به نام خالق یکتا

مقدمه‌ای بر نظریه کدگذاری

ویراست سوم

تالیف:

ج. اچ. ون لینت

ترجمه:

محمد غلامی

استادیار دانشگاه شهرکرد

و

رضا سبحانی

استادیار دانشگاه اصفهان

ویراستار: دکتر مسعود فروزنده

طراح روی جلد: مصطفی غلامی

مقدمه مترجمین

نظریه کدگذاری کانال، یکی از شاخه‌های پرکاربرد مخابرات است که هدف از آن ارسال اطلاعات از فرستنده از طریق یک کانال فیزیکی دارای اغتشاش، به گیرنده می‌باشد. کلود شانون را می‌توان پایه‌گذار این نظریه دانست که در مقاله‌ای اساسی در سال ۱۹۴۸ ثابت نمود کدهای تصحیح‌کننده خطا با نرخ ارسال کمتر از ظرفیت کانال وجود دارند که پس از ارسال بر روی کانال، دارای احتمال خطای کدگشایی نزدیک به صفر می‌باشند. شانون این مطلب را به‌صورت وجودی اثبات کرد و روند اثبات او بر پایه نظریه احتمال بوده و روش خاصی را جهت معرفی کد مطلوب مشخص نمی‌کرد. پس از آن بود که تلاش‌های زیادی برای رسیدن به کدهای مطلوب آغاز گردید و کدهای معروفی نظیر کدهای همینگ، گُلِی، رید—مولر، کانولوشن، BCH، رید—سولومن، کدهای توربو و سرانجام کدهای خلوت یا LDPC مطرح شدند.

اگرچه در دانشکده مهندسی برق و کامپیوتر، این شاخه دارای قدمتی طولانی است و اکثر کتاب‌ها و مقالاتی که در این زمینه به رشته تحریر در آمده، توسط مهندسین برق و مخابرات بوده است، اما در سال‌های گذشته به دلیل توجه خاص به تحلیل مباحث تئوری در ساخت و کدگشایی کدهای تصحیح—کننده خطا، علاقه ریاضی‌دانان در این زمینه، رشد خاصی در کشورهای مختلف و هم‌چنین در کشور ما داشته است. با نگاهی اجمالی می‌توان مشاهده نمود که بسیاری از شاخه‌های ریاضیات محض و کاربردی، مانند جبر، هندسه، گراف، ترکیبیات و غیره، هر کدام به گونه‌ای در این زمینه نقش موثر داشته و دارند. با این وجود نمی‌توان این رشته را تنها در این دروس محدود نمود.

در کشور ما، در سال‌های اخیر کتاب‌هایی در این زمینه تالیف و ترجمه شده، اما این کتاب‌ها تا حدودی مقدماتی بوده و یا بیشتر مربوط به شاخه‌های دیگر مخابرات است. از این‌رو بر آن شدیم تا کتابی مناسب در این زمینه یافته و آن را ترجمه نماییم. کتاب حاضر که سال‌ها به عنوان یکی از مراجع کلاسیک در زمینه‌های مهمی از رشته‌های نظریه اطلاعات و کدگذاری مورد استفاده قرار گرفته است، یک کتاب درسی مفید در نظریه کدگذاری است که نویسنده سعی نموده تا بسیاری از مباحث اولیه و اساسی کدگذاری مانند کدهای خطی و غیرخطی، کدهای دوری و کدهای کانولوشن را به نحو موثری در آن پوشش دهد. در اینجا فرض شده است که خواننده با برخی مفاهیم مقدماتی از جبر و نظریه احتمالات آشنایی دارد. نویسنده همچنین سعی نموده تا مباحث را به‌صورت تئوری و دقیق بیاورد و برای فهم بیشتر مطالب در آخر مثال‌هایی آورده است. نسخه سوم که مطالب در آن بهبود داده شده و گسترش یافته است، شامل

فصل‌هایی از هندسه جبری، کلاس‌های جدیدی از کدها و پیشرفت‌های اخیر در نظریه کدگذاری می‌باشد که متاسفانه با مرگ نویسنده در سال ۲۰۰۴ تجدید چاپ آن متوقف شد. همچنین در آخر هر فصل تمرین‌های مفیدی آورده شده که جواب‌های کامل آن در آخر کتاب آمده است.

نسخه سوم که ترجمه آن هم‌اکنون در اختیار شماست، می‌تواند به عنوان یک کتاب درسی مفید در مقطع کارشناسی ارشد و قسمت‌هایی از آن در مقطع کارشناسی، تدریس شود. با آن‌که سعی شده تا روان بودن و حفظ معنای جملات تا حد ممکن رعایت شود ولی مترجمین، این ترجمه را خالی از اشکال ندانسته و از خوانندگان محترم می‌خواهند تا در صورت مشاهده هر گونه اشکال، آن را با ما در میان بگذارند. امید داریم تا این ترجمه، هدیه کوچکی باشد تقدیم به روح حضرت امام (قدس سره) و شهدای والامقام که رشد علمی جامعه اسلامی ما مدیون خون آن بزرگ‌مردان است.

مقدمه مولف

این مطلب که این کتاب درسی به‌عنوان سومین نسخه، هنوز به اندازه کافی محبوب است، لذت‌بخش است. من از این فرصت به‌منظور بهبود و گسترش کتاب استفاده نموده‌ام.

هنگامی که نسخه دوم آماده شد، تنها دو صفحه درباره کدهای هندسه جبری اضافه شد. این مطالب هم‌اکنون حذف گردیده و به‌جای آن یک فصل نسبتاً طولانی درباره این موضوع اضافه شده است. هر چند که آن هنوز هم در حد یک مقدمه است، اما احتیاج به پیش‌نیازهای ریاضی بیشتری از خواننده، نسبت به سایر مطالب این کتاب دارد.

یکی از پیشرفت‌های بسیار جالب در سال‌های اخیر، مربوط به کدهای دوتایی تعریف‌شده با استفاده از کدهای ساخته‌شده بر روی الفبای $\mathbb{Z}_4$ می‌باشد. وجود علاقه وافر در این زمینه باعث شد تا یک فصل در رابطه با ملزومات آن، اضافه شود. داشتن آگاهی در رابطه با این فصل، به خواننده اجازه خواهد داد تا متون اخیر در رابطه با $\mathbb{Z}_4$–کدها را مطالعه نماید.

علاوه‌براین، برخی مطالب مربوط به کدهای رید–سولومن گسترش‌یافته و کدهای رید–مولر گسترش‌یافته، اضافه شده‌اند که در سخنرانی‌های من در اشپرینگر[۱] ۲۰۱ بیان شده، اما در جدیدترین نسخه این کتاب وارد نشده بود. در فصل ۲ هم، یک بخش درباره "بهره کدگذاری" (توجیه مهندسی برای استفاده از کدهای تصحیح‌کننده خطا) اضافه شد.

برای نویسنده، تهیه این ویرایش سوم، مهم‌ترین بازگشت خوشایند به ریاضیات، پس از هفت سال مدیریت، بود. برای مباحث ارزشمند درباره مطالب جدید، از باگن[۲]، دورسما[۳]، هالمن[۴] ون تیلبرگ[۵]، و ویلسن[۶] تشکر می‌کنم. هم‌چنین از لطف پلیکان[۷] و کمک او در تهیه فصل ۷ تشکر مخصوص دارم.

ون‌لینت[۸]

شهر آیندهوون[۹]، نوامبر ۱۹۹۸.

---

[۱] Springer
[۲] C.P.J.M. Baggen
[۳] I.M. Duursma
[۴] H.D.L. Hollmann
[۵] H.C.A. van Tilborg
[۶] R. M. Wilson
[۷] R.A. Pellikaan
[۸] J. H. van Lint
[۹] Eindhoven

فهرست مطالب

فصل ۱

پیش‌زمینهٔ ریاضی

به‌جهت داشتن توانایی لازم برای خواندن این کتاب، یک پیش زمینه نسبتاً کلی از ریاضیات لازم است. در فصل‌های مختلف، بسیاری از جنبه‌های متفاوت ریاضیات ایفای نقش می‌نمایند. مهم‌ترین آنها به‌طور یقین جبر است. اما خواننده باید علاوه بر آن مطالبی از نظریه اعداد، نظریه احتمالات و برخی از مفاهیم نظریه ترکیبیات مانند طرح‌ها[۱] و هندسه‌ها [۲] را بداند. در بخش‌های ذیل، یک بررسی مجمل از این مطالب را ارایه خواهیم نمود. به‌طور معمول اثبات‌ها حذف می‌گردد. برای دیدن این اثبات‌ها، به کتاب‌های درسی استانداردی ارجاع خواهیم داد. در برخی از فصل‌های این کتاب، به تعداد زیادی از قوانین مربوط به کلاسی نه‌چندان معروف از چندجمله‌ای‌های متعامد[۳] ، به‌نام چندجمله‌ای‌های کراچوک، [۴] نیاز داریم. این خواص در بخش ۱.۲ مورد بحث قرار می‌گیرد. علامت‌گذاری به‌کار رفته، نسبتاً استاندارد می‌باشد. تعداد کمی از علامت‌هایی که به کار می‌بریم، به‌طور معمول شناخته شده نمی‌باشند. اگر C یک مجموعه متناهی باشد، تعداد عناصر آن را با $|c|$ نمایش می‌دهیم. اگر عبارت B به‌معنای مفهوم A باشد، می‌نویسیم $A := B$. یک ماتریس همانی را با I نمایش داده و J یک ماتریس تماماً یک می‌باشد. به‌طور مشابه، بردار با عناصر صفر یا یک را به‌ترتیب با $\mathbf{0}$ یا $\mathbf{1}$ نمایش می‌دهیم. به‌جای $[x]$ می‌نویسیم $\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$ و نماد $\lceil x \rceil$ را برای گِرد کردن به بالا به‌کار می‌بریم.

---

[۱] designs

[۲] geometries

[۳] orthogonal polynomials

[۴] Krawtchouk

۱.۱ جبر

ما تنها به مقدمات بسیار کمی از نظریه اعداد نیاز داریم. از قبل می‌دانیم که هر عضو $\mathbb{N}$ را می‌توان تنها به یک روش، به‌صورت حاصل‌ضرب اعداد اول نوشت (اگر از ترتیب عوامل صرف‌نظر کنیم). اگر b بر a بخش‌پذیر باشد، می‌نویسیم $a \mid b$. اگر p یک عدد اول باشد و $p^r \mid a$، اما $p^{r+1} \nmid a$ می‌نویسیم $p^r \mid\mid a$. اگر $k \in \mathbb{N}$، $k > 1$، آن‌گاه برای $0 \leq i \leq l$، یک نمایش از n در پایه k به‌صورت:

$$n = \sum_{i=0}^{l} n_i k^i,$$

$0 \leq n_i < k$ می‌باشد. بزرگ‌ترین عدد صحیح n به‌طوری که $n \mid a$ و $n \mid b$، بزرگ‌ترین مقسوم‌علیه مشترک a و b نامیده می‌شود و با نماد (a, b) ب.م.م یا به اختصار (a, b) نمایش داده می‌شود. اگر $m \mid (a - b)$، آن‌گاه می‌نویسیم $a \equiv b \bmod m$.

قضیه ۱.۱.۱. اگر:

$$\varphi(n) := |\{m \in \mathbb{N} \mid 1 \leq m \leq n, (m, n) = 1\}|,$$

آن‌گاه:

۱) $\varphi(n) = n \prod_{p \mid n}(1 - 1/p)$؛

۲) $\sum_{d \mid n} \varphi(d) = n$.

تابع φ شاخص اویلر[۵] نامیده می‌شود.

قضیه ۲.۱.۱. اگر $(a, m) = 1$ آن‌گاه $a^{\varphi(m)} \equiv 1 \bmod m$.

قضیه ۲.۱.۱، قضیه اویلر—فرما نامیده می‌شود.

تعریف ۳.۱.۱. تابع موبیوس[۶] μ، به‌صورت زیر تعریف می‌شود:

$$\mu(n) := \begin{cases} 1, & \text{اگر } n = 1, \\ (-1)^k, & \text{اگر } n \text{ حاصل‌ضرب } k \text{ عامل اول مجزا باشد}, \\ 0, & \text{در غیر این‌صورت}. \end{cases}$$

[۵] Euler indicator

[۶] Möbius

قضیه ۴.۱.۱. اگر f و g توابعی تعریف شده روی $\mathbb{N}$ باشند، به‌طوری که:

$$g(n) = \sum_{d \mid n} f(d),$$

آن‌گاه:

$$f(n) = \sum_{d \mid n} \mu(d) g(\frac{n}{d}).$$

قضیه ۴.۱.۱ به فرمول معکوس موبیوس[۷] معروف است.

ساختارهای جبری

فرض می‌کنیم خواننده با مفاهیم و قضایای اصلی جبرخطی آشناست، اگرچه این مطالب را در زیر یادآوری می‌کنیم. در ابتدا ما یک سری تعریف ساختارهای جبری را که خواننده باید با آنها آشنا باشد، به منظور درک نظریه کدگذاری جبری می‌آوریم.

تعریف ۵.۱.۱. یک گروه $(G,)$ یک مجموعه G می‌باشد؛ به‌طوری که یک عمل‌گر حاصل‌ضرب روی آن تعریف شده و این عمل‌گر در خواص زیر صدق می‌کند:

$$\forall_{a \in G} \forall_{b \in G} \; [ab \in G], \qquad (۱)$$

$$\forall_{a \in G} \forall_{b \in G} \forall_{c \in G} \; [(ab)c = a(bc)], \qquad (۲)$$

$$\exists_{e \in G} \forall_{a \in G} \; [ae = ea = a], \qquad (۳)$$
(عضو e یکتاست)

$$\forall a \in G \exists_{b \in G} \; [ab = ba = e], \qquad (۴)$$
(b وارون a نامیده می‌شود و با a^{-1} نمایش داده می‌شود.)

علاوه‌براین اگر:

$$\forall_{a \in G} \forall_{b \in G} \; [ab = ba], \qquad (۵)$$

آن‌گاه گروه یادشده، آبلی یا جابه‌جایی نامیده می‌شود.

[۷] Möbius inversion formula

اگر $(G,)$ یک گروه باشد و $H \subset G$ به‌طوری‌که $(H,)$ نیز یک گروه باشد، آن‌گاه $(H,)$ یک زیرگروه $(G,)$ نامیده می‌شود. تعداد عناصر یک گروه متناهی، مرتبه آن گروه نامیده می‌شود. اگر $(G,)$ یک گروه باشد و $a \in G$ آن‌گاه کوچک‌ترین عدد صحیح مثبت n به‌طوری که $a^n = e$ (اگر چنین nی موجود باشد)، مرتبه a نامیده می‌شود. دراین حالت عناصر e، a، $a^۲$، ...، $a^{n-۱}$ تشکیل یک زیرگروه، معروف به زیرگروه دوری، می‌دهند که a به‌عنوان مولد آن شناخته می‌شود. اگر $(G,)$ آبلی باشد و $(H,)$ یک زیرگروه آن باشد، آن‌گاه مجموعه‌های $aH := \{ah \,|\, h \in H\}$ هم‌مجموعه‌های H نامیده می‌شوند. از آنجا که دو هم‌مجموعه به‌وضوح برابر یا مجزا می‌باشند، هم‌مجموعه‌ها تشکیل یک افراز برای G می‌دهند. یک عضو انتخابی از یک هم‌مجموعه یک نماینده از آن هم‌مجموعه نامیده می‌شود. اگر حاصل‌ضرب هم‌مجموعه‌ها را با $(aH)(bH) := abH$ تعریف کنیم، نشان‌دادن این‌که هم‌مجموعه‌ها مجدداً یک گروه تشکیل می‌دهند، مشکل نیست. این گروه، گروه خارج قسمتی[۸] نامیده می‌شود و با G/H نمایش داده می‌شود. به‌عنوان یک نتیجه، دقت دارید که اگر $a \in G$ آن‌گاه مرتبه a مرتبه G را عاد می‌کند (هم‌چنین اگر G آبلی نباشد).

یک قضیه اساسی از نظریه گروه‌ها بیان می‌کند که یک گروه آبلی متناهی، مجموع مستقیم گروه‌های دوری است.

تعریف ٦.١.١. یک مجموعه R با دو عملگر، که معمولاً جمع و ضرب نامیده می‌شوند، و نمایش داده شده به‌وسیله $(R, +,)$، یک حلقه است اگر:

(۱) $(R, +)$ یک گروه آبلی باشد.

(۲) $\forall_{a\in R}\forall_{b\in R}\forall_{c\in R}[(ab)c = a(bc)]$,

(۳) $\forall_{a\in R}\forall_{b\in R}\forall_{c\in R}[a(b + c) = ab + ac \wedge (a + b)c = ac + bc]$.

عضو همانی $(R, +)$ معمولا با **0** نماش داده می‌شود.

اگر خاصیت اضافی

(۴) $\forall_{a\in R}\forall_{b\in R}[ab = ba]$,

برقرار باشد، آن‌گاه این حلقه را جابه‌جایی می‌نامیم.

اعداد صحیح $\mathbb{Z}$ بهترین مثال شناخته‌شده از یک حلقه می‌باشد.

اگر $(R, +,)$ یک حلقه جابه‌جایی باشد، آن‌گاه یک عضو ناصفر $a \in R$ یک مقسوم‌علیه صفر نامیده می‌شود اگر یک عضو ناصفر $b \in R$ موجود باشد، به‌قسمی که $ab = ۰$. حلقه‌ای که شامل هیچ مقسوم‌علیه صفری نباشد، یک قلمرو صحیح نامیده می‌شود. مشابه روشی که $\mathbb{Z}$ به اعداد $\mathbb{Q}$ گسترش داده می‌شود،

[۸] factor group

یک قلمرو صحیح می‌تواند در میدان خارج‌قسمت‌ها یا میدان کسری خود نشانده شود.

تعریف ۷.۱.۱. اگر $(R,+,\ )$ یک حلقه باشد و $\emptyset \neq S \subseteq R$ آن‌گاه S یک ایده‌آل نامیده می‌شود، اگر:

۱) $\forall_{a\in S}\forall_{b\in S}[a-b\in S]$؛

۲) $\forall_{a\in S}\forall_{b\in R}[ab\in S \wedge ba\in S]$.

روشن است که اگر S یک ایده‌آل در R باشد، آن‌گاه $(S,+,\ )$ یک زیرحلقه می‌باشد، اما شرط (۲) چیز بیشتری از این را بیان می‌کند.

تعریف ۸.۱.۱. یک میدان، یک حلقه $(R,+,\ )$ است به‌طوری که $(R-\{۰\},\ )$ یک گروه آبلی است.

قضیه ۹.۱.۱. هر حلقه متناهی R با حداقل دو عضو به‌طوری:

$$\forall_{a\in R}\forall_{b\in R}[ab=۰ \Rightarrow (a=۰ \vee b=۰)],$$

یک میدان است.

تعریف ۱۰.۱.۱. فرض کنید $(V,+)$ یک گروه آبلی، $\mathbb{F}$ یک میدان و ضرب $\mathbb{F}\times V\to V$ با خواص زیر تعریف شده باشد:

۱) $\forall_{a\in V}[۱a=a]$،

$\forall_{\alpha\in\mathbb{F}}\forall_{\beta\in\mathbb{F}}\forall_{a\in V}[\alpha(\beta a)=(\alpha\beta)a]$،

۲) $\forall_{\alpha\in\mathbb{F}}\forall_{a\in V}\forall_{b\in V}[\alpha(a+b)=\alpha a+\alpha b]$،

$\forall_{\alpha\in\mathbb{F}}\forall_{\beta\in\mathbb{F}}\forall_{a\in V}[(\alpha+\beta)a=\alpha a+\beta a]$.

در این‌صورت سه‌تایی $(V,+,\mathbb{F})$ یک فضای برداری روی میدان $\mathbb{F}$ نامیده می‌شود. هم‌چنین عضو همانی $(V,+)$ با ۰ نمایش داده می‌شود.

فرض می‌کنیم خواننده با فضای برداری $\mathbb{R}^n$ شامل تمامی $n-$تایی‌های $(a_۱,a_۲,...,a_n)$ با قوانین ضرب و جمع بدیهی، آشنا می‌باشد. به خواننده این واقعیت را یادآوری می‌کنیم که زیرفضای $k-$بعدی C از این فضای برداری، یک فضای برداری با پایه‌ای متشکل از بردارهای $a_۱ := (a_{۱۱},a_{۱۲},...,a_{۱n})$،

$a_k := (a_{k1}, a_{k2}, ..., a_{kn})$ ، ...، $a_2 := (a_{21}, a_{22}, ..., a_{2n})$ است که در آن، کلمه پایه به این معناست که هر $a \in C$ را بتوان به‌طور یکتا به‌صورت $\alpha_1 a_1 + \alpha_2 a_2 + ... + \alpha_k a_k$ نوشت. خواننده هم‌چنین باید با فرایند رفتن از یک پایه C به پایه دیگر آن با استفاده از ترکیب نمودن بردارهای پایه و موارد مشابه آشنا باشد. همان‌گونه که در بالا انجام شد، به‌طور معمول بردارها را به‌عنوان بردارهای سطری می‌نویسیم. ضرب داخلی $< a, b >$ از دو بردار a و b به‌صورت:

$$< a, b >:= a_1 b_1 + a_2 b_2 + ... + a_n b_n,$$

تعریف می‌شود. عناصر یک پایه، به‌طور خطی مستقل نامیده می‌شوند. معنای آن این است که یک ترکیب خطی از این بردارها برابر با ۰ است اگر و تنها اگر تمامی ضرایب برابر با صفر باشند. اگر a_1، ...، a_k، k تا بردار به‌طور خطی مستقل باشند؛ یعنی یک زیرفضای k–بعدی از C، آن‌گاه جواب سیستم معادلات $< a_i, y >= 0$، $i = 1, 2, \cdots, k$، شامل تمامی بردارها در یک زیرفضای $(n-k)$–بعدی است که ما آن را با $C^\perp$ نمایش می‌دهیم؛ بنابراین:

$$C^\perp := \{y \in \mathbb{R}^n \mid \forall_{x \in C}[< x, y >= 0]\}.$$

در ادامه، وقتی‌که $\mathbb{R}$ با یک میدان متناهی $\mathbb{F}$ جای‌گزین شود، این ایده‌ها یک نقش اساسی بازی می‌کنند. دقت کنید که نظریه بررسی شده در بالا، در این حالت نیز قابل پیاده‌سازی است.

تعریف ۱.۱.۱. فرض کنید $(V, +)$ یک فضای برداری روی میدان $\mathbb{F}$ باشد و ضرب $V \times V \to V$ با خواص زیر تعریف شده باشد:

۱) $(V, +,)$ یک حلقه باشد،

۲) $\forall_{\alpha \in \mathbb{F}} \forall_{a \in V} \forall_{b \in V}[(\alpha a)b = a(\alpha b)]$.

در این‌صورت این دستگاه را یک جبر روی $\mathbb{F}$ می‌گوییم.

فرض کنید یک گروه متناهی $(G, .)$ داریم و عناصر G را به‌عنوان پایه‌ی یک فضای برداری $(V, +)$ روی میدان $\mathbb{F}$ درنظر گرفته‌ایم. در این‌صورت عناصر V توسط ترکیبات خطی $\alpha_1 g_1 + \alpha_2 g_2 + ... + \alpha_n g_n$ نمایش داده می‌شوند که در آن:

$$a_i \in \mathbb{F}, \quad g_i \in G, \quad (1 \leq i \leq n = |G|).$$

می‌توانیم یک ضرب $*$ را برای این بردارها به‌روش بدیهی تعریف نماییم؛ یعنی:

$$(\sum_i \alpha_i g_i) * (\sum_j \beta_j g_j) := \sum_i \sum_j (\alpha_i \beta_j)(g_i . g_j),$$

که می‌تواند به‌صورت $\sum_k \gamma_k g_k$ نوشته شود، جایی که γ_k مجموع عناصر $\alpha_i b_j$ روی تمامی زوج‌های (i,j) می‌باشد به‌طوری‌که $g_i.g_j = g_k$. این ضرب، یک جبر را القا می‌کند که جبر گروهی G روی میدان $\mathbb{F}$ نامیده می‌شود و با $\mathbb{F}G$ نمایش داده می‌شود.

مثال‌ها. در اینجا تعدادی مثال از مفاهیم ارائه‌شده در بالا را می‌آوریم.

اگر $A := \{a_1, a_2, ..., a_n\}$ یک مجموعه متناهی باشد، آن‌گاه تمامی توابع یک‌به‌یک از A به A را درنظر بگیرید. اینها جای‌گشت‌ها نامیده می‌شوند. اگر σ_1 و σ_2 جای‌گشت‌هایی باشند، آن‌گاه $\sigma_1\sigma_2$ را با $(\sigma_1\sigma_2)(a) := \sigma_1(\sigma_2(a))$ برای تمامی $a \in A$ تعریف می‌کنیم. به‌آسانی دیده می‌شود که مجموعه S_n شامل تمامی جای‌گشت‌های A با عمل ضرب، یک گروه است که به گروه متقارن مرتبه n معروف است. در این کتاب، ما اغلب به گروه‌های جایگشتی خاصی علاقه‌مند هستیم. اینها زیرگروه‌های S_n می‌باشند. یک مثال می‌آوریم. فرض کنید C یک زیرفضای k–بعدی $\mathbb{R}^n$ باشد. تمامی جای‌گشت‌های σ از اعداد صحیح ۱، ۲، ...، n را درنظر بگیرید که برای هر $(c_1, c_2, ..., c_n) \in C$، بردار $(c_{\sigma(1)}, c_{\sigma(2)}, ..., c_{\sigma(n)})$ نیز در C باشد. به‌وضوح این بردارها تشکیل یک زیرگروه می‌دهند. البته C اغلب به‌گونه‌ای است که این زیرگروه S_n تنها شامل عضو همانی باشد، اما مثال‌های جالب‌تری وجود دارند! مثال دیگری از یک گروه جایگشتی که در ادامه مطالب خواهد آمد، یک گروه جایگشتی آفین می‌باشد که به‌صورت زیر تعریف می‌شود:

فرض کنید $\mathbb{F}$ یک میدان (متناهی) باشد. نگاشت $f_{u,v}$ که در آن $u \in \mathbb{F}$، $v \in \mathbb{F}$ و $u \neq 0$ روی $\mathbb{F}$ با ضابطه $f_{u,v}(x) := ux + v$ برای تمامی $x \in \mathbb{F}$ تعریف می‌شود. این نگاشت ها، جای‌گشت‌هایی از $\mathbb{F}$ هستند و به‌وضوح تحت ترکیب توابع تشکیل یک گروه می‌دهند.

یک ماتریس جایگشتی P یک $(0,1)$–ماتریس است که دارای دقیقاً یک ۱ در هر سطر و ستون می‌باشد. گوییم P متناظر با جای‌گشت σ از $\{1, 2, ..., n\}$ می‌باشد وقتی‌که $p_{ij} = 1$ اگروتنهااگر $i = \sigma(j)$، $i = 1, 2, \cdots, n$. با این قرارداد، حاصل‌ضرب جای‌گشت‌ها متناظر با حاصل‌ضرب ماتریس‌های آنها می‌باشد. با این روش، نمایش ماتریسی معروفی از یک گروه جای‌گشت‌ها به‌دست می‌آید.

یک گروه G متشکل از جای‌گشت‌های روی مجموعه Ω، یک k–تراگذر روی Ω نامیده می‌شود اگر برای هر k–تایی مرتب $(a_1, a_2, ..., a_k)$ از عناصر متمایز Ω و برای هر k–تایی $(b_1, b_2, ..., b_k)$ از عناصر متمایز Ω یک عضو $\sigma \in G$ موجود باشد به‌طوری که برای هر $1 \leq i \leq k$ داشته باشیم $b_i = \sigma(a_i)$. اگر $k = 1$ این گروه را گروه تراگذر می‌نامیم.

فرض کنید S یک ایده‌آل در حلقه $(R, +,)$ باشد. چون $(S, +)$ یک زیرگروه از گروه آبلی $(R, +)$ است می‌توانیم گروه عامل را تشکیل دهیم. این هم‌مجموعه‌ها در اینجا کلاس‌های باقی‌مانده به پیمانه S

نامیده می‌شوند. برای این کلاس‌ها، ما ضرب بدیهی $(a+S)(b+S) := ab+S$ را تعریف می‌کنیم. خواننده‌ای که با این مفهوم آشنا نیست، باید خوش‌تعریف بودن آن‌را چک نماید (به این معنی که این تعریف به انتخاب نماینده‌های a و b بستگی ندارد). با این روش ما یک حلقه ساخته‌ایم که آن را حلقه کلاس باقی‌مانده R به پیمانه S می‌نامیم و با R/S نمایش می‌دهیم. مثال زیر قطعاً آشنا خواهد بود. فرض کنید $R := \mathbb{Z}$ و p یک عدد اول باشد. فرض کنید S همان $p\mathbb{Z}$، مجموعه تمامی مضارب p، باشد که برخی اوقات با نماد (p) نیز نمایش داده می‌شود؛ در این‌صورت R/S حلقه اعداد صحیح به پیمانه p است. عناصر R/S با ۰، ۱، ...، $p-1$ نمایش داده می‌شوند؛ بنابراین، ضرب و جمع در آن همان عمل‌گرهای متداول در $\mathbb{Z}$ هستند که به پیمانه p تقلیل یافته‌اند؛ به‌عنوان مثال، اگر قرار دهیم $p = ۷$، در این‌صورت $۲ = ۵ + ۴$ زیرا در $\mathbb{Z}$ داریم $۵ + ۴ \equiv ۲ \bmod ۷$. به روش مشابه $۴.۵ = ۶$ در $\mathbb{Z}/(۷) = \mathbb{Z}/۷\mathbb{Z}$. اگر S یک ایده‌آل در $\mathbb{Z}$ باشد و $S \neq \{۰\}$، آن‌گاه کوچک‌ترین عدد صحیح k در S وجود دارد. فرض کنید $s \in S$. می‌توانیم s را به‌صورت $ak+b$ بنویسیم که در آن $۰ \leq b < k$. با تعریف ایده‌آل، داریم $ak \in S$؛ بنابراین، $b = s - ak \in S$ و بنابر تعریف k نتیجه می‌شود $b = ۰$. از این‌رو $S = (k)$. یک ایده‌آل که شامل تمامی مضارب یک عضو ثابت است، یک ایده‌آل اصلی نامیده می‌شود. اگر تمامی ایده‌آل‌های حلقه R اصلی باشند آن‌گاه R یک حلقه ایده‌آل اصلی نامیده می‌شود؛ بنابراین، $\mathbb{Z}$ یک چنین حلقه‌ای است.

ایده‌آل S یک ایده‌آل اول نامیده می‌شود اگر $ab \in S$ ایجاب کند که $a \in S$ یا $b \in S$. ایده‌آل S در حلقه R ماکسیمال نامیده می‌شود، اگر برای هر ایده‌آل I با شرط $S \subset I \subset R$ بتوان نتیجه گرفت $I = S$ یا $I = R$ $(S \neq R)$. اگر یک حلقه دارای یک ایده‌آل یکتای ماکسیمال باشد، آن را یک حلقه موضعی می‌نامیم.

قضیه ۱۲.۱.۱. اگر p یک عدد اول باشد آن‌گاه $\mathbb{Z}/p\mathbb{Z}$ یک میدان است.

قضیه فوق یک نتیجه فوری و بلکه سرراست از قضیه ۹.۱.۱ است. یک میدان متناهی با n عضو، با $\mathbb{F}_n$ یا $GF(n)$ (میدان گالوا) نمایش داده می‌شود.

حلقه‌ها و میدان‌های متناهی

مطالب بیشتری از میدان‌های متناهی در اینجا دنبال خواهد شد. درابتدا مطالب بیشتری درباره حلقه‌ها و ایده‌آل‌ها را بیان می‌کنیم. فرض کنید $\mathbb{F}$ یک میدان متناهی باشد. مجموعه $\mathbb{F}[x]$ شامل تمامی چندجمله‌ای‌ها به‌صورت $a_۰ + a_۱x + ... + a_nx^n$ می‌باشد که در آن n می‌تواند هر عدد صحیح در $\mathbb{N}$ باشد و برای $۰ \leq i \leq n$ داریم $a_i \in \mathbb{F}$. با تعریف متداول جمع و ضرب چندجمله‌ای‌ها، $(\mathbb{F}, +,)$ یک

حلقه می‌باشد که معمولاً با $\mathbb{F}[x]$ نمایش داده می‌شود. مجموعه چندجمله‌ای‌هایی که مضربی از یک چندجمله‌ای ثابت $g(x)$ می‌باشند؛ یعنی مجموعه تمامی چندجمله‌ای‌ها به شکل $a(x)g(x)$ که در آن $a(x) \in \mathbb{F}[x]$، تشکیل یک ایده‌آل در $\mathbb{F}[x]$ می‌دهند.

مانند قبل، این ایده‌آل را با $(g(x))$ نمایش می‌دهیم. قضیه زیر نشان می‌دهد که تمامی ایده‌آل‌های $\mathbb{F}[x]$ به این‌صورت می‌باشند.

قضیه ۱.۱.۱۳. $\mathbb{F}[x]$ یک حلقه ایده‌آل اصلی می‌باشد.

حلقه کلاس‌های باقی‌مانده $\mathbb{F}/(g(x))$ را می‌توان به‌صورت چندجمله‌ای‌های با درجه کمتر از درجه $g(x)$ نمایش داد. در روشی مشابه با مثال $\mathbb{Z}/7\mathbb{Z}$ که در بالا بیان شد، می‌توانیم این نماینده‌ها را به‌طریق متداول، ضرب و جمع نمود و بعد باقی‌مانده آن‌را به پیمانه $g(x)$ محاسبه کرد. برای نمونه، قرار دهید $\mathbb{F} = \mathbb{F}_2 = \{0,1\}$ و $g(x) = x^3 + x + 1$. آن‌گاه $(x+1)(x^2+1) = x^3 + x^2 + x + 1 = x^2$. این مثال برای مطالعه دقیق کسی که با میدان‌های متناهی ناآشناست، یک نمونه مفید است. درابتدا مشاهده می‌کنید که $g(x)$ تحویل‌ناپذیر است؛ یعنی چندجمله‌ای‌های $a(x)$ و $b(x)$ در $\mathbb{F}[x]$ وجود ندارند به طوری که هر دو دارای درجه‌های کمتر از ۳ بوده و $g(x) = a(x)b(x)$. سپس تحقیق کنید که این بدان معناست که در $\mathbb{F}_2[x]/(g(x))$، حاصل‌ضرب هر دو عضو $a(x)$ و $b(x)$ برابر با صفر است اگروتنها اگر $a(x) = 0$ یا $b(x) = 0$. با استفاده از قضیه ۹.۱.۱، این بدان معناست که $\mathbb{F}_2[x]/(g(x))$ یک میدان است. چون نماینده‌های این حلقه، کلاس‌های باقی‌مانده با درجه حداکثر ۳ می‌باشند، دقیقاً هشت تا از آنان وجود دارد؛ بنابراین، ما یک میدان با دقیقاً هشت عضو یافته‌ایم. این یک مثال از روشی است که میدان‌های متناهی ساخته می‌شوند.

قضیه ۱.۱.۱۴. فرض کنید p یک عدد اول و $g(x)$ یک چندجمله‌ای تحویل‌ناپذیر با درجه r در حلقه $\mathbb{F}_p[x]$ باشد؛ در این‌صورت حلقه کلاس‌های باقی‌مانده $\mathbb{F}_p[x]/(g(x))$ یک میدان با p^r عضو است.

اثبات. اثبات، مشابه با مثال فوق است که در آن $p = 2$، $r = 3$ و $g(x) = x^3 + x + 1$. □

قضیه ۱.۱.۱۵. فرض کنید $\mathbb{F}$ یک میدان با n عضو باشد؛ در این‌صورت n توانی از یک عدد اول است.

