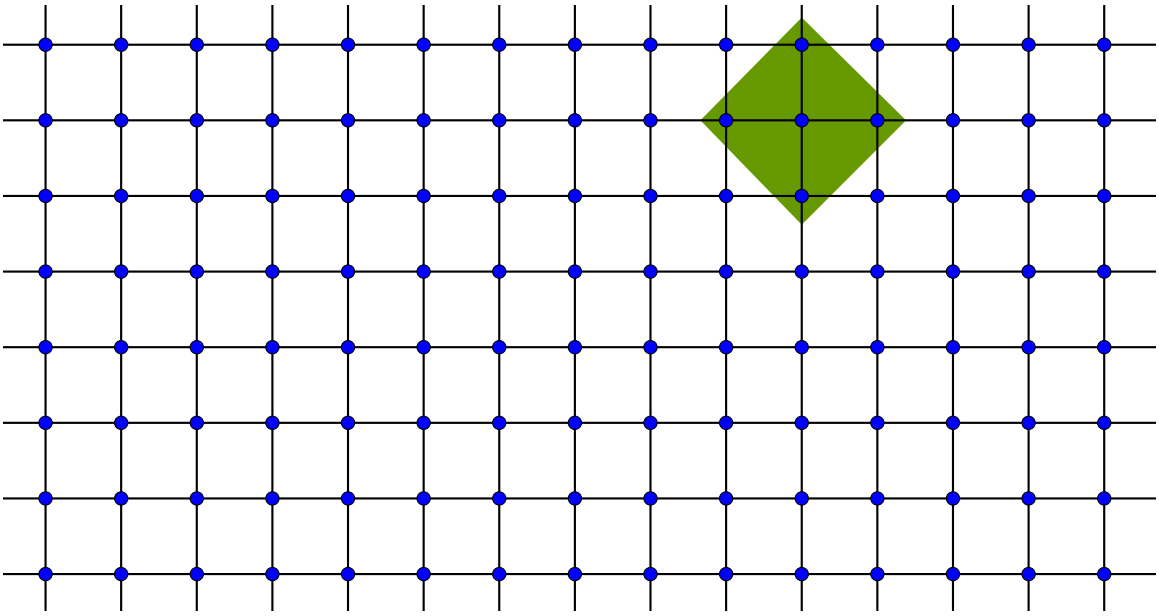
فصل ۴

بررسی کدهای کامل در مشبکه‌های $\mathbb{Z}^n$ و A_n

بسته‌بندی در مشبکه یک مسأله با زمینه هندسی تصحیح خطا، در بسیاری از سیستم های انتقال اطلاعات و ذخیره سازی می‌باشد. در این فصل به بررسی بسته‌بندی در مشبکه‌های A_n و $\mathbb{Z}^n$ با استفاده از متر ℓ_1 می‌پردازیم.