اثبات. با استفاده از تعریف، می‌توان دید که یک عضو همانی ضرب در $\mathbb{F}$ وجود دارد. ما این عضو را با ۱ نمایش می‌دهیم. البته $1 + 1 \in \mathbb{F}$ و ما این عضو را با ۲ نمایش می‌دهیم. این روش را ادامه می‌دهیم؛ یعنی $3 = 1 + 2$ و به همین ترتیب الی آخر. پس از یک تعداد متناهی مرحله، سرانجام به یک عضو

میدان خواهیم رسید که قبلاً تکرار شده است. فرض کنید مجموع k تا ۱ برابر با مجموع l تا ۱ باشد $(k > l)$. بنابراین، مجموع $(k-l)$ تا ۱ برابر با صفر است؛ یعنی اولین باری که با یک عضو تکراری مواجه شدیم، آن عضو صفر است. گوییم ۰ مجموع k تا ۱ است. اگر k یک عدد مرکب باشد، $k = ab$، آن‌گاه حاصل‌ضرب عناصری که آنها را به‌ترتیب a و b نامیده‌ایم، برابر با صفر می‌باشد که یک تناقض است؛ بنابراین، k یک عدد اول مانند p می‌باشد و ما نشان داده‌ایم که $\mathbb{F}_p$ زیرمیدانی از $\mathbb{F}$ است. استقلال خطی یک مجموعه از عناصر $\mathbb{F}$ را نسبت به (ضرایبی از) $\mathbb{F}_p$ به‌طور طبیعی تعریف می‌کنیم. در میان تمام زیرمجموعه‌های مستقل خطی $\mathbb{F}$، فرض کنید $\{x_1, x_2, ..., x_r\}$ دارای بیشترین عضو باشد. اگر x متعلق به $\mathbb{F}$ باشد، آن‌گاه عناصر x، x_1، x_2، ...، x_r مستقل خطی نیستند؛ یعنی ضرایب $\alpha, \alpha_1, ..., \alpha_r \neq 0$ موجودند به‌طوری که $\alpha x + \alpha_1 x_1 + ... + \alpha_r x_r = 0$ و از این‌رو x یک ترکیب خطی از x_1 تا x_r است. چون به‌طور آشکار p^r ترکیب خطی مجزا از عناصر x_1 تا x_r وجود دارد، اثبات کامل است. □

از قضایای قبل می‌دانیم که یک میدان با n عضو وجود دارد اگر و تنها اگر n توانی از یک عدد اول باشد. به این‌صورت که ما می‌توانیم نشان دهیم برای هر $r \geq 1$ یک چندجمله‌ای تحویل‌ناپذیر با درجه r در $\mathbb{F}_p[x]$ وجود دارد. ما این مطلب را با محاسبه تعداد چنین چندجمله‌ای‌هایی اثبات خواهیم نمود. p را ثابت فرض کنید و I_r را تعداد چندجمله‌ای‌های تحویل‌ناپذیر با درجه r تعریف کنید که تکین هستند؛ یعنی ضریب x^r در آنها برابر با ۱ است. ادعا می‌کنیم:

$$(1 - pz)^{-1} = \prod_{r=1}^{\infty} (1 - z^r)^{-I_r} \qquad (1)$$

برای اثبات آن درابتدا می‌بینیم که ضرایب z^n در طرف چپ معادله فوق برابر با p^n می‌باشد که برابر با تعداد چندجمله‌ای‌های تکین با درجه n و ضرایب در $\mathbb{F}_p$ است. می‌دانیم هر چنین چندجمله‌ایی را می‌توان به‌طور یکتا به‌صورت حاصل‌ضرب عوامل تحویل‌ناپذیر تجزیه نمود؛ بنابراین، باید خود را قانع کنیم که این عوامل در طرف راست معادله ۱ شمارش شده‌اند. برای نشان دادن این مطلب، دو چندجمله‌ای تحویل‌ناپذیر $a_1(x)$ با درجه r و $a_2(x)$ با درجه s را درنظر می‌گیریم. یک تناظر یک به یک میان عوامل $(a_1(x))^k (a_2(x))^l$ و جملات $z_1^{kr} z_2^{ls}$ در عوامل $(... + z_1^r + z_1^{2r} + ... + 1)$ و $(... + z_2^s + z_2^{2s} + ... + 1)$ وجود دارد. اگر ما z_1 و z_2 را برابر با z قرار دهیم، آن‌گاه توان z برابر با درجه $(a_1(x))^k (a_2(x))^l$ می‌باشد. حال به‌جای دو چندجمله‌ای $a_1(x)$ و $a_2(x)$، تمامی چندجمله‌ای‌های تحویل‌ناپذیر را درنظر می‌گیریم و رابطه ۱ نتیجه می‌شود.

در رابطه ۱، از دو طرف لگاریتم گرفته و سپس مشتق می‌گیریم. سرانجام دو طرف را در z ضرب

می‌کنیم؛ داریم:

$$\frac{pz}{1-pz} = \sum_{r=1}^{\infty} I_r \frac{rz^r}{1-z^r} \qquad (۲)$$

با مقایسه ضرایب z^n در دو طرف رابطه ۲ داریم:

$$p^n = \sum_{r \mid n} r I_r. \qquad (۳)$$

حال قضیه ۴.۱.۱ را بر روی رابطه ۳ به‌کار می‌گیریم؛ داریم:

$$\begin{aligned} I_r &= \tfrac{1}{r} \sum_{d \mid r} \mu(d) p^{r/d} > \tfrac{1}{r}\{p^r - p^{r/2} - p^{r/3} - \ldots\} \\ &> \tfrac{1}{r}(p^r - \sum_{i=0}^{r/2} p^i) > \tfrac{1}{r} p^r (1 - p^{-r/2+1}) > 0. \end{aligned} \qquad (۴)$$

اکنون که می‌دانیم برای چه مقادیری از n یک میدان با n عضو وجود دارد می‌خواهیم درباره این میدان‌ها مطالب بیشتری بدانیم. ساختار $\mathbb{F}_{p^r}$ یک نقش بسیار مهم در بسیاری از فصل‌های این کتاب ایفا می‌کند. برای شروع، میدان متناهی $\mathbb{F}$ و چندجمله‌ای $f(x) \in \mathbb{F}[x]$ را که در آن برای یک $a \in \mathbb{F}$ داریم $f(a) = 0$، درنظر بگیرید. سپس با تقسیم کردن، متوجه می‌شویم که یک $g(x) \in \mathbb{F}[x]$ وجود دارد به‌طوری که $f(x) = (x-a)g(x)$. با ادامه این روش، این مطلب بدیهی را ثابت می‌کنیم که چندجمله‌ای $f(x)$ با درجه r در $\mathbb{F}[x]$ دارای حداکثر r ریشه در $\mathbb{F}$ است.

اگر α یک عضو با مرتبه e در گروه حاصل‌ضربی $(\mathbb{F}_{p^r} - \{0\},)$ باشد، آن‌گاه α یک ریشه از چندجمله‌ای $x^e - 1$ است. در واقع داریم:

$$x^e - 1 = (x-1)(x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{e-1}).$$

در نتیجه تنها عناصر با مرتبه e در این گروه، توان‌های α^i هستند، که در آن $1 \le i < e$ و $(i,e) = 1$. تعداد $\varphi(e)$ عنصر به این شکل وجود دارند؛ بنابراین، برای هر e که $p^r - 1$ را عاد نماید، تعداد 0 یا $\varphi(e)$ عضو با مرتبه e در این میدان موجود است. با استفاده از قضیه ۱.۱.۱، امکان 0 بودن هیچ‌گاه رخ نمی‌دهد. به‌عنوان یک نتیجه، در واقع دقیقاً $\varphi(p^r - 1)$ عنصر با مرتبه $p^r - 1$ وجود دارند. پس قضیه زیر را اثبات نموده‌ایم:

قضیه ۱۶.۱.۱. در $\mathbb{F}_q$ گروه حاصل‌ضربی $(\mathbb{F}_q - \{0\},)$ یک گروه دوری است.

این گروه را اغلب با $\mathbb{F}_q^*$ نمایش می‌دهیم.

تعریف ۱۷.۱.۱. یک مولد از گروه حاصل‌ضربی میدان $\mathbb{F}_q$ عضو اولیه آن میدان نامیده می‌شود.

دقت کنید که قضیه ۱۶.۱.۱ بیان می‌کند که عناصر $\mathbb{F}_q$ دقیقاً q ریشهٔ متمایز از چندجمله‌ای $x^q - x$ هستند. یک عضو β که $\beta^k = 1$ و برای $0 < l < k$ داشته باشیم $\beta^l \neq 1$، kامین ریشه اولیه واحد نامیده می‌شود. به‌وضوح یک عضو اولیه α از $\mathbb{F}_q$، $(q-1)$امین ریشه اولیه واحد نامیده می‌شود. اگر $q-1$ بر e بخش‌پذیر باشد آن‌گاه α^e یک $(q-1)/e$امین ریشه اولیه واحد نامیده می‌شود. علاوه‌بر آن به عنوان یک نتیجه از قضیه ۱۶.۱.۱ داریم $\mathbb{F}_{p^r}$ زیرمیدانی از $\mathbb{F}_{p^s}$ است اگر و تنهااگر s بر r بخش‌پذیر باشد. درواقع این مطلب ممکن است برای خواننده کمی گیج‌کننده به نظر آید. در نمادگذاری‌هایمان این‌طور به‌نظر می‌رسید که برای عدد داده شده q، میدان $\mathbb{F}_q$ یکتاست. این مطلب در واقع درست است و از رابطه ۳ نتیجه می‌شود. ما نشان داده‌ایم که برای $q = p^n$ هر عضو $\mathbb{F}_q$ یک ریشه از یک عامل تحویل‌ناپذیر از $x^q - x$ است و با توجه به مطلب فوق و قضیه ۱۴.۱.۱ می‌بینیم که این عامل باید دارای درجه r باشد به‌طوری‌که $r \mid n$. از رابطه ۳ نتیجه می‌شود که ما تمامی چندجمله‌ای‌های تحویل‌ناپذیر با درجه r را که در آن $r \mid n$، به‌کار برده‌ایم. به عبارت دیگر، حاصل‌ضرب این چندجمله‌ای‌ها برابر با $x^q - x$ است. این مطلب، این واقعیت را اثبات می‌کند که دو میدان $\mathbb{F}$ و $\mathbb{F}'$ از مرتبه q یک‌ریخت هستند؛ یعنی نگاشت $\varphi : \mathbb{F} \to \mathbb{F}'$ وجود دارد که یک به یک است و جمع و ضرب را حفظ می‌کند.

قضیه زیر بیشتر اوقات در این کتاب به‌کار برده می‌شود.

قضیه ۱۸.۱.۱. فرض کنید $q = p^r$ و $0 \neq f(x) \in \mathbb{F}_q[x]$.

۱) اگر $\alpha \in \mathbb{F}_{q^k}$ و $f(\alpha) = 0$ آن‌گاه $f(\alpha^q) = 0$.

۲) به‌عکس: فرض کنید $g(x)$ یک چندجمله‌ای با ضرایبی از یک میدان گسترش‌یافته از $\mathbb{F}_q$ باشد. اگر برای هر α که $g(\alpha) = 0$ داشته باشیم $g(\alpha^q) = 0$، آن‌گاه $g(x) \in \mathbb{F}_q[x]$.

اثبات.

۱) با به‌کارگیری قضیه چندجمله‌ای داریم $(a+b)^p = a^p + b^p$ زیرا که برای هر $1 \leq k \leq p-1$، عدد $\binom{p}{k}$ بر p بخش‌پذیر است. در نتیجه $(a+b)^p = a^p + b^p$. اگر $f(x) = \sum a_i x^i$ آن‌گاه $(f(x))^q = \sum a_i^q (x^q)^i$.

از آنجا که $a_i \in \mathbb{F}_q$، داریم $a_i^q = a_i$. با جایگذاری $x = \alpha$ خواهیم داشت $f(\alpha^q) = (f(\alpha))^q$.

۲) از قبل می‌دانیم که در یک میدان به‌اندازه کافی گسترش‌یافته از $\mathbb{F}_q$، چندجمله‌ای $g(x)$، حاصل‌ضرب عوامل $x - \alpha_i$، یعنی عوامل مرتبه ۱، می‌باشد و اگر $x - \alpha_i$ یکی از آن عوامل باشد، آن‌گاه $x - \alpha_i^q$

نیز یکی از آنها خواهد بود. اگر $g(x) = \sum_{k=0}^{n} a_k x^k$ آن‌گاه a_k یک تابع متقارن از ریشه‌های α_i می‌شود که نتیجه می‌دهد $a_k = a_k^q$ و این؛ یعنی $a_k \in \mathbb{F}_q$.

اگر $\alpha \in \mathbb{F}_q$ که $q = p^r$ آن‌گاه چندجمله‌ای مینیمال α روی $\mathbb{F}_q$، چندجمله‌ای تحویل‌ناپذیر $f(x) \in \mathbb{F}_p[x]$ است به‌طوری که $f(\alpha) = 0$. اگر α دارای مرتبه e باشد آن‌گاه از قضیه ۱۸.۱.۱ می‌دانیم که این چندجمله‌ای مینیمال برابر با $\prod_{i=0}^{m-1}(x - \alpha^{p^i})$ است، که در آن m برابر با کوچک‌ترین عدد صحیح است به‌طوری که $p^m \equiv 1 \bmod e$.

برخی اوقات، یک میدان $\mathbb{F}_q$ را با یک عضو اولیه ثابت α مشخص می‌کنیم. در آن حالت $m_i(x)$ را به عنوان چندجمله‌ای مینیمال α^i به‌کار می‌بریم. چندجمله‌ای تحویل‌ناپذیری که چندجمله‌ای مینیمال یک عضو اولیه در میدان متناظر باشد، چندجمله‌ای اولیه نامیده می‌شود. چنین چندجمله‌ای‌هایی، مناسب‌ترین نوع برای استفاده در ساختار قضیه ۱۴.۱.۱ هستند. در اینجا مثالی را با جزییات آن می‌آوریم.

مثال ۱۹.۱.۱. چندجمله‌ای $x^4 + x + 1$ روی $\mathbb{F}_2$ یک چندجمله‌ای اولیه است. میدان $\mathbb{F}_{24}$ به‌وسیله چندجمله‌ای‌های با درجه کمتر از ۴ نمایش داده می‌شود. چندجمله‌ای x یک عضو اولیه است. از آنجایی که ما به‌کارگیری نماد x را برای اهداف دیگری ترجیح می‌دهیم، این عضو اولیه را α می‌نامیم. توجه دارید که $\alpha^4 + \alpha + 1 = 0$. هر عضو $\mathbb{F}_{24}$ یک ترکیب خطی از عناصر 1، α، α^2 و α^3 است. جدول ۱.۱ را برای $\mathbb{F}_{24}$ آورده‌ایم. خواننده باید توجه داشته باشد که این جدول، هم‌ارز با جدول لگاریتم‌ها در میدان $\mathbb{R}$ است.

نمایش سمت راست، این مطلب را مجدداً نشان می‌دهد که $\mathbb{F}_{24}$ می‌تواند به عنوان فضای برداری $(\mathbb{F}_2)^4$ تفسیر شود، جایی که $\{1, \alpha, \alpha^2, \alpha^3\}$ یک پایه است. ستون طرف چپ ساده‌ترین روش برای حاصل‌ضرب (جمع توان‌ها در پیمانه ۱۵) است و ستون سمت راست برای حاصل‌جمع (جمع بردارها). حال به‌آسانی می‌توان بررسی نمود که:

$$
\begin{aligned}
m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) &= x^4 + x + 1,\\
m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) &= x^4 + x^3 + x^2 + x + 1,\\
m_5(x) = (x-\alpha^5)(x-\alpha^{10}) &= x^2 + x + 1,\\
m_7(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11}) &= x^4 + x^3 + 1.
\end{aligned}
$$

جدول ۱.۱: جدول عناصر $\mathbb{F}_{۲^۴}$

۰	=								= (۰۰۰۰)
۱	=	۱							= (۱۰۰۰)
α	=			α					= (۰۱۰۰)
$\alpha^۲$	=					$\alpha^۲$			= (۰۰۱۰)
$\alpha^۳$	=							$\alpha^۳$	= (۰۰۰۱)
$\alpha^۴$	=	۱	+	α					= (۱۱۰۰)
$\alpha^۵$	=			α	+	$\alpha^۲$			= (۰۱۱۰)
$\alpha^۶$	=					$\alpha^۲$	+	$\alpha^۳$	= (۰۰۱۱)
$\alpha^۷$	=	۱	+	α			+	$\alpha^۳$	= (۱۱۰۱)
$\alpha^۸$	=	۱			+	$\alpha^۲$			= (۱۰۱۰)
$\alpha^۹$	=			α			+	$\alpha^۳$	= (۰۱۰۱)
$\alpha^{۱۰}$	=	۱	+	α	+	$\alpha^۲$			= (۱۱۱۰)
$\alpha^{۱۱}$	=			α	+	$\alpha^۲$	+	$\alpha^۳$	= (۰۱۱۱)
$\alpha^{۱۲}$	=	۱	+	α	+	$\alpha^۲$	+	$\alpha^۳$	= (۱۱۱۱)
$\alpha^{۱۳}$	=	۱			+	$\alpha^۲$	+	$\alpha^۳$	= (۱۰۱۱)
$\alpha^{۱۴}$	=	۱					+	$\alpha^۳$	= (۱۰۰۱)

و تجزیه $x^{۱۶} - x$ به عوامل تحویل‌ناپذیر برابر است با:

$$\begin{aligned} x^{۱۶} - x = \; & x(x-۱)(x^۲+x+۱)(x^۴+x+۱) \\ & x(x^۴+x^۳+۱)(x^۴+x^۳+x^۲+x+۱). \end{aligned}$$

دقت دارید که $x^۴ - x = x(x-۱)(x^۲+x+۱)$ متناظر با اعضای ۰، ۱، $\alpha^۵$ و $\alpha^{۱۰}$ می‌باشد که تشکیل زیرمیدان $\mathbb{F}_۴ = \mathbb{F}_۲[x]/(x^۲+x+۱)$ را می‌دهند. چندجمله‌ای $m_۳(x)$ تحویل‌ناپذیر است، اما اولیه نمی‌باشد.

خواننده‌ای که با میدان‌های متناهی آشنا نیست باید از قضیه ۱۴.۱.۱ تا مثال ۱۹.۱.۱ را به‌طور کلی مطالعه نماید و چندین مثال مانند $\mathbb{F}_۹$، $\mathbb{F}_{۲۷}$ و $\mathbb{F}_{۶۴}$ را با چندجمله‌ای‌های مینیمال و زیر میدان‌های متناظر آن بسازد. درمورد جدول میدان‌های متناهی می‌توان به منابع [۹] و [۱۰] رجوع نمود.

چندجمله‌ای‌ها

ما نیاز به مطالب بیشتری درباره چندجمله‌ای‌ها داریم. اگر $f(x) \in \mathbb{F}_q[x]$، آن‌گاه می‌توانیم مشتق $f'(x)$ را از دیدگاه محض و به‌صورت نمادی، به‌شکل:

$$(\sum_{k=0}^{n} a_k x^k)' := \sum_{k=1}^{n} k a_k x^{k-1},$$

تعریف نماییم. قواعد عمومی مشتق مجموع و حاصل‌ضرب برقرار است و می‌توان برای نمونه مشاهده نمود که مشتق $(x-\alpha)^2 f(x)$ برابر با $(x-\alpha)^2 f'(x) + 2(x-\alpha)f(x)$ می‌باشد؛ بنابراین، قضیه زیر واضح است.

قضیه ۲۰.۱.۱. اگر $f(x) \in \mathbb{F}_q[x]$ و α یک ریشه تکراری در یک میدان گسترش‌یافته از $\mathbb{F}_q$ باشد، آن‌گاه α یک ریشه از $f'(x)$ نیز خواهد بود.

البته دقت می‌کنید که اگر $q = 2^r$، آن‌گاه مشتق دوم هر چندجمله‌ای در $\mathbb{F}_q[x]$ هم‌ارز با صفر می‌باشد. این مطلب چیزی درباره تعداد تکرارهای ریشه‌های یک چندجمله‌ای به ما نمی‌گوید. به‌منظور دسترسی به شباهت کامل با نظریه چندجمله‌ای‌ها بر روی $\mathbb{R}$، مشتق هسه [۹] از یک چندجمله‌ای $f(x) \in \mathbb{F}_q[x]$ را به‌صورت زیر مطرح می‌کنیم:

$$f^{[k]}(x) := \frac{1}{k!} f^{(k)}(x);$$

(بنابراین، k–امین مشتق هسه x^n برابر با $\binom{n}{k} x^{n-k}$ است).

خواننده نباید مشکلی برای اثبات این موضوع داشته باشد که α یک ریشه از $f(x)$ با تکرار k است اگر و تنها اگر برای $0 \le i < k$، α ریشه‌ای از $f^{[i]}(x)$ بوده و ریشه $f^{[k]}(x)$ نباشد.

نتیجه دیگری که بعداً به کار می‌رود این است که اگر $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$، آن‌گاه:

$$f'(x) = \sum_{i=1}^{n} f(x)/(x-\alpha_i).$$

قضیه زیر معروف است.

قضیه ۲۱.۱.۱. اگر چندجمله‌ای‌های $a(x)$ و $b(x)$ در $\mathbb{F}[x]$ دارای بزرگ‌ترین مقسوم علیه اول ۱ باشند آن‌گاه چندجمله‌ای‌های $p(x)$ و $q(x)$ وجود دارند؛ به‌طوری که:

$$a(x)p(x) + b(x)q(x) = 1.$$

[۹] Hasse derivate

اثبات. این یک نتیجه فوری از قضیه ۱۳.۱.۱ است. □

اگرچه از رابطه ۴ می‌دانیم که چندجمله‌ای‌های تحویل‌ناپذیر از هر درجه r وجود دارند، اما در برخی از حالات کارهای زیادی برای یافتن آنها باید انجام شود. اثبات رابطه ۴، یک روش انجام آن را نشان می‌دهد. می‌توان با تمامی چندجمله‌ای‌های ممکن با درجه ۱ شروع نمود و تمامی چندجمله‌ای‌های تحویل‌ناپذیر با درجه ۲ را تشکیل داد. هر چندجمله‌ای با درجه ۲ در این لیست، تحویل‌ناپذیر است. به این‌صورت، روش قبل را می‌توان ادامه داد تا چندجمله‌ای‌های تحویل‌ناپذیر با درجه ۳ را تولید نمود و به‌همین ترتیب ادامه داد. در بخش ۹.۲، چندجمله‌ای‌های تحویل‌ناپذیر روی $\mathbb{F}_۲$ با درجات به‌دلخواه بزرگ را نیاز خواهیم داشت. فرایند ترسیم‌شده در فوق برای این منظور رضایت‌بخش نمی‌باشد. در واقع به‌جای این فرایند، کار را به روش زیر ادامه می‌دهیم:

لم ۲۲.۱.۱.

$$۳^{\beta+۱} \mid\mid (۲^{۳^{\beta}} + ۱).$$

اثبات.

۱) برای $\beta = ۰$ و $\beta = ۱$ این ادعا درست می‌باشد.

۲) فرض کنید $۳^t \mid\mid (۲^{۳^{\beta}} + ۱)$؛ در این‌صورت از:

$$(۲^{۳^{\beta+۱}} + ۱) = (۲^{۳^{\beta}} + ۱)\{(۲^{۳^{\beta}} + ۱)(۲^{۳^{\beta}} - ۲) + ۳\},$$

نتیجه می‌شود که اگر $t \geq ۲$ آن‌گاه $۳^{t+۱} \mid\mid (۲^{۳^{\beta+۱}} + ۱)$.

□

لم ۲۳.۱.۱. اگر m دارای مرتبه ۲ (به پیمانه ۳^l) باشد، آن‌گاه:

$$m = \varphi(۳^l) = ۲.۳^{l-۱}.$$

اثبات. اگر $2^\alpha \equiv 1 \bmod 3$ آن‌گاه α زوج می‌باشد؛ بنابراین، $m = 2s$. از این‌رو $2^s + 1 \equiv 0 \bmod 3^l$. اکنون، حکم از قضیه ۲.۱.۱ و لم ۲۲.۱.۱ به‌دست می‌آید. □

قضیه ۲۴.۱.۱. قرار دهید $m = 2.3^{l-1}$؛ در این صورت:

$$x^m + x^{m/2} + 1$$

روی $\mathbb{F}_2$ تحویل‌ناپذیر است.

اثبات. میدان $\mathbb{F}_{2^m}$ را درنظر بگیرید. در این میدان فرض کنید ξ، 3^l امین ریشه واحد باشد؛ بنابراین، با استفاده از لم ۲۳.۱.۱ چندجمله‌ای مینیمال ξ به‌صورت:

$$f(x) = (x-\xi)(x-\xi^2)(x-\xi^4)...(x-\xi^{2^{m-1}}),$$

یک چندجمله‌ای از درجه m می‌باشد. دقت دارید که:

$$x^{3l} + 1 = (1+x)(1+x+x^2)(1+x^3+x^6)...(1+x^{3^{l-1}} + x^{2.3^{l-1}}),$$

تجزیه‌ای است که شامل تنها یک چندجمله‌ای از درجه m می‌باشد؛ بنابراین، عامل آخر باید $f(x)$ باشد و این؛ یعنی آن عامل، تحویل‌ناپذیر است. □

باقی‌مانده‌های درجه دوم

یک نتیجه از وجود یک عضو اولیه در یک میدان $\mathbb{F}_q$ این است که به آسانی می‌توان مربع‌ها را در این میدان مشخص نمود. اگر q زوج باشد، آن‌گاه هر عضو یک مربع است. اگر q فرد باشد، آن‌گاه $\mathbb{F}_q$ شامل ۰، $\frac{1}{2}(q-1)$ مربع ناصفر و $\frac{1}{2}(q-1)$ نامربع است. اعداد صحیح k، $1 \le k \le p-1$، که مربع‌هایی در $\mathbb{F}_p$ هستند معمولاً باقی‌مانده‌های مربعی (به پیمانه p) نامیده می‌شوند. با درنظر گرفتن $k \in \mathbb{F}_p$، به‌عنوان توانی از یک عضو اولیه در این میدان، می‌بینیم که k یک باقی‌مانده مربعی (به پیمانه p) است اگر و تنها اگر $k^{(p-1)/2} \equiv 1 \bmod p$. برای عضو $p-1 = -1$ داریم -1 یک مربع در $\mathbb{F}_p$ است اگر و تنها اگر $p \equiv 1 \bmod 4$. در بخش ۶.۹ نیاز داریم بدانیم که آیا ۲ در $\mathbb{F}_p$ یک مربع است یا نه. برای تصمیم‌گیری درباره این سوال، عناصر ۱، ۲، ...، $(p-1)/2$ را درنظر می‌گیریم و a را برابر با حاصل‌ضرب آنها قرار می‌دهیم. با ضرب هر یک از این عناصر در ۲، مقادیر ۲، ۴، ...، $p-1$ را به‌دست می‌آوریم.

این دنباله شامل $\lfloor(p-۱)/۴\rfloor$ عامل است که عوامل a می‌باشند و برای هر عامل دیگر k از a می‌بینیم که $-k$ یکی از اعداد صحیح زوج بزرگ‌تر از $(p-۱)/۲$ می‌باشد. این نتیجه می‌دهد که در $\mathbb{F}_p$ داریم $۲^{(p-۱)/۲}a = (-۱)^{(p-۱)/۲-\lfloor(p-۱)/۴\rfloor}a$ و چون $a \neq ۰$ می‌بینیم که ۲ یک مربع است اگر و تنها اگر:

$$\frac{p-۱}{۲} - \lfloor\frac{p-۱}{۴}\rfloor,$$

زوج باشد و این؛ یعنی $p \equiv \pm ۱ \bmod ۸$.

اثر

فرض کنید $q = p^r$. نگاشت $Tr : \mathbb{F}_q \to \mathbb{F}_p$ که اثر [۱۰] نامیده می‌شود، به‌صورت زیر تعریف می‌شود:

تعریف ۲۵.۱.۱. اگر $\xi \in \mathbb{F}_q$، آن‌گاه:

$$Tr(\xi) := \xi + \xi^p + \xi^{p^۲} + \cdots + \xi^{p^{r-۱}}.$$

قضیه ۲۶.۱.۱. تابع اثر دارای خواص زیر است:

۱) برای هر $\xi \in \mathbb{F}_q$ اثر $Tr(\xi)$ در $\mathbb{F}_p$ است.

۲) اعضای $\xi \in \mathbb{F}_q$ وجود دارند؛ به‌طوری که $Tr(\xi) \neq ۰$.

۳) Tr یک نگاشت خطی است.

اثبات.

۱) با استفاده از تعریف داریم $(Tr(\xi))^p = Tr(\xi)$.

۲) معادله $x + x^p + \cdots + x^{p^{r-۱}} = ۰$ نمی‌تواند در $\mathbb{F}_q$ دارای q ریشه باشد.

۳) چون $(\xi + \mu)^p = \xi^p + \mu^p$ و برای هر $a \in \mathbb{F}_p$ داریم $a^p = a$، اثبات بدیهی است.

□

البته این قضیه دلالت می‌کند که تابع اثر هر مقداری را $p^{-۱}q$ بار اختیار می‌کند و می‌بینیم که تابع چندجمله‌ای $x + x^p + \cdots + x^{p^{r-۱}}$ حاصل‌ضرب چندجمله‌ای‌های مینیمال است (برای بررسی آن به مثال ۱۹.۱.۱ رجوع نمایید).

[۱۰] trace

سرشت‌ها

فرض کنید $(G,+)$ یک گروه باشد و $(T,\ )$ گروه شامل اعداد مختلط با اندازه ۱ و عمل ضرب. یک سرشت [۱۱]، یک هم‌ریختی $\chi : G \to T$ می‌باشد؛ یعنی:

$$\forall_{g_1 \in G} \forall_{g_2 \in G} [\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)]. \qquad (۵)$$

از این تعریف نتیجه می‌شود که برای هر سرشت χ داریم $\chi(۰) = ۱$. اگر برای هر $g \in G$ داشته باشیم $\chi(g) = ۱$، آن‌گاه χ یک سرشت اصلی نامیده می‌شود.

لم ۲۷.۱.۱. اگر χ یک سرشت برای $(G,\ )$ باشد، آن‌گاه:

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{اگر } \chi \text{ سرشت اصلی باشد,} \\ ۰, & \text{در غیر این‌صورت.} \end{cases}$$

اثبات. فرض کنید $h \in G$؛ در این‌صورت:

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g + h) = \sum_{k \in G} \chi(k).$$

اگر χ سرشت اصلی نباشد، آن‌گاه می‌توان h را به‌گونه‌ای یافت که در آن $\chi(h) \neq ۱$. □

۱.۲ چندجمله‌ای‌های کراچوک

در این بخش، دنباله‌ای از چندجمله‌ای‌ها را معرفی می‌کنیم که یک نقش اساسی در قسمت‌های متفاوتی از نظریه کدگذاری ایفا می‌نمایند؛ یعنی چندجمله‌ای‌های معروف کراچوک [۱۲]. این چندجمله‌ای‌ها نمونه‌ای از چندجمله‌ای‌های متعامد هستند و بیشترین قضایایی که ما بیان می‌کنیم، حالت‌های خاصی از قضایای کلی هستند که در هر دنباله از چندجمله‌ای‌های متعامد معتبرند. به خواننده‌ای که با این قسمت‌های ظریف از آنالیز آشنا نمی‌باشد توصیه می‌شود که به یکی از کتاب‌های درسی درباره چندجمله‌ای‌های متعامد رجوع نماید (به‌طور نمونه زگو[۱۳] [۶۷]، جکسون[۱۴] [۳۶] و تریکومی[۱۵] [۷۰]). درواقع، خواننده

[۱۱] character
[۱۲] Krawtchouk polynomial
[۱۳] G. Szegö
[۱۴] D. Jackson
[۱۵] F. G. Tricomi

را در مورد برخی از اثبات قضایایی که در زیر بیان می‌کنیم، به متون مربوط با آن ارجاع می‌دهیم. به‌جهت اهمیت این چندجمله‌ای‌ها در این مقوله، ما به آنها با عمق بیشتری، نسبت به موضوعاتی در این مقدمه بیان کردیم، خواهیم پرداخت.

معمولاً چندجمله‌ای‌های کراچوک در مواقعی ظاهر می‌شوند که دو پارامتر n و q ثابت فرض شوند. این پارامترها، معمولاً در نمادگذاری چندجمله‌ای‌ها حذف می‌شوند.

تعریف ۱.۱.۲. برای $k = ۰, ۱, ۲, \cdots$، چندجمله‌ای کراچوک $K_n(x)$ به‌صورت زیر تعریف می‌شود:

$$K_k(x; n, q) := K_k(x) := \sum_{j=۰}^{k} (-۱)^j \binom{x}{j} \binom{n-x}{k-j} (q-۱)^{k-j},$$

که در آن:

$$\binom{x}{j} := \frac{x(x-۱)\cdots(x-j+۱)}{j!}, \qquad (x \in \mathbb{R}).$$

توجه کنید که در حالت $q = ۲$ داریم:

$$K_k(x) = \sum_{j=۰}^{k} (-۱)^j \binom{x}{j} \binom{n-x}{k-j} = (-۱)^k K_k(n-x). \tag{۶}$$

با ضرب سری‌های تیلور $(۱ + (q-۱)z)^{n-x}$ و $(۱-z)^x$ داریم:

$$\sum_{k=۰}^{\infty} K_k(x) z^k = (۱ + (q-۱)z)^{n-x} (۱-z)^x. \tag{۷}$$

از تعریف ۱.۱.۲ واضح است که $K_k(x)$ یک چندجمله‌ای از درجه k نسبت به x است که دارای ضریب پیش‌روی $(-q)^k/k!$ می‌باشد. نام چندجمله‌ای متعامد، مربوط به رابطه تعامد زیر است:

$$\sum_{i=۰}^{n} \binom{n}{i} (q-۱)^i K_k(i) K_l(i) = \delta_{kl} \binom{n}{k} (q-۱)^k q^n. \tag{۸}$$

خواننده به‌آسانی می‌تواند این رابطه را اثبات نماید. کافی است طرفین رابطه را در $x^k y^l$ ضرب نموده و روی k و l (از ۰ تا ∞) جمع بسته و از رابطه ۷ کمک بگیرد. از آنجا که دو مجموع برابر می‌باشند، ادعا صحیح است. از تعریف ۱.۱.۲ داریم:

$$(q-۱) \binom{n}{i} K_k(i) = (q-۱)^k \binom{n}{k} K_i(k), \tag{۹}$$

که آن‌را در رابطه ۸ جای‌گذاری می‌کنیم تا دومین نوع از رابطه تعامد به‌صورت زیر یافت شود:

$$\sum_{i=۰}^{n} K_l(i) K_i(k) = \delta_{lk} q^n. \tag{۱۰}$$

تعدادی از چندجمله‌ای‌های کراچوک را ($k \leq ۲$) لیست می‌کنیم:

$$\begin{aligned} K_۰(n,x) &= ۱, \\ K_۱(n,x) &= n(q-۱)-qx, \qquad (= n-۲x;\ q=۲ \text{ اگر}) \\ K_۲(n,x) &= \tfrac{۱}{۲}\{q^۲x^۲ - q(۲qn-q-۲n+۲)x + (q-۱)^۲n(n-۱)\}, \\ &\qquad (= ۲x^۲ - ۲nx + \tbinom{n}{۲};\ q=۲ \text{ اگر}) \end{aligned} \tag{۱۱}$$

در فصل۷ به ضرایب x^k، $x^{k-۱}$، $x^{k-۲}$ و $x^۰$ در عبارت $K_k(x)$ نیاز داریم. اگر $K_k(x) = \sum_{i=۰}^{k} c_i x^i$، آن‌گاه درحالت $q=۲$ داریم:

$$\begin{aligned} c_k &= (-۲)^k/k!, \\ c_{k-۱} &= (-۲)^{k-۱}n/(k-۱)!, \\ c_{k-۲} &= \tfrac{۱}{۲}(-۲)^{k-۲}\{۳n^۲ - ۳n + ۲k - ۴\}/(k-۲)!. \end{aligned} \tag{۱۲}$$

به چندین علت، ما به روابط بازگشتی معین برای چندجمله‌ای‌های کراچوک نیازمندیم. مهم‌ترین آن به‌صورت زیر است:

$$\begin{aligned} &(k+۱)K_{k+۱}(x) = \\ &\quad \{k+(q-۱)(n-k)-qx\}K_k(x) - (q-۱)(n-k+۱)K_{k-۱}(x). \end{aligned} \tag{۱۳}$$

این رابطه با مشتق‌گیری از طرفین رابطه ۷ نسبت به z، ضرب نتیجه در $(۱-z)(۱+(q-۱)z)$ و مقایسه ضرایب، به‌آسانی ثابت می‌شود. یا حتی یک تمرین آسان‌تر، جای‌گذاری x با $x-۱$ در رابطه ۷ است که نتیجه می‌دهد:

$$K_k(i) := K_k(i-۱) - (q-۱)K_{k-۱}(i) - K_{k-۱}(i-۱), \tag{۱۴}$$

که یک روش آسان برای محاسبه اعداد $K_k(i)$ به‌طور بازگشتی می‌باشد.

اگر $P(x)$ یک چندجمله‌ای با درجه l باشد، آن‌گاه عبارت یکتای:

$$P(x) = \sum_{k=۰}^{l} \alpha_k K_(x), \tag{۱۵}$$

توسیع کراچوک $P(x)$ نامیده می‌شود.

بعضی از خواصی را که بعداً به آنها نیاز داریم، بدون اشاره به اثبات آنها، می‌آوریم. آنها حالت‌های خاصی از قضایای عمومی چندجمله‌ای‌های متعامد هستند. شروع کار با فرمول کریستوفل—داربوکس [۱۶]

[۱۶] Christoffel-Darboux

می‌باشد.

$$\frac{K_{k+1}(x)K_k(y)-K_k(x)K_{k+1}(y)}{y-x}=\frac{2}{k+1}\binom{n}{k}\sum_{i=0}^{k}\frac{K_i(x)K_i(y)}{\binom{n}{i}}, \qquad (16)$$

رابطه اخیر ۱۳ با یک دلیل استقرایی، خاصیت پیچیده و بسیار مهم از ریشه‌های $K_k(x)$ را به‌صورت زیر نشان می‌دهد.

$$\begin{aligned}&K_k(x) \text{ دارای } k \text{ ریشه حقیقی متمایز در بازه } (0,n) \text{ است.}\\ &\text{اگر این ریشه‌ها به‌صورت } v_1<v_2<\cdots<v_k \text{ باشند}\\ &\text{و اگر } K_{k-1} \text{ ریشه‌های } u_1<u_2<\cdots<u_{k-1} \text{ باشند، آن‌گاه}\\ &0<v_1<u_1<v_2<\cdots<v_{k-1}<u_{k-1}<v_k<n.\end{aligned} \qquad (17)$$

خاصیت زیر یک‌بار دیگر از رابطه ۷ و با ضرب دو سری توانی نتیجه می‌شود ($q=2$). اگر $x=0,1,2,\cdots,n$، آن‌گاه:

$$K_i(x)K_j(x)=\sum_{k=0}^{n}\alpha_k K_k(x), \qquad (18)$$

که در آن:

$$\alpha_k:=\binom{n-k}{(i+j-k)/2}\binom{k}{(i-j+k)/2}.$$

در فصل ۷، به رابطه زیر نیاز خواهیم داشت:

$$\sum_{k=0}^{l}K_k(x)=K_l(x-1;n-1,q). \qquad (19)$$

این مطلب با جانشینی رابطه موجود در تعریف ۱.۱.۲ بر روی طرف چپ، با تغییر مرتبه جمع‌وند و به‌کارگیری رابطه $\binom{x}{j}=\binom{x-1}{j-1}+\binom{x-1}{j}(j\geq 1)$ به آسانی ثابت می‌شود. ما $K_l(x-1;n-1,q)$ را با $\Psi_l(x)$ نمایش می‌دهیم.

۱.۳ نظریه ترکیبیات

در چندین فصل، نمادها و نتایجی از نظریه ترکیبیات را به‌کار خواهیم برد. در این بخش ما تنها بعضی از تعاریف و یک قضیه را یادآوری می‌کنیم. خواننده‌ای که با این قسمت از ریاضیات آشنا نیست، می‌تواند به کتاب [۹۳] رجوع نماید.

تعریف ۱.۱.۳. فرض کنید S یک مجموعه با v عضو باشد و $\mathcal{B}$ یک مجموعه از زیرمجموعه‌های S (که آنها را بلوک می‌نامیم) باشد به‌طوری که:

۱) $|B| = k$ برای هر $B \in \mathcal{B}$؛

۲) برای هر $T \subset S$ با $|T| = t$، دقیقاً λ بلوک B موجود باشد؛ به‌طوری که $T \subset B$.

در این‌صورت زوج $(S, \mathcal{B})$ یک $t-$طرح نامیده می‌شود (نماد $t-(v,k,\lambda)$). عناصر S، نقاط[۱۷] طرح نامیده می‌شوند. اگر $\lambda = ۱$، آن‌گاه این طرح یک دستگاه اشتاینر[۱۸] نامیده می‌شود.

یک $t-$طرح اغلب با ماتریس وقوع[۱۹] خود، یعنی A، نمایش داده می‌شود که دارای $|\mathcal{B}|$ سطر و $|S|$ ستون است به‌طوری که سطرها توابع مشخصه‌ای از بلوک‌ها باشند.

تعریف ۲.۱.۳. هر طرح بلوکی با پارامترهای $(v,k;b,r,\lambda)$ یک $۲-(v,k,\lambda)$ است با $|\mathcal{B}| = b$. برای هر نقطه‌ای، r بلوک شامل آن نقطه وجود دارد. اگر $b = v$، آن‌گاه طرح بلوکی، متقارن نامیده می‌شود.

تعریف ۳.۱.۳. یک صفحه تصویری از مرتبه n یک $۲-(n^۲+n+۱, n+۱, ۱)$ طرح است. در این حالت، بلوک‌ها، خطوط صفحه نامیده می‌شوند. یک صفحه تصویری از مرتبه n، با $PG(۲,n)$ نمایش داده می‌شود.

تعریف ۴.۱.۳. هندسه آفین از بعد m بر روی میدان $\mathbb{F}_q$، فضای برداری $(\mathbb{F}_q)^m$ است (نماد $AG(m,q)$ را برای هندسه به‌کار می‌بریم). یک زیرفضای آفین $k-$بعدی از یک $k-$سطح، یک هم‌مجموعه از زیرفضای خطی $k-$بعدی (به عنوان زیرگروه) است. اگر $k = m-۱$، آن سطح را یک ابرصفحه می‌نامیم. گروه تولید شده توسط تبدیل‌های خطی $(\mathbb{F}_q)^m$ و تبدیل‌های فضای برداری، گروه تبدیل‌های آفین نامیده می‌شود و با $AGL(m,q)$ نمایش داده می‌شود. گروه جای‌گشتی آفین، تعریف شده در بخش ۱.۱، یک مثال درحالت $m = ۱$ است. هندسه تصویری با بعد m روی $\mathbb{F}_q$ (نماد $PG(m,q)$)، شامل زیرفضاهای خطی $AG(m+۱,q)$ است. زیرفضاهای با بعد ۱، نقاط نامیده می‌شوند. زیرفضاهای بابعد ۲، خطوط نامیده می‌شوند و به‌همین ترتیب.

در اینجا مثالی می‌آوریم. $AG(۳,۳)$ را درنظر بگیرید. ۲۷ نقطه و $\frac{۱}{۲}(۲۷-۱) = ۱۳$ خط وجود دارند که از $(۰,۰,۰)$ می‌گذرند و ۱۳ صفحه که از $(۰,۰,۰)$ می‌گذرند. این ۱۳ خط، نقاط $PG(۲,۳)$ هستند و ۱۳ صفحه در $AG(۳,۳)$، خطوط هندسه تصویری هستند. روشن است که این یک طرح

[۱۷] points
[۱۸] Steiner
[۱۹] incidence matrix

$(۱۳, ۴, ۱) - ۲$ است. هنگام صحبت درباره مختصات یک نقطه در $PG(m, q)$، منظور ما، مختصات هریک از نقاط متناظر است که در $AG(m+۱, q)$ متفاوت از $(۰, ۰, \cdots, ۰)$ می‌باشند؛ بنابراین، در مثال $PG(۲, ۳)$، سه‌تایی‌های $(۱, ۲, ۱)$ و $(۲, ۱, ۲)$، مختصات نقطه یکسانی در $PG(۲, ۳)$ هستند.

در فصل ۱۰، صفحه تصویری $n-$بعدی $\mathbb{P}^n$ را روی میدان k درنظر می‌گیریم. یک نقطه با $(a_۰ : a_۱ : \cdots : a_n)$ نمایش داده خواهد شد که تمامی a_iها هم‌زمان صفر نیستند و $(a_۰ : a_۱ : \cdots : a_n) = (b_۰ : b_۱ : \cdots : b_n)$ اگر برای یک $c \in k$ که $c \neq ۰$ داشته باشیم $b_i = ca_i$ برای هر $۰ \leq i \leq n$.

تعریف ۵.۱.۳. یک ماتریس مربعی H از مرتبه n با عناصر $+۱$ و -۱ به‌طوری که $HH^T = nI$، یک ماتریس هادامارد[۲۰] نامیده می‌شود.

تعریف ۶.۱.۳. ماتریس مربعی C از مرتبه n با اعضای ۰ در قطر اصلی و $+۱$ و -۱ خارج از قطر اصلی به‌طوری که $CC^T = (n-۱)I$، یک ماتریس کنفرانس[۲۱] نامیده می‌شود.

چندین روش معروف برای ساخت ماتریس‌های هادامارد وجود دارد. یکی از آنها برپایه حاصل‌ضرب معروف کرونکر[۲۲] برای ماتریس‌ها می‌باشد که به‌صورت زیر تعریف می‌شود.

تعریف ۷.۱.۳. اگر A یک ماتریس $m \times m$ با درایه‌های a_{ij} باشد و B یک ماتریس $n \times n$ باشد، آن‌گاه حاصل‌ضرب کرونکر $A \otimes B$ یک ماتریس $mn \times mn$ است که به‌صورت زیر تعریف می‌شود:

$$A \otimes B := \begin{pmatrix} a_{۱۱}B & a_{۱۲}B & \cdots & a_{۱m}B \\ a_{۲۱}B & a_{۲۲}B & \cdots & a_{۲m}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{m۱}B & a_{m۲}B & \cdots & a_{mm}B \end{pmatrix}.$$

نشان دادن این‌که حاصل‌ضرب کرونکر ماتریس‌های هادامارد، مجدداً یک ماتریس هادامارد است، مشکل نمی‌باشد. با شروع از $H_۲ = \begin{pmatrix} ۱ & ۱ \\ ۱ & -۱ \end{pmatrix}$ می‌توانیم دنباله $H_۲^{\otimes n}$ را بیابیم که در آن $H_۲^{\otimes ۲} = H_۲ \otimes H_۲$ و به‌همین ترتیب. این ماتریس‌ها در موقعیت‌های متفاوتی از این کتاب مشاهده می‌گردند (برخی اوقات به شکل پنهان).

یکی از بهترین روش‌های ساختاری مربوط به پالی[۲۳] است (ر.ک. مرجع [۹۳]). فرض کنید q یک عدد فرد اول باشد. تابع χ را بر روی $\mathbb{F}_q$ تعریف می‌کنیم به‌طوری که $\chi(۰) := ۰$ و $\chi(x) := ۱$ اگر x یک

[۲۰] Hadamard matrix
[۲۱] conference matrix
[۲۲] Kronecker product
[۲۳] R. E. A. C. Paley

مربع ناصفرباشد و در غیر این‌صورت $\chi(x) = -1$. دقت دارید که χ، محدود شده به گروه ضربی $\mathbb{F}_q$، یک سرشت است. عناصر $\mathbb{F}_q$ را با یک روش دلخواه به‌صورت $a_0, a_1, \cdots, a_{q-1}$ شماره‌گذاری کنید که در آن $a_0 = 0$.

قضیه ۸.۱.۳ ماتریس پالی S از مرتبه q تعریف شده به‌صورت $S_{ij} := \chi(a_i - a_j)$ دارای خواص زیر است:

۱) $SJ = JS = 0$؛

۲) $SS^T = qI - J$؛

۳) $S^T = (-1)^{(q-1)/2} S$.

ماتریس S به این‌صورت را درنظر گرفته و ماتریس C از مرتبه $q+1$ را به‌صورت زیر تشکیل می‌دهیم:

$$C := \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ -1 & & & & \\ -1 & & S & & \\ \vdots & & & & \\ -1 & & & & \end{pmatrix}, \qquad (20)$$

در این‌صورت C یک ماتریس کنفرانس از مرتبه $q+1$ است. اگر $q \equiv 3 \bmod 4$، آن‌گاه می‌توانیم فرض کنیم $H := I + C$. از آنجا که -1 یک مربع در $\mathbb{F}_q$ نیست؛ بنابراین، $C^T = -C$ و از آنجا می‌بینیم که H یک ماتریس هادامارد از مرتبه $q+1$ است.

۱.۴ نظریه احتمالات

فرض کنید x یک متغیر تصادفی باشد به‌طوری که تعداد متناهی ازمقادیر $x_1, x_2, \cdots$ را اختیار می‌کند. به‌طور معمول، احتمال این‌که x برابر با x_i باشد؛ یعنی $P(x = x_i)$، را با p_i نشان می‌دهیم. میانگین یا امید x به صورت $\mu = \mathcal{E}(x) := \sum_i p_i x_i$ تعریف می‌شود.

اگر g تابعی تعریف شده بر روی مجموعه مقادیر x باشد، آن‌گاه $\mathcal{E}(g(x)) = \sum_i p_i g(x_i)$. تعدادی از روابط معروف، مانند رابطه:

$$\mathcal{E}(ax + by) = a\mathcal{E}(x) + b\mathcal{E}(y),$$

را به‌کار خواهیم بست. انحراف معیار σ و واریانس $\sigma^۲$ به‌صورت زیر تعریف می‌شوند:

$$\sigma^۲ := \sum_i p_i x_i^۲ - \mu^۲ = \mathcal{E}(x-\mu)^۲, \quad (\sigma > ۰),$$

که در آن $\mu = \mathcal{E}(x)$. هم‌چنین به بعضی از روابط درباره توزیع‌های دو بعدی نیاز داریم. نمادگذاری $p_{ij} := P(x = x_i \wedge y = y_i)$، $p_i := P(x = x_i) = \sum_j p_{ij}$ و برای احتمال شرطی، نمادگذاری $P(x = x_i \,|\, y = y_j) = p_{ij}/p_j$ را به‌کار می‌بریم. گوییم x و y مستقل هستند اگر برای تمامی i و j داشته باشیم $p_{ij} = p_i.p_j$. در این حالت داریم:

$$\mathcal{E}(xy) = \sum_{i,j} p_{ij} x_i y_j = \mathcal{E}(x)\mathcal{E}(y).$$

تمامی این روابط را می‌توان در کتاب‌های درسی استاندارد از نظریه احتمالات (برای نمونه فلر[۲۴] [۲۱]) یافت نمود. روابط مشابهی برای نتایج زیر برقرار خواهد بود که آنها را در فصل ۲ به‌کار خواهیم برد.

قضیه ۱.۱.۴. (نامساوی چپیشف). فرض کنید x یک متغیر تصادفی با میانگین μ و واریانس $\sigma^۲$ باشد؛ در این‌صورت برای هر $k > ۰$ داریم:

$$P(\,|\, x-\mu \,|\, \geq k\sigma) < k^{-۲}.$$

توزیع احتمالی که دارای بیشترین نقش در فصل بعد خواهد بود، توزیع دوجمله‌ای است. دراینجا x مقادیر $۰, ۱, \cdots, n$ را می‌گیرد و $P(x=i) = \binom{n}{i} p^i q^{n-i}$ که در آن $۰ \leq p \leq ۱$ و $q := ۱ - p$. برای این توزیع داریم $\mu = np$ و $\sigma^۲ = np(۱-p)$. هنگام تخمین ضرایب دوجمله‌ای، ابزار مهمی به‌کار می‌رود که در قضیه زیر آمده است:

قضیه ۲.۱.۴. (فرمول استرلینگ).

$$\log n! = (n - \tfrac{۱}{۲})\log n - n + \tfrac{۱}{۲}\log(۲\pi) + o(۱), \quad (n \to \infty),$$

$$= n\log n - n + O(\log n), \qquad (n \to \infty),$$

لم مفید دیگری که درباره ضرایب دوجمله‌ای است، لم زیر است.

لم ۳.۱.۴. داریم:

$$\binom{n}{m} \leq \frac{n^n}{m^m (n-m)^{n-m}}.$$

[۲۴] W. Feller

اثبات.

$$n^n = \{m + (n-m)\}^n \geq \binom{n}{m} m^m (n-m)^{n-m}.$$

□

حال تابعی را معرفی می‌کنیم که در نظریه اطلاعات بسیار مهم است. این تابع به تابع آنتروپی دودویی معروف است و معمولاً با H نمایش داده می‌شود. در رابطه ۲ (فصل ۵)، این تابع را به qی بزرگ‌تر از ۲ گسترش می‌دهیم. در ادامه بحث، تمامی لگاریتم‌ها در پایه ۲ هستند.

تعریف ۴.۱.۴. تابع آنتروپی دوتایی H به‌صورت زیر تعریف می‌شود:

$$H(0) := 0,$$

$$H(x) := -x \log x - (1-x)\log(1-x), \quad (0 < x \leq \tfrac{1}{2}).$$

قضیه ۵.۱.۴. فرض کنید $0 \leq \lambda \leq \frac{1}{2}$؛ در این‌صورت داریم:

۱) $\sum_{0 \leq i \leq \lambda n} \binom{n}{i} \leq 2^{nH(\lambda)}$،

۲) $\lim_{n\to\infty} n^{-1} \log \sum_{0 \leq i \leq \lambda n} \binom{n}{i} = H(\lambda)$.

اثبات.

۱)

$$\begin{aligned} 1 &= \{\lambda + (1-\lambda)\}^n \geq \sum_{0 \leq i \leq \lambda n} \binom{n}{i} \lambda^i (1-\lambda)^{n-i} \\ &\geq \sum_{0 \leq i \leq \lambda n} \binom{n}{i} (1-\lambda)^n \left(\frac{\lambda}{1-\lambda}\right)^{\lambda n} = 2^{-nH(\lambda)} \sum_{0 \leq i \leq \lambda n} \binom{n}{i}. \end{aligned}$$

۲) قرار دهید $m := \lfloor \lambda n \rfloor$؛ در این‌صورت $m = \lambda n + O(۱)$ برای $n \to \infty$؛ بنابراین، از قضیه ۲.۱.۴ داریم:

$$\begin{aligned} n^{-۱} \log \sum_{۰ \le i \le \lambda n} \binom{n}{i} &\ge n^{-۱} \log \binom{n}{m} \\ &= n^{-۱}\{n \log n - m \log m - (n-m)\log(n-m) + o(n)\} \\ &= \log n - \lambda \log(\lambda n) - (۱ - \lambda)\log((۱-\lambda)n) + o(۱) \\ &= H(\lambda) + o(۱), \qquad n \to \infty \text{ زمانی‌که} \end{aligned}$$

در این‌صورت، حکم از قسمت (۱) به‌دست می آید. □

توزیع احتمالی که نقش مهمی در نظریه اطلاعات ایفا می‌نماید، توزیع نرمال یا گوسی است. این توزیع برای توصیف انواع مشترکی از نویز بر روی کانال‌های مخابراتی به‌کار می‌رود. گوییم یک توزیع تصادفی پیوسته دارای توزیع گوسی با میانگین μ و واریانس $\sigma^۲$ است؛ اگر تابع توزیع آن به‌صورت زیر باشد:

$$p(x) := \frac{۱}{\sqrt{۲\pi\sigma^۲}} \exp\left(-\frac{(x-\mu)^۲}{۲\sigma^۲}\right).$$

فصل ۲

قضیه شانون

۲.۱ مقدمه

این کتاب، مقدمه‌ای از جنبه‌های ریاضی نظریه کدهای تصحیح‌کننده خطا را معرفی می‌نماید. این نظریه در بسیاری از موقعیت‌هایی که به‌عنوان یک خصوصیت مشترک، اطلاعاتی را که از برخی منابع می آید، توسط یک کانال مخابراتی نویزدار به گیرنده منتقل می‌کنند، کاربرد دارد. به‌عنوان مثال مکالمات تلفنی، دستگاه‌های ذخیره‌سازی مانند دستگاه‌های نوار مغناطیسی که برخی اطلاعات ذخیره‌شده را به کامپیوتر می‌رسانند، تلگراف و غیره از این نوع می‌باشند. در ادامه مثالی را که اخیراً کاربرد داشته، می آوریم. بسیاری از خوانندگان، عکس‌های باکیفیت عالی از مریخ، زحل و سایر سیاره‌هایی که با ماهواره‌هایی همچون مارینر[۱] ، وُیاگر[۲] و غیره گرفته شده را دیده‌اند. به‌منظور انتقال این عکس‌ها به زمین، شبکه‌ای نازک بر روی عکس قرار گرفته و برای هر مربع شبکه، درجه‌ای از تیرگی اندازه‌گیری می‌شود که از درجه ۰ تا ۶۳ می‌باشد. این اعداد برحسب دستگاهای دوتایی بیان می‌شوند؛ یعنی هر مربع رشته‌ای شش‌تایی از ۰ و ۱ تولید می‌نماید. این صفر و یک‌ها، توسط دو سیگنال متفاوت به ایستگاه گیرنده بر روی زمین (آزمایشگاه پرتاب جت[۳] در موسسه صنعتی کالیفرنیا در شهر پاسادنا [۴]) منتقل می‌شوند. سیگنال رسیده

---

[۱] Mariners
[۲] Voyagers
[۳] The Jet Propulsion Laboratory
[۴] Pasadena

بسیار ضعیف می‌باشد و باید تقویت شود. به‌واسطه تاثیر نویز حرارتی، گاه‌وبی‌گاه به‌نظر می آید که سیگنالی که به‌عنوان ۰ ارسال شده توسط گیرنده به ۱ تعبیر می‌شود و به‌عکس. اگر دنباله ٦تایی از ۰ و ۱ هایی که در بالا بیان کردیم، به این‌صورت منتقل شوند، آن‌گاه خطاهایی که توسط گیرنده رخ می‌دهد، تاثیر زیادی بر روی عکس‌ها می‌گذارد. برای جلوگیری از این خطا، چیزی به‌اسم افزونگی[۵] روی سیگنال اعمال می‌شود، به این معنی که دنباله منتقل‌شده از اطلاعات لازم بیشتر است. همه ما با اصل افزونگی، در زبان روزمره آشنایی داریم. کلمات زبان ما تشکیل قسمت کوچکی از تمامی رشته‌های ممکن از حروف (سمبل‌ها) را می‌دهند. درنتیجه یک اشتباه چاپی در یک کلمه طولانی (!) قابل تشخیص است، چراکه این کلمه به چیزی تبدیل می‌شود که کلمه صحیح را بیشتر از هر کلمه مشابه دیگری که می‌شناسیم، به ذهن ما متبادر می‌سازد. این بحث، اساس نظریه‌ای است که ما در این کتاب به آن می‌پردازیم. در مثال قبل، خواننده، اشتباه چاپی را تصحیح می‌نماید. مثال جدیدتر از کدگذاری برای کانال‌های مخابراتی، سیستم به‌کار رفته برای واسط زنجیره‌ای مابین یک ترمینال و یک کامپیوتر یا مابین یک کامپیوتر شخصی (PC) و صفحه کلید است. به منظور نمایش ۱۲۸ سمبل متمایز، رشته‌هایی ۷ تایی از ۰ و ۱ ها، یعنی اعداد صحیح از ۰ تا ۱۲۷ در مبنای دوتایی، به‌کار می‌روند. در عمل، یک بیت اضافی (= رقم دوتایی) به این ۷ تایی اضافه می‌شود تا نتیجه یک ۸ تایی (موسوم به بایت) دارای تعدادی زوج ۱ گردد. این کد، به‌طور مثال، در کد حرفی ASCII به‌کار می‌رود. نارسایی در این واسطه‌ها خیلی به ندرت رخ می‌دهد؛ اما ممکن است یک بیت نادرست به‌صورت اتفاقی رخ دهد. این مثال، نمونه‌ای از یک کد تشخیص دهنده یک خطا است.

در بالا گفتیم که شش‌تایی‌ها از ۰ و ۱ در انتقال عکس (مارینر ۱۹٦۹) با رشته‌های طولانی‌تر (که آنها را همیشه کدکلمات می‌نامیم) جای‌گزین شدند. در واقع، در مارینر ۱۹٦۹، کدکلمات شامل ۳۲ سمبل بودند (ر.ک. مرجع [٥٦]). دراینجا، خواننده باید این را بپذیرد که دستگاه‌هی باید طراحی شود تا ٦۴ رشته اطلاعاتی ممکن (٦ تایی‌ها از ۰ و ۱) را به ٦۴ کدکلمه ممکن (۳۲ تایی‌ها از ۰ و ۱) تغییر دهد. این دستگاه، کدکننده نامیده می‌شود. چیزهایی که انتقال می‌یابند، کدکلمات هستند. نویزها را هم تصادفی درنظر می‌گیریم؛ یعنی خطاها به پیام اضافه شده‌اند (جمع به پیمانه ۲).

در پایان، اگر کلمه دریافتی یکی از ٦۴ کدکلمه قابل قبول نباشد، دستگاهی که کدگشا نامیده می‌شود، ۳۲ تایی دریافتی را به کدکلمه با بیشترین احتمال[٦] تغییر می‌دهد و پس از آن، ٦ تایی متناظر (میزان تیرگی یک مربع از شبکه) را تعیین می‌کند. کدی که هم‌اکنون توصیف نمودیم، دارای این خاصیت است که اگر حداکثر ۷ سمبل از ۳۲ سمبل نادرست بود، آن‌گاه کدگشا درست تصمیم می‌گیرد. البته دقت

---

[۵] redundancy

[٦] most likely codeword

می‌کنیم که برای این احتمال از تصحیح خطا، باید هزینه پرداخت نمود؛ یعنی، زمانی که برای انتقال هر بیت در دسترس است، ۱/۵ برابر زمانی است که بدون کدگذاری و با احتمال خطای بالا در دسترس بود! این مثال را با جزییات بیشتر در بخش ۲.۳ خواهیم آورد.

در عمل، این وضعیت دارای پیچیدگی بیشتری است؛ چرا که مشکل اصلی به‌خاطر زمان انتقال نیست که تغییر می‌کند، بلکه به‌خاطر میزان انرژی قابل‌دسترس در هر بیت انتقال‌یافته است.

بیشترین کاربرد عملی نظریه کدهای تصحیح‌کننده خطا، سیستم صوتی دیجیتال یک دیسک فشرده است که توسط فیلیپس[۷] (هلندی‌ها) اختراع شد. موفقیت این سیستم (در میان سایر سیستم‌ها) به‌خاطر استفاده از کدهای رید—سولومن[۸] بود. این کدها در بخش ٦.٨ مورد بررسی قرار می‌گیرند. شکل ۴.٦ مدلی از وضعیت تشریح شده در بالا می‌باشد.

شکل ۲.۱:

در این کتاب، علاقه اصلی ما ساخت و تحلیل کدهای خوب است. در برخی حالات، مسائل ریاضی کدگشایی را بدون درنظر گرفتن کاربرد واقعی مورد مطالعه قرار می‌دهیم. حتی برای یک کد ثابت، روش‌های متفاوت زیادی برای طراحی الگوریتم کدگشایی وجود دارد. یک الگوریتم کدگشایی کامل، تمامی کلمات دریافتی ممکن را به یکی از کدکلمات، کدگشایی می‌نماید. در برخی از حالات، مانند هنگامی که خطای کدگشایی خیلی نامطلوب است، یک الگوریتم کدگشایی غیرکامل ممکن است ترجیح داده شود. در آن حالت، این الگوریتم آن دسته از پیام‌های دریافتی را کدگشایی می‌کند که شامل تعداد کمی خطا باشند و برای سایر پیام‌های دریافتی، کدگشایی با شکست روبرو خواهد شد. در حالت دوم، گیرنده یا از خطا صرف‌نظر می‌کند یا درصورت ممکن از فرستنده برای ارسال مجدد درخواست می‌کند. تفاوت دیگری که ایجاد می‌شود، فرق بین کدگشایی‌های معروف به تصمیم سخت[۹] و تصمیم نرم[۱۰] می‌باشد. این تصمیم به سمبل‌های ورودی وابسته است. بیشتر آنها به سیگنالی از ۰ و ۱ تشبیه می‌گردند که دریافت کننده هیچ شکی نداشته باشد. اما در سایر حالات، این مطلب درست نخواهد بود و می‌توانیم قرار دادن یک ? را به‌جای تصمیم‌گیری درباره این‌که آیا سمبل ورودی ۰ بوده یا ۱، ترجیح دهیم. این

[۷] Philips
[۸] Reed Solomon
[۹] hard decision
[۱۰] soft desision

مطلب اغلب به عنوان یک پاک‌شدگی[۱۱] تعبیر می‌شود. سیستم‌های پیچیده‌تر، یک احتمال را به این سمبل الحاق می‌کنند.

مقدمه‌ای بر قضیه شانون

به‌منظور حصول ایده بهتری درباره اصل نظریه کدگذاری، آزمایش خیالی زیر را درنظر می‌گیریم. ما در اتاقی هستیم که شخصی در حال پرتاب پرتاب یک سکه با سرعت t پرتاب در دقیقه است. این اتاق به اتاق دیگری توسط یک خط تلگراف متصل است. بیاییم فرض کنیم که بر روی این کانال مخابراتی می‌توانیم دو سمبل متفاوت بفرستیم که آنها را ۰ و ۱ می‌نامیم. این کانال، نویزدار است و تاثیر آن به این صورت است که ۰ (یا ۱) فرستاده شده با احتمال p توسط گیرنده به‌عنوان ۱ (یا ۰) تفسیر می‌شود. چنین کانالی یک کانال دوتایی متقارن (B.S.C.) نامیده می‌شود. علاوه‌برآن فرض کنید که این کانال می‌تواند $2t$ سمبل را در یک دقیقه جابه‌جا نماید و می‌توانیم از این کانال به مدت T دقیقه استفاده نماییم؛ اگر پرتاب سکه نیز T دقیقه طول بکشد. زمانی که شیر می‌آید ما ۰ را انتقال می‌دهیم و اگر خط بیاید، ۱ را انتقال می‌دهیم. در پایان انتقال، گیرنده به‌اندازه کسر p اطلاعات دریافتی خواهد داشت که ناصحیح می‌باشند. حال اگر ما محدودیت زمانی تخصیص یافته در بالا را نداشتیم، می‌توانستیم به احتمال خطای به اندازه دلخواه کوچک در گیرنده، همچنان که در ادامه می‌آید، دست یابیم. فرض کنید N فرد باشد. به‌جای ۰ (یا ۱)، N تا ۰ (یا ۱) را انتقال می‌دهیم. گیرنده N تایی دریافتی را درنظر گرفته و آن را به سمبلی کدگشایی می‌کند که بیشتر ظاهر شده است. کدی که اینک استفاده کردیم، کد تکرار به طول N نامیده می‌شود. این کد شامل دو کدکلمه، یعنی $\mathbf{0} = (0, 0, \cdots, 0)$ و $\mathbf{1} = (1, 1, \cdots, 1)$ است. به‌عنوان نمونه فرض کنیم $p = 0.001$؛ در این‌صورت احتمال این که کدگشا دچار اشتباه شود، به‌صورت زیر است:

$$\sum_{0 \le k \le N/2} \binom{N}{k} q^k p^{N-k} < (0.07)^N, \quad (q := 1 - p) \qquad (1)$$

و این احتمال وقتی $N \to \infty$، به صفر میل می‌کند (اثبات ۱ در تمرین ۱.۲.۵).

به‌خاطر وجود محدودیت زمانی، یک مشکل جدی داریم! برای هر پرتاب سکه، تنها دو سمبل را می‌توانیم انتقال دهیم. در ارسال دوبار هر سمبل به‌جای یک‌بار هم هیچ نکته خاصی وجود ندارد. برجسته‌ترین قضیه در این مورد توسط شانون[۱۲] (ر.ک. مرجع [۶۲])، بیان می‌کند که ما هنوز می‌توانیم برای T بزرگ، احتمال خطا را در گیرنده کوچک کنیم. این اثبات در بخش بعدی خواهد آمد. اولین ایده

[۱۱] erasure

[۱۲] C.E.Shannon

درباره روش اثبات می‌تواند به‌صورت زیر به‌دست آید. نتیجه دوبار پرتاب یک سکه را به‌صورت زیر انتقال می‌دهیم:

$$\begin{aligned} &\text{شیر، شیر} \rightarrow ۰۰۰۰,\\ &\text{خط، شیر} \rightarrow ۰۱۱۱,\\ &\text{شیر، خط} \rightarrow ۱۰۰۱,\\ &\text{خط، خط} \rightarrow ۱۱۱۰, \end{aligned}$$

مشاهده کنید که اولین دو سمبل ارسالی، اطلاعات واقعی را حمل می‌کنند؛ دو سمبل آخر اضافی هستند. کدگشا، الگوریتم کدگشایی کامل زیر را به‌کار می‌برد. اگر ۴ تایی دریافتی یکی از کدکلمه‌های بالا نباشد، آن‌گاه فرض کنید چهارمین سمبل درست است و این‌که یکی از سه سمبل اولیه نادرست است. اگر فرض بالا درست باشد، آن‌گاه هر ۴ تایی دریافتی می‌توانند به‌طور یکتا و صحیح کدگشایی گردد. بدون کدگذاری، احتمال این‌که دو سمبل به‌طور صحیح دریافت شده باشند، برابر با $q^۲ = ۰.۹۹۸$ است. توسط کدی که در بالا توصیف شد، این احتمال برابر با $q^۴ + ۳q^۳p = ۰.۹۹۹$ خواهد شد. جمله دوم در طرف چپ این رابطه برابر با احتمال این است که کلمه دریافتی شامل یک خطا باشد، اما نه در موقعیت چهارم؛ بنابراین، با یک روش خیلی آسان به یک پیشرفت خوب رسیده‌ایم. نیاز زمانی هم تامین شده است. ما این ایده را که در بالا به‌وسیله انتقال نتایج پرتاب سکه به‌کار رفت، به سه پرتاب در یک لحظه گسترش می‌دهیم. دراین‌صورت اطلاعاتی که قصد انتقال آن را داریم به‌صورت سه‌تایی از ۰ و ۱، که آن‌را $(a_۱, a_۲, a_۳)$ می‌نامیم، می‌باشد. به‌جای این ۳ تایی، ما ۶ تایی $\mathbf{a} = (a_۱, \cdots, a_۶)$ را انتقال می‌دهیم که در آن $a_۴ := a_۲ + a_۳$، $a_۵ := a_۱ + a_۳$ و $a_۶ := a_۱ + a_۲$ (این جمع به پیمانه ۲ است). آنچه که ما انجام دادیم، ساخت یک کد شامل هشت کلمه، هریک به طول ۶ می‌باشد. همان‌طور که قبلاً بیان شد، ما نویز را به‌عنوان چیزی که به پیام اضافه می‌شود درنظر می‌گیریم؛ یعنی کلمه دریافتی $\mathbf{b}$ به‌صورت $\mathbf{a} + \mathbf{e}$ است که در آن $\mathbf{e} = (e_۱, e_۲, \cdots, e_۶)$ الگوی خطا (بردار خطا) نامیده می‌شود؛ داریم:

$$e_۲ + e_۳ + e_۴ = b_۲ + b_۳ + b_۴ := s_۱,$$

$$e_۱ + e_۳ + e_۵ = b_۱ + b_۳ + b_۵ := s_۲,$$

$$e_۱ + e_۲ + e_۶ = b_۱ + b_۲ + b_۶ := s_۳,$$

از آنجاکه گیرنده $\mathbf{b}$ را می‌شناسد، او $s_۱, s_۲, s_۳$ را می‌شناسد. با فرض $s_۱, s_۲, s_۳$، کدگشا باید الگوی خطای $\mathbf{e}$ با بیشترین درست‌نمایی را به‌گونه‌ای انتخاب نماید که در این سه معادله صدق کند. بیشترین درست‌نمایی را آنی دارد که دارای کمترین سمبل ۱ باشد. می‌توان به‌آسانی مشاهده نمود که اگر $(s_۱, s_۲, s_۳) \neq (۱, ۱, ۱)$، آن‌گاه انتخاب یکتایی برای $\mathbf{e}$ وجود دارد. اگر $(s_۱, s_۲, s_۳) = (۱, ۱, ۱)$، آن‌گاه کدگشا باید یکی از سه احتمال $(۱, ۰, ۰, ۱, ۰, ۰)$، $(۰, ۱, ۰, ۰, ۱, ۰)$ و $(۰, ۰, ۱, ۰, ۰, ۱)$ را برای $\mathbf{e}$

داشته باشد. می‌بینیم که اگر الگوی خطا دارای یک خطا باشد، به‌طور صحیح کدگشایی می‌شود و در میان سایر الگوهای خطا هم، الگویی با دو خطا وجود دارد که به‌طور صحیح کدگشایی می‌گردد؛ بنابراین، پس از فرایند کدگشایی، احتمال این‌که تمامی سه سمبل $a_۱, a_۲, a_۳$ به‌طور صحیح تفسیر شوند، برابر است با:

$$q^۶ + ۶q^۵p + q^۴p^۲ = ۰.۹۹۹۹۸۶.$$

این یک پیشرفت عظیم است که قبلاً بیان شد.

با این مقدمه، خواننده ایده‌هایی را درباره برخی مفاهیم مهم زیر از نظریه کدگذاری، یافته است.

تعریف ۱.۲.۱. اگر کد C شامل کلماتی با طول n باشد، آن‌گاه:

$$R := n^{-۱} \log |c|$$

نرخ اطلاعاتی (یا فقط نرخ) کد نامیده می‌شود.

مفهوم نرخ با آنچه که در بالا راجع به زمان لازم برای انتقال اطلاعات بحث شد، ارتباط دارد. در مثال مربوط به رابط صفحه کلید PC، نرخ برابر با $\frac{۷}{۸}$ می‌باشد. مارینر ۱۳۶۹ از کدی با نرخ $\frac{۶}{۳۲}$ استفاده نموده است. مثالی که قبل از تعریف نرخ آمد، دارای نرخ $R = \frac{۱}{۲}$ است.