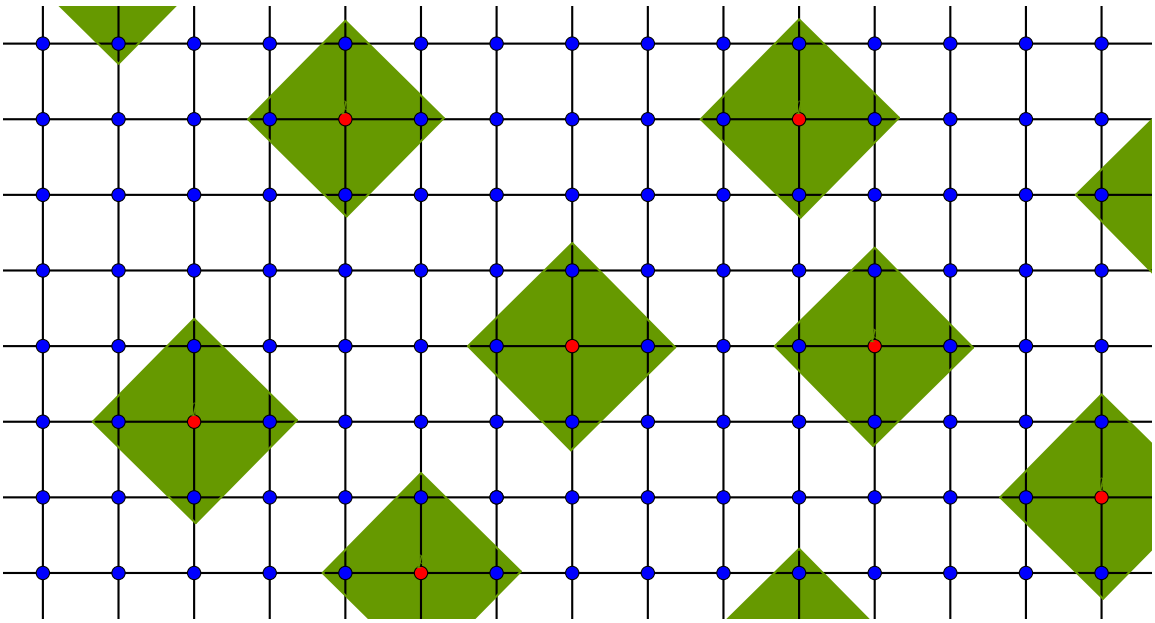
۱.۴ کدهای کامل در مشبکه $\mathbb{Z}^n$

در شکل زیر، فضای $\mathbb{Z}^2$ را نشان داده‌ایم، که در آن مجموعه S نمایش داده شده است. می‌خواهیم با استفاده از مجموعه S و مجموعه انتقال‌هایش فضای کل را پوشش دهیم.



شکل ۱.۴: مجموعه $S = \{(۰,۰),(\pm۱,۰),(۰,\pm۱)\}$ روی $\mathbb{Z}^۲$

حال مجموعه انتقال‌های مجموعه S را در شکل زیر می‌بینیم:



شکل ۲.۴: مجموعه انتقال‌های S

می‌خواهیم مجموعه T که بردارهای آن مجزا هستند و تمام مشبکه $\mathbb{Z}^n$ را فرش می‌کند پیدا کنیم، یعنی:

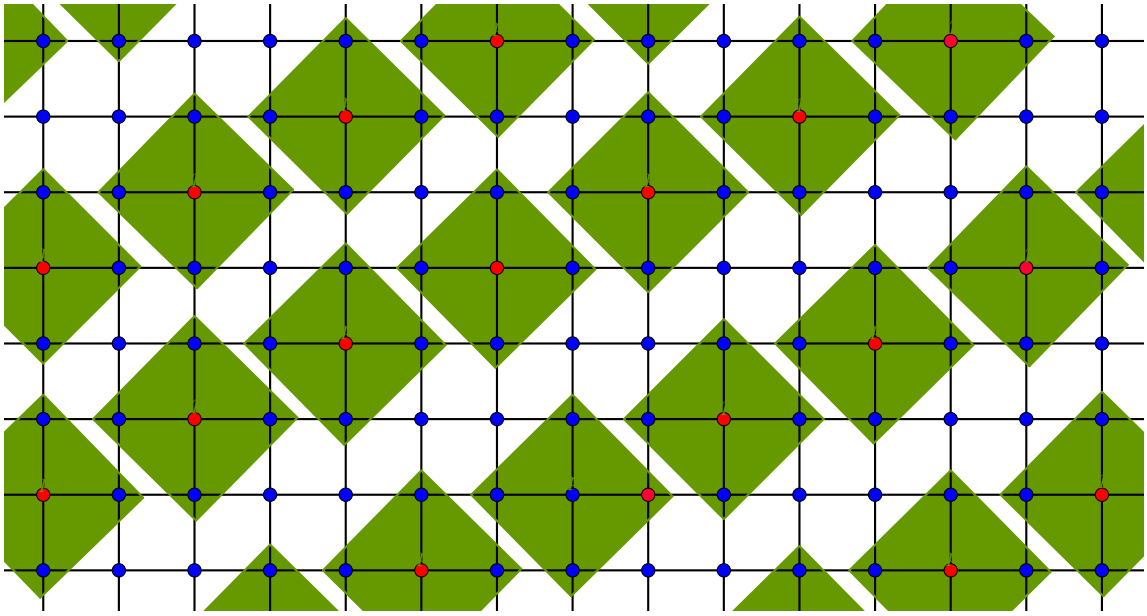
$$(X+S)\cap(Y+S)=\emptyset \qquad \forall X,Y\in T, X\neq Y.$$