یادآوری می‌کنیم که کدی که توسط مارینر ۱۹۶۹ به‌کار رفت دارای این خاصیت بود که گیرنده قادر به تصحیح تا هفت خطا در کلمه دریافتی است. دلیل این‌که چنین چیزی امکان دارد این واقعیت است که هر دو کدکلمه مجزا در حداقل ۱۶ موقعیت با یکدیگر تفاوت دارند؛ بنابراین، کلمه دریافتی با کمتر از ۸ خطا، به کدکلمه ارسالی بیشتر از سایر کدکلمات شباهت دارد. این مطلب به تعریف زیر منجر می‌شود:

تعریف ۲.۲.۱. اگر x و y دو n تایی از ۰ و ۱ باشند، آن‌گاه گوییم فاصله همینگ آنها (معمولاً فقط فاصله) برابر است با:

$$d(x, y) := |\{i : ۱ \leq i \leq n, x_i \neq y_i\}|.$$

(نیز تعریف ۱.۳.۱ را ببینید).

کد C با هشت کلمه به طول ۶ که در بالا بحث نمودیم، دارای این خاصیت است که هر دو کدکلمه مجزا دارای فاصله حداقل ۳ می‌باشند. به‌همین خاطر است که هر الگوی خطا با یک خطا، می‌تواند تصحیح شود. این کد، یک کد تصحیح‌کننده خطای واحد است.

توصیف ما از قوانین کدگشایی، برپایه دو فرض می‌باشد. اولین آنها این است که در زمان مخابره، تمامی کدکلمات دارای احتمال یکسان باشند. علاوه بر آن از این واقعیت استفاده نموده‌ایم که اگر $n_۱ > n_۲$، آن‌گاه یک الگوی خطا با $n_۱$ خطا دارای احتمال کمتری از یک الگو با $n_۲$ خطا است.

معنای آن این است که اگر y دریافت شده باشد، آن‌گاه سعی می‌کنیم تا کدکلمه x را بیابیم به‌طوری که $d(x,y)$ کمترین باشد. این اصل، قاعده کدگشایی با بیشترین درست‌نمایی[۱۳] است.

۲.۲ قضیه شانون

در اینجا قضیه شانون را در مورد مثال داده‌شده در بخش ۲.۱ بیان و اثبات می‌کنیم. بیایید مساله را بیان کنیم. ما یک کانال دوتایی متقارن با احتمال خطای p داریم که یک سمبل با خطا دریافت می‌شود (مجدداً می‌نویسیم $q := ۱ - p$). فرض کنید کد C شامل M کدکلمه به طول n را به‌کار می‌بریم؛ به‌طوری‌که هر کلمه با احتمال یکسان رخ داده است. اگر $x_۱$، $x_۲$، $\cdots$، x_M کدکلمات باشند و از قاعده کدگشایی با بیشترین درست‌نمایی استفاده کنیم، آن‌گاه فرض کنید P_i احتمال تصمیم نادرست به‌شرط انتقال x_i باشد. در این حالت احتمال کدگشایی نادرست کلمه دریافتی برابر است با:

$$P_C := M^{-۱} \sum_{i=۱}^{M} P_i. \qquad (۲)$$

حال تمامی کدهای ممکن C با پارامترهای داده شده را درنظر بگیرید و تعریف کنید:

$$P^*(M,n,p) := P_C \text{ کمترین مقدار}. \qquad (۳)$$

قضیه ۱.۲.۲. (شانون ۱۹۴۸). اگر $۰ < R < ۱ + p\log p + q\log q$ و $M_n := ۲^{\lfloor Rn \rfloor}$، آن‌گاه $P^*(M_n,n,p) \to ۰$ زمانی که $n \to \infty$.

(در اینجا تمامی لگاریتم‌ها در پایه ۲ است). توجه می‌کنیم که در مثال بخش قبل داشتیم $p = ۰.۰۰۱$ که در این حالت $۱ + p\log p + q\log q$ نزدیک به ۱ است. در عمل، شرط ما این بود که که نرخ باید حداقل $\frac{۱}{۲}$ باشد. اما می‌بینیم که برای $\varepsilon > ۰$ و n به‌قدر کافی بزرگ، کد C با طول n و نرخ نزدیک به ۱ وجود دارد به‌طوری‌که $P_C < \varepsilon$. (البته اگر T به‌اندازه کافی کوچک باشد، آن‌گاه کدهای طولانی نمی‌توانند به‌کار روند).

قبل از آوردن اثبات قضیه ۱.۲.۲ درباره برخی از جزییات تکنیکی که بعداً استفاده می‌شوند، بحث می‌کنیم.

احتمال وقوع الگوی خطا با w خطا برابر با $p^w q^{n-w}$ می‌باشد که این؛ بدان معناست که این احتمال تنها به w بستگی دارد.

[۱۳] maximum-likelihood-decoding

تعداد خطاها در یک کلمه دریافتی، یک متغیر تصادفی با مقدار میانگین np و واریانس $np(۱-p)$ می‌باشد. اگر $b := (np(۱-p)/(\varepsilon/۲))^{۱/۲}$، آن‌گاه از نامساوی چپیشف (قضیه ۱.۱.۴) داریم:

$$P(w > np + b) \leq \frac{۱}{۲}\varepsilon. \tag{۴}$$

ازآنجا که $p < \frac{۱}{۲}$، برای n به قدر کافی بزرگ، عدد $\rho := \lfloor np + b \rfloor$ کمتر از $\frac{۱}{۲}n$ می‌شود. فرض کنید $B_p(x)$ مجموعه کلمات y با شرط $d(x,y) \leq \rho$ باشد؛ در این‌صورت:

$$B_\rho(x) = \sum_{i \leq \rho} \binom{n}{i} < \frac{۱}{۲} n \binom{n}{\rho} \leq n . \frac{n^n}{\rho^\rho (n-\rho)^{n-\rho}} e \tag{۵}$$

(ارجاع به لم۳.۱.۴). مجموعه $B_\rho(x)$ معمولاً گوی به شعاع ρ و مرکز x (اگرچه اصطلاح توپ[۱۴] مناسب‌تر به نظر می‌آید) نامیده می‌شود.

تخمین‌های زیر را به‌کار خواهیم برد:

$$\frac{\rho}{n} \log \frac{\rho}{n} = \frac{۱}{n} \lfloor np + b \rfloor \log \frac{\lfloor np + b \rfloor}{n} = p \log p + O(n^{-۱/۲}), \tag{۶}$$

$$(۱ - \frac{\rho}{n}) \log (۱ - \frac{\rho}{n}) = q \log q + O(n^{-۱/۲}), \quad (n \to \infty),$$

سرانجام دو تابع زیر را که نقشی در اثبات بازی می‌کنند، معرفی می‌کنیم. قرار دهید:

$$u \in \{۰, ۱\}^n, v \in \{۰, ۱\}^n.$$

در این‌صورت:

$$f(u,v) := \begin{cases} ۰, & d(u,v) > \rho \text{ اگر}, \\ ۱, & d(u,v) \leq \rho \text{ اگر}. \end{cases} \tag{۷}$$

اگر $x_i \in C$ و $y \in \{۰, ۱\}^n$، آن‌گاه:

$$g_i(y) := ۱ - f(y, x_i) + \sum_{j \neq i} f(y, x_j). \tag{۸}$$

دقت می‌کنید اگر x_i تنها کدکلمه‌ای باشد که $d(x_i, y) \leq \rho$، آن‌گاه $g_i(y) = ۰$ و در غیر این‌صورت $g_i(y) \geq ۱$.

[۱۴] ball

اثبات قضیه ۱.۲.۲. در اثبات قضیه شانون، کدکلمات x_1، x_2، $\cdots$، x_M را به‌طور تصادفی (مستقل) برمی‌گزینیم. به‌صورت زیر کدگشایی می‌کنیم. اگر y دریافت شود و اگر دقیقاً یک کدکلمه x_i موجود باشد به‌طوری که $d(x_i, y) \leq \rho$، آن‌گاه y را به x_i کدگشایی می‌کنیم. در غیر این‌صورت وقوع یک خطا را اعلام می‌کنیم (یا اگر مجبور به کدگشایی گردیم، آن‌گاه همیشه به x_1 کدگشایی می‌کنیم).

فرض کنید P_i به‌صورت بالا تعریف شده باشد؛ داریم:

$$\begin{aligned} P_i &= \sum_{y \in \{0,1\}^n} P(y \mid x_i) g_i(y) \\ &= \sum_y P(y \mid x_i)\{1 - f(y, x_i)\} \sum_y \sum_{j \neq i} P(y \mid x_i f(y, x_j). \end{aligned}$$

در اینجا جمله سمت راست احتمال این است که کلمه دریافتی y متعلق به $B_\rho(x_i)$ نباشد. از رابطه ۴ این احتمال حداکثر برابر با $\frac{1}{2}\varepsilon$ می‌باشد.

بنابراین، داریم:

$$P_C \leq \frac{1}{2}\varepsilon + M^{-1} \sum_{i=1}^{M} \sum_y \sum_{j \neq i} P(y \mid x_i) f(y, x_j).$$

نکته اساسی در اثبات، این واقعیت است که $P^*(M, n, p)$ کمتر از مقدار میانگین P_C روی تمامی کدهای ممکن C است که به‌طور تصادفی انتخاب شده‌اند؛ بنابراین، داریم:

$$\begin{aligned} P^*(M, n, p) &\leq \tfrac{1}{2}\varepsilon + M^{-1} \sum_{i=1}^{M} \sum_y \sum_{j \neq i} \mathcal{E}(P(y \mid x_i)) \mathcal{E}(f(y, x_j)) \\ &= \tfrac{1}{2}\varepsilon + M^{-1} \sum_{i=1}^{M} \sum_y \sum_{j \neq i} \mathcal{E}(P(y \mid x_i)). \tfrac{|B_\rho|}{2^n} \\ &= \tfrac{1}{2}\varepsilon + (M-1) 2^{-n} |B_\rho|. \end{aligned}$$

حال لگاریتم می‌گیریم، عبارت‌های ۵ و ۶ را به‌کار می‌بریم و سپس بر n تقسیم می‌کنیم. در نتیجه:

$$\begin{aligned} & n^{-1} \log(P^*(M, n, p) - \tfrac{1}{2}) \\ & \leq n^{-1} \log M - (1 + p \log p + q \log q) + O(n^{-1/2}). \end{aligned}$$

با جانشینی $M = M_n$ بر روی طرف راست و با به‌کارگیری محدودیت روی R، برای $n > n_0$ داریم:

$$n^{-1} \log(P^*(M_n, n, p) - \frac{1}{2}\varepsilon) < -\beta < 0,$$

یعنی $P^*(M, n, p) < \frac{1}{2}\varepsilon + 2^{-\beta n}$.

این مطلب قضیه را اثبات می‌کند.

۲.۳ بهره کدگذاری

در بسیاری از کاربردهای عملی، شخص باید B و W را انتخاب نماید که B برابر با تعداد بیت‌ها در هر ثانیه است که باید به‌طور مطمئن از یک کانال نویزدار با به‌کارگیری توان حداکثر W وات انتقال داده شوند. یک مثال معروف، تکنولوژی موبایل است که در آن B کیفیت مکالمه را تعیین می‌کند و W مربوط به طول عمر باتری‌هاست. مثال دیگر انتقال در عمق فضاست که در آن B تعداد عکس‌هایی را که می‌تواند با گذر زمان در پرواز انتقال یابد، معین می‌کند و W توانی است که از صفحات خورشیدی، قابل دسترس است. در تمامی این حالات، انتقال دهنده دارای متوسط انرژی $E_b = W/B$ ژول در هر بیت کاربر است که سیگنال‌هایی را به گیرنده ارسال می‌نماید. کدگذاری ممکن است انتخاب‌ها را تحت تاثیر قرار دهد. تاثیر کدگذاری اغلب با عنوان بهره کدگذاری[۱۵] بیان می‌شود که در اینجا آن را تعریف می‌کنیم (جزییات از مهندسی برق بحث نمی‌شود).

اگر هیچ کدی استفاده نگردد، انرژی E_b در دسترس انتقال‌دهنده قرار می‌گیرد تا یک بیت را در صورتی که ۱ باشد، به یک سیگنال با دامنه $s := \sqrt{E_b}$ و اگر صفر باشد، به یک سیگنال با دامنه $s = -\sqrt{E_b}$ متناظر کند. اغلب، کانال انتقال به‌عنوان یک کانال جمعی با نویز گوسی سفید مدل می‌شود. این بدان معناست که دامنه سیگنال دریافتی برابر با r است به طوری که $r = s + n$ و نویز n از یک توزیع گوسی با میانگین صفر و واریانس σ^2 پیروی می‌کند. یک گیرنده، با تصمیم‌های سخت، هر سیگنال ارسالی با دامنه r را با آستانه ۰ مقایسه می‌کند و اگر $r > 0$، تصمیم به ۱ می‌گیرد و درغیر این‌صورت تصمیم به ۰ می‌گیرد. در چنین گیرنده‌ای، اگر نویز n علامت r را تغییر دهد، خطا اتفاق می‌افتد؛ بنابراین، احتمال خطای (در هر بیت) p_e برابر است با:

$$p_e = \int_{\sqrt{E}}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(\frac{-y^2}{2\sigma^2}\right) dy = Q\left(\sqrt{\frac{E_b}{\sigma^2}}\right)$$

که در آن:

$$Q(x) := \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(\frac{-y^2}{2}\right) dy = \frac{1}{2} \operatorname{erfc}\left(\frac{x}{\sqrt{2}}\right)$$

نسبت E_b/σ^2، نسبت سیگنال به نویز (SNR) نامیده می‌شود.

اگر کد C را به‌کار ببریم که k بیت را برروی n بیت برای ارسال روی کانال (بیت‌های کانال) تصویر می‌کند، آن‌گاه گوییم در حال استفاده از کدی با نرخ $R := k/n$ هستیم (رابطه ۳.۳.۱ را ببینید). مجبور هستیم که این بیت‌های کانال را $1/R$ بار سریع‌تر بفرستیم تا به سرعت موردنیاز، ارسال B بیت در هر ثانیه، برسیم. به‌خاطر این‌که توان دارای محدودیت W وات است، تنها به‌اندازه $E' := W/(B/R) = R.E_b$ ژول

[۱۵] Coding gain

در بیت کانال، انرژی را در دسترس داریم. با فرض داشتن طرحی مشابه طرح قبل برای انتقال بیت‌های کانال، نرخ خطای p'_e (در بیت کانال) به‌صورت:

$$p'_e = Q(\sqrt{\frac{RE_b}{\sigma^2}}),$$

به‌دست می‌آید.

بنابراین، کدگذاری باعث می‌شود تا داشته باشیم $p'_e > p_e$، زیرا میزان انرژی کاهش‌یافته است. تمام ایده کدگذاری زمانی تحقق می‌یابد که بتوان در عوض کاهش انرژی در هر بیت، خطاهای احتمالی تصحیح شوند.

بیایید مجدداً به مارینر ۶۹′ نگاهی دقیق‌تر بیندازیم. به‌جای نامیدن سمبل‌های ارسالی با ۰ و ۱، آنها را با ۱+ و ۱− نشان دهیم. ۶۴ دنباله به طول ۳۲ که مارینر به‌کار برد سطرهای ماتریس‌های $H_2^{\otimes 5}$ و $-H_2^{\otimes 5}$ از بخش ۱.۳ بودند. برای یک سیگنال دریافتی (با تصمیم‌های سخت)، سطر دریافتی شامل ۳۲ سمبل ± 1 برداشته شد و ضرب داخلی این سطر و ۳۲ سطر $H_2^{\otimes 5}$ محاسبه گردید. اگر خطایی رخ نمی‌داد، ۳۱ تا از این حاصل‌ضرب‌ها ۰ بودند و یکی برابر با ± 32 که نشان‌دهنده این است که سیگنال دریافتی درست بوده است. در حالت یک خطا، حاصل‌ضرب‌های داخلی ± 2 بودند، با یک استثنای ± 30، که سیگنال درست را نتیجه می‌دهد. دقت دارید که تا حداکثر هفت خطا، ضرب داخلی یکتایی با قدرمطلق بزرگ‌تر از ۱۶ وجود دارد که اشاره به درست بودن سیگنال دارد.

حال بیایید به تاثیر کدگذاری نگاهی کنیم.

مثال ۱.۲.۳. مثال کد مارینر را درنظر بگیرید. فرض کنید برای دریافت واضح یک عکس، هر ۶ تایی با احتمال P_E، که حداکثر 10^{-4} است، خطا باشد. در حالتی که کدگذاری نباشد، برای رسیدن به این احتمال خطا، نیاز به $E_b/\sigma^2 \approx 17.22$ داریم، زیرا که $p_e = Q(\sqrt{17.22}) \approx 10^{-4}/6$ و $P_E = 1 - (1 - p_e)^6 \approx 10^{-4}$.

سپس، فرض کنید که از کد $[32, 6]$ استفاده می‌کنیم، که حداکثر هفت خطا را تصحیح می‌کند، با SNR برابر با ۱۷.۲۲. چون $R = 6/32$، داریم $p'_e \approx 0.036$. (دقت دارید که این احتمال خطا ۲۰۰۰ برابر بزرگتر از قبل است!) پس از کدگشایی، ۶ تایی‌های خطادار دارای احتمال:

$$P'_E = \sum_{i>7} \binom{32}{i} (p'_e)^i (1 - p'_e)^{32-i} \approx 1.4 \times 10^{-5},$$

هستند که تقریباً یک مرتبه در توان از P_E بهتر است.

هنگام به‌کارگیری تصمیمات نرم، موج دریافتی به سطری از ۱ و ۱− ها ترجمه نمی‌شود، بلکه مستقیماً

به سطرهای $H_۴^{۵\otimes}$ مرتبط می‌شود. دراین حالت، احتمال این‌که سیگنالی که ما به‌عنوان شبیه‌ترین سیگنال انتخاب نموده‌ایم، در واقع همان سیگنال ارسالی باشد، بیشتر است.

خاطرنشان می‌کنیم که اگر تصمیم نرم را در مثال ۱.۲.۳ به‌کار برده بودیم، آن‌گاه احتمال خطا به ۲×۱۰^{-۱۱} کاهش یافته بود.

روش دیگری برای نگاه به مساله در این حالت وجود دارد. می‌توانیم کدگذاری را برای نیاز به انرژی کمتر[۱۶] به‌کار بریم. ممکن است C را نه برای کاهش نرخ خطا، بلکه برای کاهش SNR لازم، انتخاب نماییم.

در مثال مارینر، احتمال $۱۰^{-۴}$ را برای دریافت یک ٦ تایی غلط داشتیم. برای رسیدن به $P'_E = ۱۰^{-۴}$، یک SNR با مقدار ۱۴.۸۳ کافی خواهد بود (با محاسبه‌ای مشابه با حالت بالا).این بدان معناست که کاربرد کدگذاری به ما اجازه کاهش اندازه صفحات خورشیدی تقریباً به‌اندازه ۱۵ درصد را می‌دهد. به‌وسیله کدگشایی با تصمیم نرم، این کاهش تا بیش از ۵۰ درصد خواهد بود؛ (ما نیاز به یک SNR با مقدار ۷.۲۴ در آن حالت داریم).

تعریف ۲.۲.۳. وقتی‌که احتمال خطا را ثابت فرض کرده‌ایم، نسبت بین SNR (کدنشده) و SNR' (کدشده) پس از کدگشایی، بهره کدگذاری نامیده می‌شود.

بهره کدگذاری بستگی به کد، الگوریتم کدگشایی، کانال مورد بحث و احتمال خطای مورد نیاز پس از کدگشایی دارد. اغلب، این کمیت برحسب dB، یعنی ۱۰ برابر لگاریتم نسبت موجود در تعریف ۲.۲.۳ در پایه ۱۰، بیان می‌شود. در متون مهندسی، نتیجه مثال ۱.۲.۳ به‌عنوان یک بهره کدگذاری با اندازه ۰.٦۵dB توصیف می‌شود. متذکر می‌شویم که برای یک کد داده شده، همیشه نسبت سیگنال به نویزی وجود خواهد داشت که در آن کد بی‌فایده می‌باشد؛ کدگذاری باعث بدتر شدن وضعیت نسبت به زمانی است که از آن استفاده نمی‌شود.

ما تنها از دیدگاه انرژی به کدگذاری نگاه کردیم. خواننده باید متوجه باشد که هم‌چنین کدگذاری، پیچیدگی این فرایند را افزایش می‌دهد و در برخی از حالات، برای آن هزینه زیادی باید بپردازیم.

۲.۴ پیشنهادها

مقاله شانون با عنوان تئوری ریاضی مخابرات (۱۹۴۸) [٦۲] نشان از آغاز نظریه کدگذاری دارد. ازآنجا که این قضیه نشان می‌دهد کدهای خوب وجود دارند، طبیعی بود که هرکسی تلاشی را بر ساختن این

[۱۶] need less energy

کدها آغاز نماید. چون این کدها اغلب برای پشتیبانی دستگاه‌های الکتریکی خیلی کوچک به‌کار می‌رود، محققان به‌خصوص به کدهایی با ساختارهای زیاد علاقه‌مند بودند که الگوریتم‌های کدگشایی نسبتاً ساده‌ای داشته باشند. در فصل‌های بعد، خواهیم دید که به‌دست آوردن کدهای خیلی منظم بدون از دست دادن خاصیت برخاسته از قضیه ۱.۲.۲ بسیار مشکل می‌باشد. ملاحظه می‌کنیم که یکی از عرصه‌های مهمی که نظریه کدگذاری به کار می‌رود، کاربرد در ارتباطات تلفنی می‌باشد. بسیاری از نام‌هایی که خواننده با آنها در این کتاب روبرو خواهد شد، نام‌های اعضای (تشکیل دهنده) پرسنل آزمایشگاه‌های تلفن بل [۱۷] هستند. علاوه بر شانون، افرادی مانند برلیکمپ[۱۸] ، گیلبرت[۱۹] ، همینگ[۲۰] ، لوید[۲۱] ، مک‌ویلیامز[۲۲] ، اسلپیان[۲۳] و اسلون[۲۴] را ذکر می‌کنیم. این مطلب تعجب برانگیز نیست که بسیاری از متون درباره نظریه کدگذاری در ژورنال علمی آزمایشگاه بل[۲۵] می‌تواند یافت شود. نویسنده به‌طور عمیق اعتراف می‌کند که بسیاری از دانش او در زمینه کدگذاری در خلال ملاقات وسیع او با آزمایشگاه‌های بل بوده است. خواننده‌ای که به جزییات بیشتر درباره کد به‌کار رفته در مارینر ۱۹۶۹ علاقه‌مند است می‌تواند به مرجع [۵۶] مراجعه نماید. هم‌چنین در مورد کدگذاری دیسک فشرده، می‌توانید منابع [۷۷] و [۷۸] را ببینید.

با مراجعه به این منابع، خواننده می‌تواند مشاهده نماید که اکنون مهم‌ترین نتایج درباره نظریه کدگذاری در طول سال‌های بسیار در مجله IEEE Transactions on Information Theory چاپ شده است.

[۱۷] Bell Telephone Laboratories
[۱۸] Berlekamp
[۱۹] Gilbert
[۲۰] Hamming
[۲۱] Lloyd
[۲۲] MacWilliams
[۲۳] Slepian
[۲۴] Sloan
[۲۵] Bell System Technical Journal

۲.۵ مسائل

۱.۲.۵. رابطه ۱ را ثابت کنید.

۲.۲.۵. کد به طول ۶ را که در آزمایش پرتاب سکه در بخش ۲.۲ بیان شد، درنظر بگیرید. نشان دادیم که احتمال آن‌که کلمه دریافتی به‌طور صحیح کدگشایی شده باشد برابر با $q^۶ + ۶q^۵p + q^۴p^۲$ است. حال فرض کنید که پس از کدگشایی، تنها سه سمبل اول از هر کلمه کدگشایی شده را حفظ کرده‌ایم؛ یعنی اطلاعات مربوط به آزمایش پرتاب سکه. احتمال این را تعیین کنید که یک سمبل در این دنباله نادرست باشد (این احتمال را احتمال خطای سمبل[۲۶] می‌نامیم که بدون کدگذاری برابر با p خواهد بود).

۳.۲.۵. کدی شامل هشت کلمه به طول ۷ بسازید که هر دو کدکلمه متمایز دارای فاصله حداقل ۴ باشد. برای یک کانال دوتایی متقارن با احتمال خطای p، احتمال این را که یک کلمه دریافتی به‌طور صحیح کدگشایی شده باشد، تعیین کنید.

۴.۲.۵. در یک کانال دوتایی با احتمال $q = ۰.۹$ سمبل انتقال یافته به‌طور صحیح دریافت شده و با احتمال $p = ۰.۱$ پاک شده است (یعنی ما ؟ دریافت می‌کنیم). در این کانال می‌خواهیم کدی با نرخ $\frac{۱}{۲}$ را به‌کار بریم. آیا اگر ما هر سمبل انتقال را تکرار نماییم، احتمال تفسیر صحیح افزایش می‌یابد؟ آیا ممکن است کدی با هشت کلمه به طول ۶ را بسازیم به‌طوری که دو سمبل پاک شده قابل بازیابی باشند؟ احتمال‌های تفسیر صحیح این دو کد را بیابید (فرض کنید که دریافت کننده سمبل‌های پاک شده را با حدس یک سمبل تغییر ندهد).

۵.۲.۵. مثال مارینر ۱۹۶۹ را درنظر بگیرید. فرض کنید یک سطر از ۳۲ سمبل با $e_۱$ خطا و $e_۲$ سمبل پاک‌شده دریافت شده است. نشان دهید که اگر $۲e_۱ + e_۲ < ۱۶$، آن‌گاه سطر درست قابل بازیابی است.

۶.۲.۵. فرض کنید C یک کد دوتایی با طول ۱۶ باشد به‌طوری که:

الف. هر کدکلمه دارای وزن ۶ است.

ب. هر دو کدکلمه متمایز دارای فاصله ۸ هستند.

نشان دهید $|c| \leq ۱۶$. آیا چنین کدی با $|c| = ۱۶$ موجود است؟

[۲۶] symbol error probability

۷.۲.۵. فرض کنید C یک کد باینری تصحیح‌کننده خطای واحد با طول زوج n باشد. نشان دهید $|c| \leq ۲^n/(n+۲)$.

راهنمایی: تعداد زوج‌های (x, c) را بشمارید که x یک کلمه با طول n است، $\mathbf{c} \in C$ و x و $\mathbf{c}$ در دو مکان با یکدیگر متفاوت هستند.

فصل ۳

کدهای خطی

۳.۱ کدهای بلوکی

در این فصل فرض می‌کنیم که اطلاعات با استفاده از الفبای Q با q سمبل متمایز کد شده است. یک کد، کد بلوکی نامیده می‌شود اگر اطلاعات کدشده را بتوان به بلوک‌های با n سمبل که می‌توانند مستقلاً کدگشایی شوند، تقسیم نمود. این بلوک‌ها کدکلمات هستند و n طول بلوک یا طول کلمه (یا فقط طول) نامیده می‌شود. مثال‌های ذکر شده در فصل قبل همگی کدهای بلوکی بودند. در فصل ۱۳ ما به‌طور خلاصه درباره یک مجموعه کاملاً متفاوت، به‌نام کدهای کانولوشن، بحث می‌کنیم که در آنجا یک دنباله نامتناهی از سمبل‌های اطلاعاتی i_0، i_1، i_2، $\cdots$ به دنباله نامتناهی از سمبل‌های پیام، کد شده است؛ برای مثال، برای نرخ $\frac{1}{2}$ ممکن است داشته باشیم $i_0, i_1, i_2, \cdots \to i_0, i'_0, i_1, i'_1, \cdots$ که در آن i'_n تابعی از $i_0, i_1, \cdots, i_n$ است. برای کدهای بلوکی، تعریف ۲.۲.۱ را به الفبای دلخواه گسترش می‌دهیم.

تعریف ۱.۳.۱. اگر $x \in Q^n$، $y \in Q^n$، آن‌گاه فاصله x از y که با $d(x,y)$ نمایش داده می‌شود، برابر است با:

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

وزن x، $w(x)$، به صورت:

$$w(x) := d(x, 0)$$

تعریف می‌شود (همواره $(۰,۰,...,۰)$ را با ۰ و $(۱,۱,...,۱)$ را با ۱ نمایش می‌دهیم).

فاصله کد، تعریف شده توسط ۱.۳.۱، فاصله همینگ[۱] نامیده می‌شود و در واقع یک متریک روی Q^n است. اگر ما در حال استفاده از کانالی با این خاصیت باشیم که یک خطا در موقعیت i روی سایر موقعیت‌ها تاثیر ندارد و یک سمبل با خطا بتواند، با احتمال یکسان، هر یک از $q-۱$ سمبل باقی‌مانده باشد، در این‌صورت فاصله همینگ روش خوبی برای اندازه‌گیری محتوای خطای یک پیام دریافتی است. در فصل ۱۲ خواهیم دید که در موقعیت‌های دیگر توابع فاصله دیگری ترجیح داده می‌شوند.

در زیر یک کد C، یک زیر مجموعه سره ناتهی از Q^n است. اگر $|c| = ۱$، کد را بدیهی می‌نامیم. اگر $q = ۲$، کد را یک کد دوتایی می‌نامیم، برای $q = ۳$، یک کد سه‌تایی و الی آخر. مفاهیم زیر، نقش اساسی در این کتاب بازی می‌کنند (به فصل ۲ مراجعه شود):

تعریف ۲.۳.۱. کمترین—فاصله یک کد غیربدیهی C برابر است با:

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

کمترین—وزن C برابر است با:

$$\min\{w(x) \mid bfx \in C, x \neq ۰\}.$$

هم‌چنین مفهوم نرخ کد را به صورت زیر تعمیم می‌دهیم.

تعریف ۳.۳.۱. اگر $|Q| = q$ و $C \subset Q^n$، آن‌گاه:

$$R := n^{-۱} \log_q |c|$$

نرخ (— اطلاعات) کد C نامیده می‌شود.

برخی اوقات، علاقه‌مندیم بدانیم که یک کلمه دریافتی از نزدیک‌ترین کدکلمه، چقدر فاصله می‌تواند داشته باشد. برای این منظور، قرینه‌ای از کمترین—فاصله را معرفی می‌کنیم.

تعریف ۴.۳.۱. اگر $C \subset Q^n$، آن‌گاه شعاع پوششی $\rho(C)$ از C برابر است با:

$$\max\{\min\{d(x,c) \mid c \in C\} \mid x \in Q^n\}.$$

[۱] Hamming distance

به خواننده یادآوری می‌کنیم که در فصل ۲، گوی $B_\rho(x)$ با شعاع ρ و مرکز x به‌صورت مجموعه $\{y \in Q^n \mid d(x,y) \leq \rho\}$ معرفی شد. اگر ρ بزرگ‌ترین عدد صحیح باشد به‌طوری که گوی‌های $B_\rho(\mathbf{c})$ با $\mathbf{c} \in C$ مجزا باشند، آن‌گاه $d = ۲\rho + ۱$ یا $d = ۲\rho + ۲$. شعاع پوششی برابر با کوچک‌ترین ρای است به‌طوری که گوی‌های $B_\rho(\mathbf{c})$ که $\mathbf{c} \in C$، مجموعه Q^n را بپوشاند. اگر این اعداد برابر باشند، آن‌گاه کد C را کد کامل می‌نامیم. این مطلب را می‌توان به صورت زیر بیان نمود.

تعریف ۵.۳.۱. یک کد $C \subset Q^n$ با کمترین —فاصله $۲e + ۱$، کد کامل نامیده می‌شود، اگر هر $x \in Q^n$ دارای فاصله کمتر یا مساوی e با دقیقاً یک کدکلمه باشد.

این واقعیت که کمترین —فاصله برابر با $۲e + ۱$ است به این معناست که این کد تصحیح‌کننده e—خطاست. مطلب زیر واضح است:

۶.۳.۱. شرط گوی —پوششی[۲]

اگر $C \subset Q^n$ یک کد کامل تصحیح‌کننده $e-$ خطا باشد، آن‌گاه:

$$|c| \sum_{i=۰}^{e} \binom{n}{i} (q-۱)^i = q^n.$$

البته، کد بدیهی یک کد کامل است اگرچه نمی‌توان از کمترین —فاصله برای چنین کدی صحبت کرد. یک مثال ساده از یک کد کامل در فصل ۲، کد تکراری دوتایی با طول فرد n که شامل دو کلمه **0** و **1** است، می‌باشد.

۳.۲ کدهای خطی

حال، مساله ساختن کدهایی را که دارای ساختارهای جبری هستند، شروع می‌کنیم. اولین ایده، گرفتن گروه Q به عنوان الفبا و گرفتن زیرگروه C از Q^n به‌عنوان کد می‌باشد. این کد یک کد گروهی نامیده می‌شود. در این بخش (درواقع در بخش عمده‌ای از این کتاب) ما به ساختارهای بیشتر (خیلی زیاد) نیاز خواهیم داشت. در ادامه، Q میدان $\mathbb{F}_q$ است که در آن $q = p^r$ (p اول است). اکنون Q^n یک فضای برداری n—بعدی است؛ یعنی $\mathbb{F}_q^n$ (برخی اوقات با $\mathcal{R}$ نمایش داده می‌شود). در فصل‌های بعد، بعضاً از این واقعیت استفاده می‌کنیم که Q^n با گروه جمعی $\mathbb{F}_{q^n}$ یک‌ریخت است (ارجاع به بخش ۱.۱).

---

[۲] Sphere-packing

تعریف ۱.۳.۲. یک کد خطی $q-$ تایی، یک زیرفضای $\mathbb{F}_q^n$ است. اگر C دارای بعد k باشد، آن‌گاه C یک کد $[n,k]$ نامیده می‌شود.

از اینجا به بعد، کد $[n,k,d]$ را به‌عنوان نمادی برای یک کد خطی $k-$بعدی با طول n و کمترین—فاصله d به‌کار خواهیم برد. یک کد (n,M,d) می‌تواند هر کد با طول کلمه n، با M کدکلمه و کمترین—فاصله d باشد.

تعریف ۲.۳.۲. یک ماتریس مولد G برای کد C، یک ماتریس k در n است که سطرهای آن تشکیل یک پایه برای C می‌دهند.

اگر G یک ماتریس مولد باشد، آن‌گاه $C=\{\mathbf{a}G \mid \mathbf{a}\in Q^k\}$. G را فرم استاندارد (اغلب فرم پلکانی کاهش‌یافته) خواهیم گفت، اگر $G=(I_k \quad P)$، که I_k ماتریس همانی k در k می‌باشد. کد $(۶,۸,۳)$ که در مثال بخش ۲.۱ به‌کار بردیم، یک کد خطی با ماتریس مولد $G=(I \quad J-I)$ است. اگر G به فرم استاندارد باشد، آن‌گاه k سمبل اول یک کدکلمه، سمبل‌های اطلاعات نامیده می‌شوند. این سمبل‌ها می‌توانند به‌طور دلخواه اختیار شوند و سپس سمبل‌های باقی‌مانده که آنها را سمبل‌های بررسی‌توازن می‌نامیم، مشخص می‌گردند.

کد به‌کار رفته در رابط صفحه کلید PC که در مقدمه بیان شد، دارای یک بیت بررسی‌توازن (متناسب با این نام) و ماتریس مولد:

$$G=(I_۷ \quad \mathbf{1}^T)$$

است. تا آنجا که قدرت تصحیح خطا اهمیت دارد، دو کد $C_۱$ و $C_۲$ به‌طور یکسان خوب می‌باشند، اگر $C_۲$ با به‌کارگیری یک جای‌گشت ثابت از مکان‌های کد $C_۱$ به‌دست آمده باشد. چنین کدهایی را هم‌ارز می‌نامیم. برخی اوقات، تعریف هم ارزی را با پذیرفتن جای‌گشت روی سمبل‌های Q (برای یک مکان ثابت از کد) نیز می‌توان گسترش داد. این مطلب در جبرخطی مشهور است که هر کد خطی با کدی که دارای یک ماتریس مولد به‌شکل استاندارد است، هم ارز است. در حالت کلی، کد C روی k مکان، متقارن نامیده می‌شود (و سمبل‌ها در این مکان‌ها سمبل‌های اطلاعاتی نامیده می‌شوند)، اگر $|c|=q^k$ و برای هر انتخاب دلخواه از مختصات این k مکان دقیقاً یک کدکلمه متناظر با این انتخاب موجود باشد؛ بنابراین، در بالا دیدیم که یک کد $[n,k]$ خطی بر روی حداقل یک k تایی از مکان‌ها متقارن است. از آنجا که می‌توان سمبل‌های اطلاعاتی و سمبل‌های اضافی را از یکدیگر تفکیک نمود، این کدها را تفکیک‌پذیر[۳] نیز می‌نامند. از تعریف ۳.۳.۱، یک کد $[n,k]$ دارای نرخ k/n است و این در تطابق با

[۳] separable

این واقعیت است که k تا از این n سمبل، اطلاعات را حمل می‌کنند. خواننده باید بررسی نماید که کد $[۶, ۳, ۳]$ به‌کار رفته در بخش ۲.۱ بر روی ۴ تا از ۳ تایی‌های مکان‌ها، متقارن نمی‌باشد.

خواننده به این مطلب پی خواهد برد که اگر کد C دارای کمترین—فاصله $d = ۲e + ۱$ باشد، آن‌گاه تا e خطا را در کلمه دریافتی تصحیح می‌کند. اگر $d = ۲e$، آن‌گاه هر الگوی خطا با وزن حداکثر e قابل تشخیص است. در حالت کلی، اگر C دارای M کلمه باشد، آنگاه برای یافتن d باید $\binom{n}{۲}$ زوج کدکلمه را بررسی نمود. برای کدهای خطی، این کار را می‌توان آسان‌تر انجام داد.

قضیه ۳.۳.۲. برای یک کد خطی C، کمترین —فاصله برابر با کمترین —وزن است.

اثبات. $d(x, y) = d(x - y, ۰) = w(x - y)$ و اگر $x \in C$ و $y \in C$، آن‌گاه $x - y \in C$. □

تعریف ۴.۳.۲. اگر C یک کد $[n, k]$ باشد، آن‌گاه کد دوگان، $C^{\perp}$، به صورت:

$$C^{\perp} := \{y \in \mathcal{R} \,|\, \forall_{x \in C}[< x, y >= ۰]\},$$

تعریف می‌شود.

به‌وضوح کد دوگان، $C^{\perp}$، یک کد خطی می‌باشد؛ یعنی یک کد $[n, n - k]$. خواننده باید دقت کند که $C^{\perp}$ را به معنای مکمل متعامد به‌عنوان فضاهای برداری روی $\mathbb{R}$ تفسیر نکند. در حالت میدان متناهی Q، زیرفضاهای C و $C^{\perp}$ می‌توانند دارای اشتراکی بزرگ‌تر از $\{۰\}$ باشند و درواقع آنها حتی می‌توانند برابر باشند. اگر $C = C^{\perp}$، آن‌گاه C یک کد خوددوگان نامیده می‌شود.

اگر $G = (I_k \quad P)$ ماتریس مولد در فرم استاندارد برای کد C باشد، آن‌گاه $H = (-P^T \quad I_{n-k})$ ماتریس مولد $C^{\perp}$ می‌باشد. این مطلب از این واقعیت نتیجه می‌شود که H دارای طول و بعد $C^{\perp}$ است و این‌که $GH^T = ۰$ ایجاب می‌کند که ضرب داخلی هر کدکلمه $\mathbf{a}G$ با هر سطر H برابر با صفر است؛ به بیان دیگر، داریم:

$$x \in C \Leftrightarrow xH^T = ۰ \qquad (۱)$$

در رابطه ۱، $n - k$ معادله خطی داریم به‌طوری که باید هر کدکلمه در آن صدق نماید.

اگر $y \in C^{\perp}$، آن‌گاه معادله $< x, y >= ۰$ که برای هر $x \in C$ برقرار است، یک (معادله) بررسی‌توازن و H ماتریس بررسی‌توازن C نامیده می‌شود. در مورد کد $[۶, ۳]$ به‌کار رفته در بخش ۲.۱، معادله $a_۴ = a_۲ + a_۳$ یکی از معادلات بررسی‌توازن است (این کد روی مکان‌های ۲، ۳ و ۴ متقارن نیست).

تعریف ۵.۳.۲ اگر C یک کد خطی با ماتریس بررسی‌توازن H باشد، آن‌گاه برای هر $x \in Q^n$ مقدار xH^T را هم‌رفت[۴] x می‌نامیم. مشاهده می‌نمایید که شعاع پوششی $\rho(C)$ از کد $[n,k]$ (ارجاع به تعریف ۴.۳.۱)، کوچک‌ترین عدد صحیح ρ است به‌طوری که هر بردار (ستونی) در Q^{n-k} را بتوان به‌صورت مجموع حداکثر ρ ستون از H نوشت.

در رابطه ۱ می‌بینیم که تنها کدکلمات هستند که دارای هم‌رفت ۰ می‌باشند. هم‌رفت درکدگشایی بردار دریافتی x یکی از مهم‌ترین ابزار کمکی است. قبلاً هم این ایده با به‌کارگیری کد $[۶,۳]$ معرفی شده بود. چون C زیرگروهی از Q^n است، می‌توانیم Q^n را به هم‌مجموعه‌های C افراز نماییم. دو بردار x و y در هم‌مجموعه یکسانی هستند اگر و تنها اگر آنها دارای هم‌رفت یکسانی باشند $(xH^T = yH^T \Leftrightarrow x - y \in C)$؛ بنابراین، اگر بردار x دریافت شده باشد به‌طوری که e الگوی خطا باشد، آن‌گاه x و e دارای هم‌رفت یکسانی هستند. این مطلب نتیجه می‌دهد که برای کدگشایی x با قاعده بیشترین درست‌نمایی، بردار e را با وزن کمترین در هم‌مجموعه شامل x باید انتخاب نمود و سپس x را به‌صورت $x - e$ کدگشایی کرد. بردار e را سردسته[۵] می‌نامیم. نحوه انجام این کار در عمل، در بخش ۲.۱ برای کد $[۶,۳]$ تشریح شد. برای هفت تا از هشت هم‌مجموعه، یک سردسته یکتا وجود داشت. تنها برای هم‌رفت $(s_۱, s_۲, s_۳) = (۱,۱,۱)$ ما باید یکی از سه سردسته ممکن را انتخاب کنیم.

در اینجا اولین امتیاز بزرگ در معرفی ساختارهای جبری را می‌بینیم. برای یک کد $[n,k]$ روی $\mathbb{F}_q$ تعداد q^k کدکلمه و q^n پیام دریافتی ممکن وجود دارند. بیایید فرض کنیم که نرخ، به طور قابل قبولی بالاست. گیرنده نیاز به دانستن q^{n-k} سردسته متناظر با تمامی هم‌رفت‌های ممکن را دارد. اما q^{n-k} بسیار کوچک‌تر از q^n می‌باشد. اگر این کد دارای ساختاری نباشد، آن‌گاه برای هر کلمه دریافتی x، مجبور خواهیم بود که کلمات دریافتی با بیشترین احتمال را لیست نماییم.

واضح است که اگر c دارای کمترین—فاصله $d = ۲e + ۱$ باشد، آن‌گاه هر الگوی خطا با وزن حداکثر e، سردسته یکتایی از یک هم‌مجموعه است؛ چرا که دو بردار با وزن حداکثر e دارای فاصله حداکثر $۲e$ هستند؛ بنابراین، در هم‌مجموعه‌های متفاوتی هستند. اگر C کامل باشد، آن‌گاه سردسته دیگری وجود ندارد. اگر کد C دارای کمترین—فاصله $۲e + ۱$ باشد و تمامی سردسته‌ها دارای وزن حداکثر $e + ۱$ باشند، آن‌گاه این کد شبه‌کامل نامیده می‌شود. کد $[۶,۳]$ از بخش ۲.۱ یک مثال از این دست است. شعاع پوششی برابر با وزن سردسته یک هم‌مجموعه با وزن ماکسیمم است.

در اینجا مثال دیگری از یک فرایند کدگشایی خیلی ساده (ر.ک. مرجع [۳]) می‌آوریم. فرض کنید C

---

[۴] syndrome

[۵] coset leader

یک کد $[۲k, k]$ خوددوگان دوتایی با ماتریس مولد $G = (I_k \quad P)$ باشد. اگر C بتواند ۳ خطا را تصحیح نماید و احتمال این‌که بیشتر از ۳ خطا در یک بردار دریافتی رخ دهد، خیلی کوچک باشد، آن‌گاه الگوریتم کدگشایی زیر، مفید خواهد بود.

ماتریس بررسی‌توازن را به‌صورت $H = (P^T \quad I_k)$ به دست می‌آوریم. اما G نیز یک ماتریس بررسی‌توازن است؛ چرا که C خوددوگان است. فرض کنید $y = c + e$ بردار دریافتی باشد. $\mathbf{e}$ را به‌صورت $(e_۱; e_۲)$ می‌نویسیم که در آن $e_۱$ متناظر با k مکان اول است و $e_۲$ متناظر با k مکان آخر. دو هم‌رفت زیر را محاسبه می‌کنیم:

$$s^{(۱)} := yH^T = e_۱P + e_۲,$$

$$s^{(۲)} := yG^T = e_۱ + e_۲P^T.$$

اگر $t \leq ۳$ خطا همگی در نیمه ابتدایی یا انتهایی y، یعنی $e_۱ = ۰$ یا $e_۲ = ۰$، رخ دهند، آن‌گاه یکی از هم‌رفت‌ها دارای وزن ≥ ۳ است و ما فوری $\mathbf{e}$ را به‌دست می‌آوریم. اگر این حالت اتفاق نیفتد، آن‌گاه فرض $t \leq ۳$ ایجاب می‌کند که $e_۱$ یا $e_۲$ دارای وزن ۱ باشد. $۲k$ بردار $y^{(i)}$ حاصل از تغییر i امین مختصات y $(۱ \leq i \leq ۲k)$ را درنظر می‌گیریم. برای هر یک از این بردارها $s_۱$ (برای $i \leq k$) و $s_۲$ (برای $i > k$) را به‌ترتیب محاسبه می‌کنیم. اگر ما هم‌رفت با وزن ≥ ۲ را بیابیم، می‌توانیم خطاهای باقی‌مانده را تصحیح کنیم. اگر ما همرفتی با وزن ۳ را بیابیم، چهار خطا را تشخیص داده‌ایم، اگر C یک کد با فاصله ۸ باشد و اگر C دارای فاصله ≤ ۱۰ باشد، آن‌گاه می‌توانیم این الگوی چهار خطا را هم تصحیح کنیم.

اغلب ثابت می‌شود که الحاق یک بیت اضافی، مطابق برخی قواعد طبیعی، به هر کدکلمه از کد C، مفید خواهد بود. متعارف‌ترین اینها در تعریف زیر داده شده است.

تعریف ۶.۳.۲. اگر C یک کد با طول n روی الفبای $\mathbb{F}_q$ باشد، آن‌گاه کد توسیع $\overline{C}$ به‌صورت زیر تعریف می‌شود:

$$\overline{C} := \{(c_۱, c_۲, ..., c_n, c_{n+۱}) \mid (c_۱, ..., c_n) \in C, \sum_{i=۱}^{n+۱} c_i = ۰\}.$$

اگر C یک کد خطی با ماتریس مولد G و ماتریس بررسی‌توازن H باشد، آن‌گاه $\overline{C}$ دارای ماتریس مولد $\overline{G}$ و ماتریس بررسی‌توازن $\overline{H}$ است که در آن $\overline{G}$ با اضافه‌نمودن یک ستون به G به‌دست آمده است،

به‌طوری که مجموع ستون‌های $\overline{G}$ برابر با ۰ گردد و

$$\overline{H} := \begin{pmatrix} ۱ & ۱ & ۱ & \cdots & ۱ \\ & & & & ۰ \\ & & H & & ۰ \\ & & & & \vdots \\ & & & & ۰ \end{pmatrix}.$$

اگر C یک کد دوتایی با کمترین—فاصله فرد d باشد، آن‌گاه $\overline{C}$ دارای کمترین—فاصله $d+۱$ است؛ زیرا تمامی وزن‌ها و فاصله‌ها برای $\overline{C}$ زوج هستند.

۳.۳ کدهای همینگ

فرض کنید G ماتریس مولد k در n از یک کد خطی $[n,k]$، C روی $\mathbb{F}_q$ باشد. اگر هر دو ستون G مستقل خطی باشند؛ یعنی ستون‌ها متناظر با نقاط متمایز $PG(k-۱,q)$ باشند، آن‌گاه C یک کد تصویری[۶] نامیده می‌شود. کد دوگان $C^\perp$ دارای ماتریس بررسی‌توازن G است. اگر $c \in C^\perp$ و $\mathbf{e}$ بردار خطا با وزن ۱ باشد، آن‌گاه هم‌رفت $(\mathbf{c}+\mathbf{e})G^T$ مضربی از یک ستون G می‌باشد. چون این مقدار به‌طور یکتا ستون G را مشخص می‌کند، نتیجه می‌شود که $C^\perp$ کدی است که یک خطا را تصحیح می‌کند. حال به حالتی نگاه می‌کنیم که n بیشترین باشد (برای k مفروض).

تعریف ۱.۳.۳. فرض کنید $n := (q^k-۱)/(q-۱)$. کد همینگ $[n,n-k]$ روی $\mathbb{F}_q$ کدی است که ستون‌های ماتریس بررسی‌توازن آن دو به دو مستقل خطی (روی $\mathbb{F}_q$) می‌باشند؛ یعنی ستون‌ها یک مجموعه ماکسیمال از بردارهای مستقل خطی هستند.

در اینجا، به‌وضوح بین تمامی کدهای هم ارز تفاوتی قائل نیستیم. بدیهی است که کمترین—فاصله کد همینگ برابر با ۳ است.

قضیه ۲.۳.۳. کدهای همینگ، کدهای کاملی هستند.

اثبات. فرض کنید C یک کد $[n,n-k]$ همینگ روی $\mathbb{F}_q$ باشد، که در آن $n=(q^k-۱)/(q-۱)$. اگر $x \in C$، آن‌گاه:

$$B_۱(x) = ۱ + n(q-۱) = q^k.$$

[۶] projective code

بنابراین، q^{n-k} گوی متمایز با شعاع ۱ به مرکز کدکلمات C در مجموع دارای $|c|q^k = q^n$ کلمه هستند، که این تمامی کلمات ممکن است؛ بنابراین، C کامل است (ارجاع به تعریف ۵.۳.۱ و شرط پوششی ٦.۳.۱).

مثال ۳.۳.۳. کد همینگ دوتایی $[۷, ۴]$ دارای ماتریس بررسی‌توازن به شکل زیر است:

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

اگر ما دو ستون از H و مجموع این دو (برای مثال سه ستون اول H) را درنظر بگیریم، آن‌گاه یک کلمه با وزن ۳ در C با ۱ هایی در مکان‌های متناظر با این ستون‌ها (برای مثال (۱۱۱۰۰۰۰)) موجود است؛ بنابراین، C دارای هفت کلمه به وزن ۳ است به‌طوری که وقتی به‌عنوان سطرهای یک ماتریس لیست شوند، $PG(۲, ۲)$ را تشکیل می‌دهند. کلمات با وزن زوج در C جوابی برای مساله ۳.۲.۴ هستند. با نگاهی به H می‌بینیم که کد گسترش‌یافته $\overline{C}$ خوددوگان است.

مثال ۴.۳.۳. فرض کنید که ما یک کد همینگ گسترش‌یافته با طول ۲^m را روی کانال BSC با احتمال خطای بیت p ($q := ۱ - p$) به‌کار می‌بریم. میانگین خطاها در هر بلوک قبل از کدگشایی برابر با np است. اگر یک خطا رخ دهد، تصحیح می‌شود. اگر دو خطا رخ دهد، آن‌گاه خطا تشخیص داده می‌شود، اما تصحیح خطا نداریم؛ بنابراین، دو خطا باقی می‌ماند. در غیر این‌صورت، اگر بخواهیم خطاها را اصلاح کنیم، کدگشا ممکن است با تغییر کلمه دریافتی با حداقل ۳ خطا به نزدیک‌ترین کدکلمه، یک خطای بیشتر را مطرح کند؛ بنابراین، میانگین خطاها در هر بلوک پس از کدگشایی، حداکثر برابر است با:

$$\begin{aligned} &۲\tbinom{n}{۲}p^۲q^{n-۲} + \sum_{i=۳}^{n}(i+۱)\tbinom{n}{i}p^iq^{n-i} \\ &= ۲\tbinom{n}{۲}p^۲\{q^{n-۲} + \sum_{i=۳}^{n}\frac{(i+۱)\binom{n}{i}}{۲\binom{n}{۲}}p^{i-۲}q^{n-i}\} \\ &\le ۲\tbinom{n}{۲}p^۲\{q^{n-۲} + \sum_{i=۳}^{n}\tbinom{n-۲}{i-۲}p^{i-۲}q^{n-i}\} \\ &= n(n-۱)p^۲ < (np)^۲. \end{aligned}$$

اگر p به‌اندازه کافی کوچک باشد، آن‌گاه این دست‌آورد یک پیشرفت قابل ملاحظه می‌باشد. این تخمین خطا را در بخش ۴.۴ به‌کار خواهیم برد.

۳.۴ کدگشایی با منطق اکثریت

در این بخش، به‌طور خلاصه طراحی یک روش کدگشایی را که در بسیاری از کدهای خطی به‌کار می‌رود، ترسیم خواهیم نمود. توسیع این بحث در فصل‌های بعد بیان خواهد شد. این روش ساده بوده و دارای این مزیت است که در برخی حالات، خطاهای بیشتری نسبت به آنچه که انتظار تصحیح آن می‌رود، تصحیح می‌گردد.

تعریف ۱.۳.۴. یک دستگاه معادلات بررسی‌توازن $< x, y^{(v)} > = ۰$، $(۱ \leq v \leq r)$، **متعامد نسبت به** مکان i (برای کد C؛ $y^{(v)} \in C^{\perp}$) نامیده می‌شود، اگر:

۱) $y_i^{(v)} = ۱$، $(۱ \leq v \leq r)$.

۲) اگر $j \neq i$، آن‌گاه برای حداکثر یک مقدار v داشته باشیم $y_j^{(v)} \neq ۰$.

حال فرض کنید x یک کلمه دریافتی باشد که شامل t خطاست و $t \leq \frac{۱}{۲}r$؛ بنابراین:

$$< x, y^{(v)} > \neq ۰ \text{ برای } \begin{cases} t \geq \text{ مقدار } v، & \text{اگر } x_i \text{ درست باشد.} \\ r-(t-۱) \leq \text{ مقدار } v، & \text{اگر } x_i \text{ نادرست باشد.} \end{cases}$$

چون $r-(t-۱) > t$، اکثریت مقادیر $< x, y^{(v)} >$، یعنی صفر، به‌ترتیب ناصفر، برای ما تعیین می‌کند که آیا x_i صحیح است یا ناصحیح. در حالت کد دوتایی، متعاقباً می‌توانیم این خطا را تصحیح کنیم. اگر ما چنین مجموعه‌های بررسی متعامدی را برای هر i داشته باشیم، آن‌گاه می‌توانیم مکان‌های متفاوت را یکی یکی تصحیح کنیم.

به‌عنوان مثال، دوگان کد همینگ [۷, ۴] را درنظر می‌گیریم (ارجاع به مثال ۳.۳.۳). معادلات بررسی‌توازن:

$$x_۱ + x_۲ + x_۳ = ۰,$$

$$x_۱ + x_۴ + x_۵ = ۰,$$

$$x_۱ + x_۶ + x_۷ = ۰,$$

نسبت به مکان ۱ متعامد هستند. اگر x شامل یک خطا باشد، آن‌گاه اگر $x_۱$ نادرست باشد این سه معادله به ترتیب دارای مقادیر ۱، ۱، ۱ و اگر $x_۱$ درست باشد دوتا ۰ و یکی ۱ خواهند بود. اگر دو تا از نتایج برابر با ۱ باشد، می‌بینیم که بیشتر از یک خطا ایجاد شده است (این کد تشخیص دهنده دو خطاست).

کد $[۶, ۳, ۳]$ با ماتریس مولد $G := (I \quad J - I)$ را درنظر بگیرید و دو سمبل را به‌صورت $a_۷ = a_۸ = a_۱$ الحاق نمایید. خواننده باید بررسی نماید که هنوز داریم $d = ۳$، اما ماتریس بررسی‌توازن جدید دارای چهار سطر است که نسبت به مکان ۱ متعامد می‌باشند. بنابراین، حتی اگر دو خطا رخ دهد، مکان ۱ پس از کدگشایی صحیح می‌باشد.

۳.۵ شمارنده‌های وزن

کمترین—فاصله یک کد خطی به ما می‌گوید که یک کلمه دریافتی می‌تواند شامل چه تعداد خطا باشد و هنوز به‌طور صحیح کدگشایی گردد. اغلب داشتن اطلاعات جزیی بیشتر درباره فاصله کد لازم به‌نظر می‌رسد. برای این هدف، ما مفهومی معروف به شمارنده وزنی[۷] کد را معرفی می‌کنیم.

تعریف ۱.۳.۵. فرض کنید C یک کد خطی با طول n باشد و A_i تعداد کدکلمات با وزن i؛ در این‌صورت:

$$A(z) := \sum_{i=۰}^{n} A_i z^i$$

شمارنده وزنی C نامیده می‌شود. دنباله $(A_i)_{i=۰}^{n}$ توزیع وزنی C نامیده می‌شود.

اگر C خطی باشد و $\mathbf{c} \in C$، آن‌گاه تعداد کدکلمات با فاصله i از $\mathbf{c}$ برابر با A_i می‌باشد. برای یک کد غیرخطی، این مطلب درحالت کلی درست نیست. کدی که دارای این خاصیت باشد (برای تمام کدکلمات و برای تمامی iها)، پایا فاصله[۸] نامیده می‌شود (تعریف ۲.۵.۳ را نیز ببینید).

به‌عنوان یک مثال شمارنده وزنی کد دوتایی همینگ با طول n را محاسبه می‌کنیم. $i - ۱$ ستون از ماتریس بررسی‌توازن این کد را درنظر بگیرید. سه احتمال وجود دارد:

۱) مجموع این ستون‌ها برابر صفر باشد.

۲) مجموع این ستون‌ها برابر با یکی از ستون‌های انتخاب شده باشد.

۳) مجموع این ستون‌ها برابر با یکی از ستون‌های باقی‌مانده باشد.

می‌توانیم $i - ۱$ ستون را به $\binom{n}{i-۱}$ طریق انتخاب کنیم. امکان (۱) $A_{i-۱}$ بار رخ می‌دهد، امکان (۲) $(n - (i - ۲))A_{i-۲}$ بار و امکان (۳) iA_i بار رخ می‌دهد؛ بنابراین:

$$iA_i = \binom{n}{i - ۱} - A_{i-۱} - (n - i + ۲)A_{i-۲},$$

---

[۷] weight enumerator

[۸] distance invariant

که اگر $i > n+1$، به‌طور بدیهی درست است. اگر ما دوطرف را در z^{i-1} ضرب کرده و روی i جمع ببندیم، آن‌گاه داریم:

$$A'(z) = (1+z)^n - A(z) - nzA(z) + z^2 A'(z).$$

چون $A(0) = 1$، این معادله دیفرانسیل دارای جواب یکتای:

$$A(z) = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{(n-1)/2}(1-z)^{(n+1)/2}. \qquad (2)$$

می‌باشد. یکی از نتایج بسیار اساسی در نظریه کدگذاری که توسط مک‌ویلیامز[9] (۱۹۶۳) ارائه شده است، قضیه‌ای است که رابطه بین شمارنده وزنی یک کد و دوگان آن‌را بیان می‌کند.

قضیه ۲.۳.۵. فرض کنید C یک کد $[n,k]$ روی $\mathbb{F}_q$ با شمارنده وزنی $A(z)$ باشد و $B(z)$ شمارنده وزنی $C^\perp$ باشد؛ در این‌صورت:

$$B(z) = q^{-k}(1+(q-1)z)^n A(\frac{1-z}{1+(q-1)z}).$$

اثبات. فرض کنید χ سرشت نابدیهی $(\mathbb{F}_q, +)$ باشد. به‌طور معمول فرض کنید $\mathcal{R} = \mathbb{F}_q^n$. تعریف می‌کنیم:

$$g(\mathbf{u}) := \sum_{\mathbf{v}\in\mathcal{R}} \chi(<\mathbf{u},\mathbf{v}>) z^{w(\mathbf{v})}.$$

در این‌صورت داریم:

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) = \sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in\mathcal{R}} \chi(<\mathbf{u},\mathbf{v}>) z^{w(\mathbf{v})} = \sum_{\mathbf{v}\in C} z^{w(\mathbf{v})} \sum_{\mathbf{u}\in\mathcal{R}} \chi(<\mathbf{u},\mathbf{v}>).$$

دراینجا، اگر $\mathbf{v}\in C^\perp$ مجموع داخلی برابر با $|c|$ است. اگر $\mathbf{v}\notin C^\perp$ آنگاه در مجموع داخلی $<\mathbf{u},\mathbf{v}>$ هر مقدار در $\mathbb{F}_q$ را به تعداد دفعات یکسانی می‌گیرد؛ یعنی مجموع داخلی برابر با ۰ است؛ بنابراین:

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) = |c| \cdot B(z). \qquad (3)$$

[9] F.J.MacWilliams

این تابع وزن را به $\mathbb{F}_q$، با قرار دادن $w(\mathbf{v}) = ۰$ اگر $v = ۰$ و $w(\mathbf{v}) = ۱$ در غیر این‌صورت، گسترش دهید؛ در این‌صورت، با نوشتن $\mathbf{u} = (u_۱, u_۲, \cdots, u_n)$ و $\mathbf{v} = (v_۱, v_۲, \cdots, v_n)$، از تعریف $g(\mathbf{u})$ داریم:

$$\begin{aligned} g(u) &= \sum_{(v_۱, v_۲, \cdots, v_n) \in \mathcal{R}} z^{w(v_۱)+\cdots+w(v_n)} \chi(u_۱ v_۱ + \cdots + u_n v_n) \\ &= \sum_{(v_۱, v_۲, \cdots, v_n) \in \mathcal{R}} z^{w(v_۱)} \chi(u_۱ v_۱) z^{w(v_۲)} \chi(u_۲ v_۲) \cdots z^{w(v_n)} \chi(u_n v_n) \\ &= \prod_{i=۱}^{n} \sum_{v \in \mathbb{F}_q} z^{w(v)} \chi(u_i v) \end{aligned}$$

در عبارت آخر، اگر $u_i = ۰$، آن‌گاه مجموع داخلی برابر با $۱ + (q-۱)z$ است و اگر $u_i \notin ۰$، آنگاه این مجموع برابر با:

$$۱ + z \sum_{\alpha \in \mathbb{F}_q \setminus \{۰\}} \chi(\alpha) = ۱ - z,$$

است؛ بنابراین:

$$g(u) = (۱ - z)^{w(u)} (۱ + (q-۱)z)^{n - w(u)}. \qquad (۴)$$

حال چون $|c| = q^k$ اثبات قضیه با جانشینی رابطه ۴ در ۳ کامل می‌شود. □

برای یک تعمیم کلی به بخش ۷.۲ ارجاع می‌دهیم.

برخی اوقات، شمارنده وزنی کد C در فرم همگن به‌صورت زیرداده می‌شود:

$$Ham_C(x, y) := \sum_{\mathbf{c} \in C} x^{n - w(\mathbf{c})} y^{w(\mathbf{c})}.$$

با این نمادگذاری، رابطه مک‌ویلیامز برای یک دوتایی C و دوگان آن $C^\perp$ به‌صورت زیر بیان می‌شود:

$$Ham_{C^\perp}(x, y) = \frac{۱}{|c|} Ham_C(x + y, x - y).$$

این رابطه مستقیماً از قضیه ۲.۳.۵ نتیجه می‌شود.

۳.۶ متریک لی

در بسیاری از موضوعات مخابرات که در عمل به‌کار رفته، می‌توان حروف را به‌عنوان مجموعه‌ای از نقاطی که به‌طورمنظم بر روی یک دایره واقع شده‌اند، مدل نمود. به‌عنوان مثال، الفبایی از این نوع شامل هفت سمبل را درنظر بگیرید. ما این سمبل‌ها را (که هنوز بر دایره واقع هستند) با عناصر $\mathbb{Z}_۷$ نشان می‌دهیم. در

این کانال، تاثیر نویز گوسی سفید باعث نمی‌گردد تا تمامی خطاها دارای احتمال یکسان گردند. احتمال آن‌که سمبل انتقال یافته به‌صورت سمبلی که به آن نزدیک است، دریافت گردد بسیار زیاد است. در اصطلاحات علمی این بدان معناست که اگر یک ۴ فرستاده شود و یک خطا رخ دهد، احتمال دریافت ۳ یا ۵ نسبت به ۲ یا ۶ بیشتر است و به همین منوال.

بنابراین، برای این کانال‌ها فاصله همینگ یک متریک طبیعی برای اندازه‌گیری خطاها نیست. درواقع، می‌توان از وزن و فاصله معروف به لی استفاده نمود.

تعریف ۱.۳.۶. $\mathbb{Z}_m$ را به‌عنوان الفبا درنظر بگیرید. وزن لی عدد صحیح i $(0 \leq i < m)$ به‌صورت زیر تعریف شده است:

$$w_L(i) := \min\{i, m-i\}.$$

متریک لی روی $\mathbb{Z}_m^n$ به‌صورت:

$$w_L(\mathbf{a}) := \sum_{i=1}^{n} w_L(a_i),$$

تعریف می‌شود، که در آن این مجموع در $\mathbb{N}_0$ محاسبه شده است. فاصله لی را توسط رابطه:

$$d_L(x,y) := w_L(x-y),$$

تعریف می‌کنیم. دیدن این‌که فاصله لی در واقع یک تابع فاصله است مشکل نیست.

در فصل بعد، به‌طور خاص علاقه‌مند به الفبای $\mathbb{Z}_4$ خواهیم بود. حال این مطلب را با جزییات بیشتر می‌آوریم. در $\mathbb{Z}_4$، وزن‌های لی ۰، ۱ و ۲ به‌ترتیب برابر با ۰، ۱ و ۲ است، اما وزن لی ۳ برابر با ۱ می‌باشد.

برای یک کد $C \subset \mathbb{Z}_4^n$ (۱.۸.۱ را ببینید)، دو شمارنده وزنی تعریف می‌کنیم، شمارنده وزنی متقارن شده[۱۰] و شمارنده وزن لی[۱۱] .

تعریف ۲.۳.۶. شمارنده وزنی متقارن شده کد $C \subset \mathbb{Z}_4^n$ به‌صورت:

$$\mathrm{swe}_C(w,x,y) := \sum_{\mathbf{c}\in C} w^{n_0(\mathbf{c})} x^{n_1(\mathbf{c})+n_3(\mathbf{c})} y^{n_2(\mathbf{c})},$$

داده شده است که در آن $n_i(\mathbf{c})$ نمایش‌دهنده تعداد مولفه‌هایی از $\mathbf{c}$ است که برابر با i هستند.

[۱۰] symmetrized weight enumerator

[۱۱] Lee weight enumerator

تعریف ۳.۳.٦. شمارنده وزن لی یک کد $C \subseteq \mathbb{Z}_4^n$ توسط رابطه:

$$\mathrm{Lee}_C(x,y) := \sum_{\mathbf{c}\in C} x^{2n-w_L(\mathbf{c})} y^{w_L(\mathbf{c})},$$

داده می‌شود.

دقت کنید که:

$$Lee_C(x,y) = swe_C(x^2, xy, y^2). \qquad (۵)$$

بیایید ببینیم که آیا یک تغییر کوچک بر روی اثبات قضیه ۲.۳.۵ می‌تواند باعث یک تعمیم از رابطه مک‌ویلیامز به کدهای روی $\mathbb{Z}_4$ گردد؟ تابع χ را به‌صورت سرشتی روی $(\mathbb{Z}_4, +)$ درنظر می‌گیریم؛ حال تعریف می‌کنیم $\chi(a) := i^a$ که $i^2 = -1$ در $\mathbb{C}$.

تابع f تعریف شده روی $\mathcal{R} := \mathbb{Z}_4^n$ را درنظر گرفته و تعریف می‌کنیم:

$$g(\mathbf{u}) := \sum_{\mathbf{v}\in\mathcal{R}} \chi(<\mathbf{u},\mathbf{v}>) f(\mathbf{v}).$$

با روش مشابهی همانند ۳ داریم:

$$\sum_{\mathbf{u}\in C} g(\mathbf{u}) = |c| \sum_{\mathbf{v}\in C^\perp} f(\mathbf{v}). \qquad (٦)$$

در قسمت بعدی اثبات، فرض می‌کنیم:

$$f(v) := w^{n_0(v)} x^{n_1(v)+n_3(v)} y^{n_2(v)}.$$

در ادامه، با اثباتی دقیقاً مشابه با اثبات ۲.۳.۵، داریم:

$$g(\mathbf{u}) = \prod_{i=1}^{n} \sum_{v\in\mathbb{Z}_4} \chi(u_i v) w^{n_0(v)} x^{n_1(v)+n_3(v)} y^{n_2(v)}.$$

برای محاسبه مجموع داخلی، باید بین $u_i = 0$،۳ یا $u_i = 1$ و $u_i = 2$ تمایز قائل شویم. در این سه حالت، به ترتیب مقادیر $(w+2x+y)$، $(w-y)$ و $(w-2x+y)$ را داریم؛ بنابراین:

$$g(u) = (w+2x+y)^{n_0(u)} (w-y)^{n_1(u)+n_3(u)} (w-2x+y)^{n_2(u)}. \qquad (۷)$$

با جانشینی ۷ در ٦ داریم:

$$swe_{c^\perp}(w,x,y) = \frac{1}{|c|} swe_C(w+2x+y, w-y, w-2x+y). \qquad (۸)$$

تعمیم قضیه ۲.۳.۵ را به‌صورت زیر داریم:

قضیه ۴.۳.٦. اگر C یک کد چهارتایی با دوگان $C^{\perp}$ باشد، آن‌گاه:

$$\mathrm{Lee}_{C^{\perp}}(x,y) = \frac{1}{|C|}\mathrm{Lee}_{C}(x+y, x-y).$$

اثبات. روابط ۵ تا ۸ را به‌کار بگیرید.

۳.۷ پیشنهادها

موضوع کدهای خطی به‌طور زیاد توسط مقالاتی از اسلپیان[۱۲] و همینگ[۱۳] در سال ۱۹۵۰ تحت تاثیر قرار گرفت. خواننده علاقه‌مند به کدگشایی با منطق اکثریت، می‌تواند به کتاب مَسِی[۱۴] [۴۷] مراجعه نماید. چندین توسیع از قضیه مک‌ویلیامز، حتی برای کدهای غیرخطی، وجود دارد. یک بحث فراگیر در این‌باره را می‌توان در فصل ۵ مرجع [۴٦] یافت. به‌عنوان کاربردی از رابطه ۲ می‌توان به فصل ۲ از مرجع [۴۲] رجوع نمود.

۳.۸ مسائل

۱.۳.۸. فرض کنید C یک کد دوتایی کامل با طول n و کمترین —فاصله ۷ باشد. نشان دهید $n = ۷$ یا $n = ۲۳$.

۲.۳.۸. فرض کنید C یک کد $[n,k]$ روی $\mathbb{F}_q$ باشد که روی هر مجموعه از k مکان متقارن است. نشان دهید C دارای کمترین —فاصله $d = n-k+۱$ است.

۳.۳.۸. فرض کنید C یک کد $[۲k+۱,k]$ دوتایی است به‌طوری که $C \subset C^{\perp}$. $C^{\perp}\backslash C$ را توصیف کنید.

---

[۱۲] D. E. Slepian
[۱۳] R. W. Hamming
[۱۴] J. L. Massey

۴.۳.۸. فرض کنید $\mathcal{R} = \mathbb{F}_۲^۶$ و $x \in \mathcal{R}$. $|B_۱(x)|$ را تعیین کنید. آیا ممکن است مجموعه $C \subset \mathcal{R}$ با $|c| = ۹$ یافت نمود به‌طوری که برای تمامی $x \in C$ و $y \in C$، $x \neq y$، فاصله $d(x,y)$ حداقل برابر با ۳ باشد؟

۵.۳.۸. فرض کنید C یک کد $[n,k]$ روی $\mathbb{F}_q$ با ماتریس مولد G باشد. اگر G شامل ستون ۰ نباشد، آن‌گاه مجموع وزن کدکلمات C برابر با $n(q-۱)q^{k-۱}$ است. این مطلب را اثبات نمایید.

۶.۳.۸. فرض کنید C یک کد $[n,k]$ دوتایی باشد. اگر C شامل کلمه به طول فرد باشد، آن‌گاه کلمات به طول زوج در C تشکیل یک کد $[n,k-۱]$ می‌دهند. این مطلب را اثبات نمایید.

۷.۳.۸. فرض کنید C یک کد دوتایی با ماتریس مولد زیر باشد:

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

کلمات دریافتی زیر را کدگشایی نمایید:

الف . (۱ ۱ ۰ ۱ ۰ ۱ ۱)

ب. (۱ ۱ ۰ ۱ ۱ ۰ ۰)

ج. (۰ ۰ ۰ ۱ ۰ ۰ ۰)

۸.۳.۸. فرض کنید p یک عدد اول باشد. آیا کد $[۸,۴]$ خوددوگان روی $\mathbb{F}_p$ وجود دارد؟

۹.۳.۸. برای $q = ۲$ فرض کنید R_k نرخ کد همینگ تعریف شده توسط ۱.۳.۳ باشد. $\lim_{k\to\infty} R_k$ را بیابید.