و

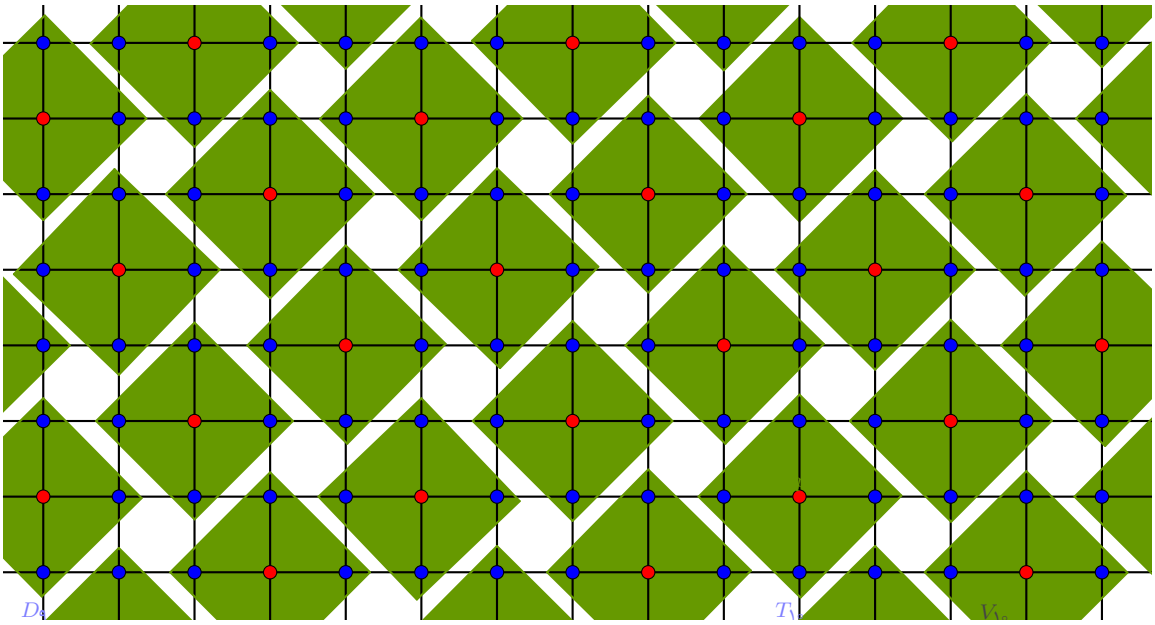
$$\bigcup_{X\in T}(X+S)=\mathbb{Z}^n$$

درواقع فرش کردن، متراکم‌ترین پوشش ممکن است.

اگر $(S,\mathcal{L})$ یک پوشش مشبکه‌ای باشند، آنگاه $\mathcal{L}$ یک کد خطی است. اگر $(S,\mathcal{L})$ قابل فرش کردن باشد، T کد کامل است. در شکل زیر حالت بسته‌بندی و فرش شده‌ی مشبکه $\mathbb{Z}^2$ را می‌بینیم:



شکل ۳.۴: یک نوع بسته‌بندی در $\mathbb{Z}^2$

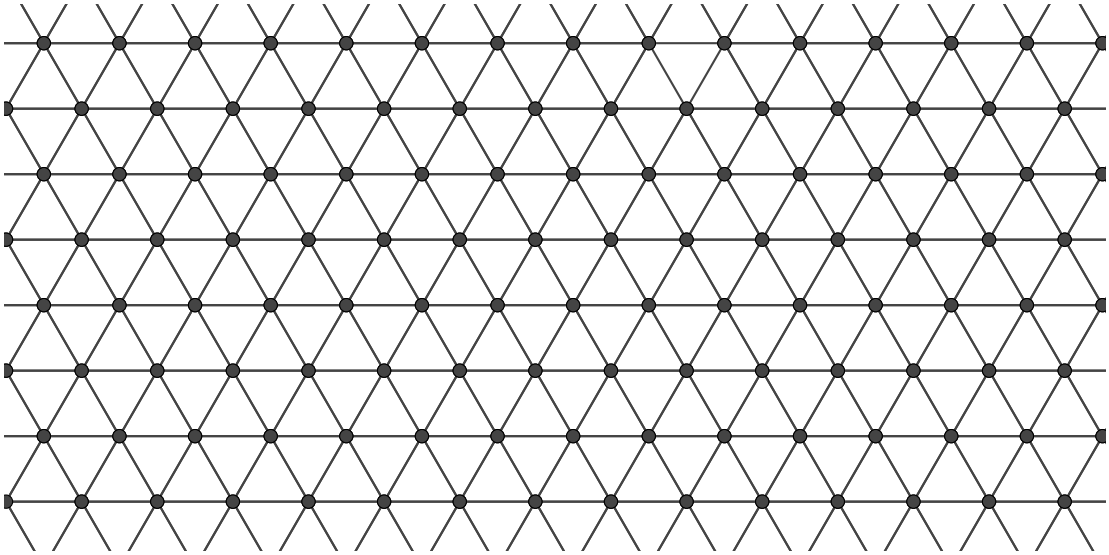


شکل ۴.۴: فرش کردن $\mathbb{Z}^2$

همانطور که از شکل‌ها پیداست، با هر شعاعی می‌توان گوی‌هایی در این مشبکه رسم کرد تا کد کامل داشته باشیم.

۲.۴ کدهای کامل در مشبکه A_n

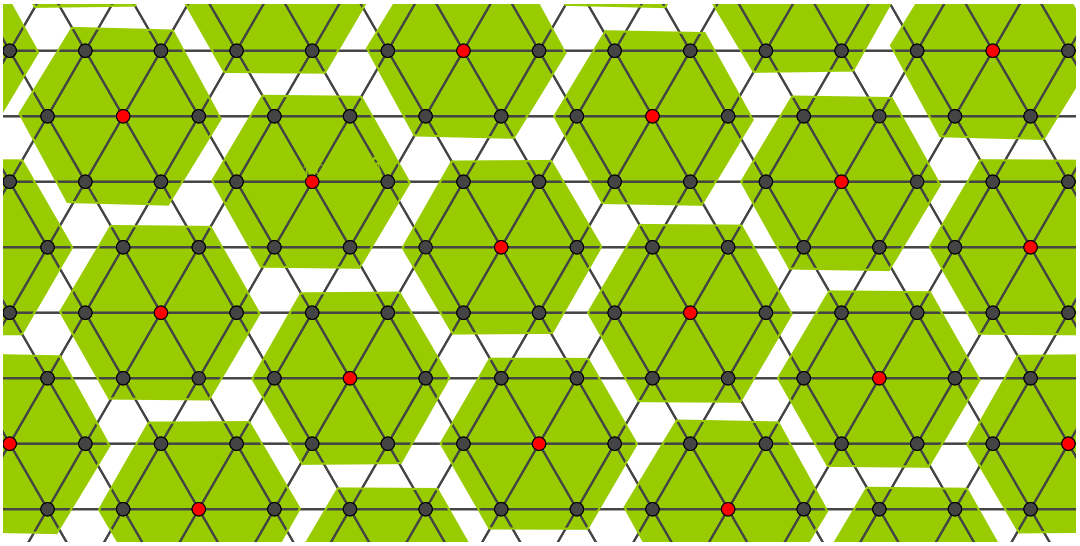
حال به بررسی مشبکه A_n می‌پردازیم. فرض کنید A مجموعه متناهی از نمادها باشد که آن را الفبای کانال می‌نامیم. کانال جایگشتی روی الفبای کانال، کانالی ارتباطی است که دنباله‌ای از نمادهای A را به‌عنوان ورودی می‌گیرد و به ازای هر ورودی یک جایگشت تصادفی از آن دنباله را خارج می‌کند. در کانال جایگشتی خطاهایی رخ می‌دهد که شامل حذف، افزایش و یا جابجایی می‌باشد. مشبکه $A_۲$ در زیر نشان داده شده است. همانطور که مشخص است فضای $\Delta_\ell^۲$ قسمتی از این مشبکه می‌باشد.