۱۰.۳.۸. فرض کنید C یک کد دوتایی با شمارنده وزن $A(z)$ باشد. شمارنده وزنی $\overline{C}$ چیست؟ شمارنده وزنی دوگان کد همینگ دوتایی گسترش‌یافته با طول ۲^k چیست؟

۱۱.۳.۸. فرض کنید C یک کد دوتایی $[n,k]$ با شمارنده وزن $A(z)$ باشد. ما C را روی کانال دوتایی متقارن با احتمال خطای p به‌کار می‌بریم. هدف ما تنها تشخیص خطاست. احتمال این‌که یک کلمه نادرست دریافت شود و خطا تشخیص داده نشود چه میزان است؟

۱۲.۳.۸. ماتریس‌های n_2 در n_1 روی $\mathbb{F}_2$ به‌وضوح تشکیل یک فضای برداری روی $\mathcal{R}$ با بعد n_1n_2 می‌دهند. فرض کنید C_i یک کد دوتایی $[n_i, k_i]$ با کمترین —فاصله d_i $(i = 1, 2)$ باشد. فرض کنید C زیرمجموعه‌ای از $\mathcal{R}$ شامل آن ماتریس‌ها باشد به‌طوری که هر ستون، به‌ترتیب هر سطر، یک کدکلمه در C_1، به‌ترتیب در C_2، است. نشان دهید C یک $[n_1n_2, k_1k_2]$ کد با کمترین —فاصله d_1d_2 است. این کد حاصل‌ضرب مستقیم C_1 و C_2 نامیده می‌شود.

۱۳.۳.۸. فرض کنید C یک کد دوتایی $[10, 5]$ با ماتریس مولد به‌صورت زیر باشد:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

نشان دهید C به‌طور یکتا کدگشاپذیر به معنای زیر است: برای هر کلمه دریافتی x یک کدکلمه یکتای $\mathbf{c}$ وجود دارد به‌طوری که $d(x, c)$ کمترین است.

۱۴.۳.۸. کوچک‌ترین کدهای دوتایی با ترتیب قاموسی با فاصله d را به‌صورت زیر تعریف کنید. طول کلمه در ابتدا مشخص نیست. با کدکلمات $\mathbf{c}_0 = 0$ و $\mathbf{c}_1 = (1, \cdots, 1, 0, \cdots, 0)$ با وزن d، شروع نمایید. اگر $\mathbf{c}_0$، $\mathbf{c}_1$، $\cdots$، $\mathbf{c}_{l-1}$ انتخاب شده باشند، آن‌گاه $\mathbf{c}_l$ را طوری انتخاب کنید که در ترتیب قاموسی در ابتدا آید و (با ۱ها در سمت چپ تاآنجا که ممکن است) $d(\mathbf{c}_i, \mathbf{c}_l) \geq d$، $(0 \leq i \leq l-1)$. پس از l مرتبه، طول کد به‌صورت طول قسمتی که مختص‌های ۱ رخ داده است، تعریف می‌شود.

الف. نشان دهید پس از آن‌که 2^k بردار انتخاب شدند، کوچک‌ترین کد با ترتیب قاموسی، خطی است!

ب. برای $d = 3$، کدهای همینگ درمیان کوچک‌ترین کدهای با ترتیب قاموسی، رخ می‌دهند. این مطلب را اثبات نمایید.

۱۵.۳.۸. نشان دهید که هیچ $[15, 8, 5]$ کدی وجود ندارد.

راهنمایی: نشان دهید که چنین کدی دارای یک ماتریس مولد با یک سطر با وزن ۵ است و زیرکد تولید شده توسط سایر سطرها را درنظر بگیرید.

فصل ۴

برخی کدهای خوب

۴.۱ کدهای هادامارد و تعمیم‌ها

فرض کنید H_n یک ماتریس هادامارد مرتبه n (تعریف ۵.۱.۳ را ببینید) باشد. در H_n و $-H_n$، ۱ − را با ۰ جای‌گزین می‌کنیم. در این روش، $2n$ سطر داریم که کلماتی در $\mathbb{F}_2^n$ هستند. از آنجا که هر دو سطر در ماتریس هادامارد در نیمی از مکان‌ها متفاوت هستند، یک کد $(n, 2n, \frac{1}{2}n)$ ساخته‌ایم. برای $n = 8$، این کد یک کد همینگ گسترش‌یافته است. برای $n = 32$ این کد همان است که در مارینر ۱۹۶۹ که در بخش ۲.۱ بیان شد، به‌کار رفت. به‌طور کلی، این کدها، کدهای هادامارد نامیده می‌شوند.

یک روش ساختاری مشابه، با ماتریس پالی S از مرتبه n (قضیه ۸.۱.۳ را ببینید) شروع می‌کند. کد C با کدکلمات **0**، **1**، سطرهای $\frac{1}{2}(S + I + J)$ و $\frac{1}{2}(-S + I + J)$ را می‌سازیم. از قضیه ۸.۱.۳ نتیجه می‌شود که C یک کد $(n, 2(n+1), d)$ کد است که در آن $d = \frac{1}{2}(n-1)$ اگر $n \equiv 1 \bmod 4$ و

$d = \frac{1}{4}(n-3)$ اگر $n \equiv 3 \bmod 4$. در حالت $n = 9$، این کد شامل سطرهای ماتریس زیر است:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ J & & & P^2 & & & P & & \\ P & & & J & & & P^2 & & \\ P^2 & & & P & & & J & & \\ I & & & J-P^2 & & & J-P & & \\ J-P & & & I & & & J-P^2 & & \\ J-P^2 & & & J-P & & & I & & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad (1)$$

که در آن I و J، ۳ در ۳ هستند و

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

۴.۲ کد دوتایی گُلِی

مشهورترین کد در میان تمامی کدهای (دوتایی)، کد دوتایی معروف به کد گلی[1] $\mathcal{G}_{23}$ می‌باشد. ساختارهای بسیار زیادی از این کد وجود دارد که برخی از آنها کاملاً زیبا و با اثبات‌های کوتاه از خواص این کد می‌باشد. اثبات خواهیم نمود که $\mathcal{G}_{24}$، کد گلی دوتایی گسترش‌یافته، یکتاست و تعداد کمی از این ساختارها را مرور می‌کنیم. از آنچه اثبات می‌شود نتیجه می‌گیریم که گروه خودریختی کد گسترش‌یافته، متعدی می‌باشد؛ بنابراین، کد $\mathcal{G}_{23}$ نیز یکتاست.

ماتریس وقوع N از یک طرح $2-(11, 6, 3)$ را درنظر می‌گیریم. به‌آسانی می‌توان نشان داد (دستی) که این طرح یکتاست. داریم $NN^T = 3I + 3J$. N را به عنوان ماتریسی با درایه‌هایی در $\mathbb{F}_2$ درنظر بگیرید؛ در این‌صورت $NN^T = I + J$؛ بنابراین، N دارای رتبه ۱۰ می‌باشد و تنها بردار ناصفر x با $xN = 0$ برابر با $\mathbf{1}$ می‌باشد. خواص این طرح به‌وضوح باعث می‌گردد تا تمامی سطرهای N دارای وزن ۶ باشند و این‌که مجموع هر دو سطر متمایز N نیز دارای وزن ۶ باشد. علاوه‌برآن، می‌دانیم که مجموع سه یا چهار سطر N برابر با $\mathbf{0}$ نیست.

در ادامه، فرض کنید G ماتریس ۱۲ در ۲۴ (روی $\mathbb{F}_2$) داده شده توسط $G := (I_{12} P)$ باشد که در

[1] Golay code

آن:

$$P := \begin{pmatrix} ۰ & ۱ & \cdots & ۱ \\ ۱ & & & \\ \vdots & & N & \\ ۱ & & & \end{pmatrix}. \qquad (۲)$$

هر سطر G در پیمانه ۴، وزنی برابر با ۰ دارد. هر دو سطر G دارای ضرب داخلی صفر است. این مطلب باعث می‌گردد تا وزن هر ترکیب خطی از سطرهای G در پیمانه ۴، برابر با صفر گردد (اثبات با استقرا). مشاهدات انجام شده درباره N نشان می‌دهد که یک ترکیب خطی از هر تعداد از سطرهای G حداقل برابر با ۸ می‌باشد. کد دوتایی تولید شده توسط G را درنظر بگیرید و آن را $\mathcal{G}_{۲۴}$ بنامید. با حذف هر مولفه از آن می‌توان یک کد دوتایی $[۲۳, ۱۲]$ با کمترین—فاصله حداقل ۷ را یافت. این فاصله نمی‌تواند بیشتر باشد، چرا که شرط ۶.۳.۱ با $e = ۳$ برقرار است که در واقع نشان می‌دهد کد $[۲۳, ۱۲, ۷]$ یک کد کامل است! این کد را با $\mathcal{G}_{۲۳}$ نشان می‌دهیم؛ (همان‌طور که در بالا بیان شد، یکتایی آن را با پذیرش این نمادگذاری اثبات خواهیم نمود).

قضیه ۱.۴.۲. کدکلمات به وزن ۸ در $\mathcal{G}_{۲۴}$ تشکیل یک $(۲۴, ۸, ۱) - ۵$ طرح می‌دهند.

اثبات. با استفاده از یک بحث آسان مبتنی بر شمارش، می‌توان نشان داد که شمارنده وزنی یک کد کامل شامل **0** به‌طور یکتا تعیین می‌شود. درواقع، داریم $A_۰ = A_{۲۳} = ۱$، $A_۷ = A_{۱۶} = ۲۵۳$، $A_۸ = A_{۱۵} = ۵۰۶$، $A_{۱۱} = A_{۱۲} = ۱۲۸۸$؛ بنابراین، $\mathcal{G}_{۲۴}$ دارای ۷۵۹ کلمه با وزن ۸ است که هیچ دو تایی از آنها در بیشتر از چهار مکان، هم‌پوشانی[۲] ندارند؛ بنابراین، این کلمات با یک‌دیگر $\binom{۲۴}{۵} = \binom{۸}{۵} \cdot ۷۵۹$ پنج‌تایی را می‌پوشانند. □

قضیه ۲.۴.۲. اگر C یک کد دوتایی به طول ۲۴، با $|c| = ۲^{۱۲}$ و کمترین—فاصله ۸ باشد و $\mathbf{0} \in C$، آن‌گاه C با $\mathcal{G}_{۲۴}$ هم‌ارز می‌باشد.

اثبات.

۱) قسمت مشکل اثبات این است که باید نشان داد C یک کد خطی است. برای اثبات این مطلب، مشاهده می‌کنید که حذف هر یک از مختص‌های کد C، کد C' با طول ۲۳ و کمترین—فاصله ۷ با $|c'| = ۲^{۱۲}$ را تولید می‌نماید؛ بنابراین، این کد کامل است و شمارنده وزنی آن همانند اثبات قضیه

[۲] overlapping

قبل است. از این واقعیت که در این حالت اهمیتی ندارد که کدام یک از ۲۴ موقعیت حذف گردند، نتیجه می‌گردد که تمامی کدکلمات در کد C دارای وزن ۰، ۸، ۱۲، ۱۶ یا ۲۴ هستند. علاوه‌براین، یک تغییر در اصل کد، حاصل از اضافه نمودن یک کدکلمه ثابت از C به تمامی کلمات C، نشان می‌دهد که می‌توانیم نتیجه بگیریم که فاصله بین هر دو کلمه از C نیز برابر با ۰، ۸، ۱۲، ۱۶ یا ۲۴ می‌باشد. از آنجا که تمامی وزن‌ها و تمامی فاصله‌ها در پیمانه ۴، برابر با صفر است، هر دو کدکلمه‌ای دارای ضرب داخلی صفر می‌باشند؛ بنابراین، کدکلمات C تشکیل یک کد خطی می‌دهند که خودمتعامد می‌باشد. این مطلب نتیجه می‌دهد که این کد خطی باید همان C باشد. به‌عبارت دیگر، C یک کد خطی خوددوگان است!

۲) با درنظر گرفتن یک کلمه با وزن ۱۲ به عنوان سطر اول، ماتریس مولد G از کد C را تشکیل می‌دهیم. تحت جای‌گشت مکان‌ها داریم:

$$G = \begin{pmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ & A & & & B & \end{pmatrix}.$$

می‌دانیم که هر ترکیب خطی از سطرهای B باید دارای وزن زوج مخالف صفر باشد؛ بنابراین، B دارای رتبه ۱۱ است. در نتیجه کد تولید شده توسط B یک کد $[12, 11, 2]$ وزن زوج است؛ بنابراین، ممکن است فرض کنیم که B ماتریس I_{11} است که یک ستون با عناصر ۱ در کنار آن آمده است. جای‌گشت دومی از ستون‌های G، ماتریس مولد G' به شکل $(I_{12} \quad P)$ را نتیجه می‌دهد که در آن P شکل یکسانی همانند ۲ دارد. در این حالت ما از ماتریس N چه می‌دانیم؟ به وضوح، هر سطر N باید دارای وزن ۶ باشد (به اولین سطر G' نگاه کنید). به طریق مشابه، می‌بینیم که مجموع هر دو سطر N دارای وزن ۶ است. این باعث می‌شود تا N ماتریس وقوع یک طرح (یکتای!) $(11, 6, 3) - 2$ باشد؛ بنابراین، C هم‌ارز $\mathcal{G}_{24}$ است.

□

ساختار زیر از $\mathcal{G}_{24}$ توسط تورین[۳] داده شده است. H کد همینگ $[7, 4]$ با نمایش زیر را درنظر می‌گیریم. بردار $\mathbf{0}$ و هفت شیفت دوری بردار $(0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1)$ را درنظر بگیرید (دقت کنید که این هفت بردار، ماتریس وقوع $PG(2, 2)$ را تشکیل می‌دهند). سپس هشت مکمل از این کلمات را درنظر بگیرید. اینها با یکدیگر تشکیل H را می‌دهند. فرض کنید H^* با معکوس نمودن ترتیب سمبل‌ها در کلمات H به‌دست آمده باشد. با یک بررسی، می‌بینیم که $\overline{H}$ و $\overline{H^*}$ کدهای $[8, 4]$ با خاصیت $\overline{H} \cap \overline{H^*} = \{\mathbf{0}, \mathbf{1}\}$ هستند. می‌دانیم که کدهای $\overline{H}$ و $\overline{H^*}$ کدهای خوددوگان با کمترین—فاصله ۴ هستند.

[۳] R. J. Turyn

حال کد C با طول کلمه ۲۴ را با استفاده از چسباندن کدها به‌صورت زیر، تشکیل می‌دهیم:

$$C := \{(\mathbf{a}+\mathbf{x}, \mathbf{b}+\mathbf{x}, \mathbf{a}+\mathbf{b}+\mathbf{x}) \,|\, \mathbf{a} \in \overline{H}, \mathbf{b} \in \overline{H}, x \in \overline{H^*}\}.$$

اجازه می‌دهیم $\mathbf{a}$ و $\mathbf{b}$ در میان عناصر یک پایه $\overline{H}$ و x در میان عناصر یک پایه $\overline{H^*}$ تغییر کنند. می‌بینیم که کلمات $(\mathbf{a}, \mathbf{0}, \mathbf{a})$، $(\mathbf{0}, \mathbf{b}, \mathbf{b})$، $(\mathbf{x}, \mathbf{x}, \mathbf{x})$ تشکیل یک پایه برای کد C می‌دهند؛ بنابراین، C یک کد $[۲۴, ۱۲]$ می‌باشد. هر دو (نه لزوماً مجزا) بردار از عناصر پایه C متعامد هستند و این؛ یعنی C خوددوگان است. چون تمامی بردارهای پایه دارای وزنی بخش‌پذیر بر ۴ می‌باشند، این رابطه برای هر کلمه در C برقرار می‌باشد. آیا یک کلمه $\mathbf{c} \in C$ می‌تواند دارای وزن کمتر از ۸ باشد؟ چون هر سه مولفه $\mathbf{a}+\mathbf{x}$، $\mathbf{b}+\mathbf{x}$، $\mathbf{a}+\mathbf{b}+\mathbf{x}$ آشکارا دارای وزن زوج می‌باشند، یکی از آنها باید برابر با $\mathbf{0}$ باشد. مشاهده ما بر روی اشتراک $\overline{H}$ و $\overline{H^*}$ منجر به این نتیجه می‌گردد که $x = ۰$ یا $x = ۱$. بدون کاستن از کلیت فرض کنییم $x = ۰$. چون کلمات H دارای وزن ۰، ۴ یا ۸ می‌باشند، نتیجه می‌شود که $\mathbf{c} = \mathbf{0}$.

ما نشان داده‌ایم که C یک کد $[۲۴, ۱۲, ۸]$ است؛ بنابراین، $C = \mathcal{G}_{۲۴}$.

ساختار بعدی توسط کانوی[۴] داده شده است. فرض کنید $\mathbb{F}_۴ = \{۰, ۱, \omega, \overline{\omega}\}$. هم‌چنین فرض کنید C، کد $[۶, ۳]$ بر روی $\mathbb{F}_۴$ با کدکلمات $(a, b, c, f(۱), f(\omega), f(\overline{\omega}))$ باشد که در آن $f(x) := ax^۲ + bx + c$. نشان دادن این‌که C دارای کمترین—فاصله ۴ است و شامل هیچ کلمه با وزن ۵ نمی‌باشد، کار آسانی است. کد C به نام کد شش‌تایی[۵] معروف است.

حال فرض کنید G یک کد دوتایی به طول ۲۴ باشد به‌طوری که کلمات آن با ماتریس‌های ۴ در ۶ دوتایی A نمایش داده شوند. چهار سطر چنین ماتریس Aی را با $\mathbf{a}_۰$، $\mathbf{a}_۱$، a_ω و $a_{\overline{\omega}}$ نمایش می‌دهیم. یک ماتریس A متعلق به G است اگر و تنها اگر دو شرط زیر برقرار باشند:

۱) هر ستون A دارای توازنی همانند سطر اول $\mathbf{a}_۰$ باشد.

۲) $\mathbf{a}_۱ + \omega\mathbf{a}_\omega + \overline{\omega}\mathbf{a}_{\overline{\omega}} \in C$.

این شرایط به‌وضوح یک کد خطی تعریف می‌کنند.

اگر سطر اول A دارای توازن زوج باشد و کدکلمه موجود در رابطه (۲) برابر با صفر نباشد، آن‌گاه A داری حداقل ۴ ستون با وزن بیشتر یا مساوی ۲ می‌باشد؛ یعنی وزن کد بزرگ‌تر یا مساوی ۸ است. از طرف دیگر، اگر کدکلمه موجود در (۲) برابر با صفر باشد، آن‌گاه یا A برابر با کلمه صفر است یا A دارای حداقل دو ستون با وزن ۴ است که مجدداً وزن کلی، حداقل ۸ است. اگر سطر اول A دارای توازن فرد باشد، آن‌گاه تمامی ستون‌های A دارای وزن فرد می‌باشند. این وزن‌ها نمی‌توانند همگی ۱ باشند، زیرا

[۴] J. H. Conway

[۵] hexacode

این باعث می‌گردد که کدکلمه C موجود در شرط (۲) دارای وزن فرد باشد. نشان داده‌ایم که G دارای کمترین—فاصله ۸ است. نشان دادن این مطلب که اگر شرایط (۱) و (۲) برقرار باشند و کد C دارای بعد ۳ باشد، آنگاه G دارای بعد ۱۲ است، به‌صورت تمرین به خواننده واگذار می‌گردد؛ بنابراین، ماتریس‌های A، کد $\mathcal{G}_{۲۴}$ را تشکیل می‌دهند.

در بخش ۶.۹، ساختار دیگری از $\mathcal{G}_{۲۳}$ را به‌عنوان یک کد دوری خواهیم داشت؛ یعنی کدی با یک همریختی از مرتبه ۲۳. تمامی این ساختارها با یکدیگر نشان می‌دهند که گروه خودریختی $\mathcal{G}_{۲۴}$ متعدی است (درواقع ۵—متعدی؛ آن گروه متیو[۶] $M_{۲۴}$ است)؛ بنابراین، $\mathcal{G}_{۲۳}$ نیز یکتاست.

یادآوری می‌کنیم که ساختار تمرین ۱۴.۳.۸ با $d = ۸$ و $k = ۱۲$ نیز، کد گلی دوتایی گسترش‌یافته $\mathcal{G}_{۲۴}$ را تولید می‌کند.

الگوریتم کدگشایی زیر برای $\mathcal{G}_{۲۴}$ یک توسیع از بخش ۳.۴ مبتنی بر قضیه ۱.۴.۲ است. فرض کنید y_i، $۱ \le i \le ۲۵۳$، ۲۵۳ کدکلمه با وزن ۸ از $\mathcal{G}_{۲۴}$ باشند با یک ۱ در یک مکان مفروض، گیریم مکان ۱. بررسی‌توازن‌های $< x, y_i >$، $۱ \le i \le ۲۵۳$، را درنظر بگیرید؛ در اینجا ما این واقعیت را که $\mathcal{G}_{۲۴}$ خوددوگان است به‌کار می‌بریم. فرض کنید x دریافت شده و شامل حداکثر ۴ خطاست. از قضیه ۲ نتیجه می‌شود که تعداد بررسی‌توازن‌هایی که رد می‌شوند، به صورت جدول زیر است:

	$x_۱$ درست	$x_۱$ نادرست
$t = ۱$	۷۷	۲۵۳
۲	۱۱۲	۱۷۶
۳	۱۲۵	۱۴۱
۴	۱۲۸	۱۲۸

بنابراین، در حالت $t \le ۳$ می‌توانیم سمبل $x_۱$ را تصحیح کنیم. خط متناظر با $t = ۴$ نشان می‌دهد که $\mathcal{G}_{۲۴}$ تشخیص‌دهنده ۴ خطا است، اما تصحیح‌کننده ۴ خطا نیست.

دقت می‌کنیم که این روش برای کدهای خوددوگانی که ما در بخش ۳.۲ توصیف کردیم، هنگامی که بر کد گلی دوتایی گسترش‌یافته اعمال می‌گردد، شامل محاسبه حداکثر $۲۶ \times ۱۲ = ۳۱۲$ بررسی‌توازن است و تمامی مختص‌های بردار خطا را تولید می‌کند (اگر $t \le ۳$).

[۶] Mathieu

۴.۳ کد گلی سه‌تایی

فرض کنید S_5 ماتریس پالی مرتبه ۵ تعریف شده در ۵.۱.۳ باشد؛ یعنی:

$$S_5 = \begin{pmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{pmatrix}.$$

کد $[11,6]$ سه‌تایی C تعریف شده توسط ماتریس مولد زیر را درنظر بگیرید:

$$G = \begin{pmatrix} & & 1 & 1 & 1 & 1 & 1 \\ & I_6 & \multicolumn{5}{|c|}{\multirow{5}{*}{S_5}} \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{pmatrix}$$

کد C یک کد $[11,6]$ است. از ۸.۱.۳ نتیجه می‌شود که $\overline{C}$ خوددوگان است؛ بنابراین، تمامی کلمات $\overline{C}$ دارای وزن بخش‌پذیر بر ۳ هستند. ماتریس مولد $\overline{G}$ برای $\overline{C}$ با اضافه نمودن ستون $(0,-1,-1,-1,-1,-1)^T$ به G به‌دست می‌آید. هر سطر $\overline{G}$ دارای وزن ۶ است. یک ترکیب خطی از دو سطر $\overline{G}$ دارای وزن حداقل $2+2$ است، بنابراین، یک ترکیب خطی از دو سطر $\overline{G}$ دارای دقیقاً دو صفر در ۶ مکان آخر است و این باعث می‌شود که یک ترکیب خطی از سه سطر $\overline{G}$ دارای وزن حداقل $1+3$ گردد؛ یعنی وزن حداقل ۶؛ بنابراین، $\overline{C}$ دارای کمترین—فاصله ۶ است. این نتیجه می‌دهد که C یک کد $(11,3^6,5)$ است. از $|B_2(x)| = \sum_{i=0}^{2} \binom{11}{i} 2^i = 35$ هم نتیجه می‌شود که C یک کد کامل است. این کد به‌عنوان یک کد گلی سه‌تایی[7] معروف است. نشان داده شده است که هر کد $(11,3^6,5)$ با C هم‌ارز است (ر.ک. مرجع [۴۶]). اثبات ساده‌ای برای یکتایی این کد، نظیر آنچه که ما برای کد گلی دوتایی ارائه دادیم، هنوز یافت نشده است.

۴.۴ ساختن کدها از کدهای دیگر

بسیاری از کدهای خوب با تغییری (با روش‌های متفاوت) در کدهای ساخته شده قبلی ساخته شده‌اند. در این بخش، چندین مثال می‌آوریم. اولین روش در تعریف ۶.۳.۲ معرفی شد؛ یعنی توسیع یک کد با اضافه نمودن یک سمبل اضافی به نام بررسی‌توازن کلی بود. فرایند معکوس، که ما آن را در بخش ۴.۲ به کار بردیم تا کد گلی دوتایی را از توسیع آن به دست آوریم، به پنچرنمودن یک کد معروف است. اگر به

[7] ternary Golay code

عنوان مثالی دیگر کد $(۹, ۲۰, ۴)$ با ماتریس موجود در رابطه ۱ را درنظر بگیریم و آن را پنچر کنیم؛ یعنی سمبل آخر در هر کلمه را حذف کنیم، یک کد $(۸, ۲۰, ۳)$ به دست می‌آوریم. در بخش بعد خواهیم دید که این کد در اصل کد خوبی است. توجه داریم که هم‌چنین یک کد هم‌ارز می‌تواند با قراردادن تمامی جای‌گشت‌های کلمات ۱۱۰۱۰۰۰۰، ۱۱۱۰۰۱۰۰ و ۱۰۱۰۱۰۱۰ به‌همراه **0** و **1** به‌دست آید.

روش سوم، کوتاه نمودن[۸] کد C می‌باشد. در اینجا تمامی کدکلمات از C را درنظر می‌گیریم که به سمبل یکسانی ختم شده باشند و در ادامه این سمبل را حذف می‌کنیم. این روش، طول و تعداد کدکلمات را کاهش می‌دهد، اما کمترین—فاصله کمتری نخواهد داشت. دقت کنید که اگر سمبل حذف شده برابر با صفر نباشد این روش یک کد خطی را به یک کد غیرخطی تغییر می‌دهد (به‌طور معمول).

بیایید به روشی کمی پیچیده‌تر نگاهی بیندازیم. از یکی از ساختارهای کد گلی دوتایی گسترش‌یافته $\mathcal{G}_{۲۴}$ در بخش ۴.۲ فوراً می‌توان مشاهده نمود که $\mathcal{G}_{۲۴}$ شامل زیرکدی با ۳۲ کلمه است که هشت مکان اول آنها برابر با صفر است. به‌طور مشابه، اگر قرار دهیم $c_۸ = ۱$ و دقیقاً یکی از سمبل‌های $c_۱$ تا $c_۷$ برابر با ۱ باشد، آن‌گاه زیرکدی با ۳۲ کلمه $(c_۱, c_۲, \cdots, c_{۲۴})$ یافت نموده‌ایم. با انجام این کار در تمامی حالات ممکن، زیرمجموعه‌ای از ۲۵۶ کلمهٔ $\mathcal{G}_{۲۴}$ با این خاصیت که هر دوتای آنها در حداکثر ۲ مکان از میان ۸ تای اول متفاوت می‌باشند، داریم. حال هشت سمبل اول از این کلمات را حذف می‌کنیم. نتیجه یک کد دوتایی $(۱۶, ۲۵۶, ۶)$ است که غیرخطی است. این کد کد نورداستروم[۹] —رابینسن[۱۰] نامیده می‌شود. این کد، اولین کد در میان یک دنباله نامتناهی است که در بخش ۷.۴ بررسی می‌نماییم. اگر ما این کد را دوبار کوتاه نماییم و سپس یک‌بار پنچر کنیم، نتیجه یک کد $(۱۳, ۶۴, ۵)$ می‌باشد که آن را با Y نمایش می‌دهیم. این کد مثال مهمی در فصل بعد خواهد بود. نشان داده شده که Y یکتاست و این‌که اگر Y را کوتاه نماییم، آن‌گاه دو نتیجه ممکن وجود دارد (گوتالز[۱۱] ۱۹۷۷، مرجع [۲۶]). این دو کد عبارت‌اند از: کد معروف به کد نادلر[۱۲] و کد موجود در مساله ۷.۴.۸.

ساختاری مشابه با ساختار کد دوتایی گلی به‌صورت $(\mathbf{u}, \mathbf{u}+\mathbf{v})$—ساختار معروف است. فرض کنید C_i یک کد دوتایی (n, M_i, d_i) باشد $(i = ۱, ۲)$؛ تعریف کنید:

$$C := \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) \,|\, \mathbf{u} \in C_۱, \mathbf{v} \in C_۲\}. \qquad (۳)$$

در این‌صورت C یک کد $(۲n, M_۱M_۲, d)$ است که در آن $d = \min\{۲d_۱, d_۲\}$. برای نشان دادن این مطلب، دو کدکلمه $(\mathbf{u}_۱, \mathbf{u}_۱ + \mathbf{v}_۱)$ و $(\mathbf{u}_۲, \mathbf{u}_۲ + \mathbf{v}_۲)$ را درنظر بگیرید. اگر $\mathbf{v}_۱ = \mathbf{v}_۲$ و

[۸] shortening
[۹] Nordstrom
[۱۰] Robinson
[۱۱] J.-M.Goethals
[۱۲] Nadler

$\mathbf{u}_۱ \neq \mathbf{u}_۲$، آن‌گاه فاصله آنها حداقل برابر با $۲d_۱$ است. اگر $\mathbf{v}_۱ \neq \mathbf{v}_۲$، آن‌گاه این فاصله برابر با $w(\mathbf{u}_۱ - \mathbf{u}_۲) + w(\mathbf{u}_۱ - \mathbf{u}_۲ + \mathbf{v}_۱ - \mathbf{v}_۲)$ است که به‌وضوح از $w(\mathbf{v}_۱ - \mathbf{v}_۲)$ بیشتر است؛ یعنی حداقل برابر $d_۲$ است. به‌عنوان مثال برای $C_۲$، کد $(۸, ۲۰, ۳)$ ساخته‌شده در بالا را درنظر می‌گیریم و برای $C_۱$، کد با وزن زوج $[۸, ۷]$ را درنظر می‌گیریم. این ساختار یک کد $(۱۶, ۵ \cdot ۲^۹, ۳)$ را نتیجه می‌دهد. تا به حال هیچ کد $(۱۶, M, ۳)$ با $M > ۵ \cdot ۲^۹$ شناخته نشده است.

بسیاری از کدهای خوب با به کارگیری ایده زیر توسط هلگرت[۱۳] و استیناف[۱۴] (۱۹۷۳ مرجع [۳۴]) ساخته شدند. فرض کنید C یک کد $[n, k]$ دوتایی با کمترین—فاصله d باشد. ممکن است فرض کنیم C دارای ماتریس مولد G با یک کلمه با وزن d به‌عنوان سطر اول آن باشد؛ مثلاً:

$$G = \left(\begin{array}{cccc|ccc} ۱ & ۱ & \cdots & ۱ & ۰ & \cdots & ۰ \\ \multicolumn{4}{c|}{G_۱} & \multicolumn{3}{c}{G_۲} \end{array}\right).$$

فرض کنید d' کمترین—فاصله کد $[n-d, k-۱]$، تولیدشده توسط $G_۲$ باشد که ما آن را کد باقی‌مانده[۱۵] می‌نامیم (نسبت به اولین سطر G). از G می‌بینیم که متناظر با هر کدکلمه از کد باقی‌مانده، دو کدکلمه از C وجود دارند که حداقل یکی از آنها در d مکان اول دارای وزن کمتر یا مساوی $\frac{۱}{۲}d$ است؛ بنابراین، $d' \geq \frac{۱}{۲}d$. برای تشریح این روش، در اینجا نشان می‌دهیم که یک کد خطی با پارامترهای کد نادلر وجود ندارد. اگر چنین کدی موجود باشد، آن‌گاه دارای یک ماتریس مولد G به‌صورت بالا خواهد بود که در آن $G_۲$ یک کد $[۷, ۴]$ با فاصله $d' \geq ۳$ را تولید می‌کند؛ بنابراین، کد باقی‌مانده یک کد همینگ است. می‌توانیم $G_۲$ را چهار سطر با وزن ۳ درنظر بگیریم؛ بنابراین، $G_۱$ چهار سطر با وزن ۲ خواهد بود. چند امکان دیگر برای بررسی باقی می‌ماند که آنها هم منجر به $d = ۵$ نمی‌شوند. حتی برای مقادیر پارامتری کوچک، اغلب یافتن کدهای خوب، کاملاً مشکل می‌باشد؛ برای مثال، یک ساختار با پیچیدگی بیشتر (ر.ک. مرجع [۴۶]، فصل ۲، بخش ۷) یک کد $(۱۰, M, ۴)$ با $M = ۳۸$ تولید نموده است و درمدت زمان طولانی، عقیده بر این بود که این کد نمی‌تواند بهتر شود. بست[۱۶] (۱۹۷۸؛ مرجع [۸]) یک کد $(۱۰, ۴۰, ۴)$ را پیدا نمود که در زیر به‌شرح آن می‌پردازیم. در فصل بعد، خواهیم دید که در حالت $n = ۱۰$، $d = ۴$، این کد درواقع بهترین کد است! کد $C_۱$ را که یک کد $[۵, ۳]$ با ماتریس مولد $\begin{pmatrix} ۱ & ۰ & ۰ & ۰ & ۱ \\ ۰ & ۱ & ۰ & ۱ & ۱ \\ ۰ & ۰ & ۱ & ۱ & ۰ \end{pmatrix}$ است، درنظر بگیرید. با دو برابر کردن تمامی کدکلمات، یک کد $[۱۰, ۳]$ با $C_۲$ کمترین—فاصله $d = ۴$ را داریم. حال $(\ ۰۰۱۰۰\ \ ۱۰۰۰۰\ )$ را به تمامی کلمات $C_۲$ اضافه نمایید. کد جدید، دیگر خطی نیست و شامل بردار $\mathbf{0}$ هم نمی‌باشد. با شماره‌گذاری مکان‌ها از ۱ تا ۱۰، مکان‌های

[۱۳] H. J. Helgert
[۱۴] R. D. Stinaff
[۱۵] residual code
[۱۶] M. R. Best

کدکلمات را با عناصری از زیرگروه $S_{۱۰}$ تولیدشده توسط $(۱۰\ ۹\ ۸\ ۷\ ۶)(۵\ ۴\ ۳\ ۲\ ۱)$ جای‌گشت می‌دهیم. این کد ۴۰ کدکلمه دارد که ثابت می‌شود کمترین—فاصله آن برابر با ۴ است.

در بسیاری از کاربردهای فنی (نظیر دیسک فشرده)، دو کد به‌کار می‌روند. این کدها به روشی باهم همکاری می‌کنند. برخی اوقات، هدف ما مقابله با خطاهای گروهی است. بسیاری از اوقات، خطاهای بیشتری نسبت به آنچه از کمترین—فاصله انتظار می‌رود، می‌تواند تصحیح شود.

مثالی از همکاری کدها را در مساله ۱۲.۳.۷؛ یعنی یک کد ضرب مستقیم را دیدیم. بیایید به چنین کدی نگاه دیگری بیندازیم. حاصل‌ضرب یک کد همینگ گسترش‌یافته $[۸, ۴, ۴]$ با یک کد همینگ گسترش‌یافته $[۱۶, ۱۱, ۴]$ را درنظر بگیرید. این حاصل‌ضرب تا ۷ خطا را می‌تواند تصحیح کند. حال فرض کنید یک کلمه دریافتی، یعنی یک ماتریس ۱۶ در ۸، دارای پنج سطر بدون خطا باشد، ۸ سطر با یک خطا و سه سطر با دو خطا. ما ۱۴ خطا داریم، دو برابر آنچه که انتظار آن را داشتیم به‌طوری که بتوانیم آن را اصلاح کنیم. اما، هنگامی که ما سطرها را کدگشایی می‌کنیم، سیزده تا تصحیح می‌شود و سه تا از بدهای آن تشخیص داده می‌شود. حال اعلام می‌کنیم که این سطرها پاک شده‌اند. هنگامی که ما ستون‌ها را کدگشایی می‌کنیم، با کلمات خطادار روبه‌رو نخواهیم شد، اما تمامی آنها دارای سه پاک‌شده می‌باشند. از آنجا که کد ستونی دارای فاصله ۴ است، می‌توانیم این پاک‌شده‌ها را اصلاح نماییم. در پایان، تمامی ۱۴ خطا تصحیح شده‌اند.

کدهایی که در عمل کاربرد دارند، تغییراتی را بر روی این ایده به‌کار می‌برند. در یک دیسک فشرده، دو کد، هر یک با فاصله ۵، با هم همکاری می‌کنند. برای یکی از آنها، کدگشا تنها کلمات با حداکثر یک خطا را تصحیح می‌کند؛ درغیر این‌صورت، اعلام می‌شود که کلمه، پاک شده است. در پایان، ثابت می‌شود که کارآیی این زوج کد هم‌کار افزایش می‌یابد.