شکل ۵.۴: مشبکه $A_۲$

قصد داریم کدهای کامل را در این مشبکه با ابعاد مختلف رسم کنیم. کدهای کامل در $A_۱$ و $A_۲$ برای هر اندازه شعاعی وجود دارد. کد کامل با شعاع $r = ۱$

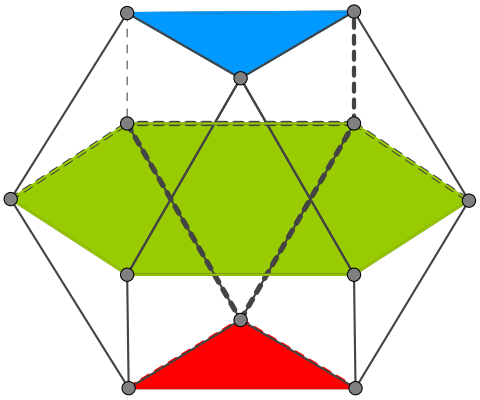
شکل ۶.۴: کد کامل در $A_۱$



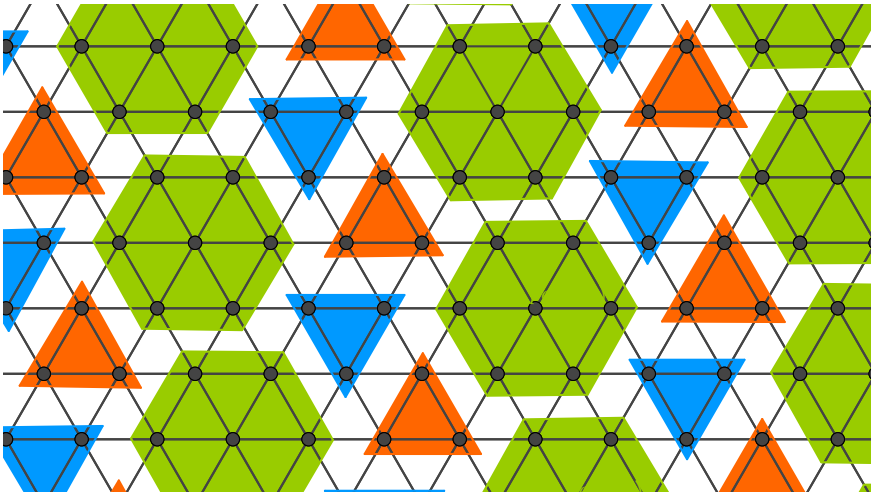
شکل ۷.۴: کد کامل در $A_۲$

شکل زیر نمایش کد کامل در $A_۳$ می‌باشد. نمایش تمام کدها در این مشبکه مشکل است، به همین علت در ادامه این کدها را روی صفحه‌ای مسطح نشان می‌دهیم.

برای ابعاد بالاتر در صورتی وجود دارد که n توانی از عدد اول باشد. به عنوان مثال، برای $n = ۸ = ۲^۳$ کد کامل با شعاع $r = ۱$ وجود دارد.



شکل ۸.۴: کد کامل در $A_۳$



شکل ۹.۴: حالت مسطح کد کامل در A_3

مراجع

[1] M. Aigner, Combinatorial Theory, *Springer*, New York (1979).

[2] B. Albdaiwi, P. Horak, L. Milazzo, Enumerating and decoding perfect linear Lee codes, *Des. Codes Cryptogr.*, 52(2). (2009), 155–162.

[3] J. Astola, On perfect Lee codes over small alphabets of odd cardinality, *Discret. Appl. Math.*, 4. (1982), 227–228.

[4] D.W. Bange, A.E. Barkauskas, Slater P.J, Efficient dominating sets in graphs. In: Ringeisen R.D., Roberts F.S. (eds.) *Applications of Discrete Mathematics*, 189–199. SIAM, Philadelphia (1988).

[5] D.P. Bertsekas, R. Gallager, *Data Networks*, 2nd edn. Prentice Hall, Englewood Cliffs (1992).

[6] M.R. Best, Perfect codes hardly exist, *IEEE Trans. Inf. Theory*,. 29(3). (1983), 349–351.

[7] N. Biggs, Perfect codes in graphs, *J. Comb. Theory* (B) 15(3). (1973),289–296.

[8] J.A. Bondy, U.S.R. Murty. *Graph theory with applications.* London: Macmillan, 1976.

[9] P.A.H. Bours, On the construction of perfect deletion-correcting codes using design theory, *Des. Codes Cryptogr.* 6(1). (1995),5–20.

[10] L. Chihara, On the zeros of the Askey–Wilson polynomials, with applications to coding theory, *SIAM J. Math. Anal.* 18(1). (1987), 191–207.

[11] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, Elsevier, Amsterdam (1997).

[12] P. Delsarte, An algebraic approach to association schemes and coding theory, *Philips J. Res.* 10.(1973), 1–97.

[13] T. Etzion, On the nonexistence of perfect codes in the Johnson scheme, *SIAM J. Discret. Math.* 9(2).(1996), 201–209.

[14] T. Etzion, Configuration distribution and designs of codes in the Johnson scheme, *J. Comb. Des.*,. 15(1).(2007), 15–34.

[15] T. Etzion, Product constructions for perfect Lee codes, *IEEE Trans. Inf. Theory*,. 57(11). (2011),7473–7481.

[16] T. Etzion, M. Schwartz, Perfect constant-weight codes, *IEEE Trans. Inf. Theory*,. 50(9). (2004), 2156–2165.

[17] T. Etzion, A. Vardy, Perfect binary codes: constructions, properties, and enumeration, *IEEE Trans. Inf. Theory* 40(3). (1994), 754–763.

[18] T. Etzion, A. Vardy, Error-correcting codes in projective space, *IEEE Trans. Inf. Theory*,. 57(2).(2011), 1165–1173.

[19] M. Gadouleau, A. Goupil, *Binary codes for packet error and packet loss correction in store and forward*, In, Proceedings of the International ITG Conference on Source and Channel Coding, Siegen, Germany (2010)

[20] M. Gadouleau, A.Goupil, Amatroid framework for noncoherent random network communications, *IEEE Trans. Inf. Theory* ,. 57(2). (2011), 1031–1045.

[21] S.W. Golomb, L.R. Welch, Perfect codes in the Lee metric and the packing of polyominoes, *SIAM J. Appl. Math*,. 18(2). (1970), 302–317.

[22] D.M. Gordon, Perfect single error-correcting codes in the Johnson scheme, *IEEE Trans. Inf. Theory* 52(10). (2006), 4670–4672.

[23] P. Horak, Tilings in Lee metric, *Eur. J. Comb.*,. 30(2). (2009), 480–489.

[24] P. Horak, On perfect Lee codes, *Discret. Math.*,. 309(18).(2009), 5551–5561.

[25] R. Kötter, F.R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theory* ,.54(8). (2008), 3579–3591.

[26] M. Kovačević, D. Vukobratović, Subset codes for packet networks, *IEEE Commun. Lett.*,. 17(4).(2013), 729–732.

[27] M. Kovačević, D. Vukobratović, Multiset codes for permutation channels, Available online at: arXiv:1301.7564.

[28] M. Kovačević, D. Vukobratović, Perfect Codes in the Discrete Simplex, *Des. Codes Cryptogr.*,. 75(1). (2015), 81–95.

[29] V.I. Levenshtein, On perfect codes in deletion and insertion metric, *Discret. Math. Appl.*,. 2(3). (1992), 241–258

[30] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam (1977).

[31] W.J. Martin, X.J. Zhu, Anticodes for the Grassmann and bilinear forms graphs. *Des. Codes Cryptogr.* 6(1). (1995), 73–79.

[32] K.A. Post, Nonexistence theorem on perfect Lee codes over large alphabets, *Inf. Control* 29(4). (1975), 369–380.

[33] C. Roos, A note on the existence of perfect constant weight codes, *Discret. Math*,. 47. (1983), 121–123.

[34] O. Shimabukuro, On the nonexistence of perfect codes in J (2w+ p2,w), *Ars Comb.*,. 75. (2005), 129–134.

[35] S. Špacapan, Non-existence of face-to-face four dimensional tiling in the Lee metric, *Eur. J. Comb.*,. 28(1). (2007), 127–133.

[36] A. Tietäväine, On the nonexistence of perfect codes over finite fields, *SIAM J. Appl. Math*,. 24(1). (1973), 88–96.