مثال بیان‌شده در بالا را تعمیم می‌دهیم تا دنباله‌ای از کدهایی را که توسط الیاس[۱۷] در سال ۱۹۵۴ تعریف شده‌اند معرفی نماییم. با کد همینگ گسترش‌یافته $C_۱$ با طول $n_۱ = ۲^m$ شروع می‌کنیم. فرض کنید این کدها بر روی یک کانال دوتایی متقارن با احتمال خطای p به‌کار رفته‌اند که درآن $n_۱p < \frac{۱}{۲}$. برای $C_۲$، کد همینگ گسترش‌یافته با طول $۲^{m+۱}$ را درنظر می‌گیریم. تعریف کنید $V_۱ := C_۱$ و $V_۲$ حاصل‌ضرب مستقیم $C_۱$ و $C_۲$ باشد. این روش را ادامه می‌دهیم: اگر V_i تعریف شده باشد، آن‌گاه $V_{i+۱}$ حاصل‌ضرب مستقیم V_i و کد همینگ گسترش‌یافته $C_{i+۱}$ با طول ۲^{m+i} می‌باشد. طول V_i را با n_i و بعد آن را با k_i نمایش می‌دهیم. سرانجام، E_i را تعداد متوسط خطا در هر بلوک درکلمات V_i پس از کدگشایی قرار دهید.

[۱۷] P. Elias

از تعریف، داریم:

$$\begin{aligned} n_{i+1} &= n_i \cdot 2^{m+i}, \\ k_{i+1} &= k_i \cdot (2^{m+i} - m - i - 1), \end{aligned}$$

و از مثال ۴.۳.۳ نتیجه می‌شود $E_{i+1} \leq E_i^2$ و $E_1 \leq (n_1 p)^2 \leq \frac{1}{4}$؛ بنابراین، این کدها دارای این خاصیت می‌باشند که وقتی $i \to \infty$، E_i به صفر میل می‌کند.

از رابطه بازگشتی برای n_i و k_i داریم:

$$n_i = 2^{mi+\frac{1}{2}i(i-1)} \quad ; \quad k_i = n_i \prod_{j=0}^{i-1} (1 - \frac{m+j+1}{2^{m+j}}).$$

بنابراین، اگر R_i نمایش نرخ V_i باشد، آن‌گاه:

$$R_i \to \prod_{j=0}^{\infty} (1 - \frac{m+j+1}{2^{m+j}})$$

زمانی که $i \to \infty$؛ بنابراین، دنباله‌ای از کدها را خواهیم داشت که طول آنها به ∞ میل می‌کند، نرخ آنها به صفر میل نمی‌کند و با این وجود احتمال خطا به صفر میل می‌کند. دقت دارید که این کدها، معروف به کدهای الیاس، دارای کمترین—فاصله $d_i = 4^i$ هستند؛ بنابراین، $d_i/n_i \to 0$ وقتی $i \to \infty$.

۴.۵ کدهای رید—مولر

حال دسته‌ای از کدهای دوتایی مرتبط با هندسه متناهی را توصیف می‌کنیم. این کدها برای اولین بار توسط مولر[۱۸] (۱۹۵۴) و رید[۱۹] (۱۹۵۴) به‌کار برده شده‌اند. این کدها به اندازه کدهایی که در فصل‌های قبل مورد بحث واقع شدند، خوب نمی‌باشند، اما در عمل، آنها دارای این مزیت هستند که کدگشایی آنها آسان می‌باشد. این روش، توسیعی از کدگشایی با منطق اکثریت است (بخش ۳.۴ را ببینید).

چندین روش برای نمایش کدکلمات کدهای رید—مولر وجود دارد. سعی خواهیم نمود تا بحث یک‌پارچه‌ای را ارائه دهیم که نشان می‌دهد چگونه دیدگاه‌های متفاوت با هم در ارتباط هستند. برای آماده‌سازی، به قضیه‌ای از نظریه اعداد نیاز داریم که قدمت آن به یک قرن پیش باز می‌گردد (لوکاس[۲۰] (۱۸۷۸)).

[۱۸] D. E. Muller
[۱۹] I. S. Reed
[۲۰] Lucas

قضیه ۱.۴.۵. فرض کنید p یک عدد اول باشد و قرار دهید:

$$n = \sum_{i=0}^{l} n_i p^i, k = \sum_{i=0}^{l} k_i p^i$$

نمایش‌های n و k درپایه p باشند؛ یعنی $0 \leq n_i \leq p-1$ و $0 \leq k_i \leq p-1$؛ در این‌صورت:

$$\binom{n}{k} \equiv \prod_{i=0}^{l} \binom{n_i}{k_i} \bmod p.$$

اثبات. از این واقعیت استفاده می‌کنیم که $(1+x)^p \equiv 1 + x^p \bmod p$. اگر $0 \leq r < p$، آن‌گاه:

$$(1+x)^{ap+r} \equiv (1+x^p)^a (1+x)^r \bmod p.$$

با مقایسه ضرایب x^{bp+s}، که در آن $0 \leq s < p$، در دوطرف داریم:

$$\binom{ap+r}{bp+s} \equiv \binom{a}{b}\binom{r}{s} \bmod p.$$

حال نتیجه با استقرا ثابت می‌شود. □

هم‌چنین قضیه زیر بر روی وزن چندجمله‌ای‌ها نیز یک آماده‌سازی است. فرض کنید $q = 2^r$. برای چندجمله‌ای $p(x) \in \mathbb{F}_q[x]$ وزن همینگ $w(p(x))$ تعداد ضرایب ناصفر در بسط $p(x)$ می‌باشد. فرض کنید $c \in \mathbb{F}_q$، $c \neq 0$. چندجمله‌ای‌های $(x+c)^i$، $i \geq 0$، یک پایه از $\mathbb{F}_q[x]$ هستند.

قضیه ۲.۴.۵. (مسی[۲۱] ۱۹۷۳، مرجع [۴۹]). فرض کنید $p(x) = \sum_{i=0}^{l} b_i (x+c)^i$ که در آن $b_l \neq 0$ و i_0 کوچک‌ترین اندیس i باشد به‌طوری که $b_i \neq 0$؛ بنابراین:

$$w(p(x)) \geq w((x+c)^{i_0}).$$

اثبات. برای $l = 0$ اثبات واضح است. استقرا را به‌کار می‌بریم. فرض کنید قضیه برای $l < 2^n$ درست است. حال قرار دهید $2^n \leq l < 2^{n+1}$؛ در این‌صورت داریم:

$$\begin{aligned} P(x) &= \sum_{i=0}^{2^n-1} b_i (x+c)^i + \sum_{i=2^n}^{l} b_i (x+c)^i \\ &= P_1(x) + (x+c)^{2^n} P_2(x) = (P_1(x) + c^{2^n} P_2(x)) + x^{2^n} P_2(x), \end{aligned}$$

که در آن $P_1(x)$ و $P_2(x)$ چندجمله‌ای‌هایی هستند که قضیه در مورد آنها صادق است. دو حالت زیر را درنظر می‌گیریم:

[۲۱] Massey

۱) اگر $P_1(x) = 0$، آن‌گاه $w(P(x)) = 2w(P_2(x))$ و چون $i_0 \geq 2^n$ داریم:

$$w((x+c)^{i_0}) = w((x^{2^n} + c^{2^n})(x+c)^{i_0 - 2^n}) = 2w((x+c)^{i_0 - 2^n}),$$

که ادعا ثابت می‌شود.

۲) اگر $P_1(x) \neq 0$، آن‌گاه برای هر جمله $c^{2^n} P_2(x)$ که یک جمله در $P_1(x)$ را حذف می‌کند، یک جمله در $x^{2^n} P_2(x)$ را داریم که حذف نمی‌شود؛ بنابراین، $w(P(x)) \geq w(P_1(x))$ و این نتیجه از فرض استقرا نتیجه می‌شود.

□

سه نمایش کدکلمات کدهای رید–مولر که در اینجا آنها را معرفی می‌نماییم، عبارتند از:

الف. توابع مشخصه مجموعه‌هایی در $AG(m, 2)$؛

ب. ضرایب بسط‌های دوتایی چندجمله‌ای‌ها؛

ج. لیست مقادیری که توسط یک تابع منطقی روی $\mathbb{F}_2^m$ گرفته شده‌اند.

درابتدا برخی نمادگذاری‌ها و تعاریف را بیان می‌کنیم. نقاط $AG(m, 2)$ را درنظر بگیرید؛ یعنی $\mathbb{F}_2^m$ به‌عنوان بردارهای ستونی و پایه استاندارد با عناصر $\mathbf{u}_0$، $\mathbf{u}_1$، ...، $\mathbf{u}_{m-1}$. فرض کنید نمایش دوتایی j به‌صورت $j = \sum_{i=0}^{m-1} \xi_{ij} 2^i$، $0 \leq j < 2^m$، باشد.

تعریف می‌کنیم $x_j := \sum_{i=0}^{m-1} \xi_{ij} \mathbf{u}_i$. این یک نقطه از $AG(m, 2)$ را نمایش می‌دهد و تمامی نقاط به این صورت به دست آمده‌اند. فرض کنید E ماتریسی با ستون‌های x_j، $0 \leq j < 2^m$، باشد. می‌نویسیم $n := 2^m$. ماتریس m در n مانند E، لیستی از نقاط $AG(m, 2)$ است که به‌صورت بردارهای ستونی نوشته شده‌اند.

تعریف ۳.۴.۵.

۱) $A - i := \{x_j \in AG(m, 2) \mid \xi_{ij} = 1\}$؛ یعنی A_i، برای هر $0 \leq i < m$، یک فضای آفین $(m-1)$–بعدی است (یک ابرصفحه).

۲) v_i برابر با iامین سطر E است؛ یعنی تابع مشخصه A_i. بردار v_i یک کلمه در $\mathbb{F}_2^n$ است؛ معمولاً می‌نویسیم $\mathbf{1} := (1, 1, ..., 1)$ برای تابع مشخصه $AG(m, 2)$؛

۳) اگر $\mathbf{a} = (a_0, a_1, ..., a_{n-1})$ و $\mathbf{b} = (b_0, b_1, ..., b_{n-1})$ کلماتی در $\mathbb{F}_2^n$ باشند، آن‌گاه داریم:

$$\mathbf{ab} := (a_0 b_0, a_1 b_1, ..., a_{n-1} b_{n-1}).$$

۴) اگر $S \subset \{۰, ۱, ..., m-۱\}$، آن‌گاه تعریف می‌کنیم:

$$C(S) := \{j = \sum_{i=۰}^{m-۱} \xi_{ij} ۲^i \,|\, i \notin S \Longrightarrow \xi_{ij} = ۰ \, (۰ \leq i < m)\}.$$

لم ۴.۴.۵. فرض کنید $l = \sum_{i=۰}^{m-۱} \xi_{ij} ۲^i$ و $i_۱, \cdots, i_s$ مقادیری از i باشند که در آن $\xi_{il} = ۰$. اگر:

$$v_{i_۱} v_{i_۲} \cdots v_{i_s} = (a_{l,۰}, a_{l,۱}, \cdots, a_{l,n-۱}),$$

آن‌گاه:

$$(x+۱)^l = \sum_{j=۰}^{n-۱} a_{l,j} x^{n-۱-j}.$$

(دراینجا، به‌طورمعمول، یک حاصل‌ضرب بدون هیچ عاملی $(s = ۰)$، برابر با 1 تعریف شده است).

اثبات. با استناد به قضیه ۱.۴.۵، ضریب دوجمله‌ای $\binom{l}{n-۱-j}$ برابر با ۱ است اگر و تنها اگر $\xi_{ij} = ۱$ برای هر i که $\xi_{il} = ۰$. هم‌چنین با استناد به تعریف ۳.۴.۵ قسمت‌های (۱)، (۲) و (۳) داریم $a_{l,j} = ۱$ اگر و تنها اگر $\xi_{ij} = ۱$ برای $i = i_۱, \cdots, i_s$. □

مطالب زیر نشان می‌دهد که چگونه می‌توان $v_{i_۱}, \cdots, v_{i_s}$ را به‌طور هندسی تفسیر نمود.

لم ۵.۴.۵. اگر $i_۱, i_۲, \cdots, i_s$ متفاوت باشند، آن‌گاه:

۱) $v_{i_۱} v_{i_۲} \cdots v_{i_s}$ تابع مشخصه $(m-s)$–سطح $A_{i_۱} \cap A_{i_۲} \cap \cdots \cap A_{i_s}$ است.

۲) وزن $w(v_{i_۱} \cdots v_{i_s})$ از بردار $v_{i_۱} \cdots v_{i_s}$ در $\mathbb{F}_۲^n$ برابر با ۲^{m-s} است.

۳) تابع مشخصه $\{x_j\}$، یعنی jامین بردار پایه $\mathbb{F}_۲^n$، برابر است با:

$$e_j = \prod_{i=۰}^{m-۱} \{v_i + (۱ + \xi_{ij})\mathbf{1}\}$$

۴) بردارهای $v_{i_۱} \cdots v_{i_s}$ $(۰ \leq s \leq m)$ یک پایه از $\mathbb{F}_۲^n$ هستند.

اثبات.

۱) این قسمت یک نتیجه از ۳.۴.۵ (۱)–(۳) است.

۲) توسط (۱)، وزن برابر با اندازه یک $(m-s)$–سطح است.

۳) ماتریس E را درنظر بگیرید. برای هر i که $\xi_{ij}=۰$ ما iامین سطر E، یعنی v_i، را با مکمل آن v_i+1 جای‌گزین می‌کنیم؛ در این‌صورت اگر سطرهای ماتریس جدید را ضرب کنیم، بردار حاصل‌ضرب شامل درایه ۱ تنها در مکان j خواهد بود، چون تمامی ستون‌های ممکن تنها یک‌بار رخ می‌دهند. به‌عنوان یک مثال $\{x_{۱۴}\}$ را در جدول زیر درنظر بگیرید. چون $۱۴=۰+۲+۲^۲+۲^۳$ می‌بینیم که $\xi_{ij}+۱=۱$ تنها اگر $i=۰$ (دراینجا $j=۱۴$)؛ بنابراین، در این جدول، ما سطر متناظر با $v_۰$ را مکمل می‌کنیم و سپس ضرب می‌کنیم تا $(v_۰+1)\ v_۱\ \ v_۲\ \ v_۳$ را بیابیم که برداری سطری است که دارای تنها یک ۱ در چهاردهمین مکان است.

۴) $n=۲^m=\sum_{s=۰}^{m}\binom{m}{s}$ بردار $v_{i_۱}\cdots v_{i_s}$ وجود دارند. این نتیجه از (۳) به‌دست می‌آید. از آنجا که چندجمله‌ای‌های $(x+۱)^l$ مستقل هستند، می‌توانیم لم ۴.۴.۵ را نیز به‌کار بریم.

□

جدول زیر لم ۴.۴.۵ را تشریح می‌کند؛ برای مثال، $v_۰v_۲$ متناظر با $l=۱۵-۲^۰-۲^۲=۱۰$ است؛ بنابراین، $(x+۱)^{۱۰}=x^{۱۰}+x^۸+x^۲+۱$.

$v_{i_۱}\ v_{i_۲}\ \cdots\ v_{i_s}$	ضرایب $(x+۱)^l$ = مولفه‌ها																$l=n-۱-\sum ۲^{i_s}$
۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱۵ = ۱۱۱۱
$v_۰$	۰	۱	۰	۱	۰	۱	۰	۱	۰	۱	۰	۱	۰	۱	۰	۱	۱۴ = ۱۱۱۰
$v_۱$	۰	۰	۱	۱	۰	۰	۱	۱	۰	۰	۱	۱	۰	۰	۱	۱	۱۳ = ۱۱۰۱
$v_۲$	۰	۰	۰	۰	۱	۱	۱	۱	۰	۰	۰	۰	۱	۱	۱	۱	۱۱ = ۱۰۱۱
$v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۱	۱	۱	۱	۱	۱	۱	۱	۷ = ۰۱۱۱
$v_۰\ v_۱$	۰	۰	۰	۱	۰	۰	۰	۱	۰	۰	۰	۱	۰	۰	۰	۱	۱۲ = ۱۱۰۰
$v_۰\ v_۲$	۰	۰	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۰	۱	۰	۱	۱۰ = ۱۰۱۰
$v_۰\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۱	۰	۱	۱	۶ = ۰۱۱۰
$v_۱\ v_۲$	۰	۰	۰	۰	۰	۰	۱	۱	۰	۰	۰	۰	۰	۰	۱	۱	۹ = ۱۰۰۱
$v_۱\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۱	۱	۱	۱	۱	۱	۱	۱	۵ = ۰۱۰۱
$v_۲\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۱	۱	۱	۳ = ۰۰۱۱
$v_۰\ v_۱\ v_۲$	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۱	۸ = ۱۰۰۰
$v_۰\ v_۱\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۰	۱	۴ = ۰۱۰۰
$v_۰\ v_۲\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰	۱	۲ = ۰۰۱۰
$v_۱\ v_۲\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۱	۱ = ۰۰۰۱
$v_۰\ v_۱\ v_۲\ v_۳$	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۰	۱	۰ = ۰۰۰۰

تعریف ۶.۴.۵. فرض کنید $0 \leq r < m$. کد خطی با طول $n = 2^m$ که دارای بردارهای $v_{i_1} \cdots v_{i_s}$ با $s \leq r$ عامل به‌عنوان پایه است، rامین مرتبه کد دوتایی رید–مولر نامیده می‌شود (RM کد؛ با نماد $\mathcal{R}(r,m)$).

حالت خاص $\mathcal{R}(0,m)$ کد تکرار است. از لم ۵.۴.۵ قسمت (۱) می‌بینیم که تابع منطقی $x_{i_1}x_{i_2}\cdots x_{i_s}$ که در آن $x=(x_0,\cdots,x_{m-1})$، ثابت می‌کند که $\mathbb{F}_2^m$ دارای مقدار ۱ است اگر و تنها اگر $x \in A_{i_1} \cap \cdots A_{i_s}$. بنابراین، $\mathcal{R}(r,m)$ شامل دنباله‌هایی با مقادیر داده شده توسط چندجمله‌ای‌هایی برحسب $x_0,\cdots,x_{m-1}$ با درجه حداکثر r است.

قضیه ۷.۴.۵. $\mathcal{R}(r,m)$ دارای کمترین–فاصله 2^{m-r} است.

اثبات. با استفاده از تعریف و قسمت (۲) از لم ۵.۴.۵، کمترین–فاصله حداکثر برابر با 2^{m-r} است و با استفاده از لم ۴.۴.۵ و قضیه ۲.۴.۵ حداقل برابر با 2^{m-r} است (نیز مساله ۹.۴.۸ را ببینید). □

قضیه ۸.۴.۵. دوگان $\mathcal{R}(r,m)$ برابر با $\mathcal{R}(m-r-1,m)$ است.

اثبات.

۱) با استفاده از تعریف و استقلال بردارهای $v_{i_1}\cdots v_{i_s}$، بعد $\mathcal{R}(r,m)$ برابر با $1+\binom{m}{1}+\cdots+\binom{m}{r}$ است؛ بنابراین، $\dim \mathcal{R}(r,m) + \dim \mathcal{R}(m-r-1,m) = n$.

۲) فرض کنید $v_{i_1}\cdots v_{i_s}$ و $v_{j_1}\cdots v_{j_t}$ به‌ترتیب بردارهای پایه $\mathcal{R}(r,m)$ و $\mathcal{R}(m-r-1,m)$ باشند؛ در این‌صورت $s+t<m$؛ بنابراین، حاصل‌ضرب بردارهای این دو پایه به فرم $v_{k_1}\cdots v_{k_u}$ خواهد بود که در آن $u<m$. با استفاده از قسمت (۲) از لم ۵.۴.۵ این حاصل‌ضرب دارای وزن زوج می‌باشد، یعنی بردارهای اصلی از دو پایه، متعامد هستند.

□

نتیجه‌گیری ۸.۴.۵ $\mathcal{R}(m-2,m)$ یک کد همینگ گسترش‌یافته $[n, n-m-1]$ است.

ما توابع مشخصه از سطوح معین را به عنوان پایه‌ای برای یک کد RM انتخاب نموده‌ایم. حال، نشان می‌دهیم که برای هر سطح با بعد مناسب، تابع مشخصه متعلق به کد RM معینی است.

قضیه ۹.۴.۵. فرض کنید $C = \mathcal{R}(m-۱, m)$ و A یک ۱—سطح در $AG(m, ۲)$ باشد؛ در این‌صورت تابع مشخصه A در C می‌باشد.

اثبات. فرض کنید $\mathrm{f} = \sum_{j=۰}^{n-۱} f_j e_j$ تابع مشخصه A باشد. با استفاده از تعریف ۳.۴.۵ و لم ۵.۴.۵ داریم:

$$e_j = \sum_{s=۰}^{m} \sum_{\substack{(i_۱, \cdots, i_s) \\ j \in C(i_۱, \cdots, i_s)}} v_{i_۱} v_{i_۲} \cdots v_{i_s};$$

بنابراین:

$$\mathrm{f} = \sum_{s=۰}^{m} \sum_{(i_۱, \cdots, i_s)} \Big(\sum_{j \in C(i_۱, \cdots, i_s)} f_j \Big) v_{i_۱} v_{i_۲} \cdots v_{i_s}.$$

دراینجا، مجموع داخلی، تعداد نقاط موجود در اشتراک A و s—سطح:

$$L = \{x_j \in AG(m, ۲) \mid j \in C(i_i, \cdots, i_s)\},$$

را شمارش می‌کند. اگر $s > m-۱$، آن‌گاه $L \cap A$ یا تهی است و یا یک زیرفضای آفین با بعد مثبت است. در هر دو حالت، $|L \cap A|$ زوج است؛ یعنی مجموع داخلی برابر با صفر است. □

این قضیه و تعریف نشان می‌دهد که یک کلمه متعلق به $\mathcal{R}(r, m)$ است اگر و تنها اگر مجموع توابع مشخصه از زیرفضاهای آفین با بعد بیشتر یا مساوی $m-r$ باشد. دراصطلاح علمی توابع منطقی، $\mathcal{R}(r, m)$ مجموعه چندجمله‌ای‌هایی برحسب $x_۰, x_۱, \cdots, x_{m-۱}$ با درجه کمتر یا مساوی r است.

در بخش ۳.۲ نماد کدهای هم‌ارز را با به‌کارگیری جای‌گشت‌ها بر روی مکان‌های کدکلمات تعریف کردیم. حال بیایید کد C با طول n و جای‌گشت‌های $\pi \in S_n$ که تمامی کلمات در C را به یک کدکلمه در C تصویر می‌کنند، درنظر بگیرید. این جای‌گشت‌ها تشکیل یک گروه می‌دهند که معروف به گروه خودریختی[۲۲] C (با نماد: $Aut(G)$) می‌باشند؛ برای مثال، اگر C کد تکرار باشد، آن‌گاه $Aut(C) = S_n$.

قضیه ۱۰.۴.۵. $AGL(m, ۲) \subset Aut(\mathcal{R}(r, m))$.

اثبات. این یک نتیجه فوری از قضیه ۹.۴.۵ و این واقعیت است که $AGL(m, ۲)$ یک k—سطح را به یک k—سطح تصویر می‌کند. □

[۲۲] automorphism group

تذکر ۱۰.۴.۵ خواننده باید متوجه باشد که ما $AGL(m,۲)$ را روی $AG(m,۲)$ به‌عنوان گروهی از جای‌گشت‌های n مکان درنظر گرفتیم که توسط عناصر $AG(m,۲)$ شمارش شده‌اند.

بدون پرداختن به جزییات، به‌طور خلاصه یک روش کدگشایی برای کدهای RM بیان می‌کنیم که گسترشی از کدگشایی منطقی است. فرض کنید $C = \mathcal{R}(r,m)$. به‌وسیله قضیه ۸.۴.۵ و ۹.۴.۵، تابع مشخصه هر $(r+۱)$–سطحی در $AG(m,۲)$ یک بردار بررسی‌توازن برای C است. برای یک r–سطح داده شده A، تعداد $۲^{m-r}-۱$، $(r+۱)$–سطح مجزا شامل A وجود دارد. نقطه‌ای که در A نباشد، متعلق به دقیقاً یکی از این $(r+۱)$–سطح می‌باشد. هریک از این $(r+۱)$–سطح شامل تقاطی از A است و دقیقاً برابر با تعداد نقاطی است که در A نباشند.

حال، بیایید به بررسی‌توازن‌ها نگاهی بیندازیم. فرض کنید یک کلمه دریافتی شامل کمتر از $۲^{m-r-۱}$ خطا باشد (قضیه ۷.۴.۵ را ببینید). فرض کنید r بررسی‌توازن غلط باشد. دو توضیح ممکن برای آن وجود دارد:

۱) ممکن است تعداد فردی خطا در مکان‌های A رخ داده باشد که به تعداد $۲^{m-r}-۱-r$ بار توسط تعداد فردی خطا در مکان‌های باقی‌مانده از مجموعه بررسی، جبران شده باشد.

۲) تعداد خطاها در مکان‌های A زوج است، اما در t معادله بررسی‌توازن تعداد فردی خطا در مکان‌های باقی‌مانده وجود دارد.

با استفاده از قاعده بیشترین درست‌نمایی، اگر $r < ۲^{m-r-۱}$، آن‌گاه (۲) نسبت به (۱) دارای احتمال بیشتری است و درغیر این‌صورت (۱) دارای احتمال بیشتری است. این بدان معناست که یافتن توازن تعداد خطاها در مکان‌های هر r–سطحی امکان پذیر است؛ بنابراین، با به‌کارگیری روشی مشابه، همان موارد برای $(r-۱)$–سطوح برقرار است و الی آخر. پس از $r+۱$ مرحله، خطاها مشخص شده‌اند. این روش، کدگشایی اکثریت چند مرحله‌ای[۲۳] نامیده می‌شود.

۴.۶ کدهای کرداک

ما به‌طور خلاصه کلاسی از کدهای غیرخطی، معروف به کدهای کرداک[۲۴] را بررسی خواهیم کرد (مراجع [۷۵]، [۱۱]). یک کد کرداک، زیرکدی از یک کد رید–مولر مرتبه دوم شامل تعدادی از هم‌مجموعه‌های

[۲۳] multistep majority decoding
[۲۴] Kerdock codes

کد رید–مولر مرتبه اول متناظر با آن است. دقت کنید که $\mathcal{R}(۲,m)$، خود اجتماعی از هم‌مجموعه‌های $\mathcal{R}(۱,m)$ است که هر هم‌مجموعه متناظر با یک فرم درجه دوم به‌صورت زیر است:

$$Q(v) := \sum_{۰\le i<j<m} q_{ij}v_iv_j. \qquad (۴)$$

متناظربا Q، یک شکل دوخطی متناوب B به‌صورت:

$$B(v,w) := Q(v+w) - Q(v) - Q(w) = vBw^T,$$

وجود دارد که در آن B یک ماتریس متقارن است (صفر روی قطر اصلی و $B = -B^T$). با استفاده از یک اثبات استقرایی ساده می‌توان نشان داد که با استفاده از یک تبدیل آفین مناسب، Q می‌تواند به شکل:

$$\sum_{i=۰}^{h-۱} v_{۲i}v_{۲i+۱} + L(v), \qquad (۵)$$

واقع شود که در آن L خطی است و $۲h$ رتبه B است. در واقع، با نگاهی به آن می‌توان دید که $v_{۲h}$ یا $L(v) = ۰, ۱$.

لم ۱.۴.۶. تعداد نقاط $(x_۰, x_۱, \cdots, x_{۲h-۱}) \in \mathbb{F}_۲^{۲h}$، که در آن $\sum_{i=۰}^{h-۱} x_{۲i}x_{۲i+۱} = ۰$، برابر با $۲^{۲h-۱} + ۲^{h-۱}$ است.

اثبات. اگر $x_۰ = x_۲ = \cdots = x_{۲h-۲} = ۰$، آن‌گاه ۲^h انتخاب برای $(x_۱, \cdots, x_{۲h-۱})$ وجود دارد. در غیر این‌صورت، $۲^{h-۱}$ انتخاب وجود دارد؛ بنابراین، تعداد صفرها برابر با $۲^{h-۱}(۲^h - ۱) + ۲^h$ است. □

با توجه به رابطه ۵ و لم ۱.۴.۶، لم زیر را داریم:

لم ۲.۴.۶. فرض کنید m زوج باشد. اگر $Q(v)$ یک فرم مرتبه دوم متناظر با یک فرم سادکی[۲۵] با رتبه n باشد، آن‌گاه هم‌مجموعه $\mathcal{R}(۱,m)$ تعیین‌شده توسط $Q(v)$، دارای ۲^m کلمه با وزن $۲^{m-۱} - ۲^{m/۲-۱}$ و ۲^m کلمه با وزن $۲^{m-۱} + ۲^{m/۲-۱}$ است.

(دقت کنید که این مطلب باعث می‌شود تا اگر Q دارای رتبه‌ای کمتر از m باشد، آن‌گاه هم‌مجموعه متناظر دارای کمترین–وزن کمتری باشد).

به‌وضوح، اجتماعی از هم‌مجموعه‌های $\mathcal{R}(r,m)$، کدی با کمترین–فاصله حداکثر $۲^{m-۱} - ۲^{m/۲-۱}$ خواهد بود. می‌خواهیم کد C را با استفاده از اجتماع هم‌مجموعه‌های متناظر با فرم‌های درجه دوم $Q_۱$، $\cdots$، Q_l (با فرم‌های سادکی $B_۱$، $\cdots$، B_l) بسازیم. برای یافتن کمترین–فاصله این کد، باید کدهای

[۲۵] symplectic

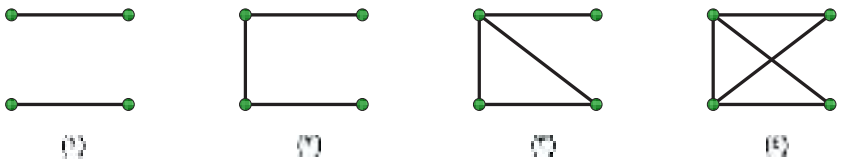
متناظر با هم‌مجموعه‌های تعریف شده توسط فرم‌های $Q_i - Q_j$ $(i \neq j)$ را درنظر بگیریم و کمترین—وزن آنها را بیابیم. بهترین حالتی که می‌توانیم به آن دست یابیم این است که هر تفاضل $Q_i - Q_j$ متناظر با یک فرم سادکی با رتبه ماکسیمال باشد که یک فرم سادکی نامنفرد است. چون فرم‌های سادکی متناظر با ماتریس‌های ضدمتقارن با قطر صفر هستند و هیچ دوتای آنها دارای سطر اول یکسان نیستند، نتیجه می‌شود که اگر کمترین—فاصله d از C برابر با $۲^{m-۱} - ۲^{m/۲-۱}$ باشد، آن‌گاه $l \leq ۲^{m-۱}$.

تعریف ۳.۴.۶. فرض کنید m زوج باشد. یک مجموعه از $۲^{m-۱}$ ماتریس سادکی با اندازه m به‌طوری که تفاضل هر دو عضو متمایز، نامنفرد است یک مجموعه کرداک نامیده می‌شود.

تعریف ۴.۴.۶. فرض کنید m زوج باشد. فرض کنید $l = ۲^{m-۱}$ و $Q_۱$، $\cdots$، Q_l یک مجموعه کرداک باشد. کد غیرخطی $\mathcal{K}(m)$ با طول $n = ۲^m$ شامل هم‌مجموعه‌های $\mathcal{R}(۱, m)$، متناظر با فرم‌های Q_i، $۱ \leq i \leq l$، کد کرداک نامیده می‌شود.

نشان دادن این‌که دراصل چنین کدهایی وجود دارند، یک مساله غیربدیهی است که مربوط به هندسه $\mathbb{F}_۴^m$ (ر.ک. مرجع [۱۱]) است. ما تنها یک مثال می‌آوریم. فرض کنید $m = ۴$. اگر Q فرم مربعی $\sum_{i=۰}^{۳} q_{ij} x_i x_j$ باشد، آن‌گاه Q را با یک گراف با رئوس $x_۰$، ...، $x_۳$ با یال $\{x_i, x_j\}$ نمایش می‌دهیم اگر و تنها اگر $q_{ij} = ۱$.

اگر Q متناظر با یک فرم سادکی نامنفرد باشد، آن‌گاه این گراف باید با یکی از گراف‌های زیر یک‌ریخت باشد:



افرازهای (۳۴)(۱۲)، (۲۴)(۱۳) و (۲۳)(۱۴) را به‌صورت دوری منظم کنید. از شش گراف نوع (۲)، با گرفتن دو ضلع از یک زوج از این افرازها و یک زوج از دیگری، به آسانی می‌توان دید که این شش گراف، گراف تهی و گراف نوع (۴) دارای این خاصیت می‌باشند که مجموع (یا تفاضل) هر دوتا متناظر با یک فرم سادکی نامنفرد است. در این روش، $۲^۸ = ۲^۵ \cdot ۸$ کلمه از یک کد $(۱۶, ۲^۸, ۶)$ را می‌یابیم، که درواقع همان کد نورداستروم—رابینسن در بخش ۴.۴ است.

در حالت کلی، $\mathcal{K}(m)$ یک کد $(۲^m, ۲^{۲m}, ۲^{m-۱} - ۲^{m/۲-۱})$ است؛ بنابراین، تعداد کلمات آن به‌طور قابل توجهی بزرگ‌تر از $\mathcal{R}(۱, m)$ است، اگر چه کمترین—فاصله آن کمی کوچک‌تر است.

۴.۷ پیشنهادها

برای دیدن جزییات درباره کاربردهای کدهای هادامارد در سفرهای مارینر، به مرجع [۵۶] مراجعه کنید.

کدهای گلی توسط گلی[۲۶] در سال ۱۹۴۹ به روشی متفاوت با بحث ما ساخته شدند. برای دانستن بیشتر درباره این کدها و چندین ارتباط آن با نظریه ترکیبیات، خواننده را به کتاب کمرون [۲۷] و ون‌لینت[۲۸] [۱۱] یا مرجع [۴۹] ارجاع می‌دهیم؛ نیز می‌تواند مرجع [۱۹] را مشاهده نماید.

خواننده‌ای که علاقه‌مند به مطالب بیشتر درباره فصل ۴.۴ این کتاب است، به مراجع [۶۴] یا [۶۵] ارجاع داده می‌شود. برای دانستن مطالب بیشتر درباره کدگذاری و کدگشایی کدهای RM، مراجع [۲] یا [۴۶] را ببینید.

۴.۸ مسائل

۱.۴.۸. فرض کنید $n = ۲^m$. نشان دهید که کد رید–مولر $\mathcal{R}(۱, m)$ یک کد هادامارد از مرتبه n است.

۲.۴.۸. نشان دهید که کد گلی سه‌تایی دارای ۱۳۲ کلمه با وزن ۵ است. برای هر زوج $\{x, ۲x\}$ از کدکلمات به وزن ۵، زیرمجموعه‌ای از مکان‌هایی که $x_i \neq ۰$ را درنظر بگیرید. نشان دهید که این ۶۶ مجموعه تشکیل یک $(۱۱, ۵, ۱) - ۴$ طرح می‌دهند.

۳.۴.۸. فرض کنید S ماتریس پالی مرتبه ۱۱ باشد و $A = \frac{۱}{۲}(S + I + J)$. سطرهای A را درنظر بگیرید و تمامی ۵۵ مجموع هر دو سطر متمایز A و مکمل‌های این بردارها را درنظر بگیرید. نشان دهید که حاصل یک کد $(۱۱, ۱۳۲, ۳)$ است.

۴.۴.۸. یک کد $(۱۷, ۳۶, ۸)$ بسازید.

۵.۴.۸. ساختار کانوی[۲۹] از $\mathcal{G}_{۲۴}$ را درنظر بگیرید. سپس زیرگروه شامل ماتریس‌های A به شکل (B, B, B) را درنظر بگیرید که در آن B یک ماتریس ۴ در ۲ است. نشان دهید که ماتریس‌های B کلمات یک کد هم‌ارز با کد همینگ گسترش‌یافته $[۸, ۴]$ هستند.

---

[۲۶] M. J. E. Golay
[۲۷] P .J. Cameron
[۲۸] J. H. vanLint
[۲۹] Conway

۶.۴.۸. نشان دهید اگر یک کد دوتایی (n, M, d) با d زوج وجود داشته باشد، آن‌گاه یک کد (n, M, d) وجود دارد که تمامی کدکلمات آن زوج می‌باشد.

۷.۴.۸. ماتریس‌های I، J و P از اندازه ۳ همانند ۱ را درنظر بگیرید؛ تعریف کنید:

$$A := \begin{pmatrix} J-I & I & I & I \\ I & J-I & I & I \\ I & I & J-I & I \\ I & I & I & J-I \end{pmatrix}, \quad B := \begin{pmatrix} J & P & I & P^2 \\ P & J & P^2 & I \\ I & P^2 & J & P \\ P^2 & I & P & J \end{pmatrix},$$

$$C := \begin{pmatrix} J-I & J-I & J-I & J-I \end{pmatrix}, \quad D := \begin{pmatrix} 000 & 111 & 111 & 111 \\ 111 & 000 & 111 & 111 \\ 111 & 111 & 000 & 111 \\ 111 & 111 & 111 & 000 \end{pmatrix}.$$

نشان دهید که $\mathbf{0}$ و سطرهای A، B، C و D کلمات یک کد $(12, 32, 5)$ است.