[37] J. H.Van Lint, *Nonexistence theorems for perfect error-correcting codes*, In: Computers in Algebra and Number Theory, vol. IV, SIAM-AMS Proceedings (1971).

[38] J.H. Van Lint, J. Hendricus. *Introduction to coding theory.* Springer Science, Business Media, 2012.

[39] V.A. Zinoviev, V.K. Leontiev, The nonexistence of perfect codes over Galois fields, *Probl. Control Inf. Theory*,. 2. (1973), 123–132.

واژه‌نامه فارسی به انگلیسی

الفبای کد ..... Code alphabet
اندازه کد ..... Code cardinality
بسته‌بندی ..... Packing
تابع چندگانگی ..... Multiplicity function
تابع مشخصه ..... Characteristic function
جایگزینی ..... Substitution
چندمجموعه ..... Multi-set
حذف ..... Deletion
سادک گسسته ..... Discrete simplex
فاصله همینگ ..... Hamming distance
فرش کردن ..... Tiling
کانال ارتباطی ..... Communication channel
کانال جایگشتی ..... Permutation channel
کد اندازه‌ـ ثابت ..... Constant-cardinality code
کد بلوکی ..... Block code
کد خطی ..... Linear code
کدگشایی ..... Decoding
کدگذاری ..... Encoding
کدواژه ..... Codeword
کدکامل ..... Perfect code
کد صحیح ..... Integer code
متر منهتن ..... Manhatan metric
مشبکه ..... Lattice
وارد کردن ..... Insertion
وزن همینگ ..... Hamming weight

واژه‌نامه انگلیسی به فارسی

کد بلوکی ..... Block code
تابع مشخصه ..... Characteristic function
الفبای کد ..... Code alphabet
اندازه کد ..... Code cardinality
کدواژه ..... Codeword
کانال ارتباطی ..... Communication channel
کد اندازه‌ـ ثابت ..... Constant-cardinality code
کدگشایی ..... Decoding
حذف ..... Deletion
سادک گسسته ..... Discrete simplex
فاصله تعدی ..... Distance transitive
کدگذاری ..... Encoding
فاصله همینگ ..... Hamming distance
وزن همینگ ..... Hamming weight
وارد کردن ..... Insertion
کدهای صحیح ..... Integer codes
مشبکه ..... Lattice
کد خطی ..... Linear code
متر منهتن ..... Manhatan metric
تابع چندگانگی ..... Multiplicity function
چندمجموعه ..... Multi-set
بسته‌بندی ..... Packing
کد کامل ..... Perfect code
کانال جایگشتی ..... Permutation channel
جایگزینی ..... Substitution
فرش کردن ..... Tiling

Abstract

Designing proper codes, in both theoretical and applied perspectives, is considered as an important problem in the coding theory. Since appearance of coding theory, many researchers has tried so much and thereby has generated various interesting kinds of these codes. In this thesis, we want to study the existence or nonexistence of perfect codes in discrete simplexes and multi-set codes in permutation channels. First, it is discussed about the introduction of coding theory and required definitions for the remaining chapters. Then perfect codes in discrete simplex are analyzed in different dimensions and we conclude that perfect codes always exists in the case of binary alphabet, whereas in the case of ternary alphabet we have perfect codes just in some special cases. Actually we show that perfect codes in 1-simplex exist for any $\ell \geq 2e + 1$, the 2-simplex admits a perfect code if and only if $\ell = 3e + 1$, while there are no perfect codes in higher dimensional simplexes. In other words, perfect codes exist only over binary and ternary alphabets. Then we investigate multi-set codes in permutation channels and errors including deletion, insertion and substitution in permutation channels. Finally, existence of perfect codes in A_n and $\mathbb{Z}^n$ lattices are investigated.

Keywords: Perfect code, Discrete simplex, Permutation channel, Multi-set code, A_n Lattice, $\mathbb{Z}^n$ Lattice, Insertion, Deletion, Substitution.

Shahrood University of Technology

Faculty Of Mathematical Sciences

MSc Thesis in: Graph and Combinatorics

On Perfect and Multi-set Codes over Permutation Channels and Discrete Simplexes

By: Anese Eslami

Supervisors

Dr. Sadegh Rahimi Sharbaf
Dr. Abdollah Alhevaz

July 2017