۸.۴.۸. فرض کنید H ماتریس هادامارد H_{12} از رابطه ۲۰ در فصل ۱ باشد و $A := H - I$، $G := \begin{pmatrix} I & A \end{pmatrix}$. نشان دهید G ماتریس مولد یک کد $[24, 12]$ سه‌تایی با کمترین–فاصله ۹ است.

۹.۴.۸. نشان دهید $(\mathbf{u}, \mathbf{u}+\mathbf{v})$–ساختار موجود در رابطه ۳ برای $C_1 = \mathcal{R}(r+1, m)$ و $C_2 = \mathcal{R}(r, m)$، ساختار $C = \mathcal{R}(r+1, m+1)$ را القا می‌کند. از این مطلب استفاده نموده و اثبات دومی برای قضیه ۷.۴.۵ بیاورید.

۱۰.۴.۸.

۱) فرض کنید $n = 2^m$. برای $x \in \mathbb{F}_2^n$ بردار $x^* \in \{1, -1\}^n$ را به‌صورت برداری که از جانشینی ۰ ها در x با $1-$ به‌دست آمده، تعریف می‌کنیم. در مساله ۱.۴.۷ دیدیم که این نگاشت تحدید شده بر روی $\mathcal{R}(1, m)$، بردارهای $\pm\mathbf{a}_1$، $\pm\mathbf{a}_2$، $\cdots$ و $\pm\mathbf{a}_n$ را نتیجه می‌دهد که در آن $\mathbf{a}_i$ سطرهای یک ماتریس هادامارد می‌باشند. با به‌کارگیری این مطالب، نشان دهید که اگر $x \in \mathbb{F}_2^n$، آن‌گاه کدکلمه $c \in \mathcal{R}(1, m)$ وجود دارد؛ به‌طوری که $d(x, c) \leq (n - \sqrt{n})/2$.

۲) اگر $m = 2k$ و x کلمه‌ای در $\mathcal{R}(2, m)$ متناظر با تابع منطقی $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$ باشد، آن‌گاه نشان دهید که برای تمامی $\mathbf{c} \in \mathcal{R}(1, m)$ داریم $d(x, c) \geq (n - \sqrt{n})/2$ (به‌عبارت دیگر، شعاع پوششی $(1, 2k)$ برابر با $2^{2k-1} - 2^{k-1}$ است).

۱۱.۴.۸. فرض کنید H ماتریس بررسی‌توازن یک کد همینگ گسترش‌یافته سه‌تایی $[۴, ۲]$ باشد و I و J به ترتیب ماتریس‌های همانی و ماتریس تماماً ۱ از مرتبه ۴ باشند. نشان دهید:

$$G := \begin{pmatrix} J+I & I & I \\ ۰ & H & -H \end{pmatrix},$$

کد C را که یک کد $[۱۲, ٦]$ با کمترین —فاصله ٦ است، تولید می‌کند و این؛ یعنی کدی معادل با کد گلی سه‌تایی گسترش‌یافته.

فصل ۵

کران‌هایی روی کدها

۵.۱ مقدمه؛ کران گیلبرت

در این فصل، علاقه‌مند به کدهایی خواهیم بود که با فرض داشتن طول و کمترین—فاصله مشخص، تا حد امکان دارای تعداد زیادی کدکلمه باشند. علاقه ما به سوالاتی همچون بی‌فایده بودن در عمل یا کدگذاری و کدگشایی چنین کدهایی نخواهد بود. مجدداً به‌عنوان الفبا مجموعه Q با q سمبل را درنظر گرفته و تعریف می‌کنیم $\theta := (q-۱)/q$. نمادگذاری در اینجا همانند بخش ۳.۱ است. فرض می‌کنیم q انتخاب شده است و سپس یک کد $(n, *, d)$ را به‌صورت کدی با طول n و کمترین—فاصله d تعریف می‌کنیم. ما علاقه‌مند به بیشترین تعداد کدکلمه، یعنی بزرگ‌ترین M که بتواند در مکان $*$ قرار گیرد، هستیم. یک کد (n, M, d) که مشمول در هیچ کد $(n, M+۱, d)$ نباشد، ماکسیمال نامیده می‌شود.

تعریف ۱.۵.۱. {یک کد (n, M, d) موجود باشد.} $A(n, d) := \max\{M \mid$ کد C به‌طوری که $|c| = A(n, d)$، بهینه[۱] نامیده می‌شود.

برخی از مولفین، جمله "بهینه" را برای کدهای $[n, k]$ با $d = n - k + ۱$ به‌کار می‌برند (مساله ۲.۳.۸ را ببینید). چنین کدهایی بنابر تعریف ۱.۵.۱ (با ۱.۵.۲ مقایسه کنید) بهینه هستند. معمولاً کدهای $[n, k, n-k+۱]$، کدهای تفکیک‌پذیر با بیشترین فاصله[۲] (کدهای MDS) نامیده می‌شوند.

---

[۱] optimal

[۲] maximum distance separable codes

مطالعه اعداد $A(n,d)$ به‌عنوان مساله‌ای اساسی در نظریه ترکیبیاتی کدگذاری درنظر گرفته شده است. در فصل ۲، آموختیم که کدهای خوب طولانی هستند، یا به‌طور دقیق‌تر، برای یک کانال با احتمال خطای خاص p، می‌توانیم احتمال خطا را با مشاهده دنباله‌ای از کدها با افزایش طول n، کاهش داد. به‌وضوح، تعداد متوسط خطای یک کلمه دریافتی برابر با np است؛ بنابراین، اگر می‌خواهیم این خطاها را تصحیح کنیم، باید d را حداقل با سرعت $۲np$ افزایش دهیم. این مطلب، اهمیت عدد $\alpha(\delta)$ که به‌صورت زیر تعریف می‌شود، روشن می‌سازد.

تعریف ۲.۵.۱.

$$\alpha(\delta) := \limsup_{n\to\infty} n^{-۱} \log_q A(n, \delta n).$$

در فصل ۲ کدهای خوب با نرخ داده شده R را مطالعه نمودیم. در این حالت، باید سوال کنیم که d/n تا چه حد می‌تواند بزرگ باشد (به‌عنوان تابعی از n). از تعریف ۲.۵.۱ دیده می‌شود که ما به معکوس تابع α علاقه‌مند هستیم.

توابع A و α در حالت کلی شناخته شده نمی‌باشند. در اینجا به بررسی کران‌های بالایی و پایینی برای هردوی آنها پرداخته و مقادیر خاص $A(n,d)$ را بررسی خواهیم نمود. تکنیک‌های گسترش دادن، کوتاه‌نمودن یا پنچرکردن (بخش ۴.۴ را ببینید) اغلب مفید خواهند بود. این مطالب فوراً قضیه زیر را نتیجه می‌دهند:

قضیه ۳.۵.۱. برای کدهای دوتایی داریم:

$$A(n, ۲l-۱) = A(n+۱, ۲l)$$

به خواننده، تعریف گوی $B_r(x)$ در بخش ۳.۱ را یادآوری می‌کنیم و تعریف می‌کنیم:

$$V_q(n,r) := |\, B_r(x) \,| = \sum_{i=۰}^{r} \binom{n}{i} (q-۱)^i. \qquad (۱)$$

(با شرط ۶.۳.۱ مقایسه کنید).

به منظور مطالعه تابع α، نیاز به توسیعی از تابع آنتروپی تعریف شده توسط ۴.۱.۴ را داریم. تابع آنتروپی H_p روی $[۰,\theta]$، که $\theta := (q-۱)/q$، به‌صورت:

$$H_q(۰) := ۰,$$

$$H_q(x) := x\log_q(q-۱) - x\log_q x - (۱-x)\log_q(۱-x), \qquad \text{برای } ۰ < x \le \theta \qquad (۲)$$

تعریف می‌شود. دقت کنید که $H_q(x)$ وقتی x از ۰ تا θ تغییر می‌کند، از ۰ تا ۱ افزایش می‌یابد.

لم ۴.۵.۱. فرض کنید $0 \leq \lambda \leq \theta$ و $q \geq 2$. در این صورت:

$$\lim_{n\to\infty} n^{-1} \log_q V_q(n, \lfloor \lambda n \rfloor) = H_q(\lambda).$$

اثبات. برای $r = \lfloor \lambda n \rfloor$، جمله آخر مجموع طرف راست ۱، بزرگ‌ترین است؛ بنابراین:

$$\binom{n}{\lfloor \lambda n \rfloor}(q-1)^{\lfloor \lambda n \rfloor} \leq V_q(n, \lfloor \lambda n \rfloor) \leq (1 + \lfloor \lambda n \rfloor)\binom{n}{\lfloor \lambda n \rfloor}(q-1)^{\lfloor \lambda n \rfloor}.$$

با گرفتن لگاریتم، تقسیم بر n و سپس پیش رفتن همانند اثبات قضیه ۵.۱.۴، نتیجه حاصل می‌گردد. □

برای پایان دادن به این بخش، یک کران پایینی برای $A(n,d)$ و کران متناظر برای $\alpha(\delta)$ را مطرح خواهیم نمود. اگرچه این نتیجه تقریباً واضح است، مدت‌های طولانی تصور می‌شد که $\alpha(\delta)$ می‌تواند با این کران پایین برابر باشد. در سال ۱۹۸۲، فسمن[۳]، ولادوت[۴] و زینک[۵] [۸۱] این کران پایینی را (برای $q \geq 49$) با استفاده از هندسه جبری بهبود بخشیدند.

قضیه ۵.۵.۱ برای $n \in \mathbb{N}$، $d \in \mathbb{N}$ و $d \leq n$، داریم:

$$A(n,d) \geq q^n / V_q(n, d-1).$$

اثبات. فرض کنید کد C به‌عنوان یک کد (n, M, d) ماکسیمال باشد. این مطلب باعث می‌شود تا کلمه‌ای در Q^n با فاصله حداقل d با تمامی کلمات C وجود داشته باشد. به عبارت دیگر؛ گوی‌های $B_{d-1}(\mathbf{c})$ با $\mathbf{c} \in C$، فضای Q^n را می‌پوشانند؛ بنابراین، مجموع "حجم‌های" آنان، یعنی $|c|V_q(n, d-1)$، متجاوز از $q^n = |Q|^n$ است. □

این اثبات نشان می‌دهد که کدی که حداقل دارای $q^n/V_q(n,d-1)$ کدکلمه است، می‌تواند به سادگی با شروع از هر کلمه $\mathbf{c}_0$ و سپس به‌طور متوالی اضافه نمودن کلمات جدیدی که دارای فاصله حداقل d با کلماتی که از قبل انتخاب شده‌اند تا رسیدن به کد ماکسیمال، ساخته شود. چنین کدی دارای هیچ ساختاری نمی‌باشد. با کمال تعجب، شرط لازم برای این‌که C خطی باشد، همان‌طور که قضیه زیر نشان می‌دهد، یک محدودیت اساسی نمی‌باشد.

---

[۳] Tsfasman
[۴] Vlăduţ
[۵] Zink

قضیه ۶.۵.۱. اگر $n, d, k \in \mathbb{N}$ در رابطه $V_q(n, d-1) \leq q^{n-k+1}$ صدق کنند، آن‌گاه یک کد $[n, k, d]$ وجود دارد.

اثبات. برای $k = 0$ این مطلب بدیهی است. فرض کنید C_{k-1} یک کد $[n, k-1, d]$ باشد. چون $|c_{k-1}| V_q(n, d-1) < q^n$، این کد ماکسیمال نمی‌باشد؛ بنابراین، کلمه $x \in Q^n$ با فاصله بیشتر یا مساوی d نسبت به تمامی کلمات C_{k-1} وجود دارد. فرض کنید C_k کد تولید شده توسط C_{k-1} و $\{x\}$ باشد. فرض کنید $\mathbf{z} = ax + y$ (که در آن $0 \neq a \in Q, y \in C_{k-1}$) یک کدکلمه در C_k باشد؛ در این‌صورت:

$$w(\mathbf{z}) = w(a^{-1}\mathbf{z}) = w(x + a^{-1}y) = d(x, -a^{-1}y) \geq d.$$

□

کدهای موجود در مساله ۱۴.۳.۸ مثالی از قضیه ۶.۵.۱ می‌باشند.

مثال ۷.۵.۱. فرض کنید $q = 2$، $n = 13$ و $d = 5$؛ بنابراین، از رابطه ۱ داریم $V_2(13, 4) = 1093$ و از این‌رو $A(13, 5) \geq \lfloor 8192/1093 \rfloor = 8$. درواقع قضیه ۶.۵.۱ وجود یک کد $[13, 3, 5]$ را ضمانت می‌کند. به‌وضوح، این، یک کد خیلی خوب نمی‌باشد؛ زیرا با استفاده از قضیه ۷.۴.۵، سه‌بار پنچرکردن $\mathcal{R}(1, 4)$ یک کد $[13, 5, 5]$ را به‌دست می‌دهد و درواقع کد Y از بخش ۴.۴ حتی از یک کد غیرخطی بهتر است؛ یعنی از یک کد $(13, 64, 5)$. این مثال یک روش را برای یافتن کران‌هایی روی $A(n, d)$ نشان می‌دهد؛ یعنی با استفاده از ساختن کدهای خوب. می‌دانیم که $A(13, 5) \geq 64$.

کران موجود در قضیه ۵.۵.۱ به کران گیلبرت[۶] (یا کران گیلبرت—ورشامو[۷]) معروف است. حال بیایید نگاهی به کران متناظر برای α بیندازیم.

قضیه ۸.۵.۱ (کران گیلبرت مجانبی[۸]). اگر $0 \leq \delta\theta$، آن‌گاه:

$$\alpha(\delta) \geq 1 - H_q(\delta).$$

اثبات. با استفاده از روابط ۵.۵.۱ و ۴.۵.۱ داریم:

$$\begin{aligned} \alpha(\delta) &= \limsup_{n\to\infty} n^{-1} \log_q A(n, \delta n) \geq \lim_{n\to\infty} \{1 - n^{-1} \log_q V_q(n, \delta n)\} \\ &= 1 - H_q(\delta) \end{aligned}$$

□

[۶] Gilbert bound
[۷] Varshamov
[۸] Asymptotic Gilbert Bound

۵.۲ کران‌های بالایی

در این بخش، تعدادی از کران‌های بالایی برای $A(n,d)$ را مطرح می‌کنیم که به‌حق به‌دست آوردن آنها آسان می‌باشد. در دهه ۱۹۷۰، روش‌های پیچیده‌تری کران‌های بهتری را تولید نمودند که ما آنها را در بخش ۵.۳ مورد بررسی قرار می‌دهیم.

با پنچرکردن یک کد (n,M,d) به‌اندازه $d-1$ بار، یک کد $(n-d+1,M,1)$ به‌دست می‌آید؛ یعنی M کلمه پنچرشده متمایز می‌باشند. بنابراین، $M \leq q^{n-d+1}$. از این‌رو قضیه زیر را که به کران سینگلتون[۹] معروف است، ثابت نموده‌ایم.

قضیه ۱.۵.۲. برای $q,n,d \in \mathbb{N}$ و $q \geq 2$ داریم:

$$A(n,d) \leq q^{n-d+1}.$$

نتیجه‌گیری ۱.۵.۲ برای یک کد $[n,k]$ روی $\mathbb{F}_q$ داریم $k \leq n-d+1$.

کدی که به این کران دست یابد را یک کد MDS می‌نامیم (مساله ۲.۳.۸ را ببینید).

مثال ۲.۵.۲. فرض کنید $q=2$، $n=13$ و $d=5$؛ در این‌صورت داریم $A(13,5) \leq 512$.

فرم مجانبی قضیه ۱.۵.۲ به‌صورت زیر است.

قضیه ۳.۵.۲. برای $0 \leq \delta \leq 1$ داریم $\alpha(\delta) \leq 1-\delta$.

کران بعدی، با محاسبه بیشترین مقدار ممکن از فاصله متوسط بین دو کدکلمهٔ متفاوت حاصل می‌گردد. فرض کنید C یک کد (n,M,d) باشد. لیستی از کلمات C را می‌سازیم. یک ستون از این لیست را درنظر بگیرید. فرض کنید jامین سمبل Q، m_jبار، $0 \leq j \leq q-1$، در این ستون رخ دهد. سهم این ستون در مجموع فاصله تمامیِ زوج کدکلماتِ متفاوت، برابر با $\sum_{j=0}^{q-1} m_j(M-m_j)$ است. چون $\sum_{j=0}^{q-1} = M$، از نامساوی کشی–شوارتز داریم:

$$\sum_{j=0}^{q-1} m_j(M-m_j) = M^2 - \sum_{j=0}^{q-1} m_j^2 \leq M^2 - q^{-1}(\sum_{j=0}^{q-1} m_j)^2 = \theta M^2.$$

چون لیست ما n ستون دارد و چون $M(M-1)$ زوج مرتب از کدکلمات وجود دارند، داریم:

$$M(M-1)d \leq n\theta M^2.$$

در اینجا ما کران معروف پلاتکین[۱۰] را اثبات نموده‌ایم.

[۹] Singleton bound

[۱۰] Plotkin

قضیه ۴.۵.۲. برای $q \geq ۲$، $q, n, d \in \mathbb{N}$ و $\theta = ۱ - q^{-۱}$ داریم:

$$A(n,d) \leq \frac{d}{d-\theta n}, \qquad \text{اگر } d > \theta n .$$

مثال ۵.۵.۲

۱) فرض کنید $q = ۲$، $n = ۱۳$ و $d = ۵$؛ در این‌صورت $\theta = \frac{۱}{۲}$. برای این‌که بتوانیم قضیه ۴.۵.۲ را به‌کار گیریم، کد $(۱۳, M, ۵)$ را درنظر بگیرید و آن‌را چهار بار کوتاه نمایید تا یک کد $(۹, M', ۵)$ با $M' \geq ۲^{-۴} M$ حاصل گردد. با استفاده از کران پلاتکین داریم $M' \leq ۵/(۵ - ۴\frac{۱}{۲}) = ۱۰$؛ بنابراین، $M \leq ۱۶۰$؛ یعنی $A(۱۳, ۵) \leq ۱۶۰$. یک کران بهتر می‌تواند به این‌صورت به‌دست آید که در ابتدا از قضیه ۳.۵.۱ استفاده نموده تا به‌دست آوریم $A(۱۳, ۵) = A(۱۴, ۶)$ و سپس استدلال فوق را تکرار نموده تا به‌دست آوریم $A(۱۴, ۶) \leq ۲^۳ \cdot ۶/(۶ - ۵\frac{۱}{۲}) = ۹۶$.

۲) قرار دهید $q = ۳$، $n = ۱۳$ و $d = ۹$؛ در این‌صورت $\theta = \frac{۲}{۳}$ و کران پلاتکین باعث می‌گردد تا برای کدهای سه‌تایی داشته باشیم $A(۱۳, ۹) \leq ۲۷$. دوگان کد همینگ سه‌تایی را درنظر بگیرید (تعریف ۱.۳.۳ را ببینید). این کد دارای ماتریس مولد زیر است:

$$G = \begin{pmatrix} ۰ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۱ & ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۲ & ۲ & ۲ \\ ۱ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ & ۰ & ۱ & ۲ \end{pmatrix}.$$

ستون‌های این ماتریس، نقاط $PG(۲, ۳)$ هستند. این مکان‌ها، که در آن $G(a_۱, a_۲, a_۳)$ دارای یک صفر می‌باشد، متناظر با نقاط $PG(۲, ۳)$ بر روی خط تصویری با معادله $a_۱x_۱ + a_۲x_۲ + a_۳x_۳ = ۰$ هستند؛ یعنی اگر $\mathbf{a} \neq \mathbf{0}$، آن‌گاه دقیقاً چهار تا از این موقعیت‌ها وجود دارد؛ بنابراین، هر کدکلمه مخالف با صفر دارای وزن ۹ می‌باشد. از این‌رو این یک کد خطی است که در قضیه ۴.۵.۲ و درحالت تساوی صدق می‌کند.

از اثبات قضیه ۴.۵.۲ می‌توان دید که تساوی تنها زمانی امکان‌پذیر است که تمامی زوج کدکلمات متمایز درواقع دارای فاصله یکسان باشند. چنین کدی یک کد هم‌فاصله[۱۱] نامیده می‌شود.

ما مجدداً یک نتیجه مجانبی را نتیجه می‌گیریم.

قضیه ۶.۵.۲. (کران پلاتکین مجانبی)؛ داریم:

$$\alpha(\delta) = ۰, \qquad \text{اگر } \theta \leq \delta \leq ۱,$$
$$\alpha(\delta) \leq ۱ - \delta/\theta, \quad \text{اگر } ۰ \leq \delta < \theta.$$

[۱۱] equidistant

اثبات. اولین ادعا نتیجه‌ای بدیهی از قضیه ۴.۵.۲ است. برای دومین ادعا، تعریف می‌کنیم $n' := \lfloor (d-1)/\theta \rfloor$؛ بنابراین، $1 \leq d - \theta n' \leq 1 + \theta$. یک کد (n, M, d) را تا رسیدن به یک کد (n', M', d)، کوتاه کنید؛ در این‌صورت $M' \geq q^{n'-n} M$ و به‌وسیله قضیه ۴.۵.۲ داریم $M' \leq d/(d - \theta n') \leq d$؛ بنابراین، $M \leq dq^{n-n'}$. از این مطلب و این‌که $n'/n \to \delta/\theta$ اگر $n \to \infty$ و نیز $d = \delta n$ داریم $\alpha(\delta) \leq 1 - \delta/\theta$. □

کران پایین که توسط گریسمر[۱۲] (۱۹۶۰) پیدا شده است، کرانی برای کدهای خطی است که به‌طور مجانبی هم‌ارز با کران پلاتکین می‌باشد، اما در برخی حالات از آن بهتر است. اگرچه اثبات مقدماتی است، ثابت می‌شود که اغلب این کران اکید می‌باشد. اثبات برپایه ایده‌هایی یکسان با روش هلگرت و استیناف است که در بخش ۴.۴ به آن پرداخته شد. فرض کنید G ماتریس مولد یک کد $[n, k, d]$ باشد. ممکن است فرض کنیم که اولین سطر G دارای وزن d است، درواقع ممکن است فرض کنیم این سطر به‌صورت $(11\cdots10\cdots0)$ با d تا ۱ است. هر سطر دیگر، حداقل دارای $\lceil d/q \rceil$ مولفه در اولین d مکان است که یکسان می‌باشند؛ بنابراین، کد باقی‌مانده نسبت به اولین سطر، یک کد $[n-d, k-1, d']$ با $d' \geq \lceil d/q \rceil$ است؛ در این‌صورت با به‌کارگیری استقرا، قضیه زیر را داریم.

قضیه ۷.۵.۲. (کران گریسمر). برای یک کد $[n, k, d]$ روی $\mathbb{F}_q$ داریم:

$$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

مثال ۸.۵.۲

۱) فرض کنید $q = 2$، $n = 13$ و $d = 5$. چون $\sum_{i=0}^{5} \lceil 5/2^i \rceil = 13$ می‌بینیم که در یک کد $[13, k, 5]$ باید $k \leq 6$. کد Y در بخش ۴.۴ دارای ۶۴ کلمه است اما، خطی نیست. درواقع، یک کد $[13, 6, 5]$ نمی‌تواند وجود داشته باشد؛ چراکه آن، وجود یک کد $[12, 5, 5]$ را نتیجه می‌دهد که با تجزیه و تحلیلی که در بخش ۴.۴ آورده شد، در تناقض است؛ بنابراین، در این حالت، کران گریسمر اکید نمی‌باشد.

۲) فرض کنید $q = 3$، $n = 14$ و $d = 9$. از $\sum_{i=0}^{3} \lceil 9/3^i \rceil = 14$ نتیجه می‌شود که در یک کد $[14, k, 9]$ سه‌تایی داریم $k \leq 4$. یک نسخه کوتاه‌شده از چنین کدی، باید شبیه مثال (۲) بعد از قضیه ۴.۵.۲ باشد. فرض کنید چنین کدی موجود باشد. مانند قبل می‌توانیم فرض کنیم

[۱۲] J. H. Griesmer

$(۰۰۰۰۰۰ ۰۰۰ ۱۱)$ دارای وزن ۹ در اولین سطر ماتریس مولد است؛ بنابراین، مشابه اثبات کران گریسمر، کد باقی‌مانده یک کد $[۵, ۳, ۳]$ سه‌تایی می‌باشد. ماتریس مولد چنین کدی به‌صورت زیر است:

$$G = \begin{pmatrix} ۱ & ۰ & ۰ & ۱ & ۱ \\ ۰ & ۱ & ۰ & a & b \\ ۰ & ۰ & ۱ & c & d \end{pmatrix},$$

که در آن a, b, c, d صفر نمی‌باشند. به‌وضوح، $a \neq b$ و $c \neq d$؛ بنابراین، ترکیبی از سطرهای ۲ و ۳ با وزن ۲ وجود دارد که یک تناقض است. مجدداً کران گریسمر اکید نمی‌باشد.

یکی از آسان‌ترین کران‌ها، تعمیم شرط ۶.۳.۱ است که به کران هامینگ یا کران گوی پوششی[۱۳] معروف است.

قضیه ۹.۵.۲. اگر $q, n, e \in \mathbb{N}$، $q \geq ۲$ و $d = ۲e + ۱$، آن‌گاه:

$$A(n, d) \leq q^n / V_q(n, e).$$

اثبات. گوی‌های $B_e(\mathbf{c})$ که در آن $\mathbf{c}$ متعلق به یک کد $(n, M, ۲e + ۱)$ است، مجزا می‌باشند؛ بنابراین، $M \cdot V_q(n, e) \leq q^n$. □

مثال ۱۰.۵.۲. فرض کنید $q = ۲$، $n = ۱۳$ و $d = ۵$؛ در این‌صورت از:

$$V_۲(۱۳, ۲) = ۱ + ۱۳ + ۷۸ = ۹۲,$$

داریم $A(۱۳, ۵) \leq \lfloor ۲^{۱۳}/۹۲ \rfloor = ۸۹$.

یک کد کامل را به این صورت تعریف کرده‌ایم که در تساوی رابطه ۹.۵.۲ صدق کند. در فصل ۷ به این سوال باز می‌گردیم.

قضیه ۱۱.۵.۲. (کران هامینگ مجانبی) داریم:

$$\alpha(\delta) \leq ۱ - H_q(\frac{۱}{۲}\delta).$$

[۱۳] sphere packing bound

اثبات. $A(n, \lceil \delta n \rceil) \leq A(n, ۲\lceil \frac{۱}{۲}\delta n \rceil - ۱) \leq q^n / V_q(n, \lceil \frac{۱}{۲}\delta n \rceil - ۱)$. پس نتیجه از لم ۴.۵.۱ حاصل می‌شود. □

حال به سراغ یک کران بالایی می‌آییم که تاحدی اثبات آن مشکل‌تر است. برای مدت‌های طولانی، این کران بهترین کران بالایی محسوب می‌شد. از اثبات کران پلاتکین، واضح است که اگر فاصله بین تمامی کدکلمات به فاصله میانگین نزدیک نباشد، آن‌گاه این کران نمی‌تواند خوب باشد. ایده زیر، توسط الیاس[۱۴] نتیجه‌ای قوی‌تر را ارائه می‌دهد. روند اثبات کران پلاتکین را برای مجموعه‌ای از کدکلمات که به‌طور مناسب در گوی‌هایی در Q^n انتخاب شده‌اند، ادامه دهید. لم زیر نشان می‌دهد که چگونه می‌توان گوی‌ها را اختیار نمود. قرار می‌دهیم $Q = \mathbb{Z}/q\mathbb{Z}$.

لم ۱۲.۵.۲. اگر A و C زیرمجموعه‌ای از Q^n باشند، آن‌گاه یک $x \in Q^n$ وجود دارد به‌طوری که:

$$\frac{|\,(x + A) \cap c|}{|\,A\,|} \geq \frac{|c|}{q^n}.$$

اثبات. $x_۰$ را طوری انتخاب کنید که $|\,(x_۰ + A) \cap c|$ ماکسیمال باشد؛ در این‌صورت:

$$\begin{aligned} |\,(x_۰ + A) \cap c| &\geq q^{-n} \sum_{x \in Q^n} |\,(x + A) \cap c| \\ &= q^{-n} \sum_{x \in Q^n} \sum_{\mathbf{a} \in A} \sum_{\mathbf{c} \in C} |\,\{x + a\} \cap \{\mathbf{c}\}\,| \\ &= q^{-n} \sum_{\mathbf{a} \in A} \sum_{\mathbf{c} \in C} \mathbf{1} = q^{-n}\,|\,A\,| \cdot |c|. \end{aligned}$$

□

حال فرض کنید C یک کد (n, M, d) و A همان $B_r(۰)$ باشد. بدون از دست دادن کلیت، فرض کنیم که نقطه $x_۰$ از این لم برابر با صفر باشد. کد $A \cap C$ را درنظر بگیرید. این یک کد (n, K, d) با $K \geq MV_q(n, r)/q^n$ است. کلمات این کد را به‌عنوان سطرهای یک ماتریس K در n لیست می‌کنیم. فرض کنید m_{ij} تعداد وقوع سمبل j در ستون iام این ماتریس باشد. می‌دانیم:

۱) $\sum_{j=۰}^{q-۱} m_{ij} = K$.

۲) $\sum_{i=۱}^{n} m_{i۰} := S \geq K(n - r)$؛ زیرا هر سطر این ماتریس دارای وزن حداکثر r است؛ بنابراین:

[۱۴] P. Elias

۳) $\sum_{j=1}^{q-1} m_{ij}^2 \geq (q-1)^{-1}(\sum_{j=1}^{q-1} m_{ij})^2 = (q-1)^{-1}(K-m_{i0})^2$.

۴) $\sum_{i=1}^{n} m_{i0}^2 \geq n^{-1}(\sum_{i=1}^{n} m_{i0})^2 = n^{-1}S^2$.

مجدداً مجموع فاصله‌های تمامی زوج مرتب‌های سطرهای این ماتریس را محاسبه می‌کنیم. با توجه به روابط (۱) تا (۴) داریم:

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=0}^{q-1} m_{ij}(K-m_{ij}) &= nK^2 - \sum_{i=1}^{n}(m_{i0}^2 + \sum_{j=1}^{q-1} m_{ij}^2) \\ &\leq nK^2 - (q-1)^{-1}\sum_{i=1}^{n}(qm_{i0}^2 + K^2 - 2Km_{i0}) \\ &\leq nK^2 - (q-1)^{-1}(qn^{-1}S^2 + nK^2 - 2KS).\end{aligned}$$

در این نامساوی، $S \geq K(n-r)$ را جانشین می‌کنیم که در آن $r \leq \theta n$ حذف شده است. اکنون به‌دست می‌آوریم $S \geq q^{-1}nK$؛ داریم $\sum_{i=1}^{n}\sum_{j=0}^{q-1} m_{ij}(K-m_{ij}) \leq K^2 r(2-(r/\theta n))$. چون تعداد زوج‌های منتخب از سطرها برابر با $K(K-1)$ است، داریم:

$$K(K-1)d \leq K^2 r(2 - r\theta^{-1}n^{-1}).$$

بنابراین، لم زیر را اثبات نموده‌ایم.

لم ۱۳.۵.۲. اگر همه کلمات یک کد (n, K, d) دارای وزن کمتر یا مساوی r باشند که در آن $r \leq \theta n$، آن گاه:

$$d \leq \frac{Kr}{K-1}(2 - \frac{r}{\theta n}).$$

قضیه ۱۴.۵.۲. (کران الیاس). فرض کنید $q, n, d, r \in \mathbb{N}$، $q \geq 2$، $\theta = 1 - q^{-1}$، $r \leq \theta n$ و $r^2 - 2\theta nr + \theta nd > 0$؛ در این‌صورت:

$$A(n,d) \leq \frac{\theta nd}{r^2 - 2\theta nr + \theta nd} \cdot \frac{q^n}{V_q(n,r)}.$$

اثبات. از لم ۱۲.۵.۲ می‌بینیم که یک کد (n, M, d) دارای زیرکدی با $K \geq MV_q(n,r)/q^n$ کلمه است که همه آنها در یک گوی $B_r(x)$ هستند؛ بنابراین، ممکن است لم ۱۳.۵.۲ را به‌کار بریم که این نتیجه می‌دهد:

$$q^{-n}MV_q(n,r) \leq K \leq \frac{\theta nd}{r^2 - 2\theta nr + \theta nd}.$$

□

دقت کنید که $r = \theta n$، $d > \theta n$ کران پلاتکین را نتیجه می‌دهد.

مثال ۱۵.۵.۲. فرض کنید $q = 2$، $n = 13$ و $d = 5$؛ بنابراین، $\theta = \frac{1}{4}$. اگر ما $A(14,6)$ در رابطه ۱۴.۵.۲ را تخمین بزنیم، آن‌گاه بهترین نتیجه به‌دست می‌آید که به صورت زیر است:

$$A(13,5) = A(14,6) \leq \frac{42}{r^2 - 14r + 42} \cdot \frac{2^{14}}{\sum_{i \leq r} \binom{14}{i}}$$

و بنابراین، بهترین انتخاب برابر با $r = 3$ است که نتیجه می‌دهد $A(13,5) \leq 162$.

نتیجه حاصل در این مثال به اندازه تخمین‌های اخیر خوب نیست. اما، به‌طور مجانبی کران الیاس بهترین نتیجه از این بخش است.

قضیه ۱۶.۵.۲. (کران الیاس مجانبی)؛ داریم:

$$\alpha(\delta) \leq 1 - H_q(\theta - \sqrt{\theta(\theta-\delta)}), \quad 0 \leq \delta \leq \theta \text{ اگر},$$

$$\alpha(\delta) = 0, \qquad \theta \leq \delta < 1 \text{ اگر}.$$

اثبات. قسمت دوم از قضیه ۶.۵.۲ نتیجه می‌شود؛ بنابراین، قرار دهید $0 < \delta \leq \theta$. مقدار $0 \leq \lambda < \theta - \sqrt{\theta(\theta-\delta)}$ را اختیار نموده و قرار دهید $r = \lfloor \lambda n \rfloor$؛ بنابراین، $\theta\delta - 2\theta\lambda + \lambda^2 > 0$. از قضیه ۱۴.۵.۲، برای $d = \lfloor \delta n \rfloor$ داریم:

$$\begin{aligned} n^{-1} \log_q A(n, \delta n) &\leq n^{-1} \log_q \left(\frac{\theta nd}{r^2 - 2\theta nr + \theta nd} \cdot \frac{q^n}{V_q(n,r)}\right) \\ &\sim n^{-1}\{\log_q \left(\frac{\theta\delta}{\lambda^2 - 2\theta\lambda + \theta\delta}\right) + n - nH_q(\lambda)\} \\ &\sim 1 - H_q(\lambda), \qquad (n \to \infty). \end{aligned}$$

بنابراین، $\alpha(\delta) \leq 1 - H_q(\lambda)$. چون این رابطه برای هر λ که $\lambda < \theta - \sqrt{\theta(\theta-\delta)}$ برقرار است، نتیجه حاصل می‌گردد. □

کران بعدی نیز بر پایه ایدهٔ مشاهده زیرمجموعه‌ای از کدکلمات است. دراین حالت، کدکلمات با یک وزن ثابت w را درنظر می‌گیریم.

درابتدا باید تعدادهای معینی را مطالعه کنیم که مشابه با $A(n,d)$ هستند. خود را به حالت $q=۲$ محدود می‌کنیم.

تعریف ۱۷.۵.۲. بیشترین تعداد کدکلمات یک کد دوتایی به‌طول n و کمترین —فاصله بزرگ‌تر یا مساوی d، به‌طوری که تمامی کدکلمات دارای وزن d باشند را با $A(n,d,w)$ نمایش می‌دهیم.

لم ۱۸.۵.۲. داریم:

$$A(n,۲k-۱,w)=A(n,۲k,w)\leq \lfloor \frac{n}{w}\lfloor \frac{n-۱}{w-۱}\lfloor \cdots \lfloor \frac{n-w+k}{k}\rfloor \cdots \rfloor \rfloor \rfloor .$$

اثبات. کلمات با وزن یکسان، دارای فاصله زوج $A(n,۲k-۱,w)=A(n,۲k,w)$ می‌باشند. فرض کنید کد C با $|c|=K$ صادق در شرایط ما باشد. کلمات C را به‌عنوان سطرهای یک ماتریس بنویسید. هر ستون این ماتریس دارای حداکثر $A(n-۱,۲k,w-۱)$ سمبل ۱ است؛ بنابراین، $Kw\leq nA(n-۱,۲k,w-۱)$؛ یعنی:

$$A(n,۲k,w)\leq \lfloor \frac{n}{w}A(n-۱,۲k,w-۱)\rfloor .$$

چون $A(n,۲k,k-۱)=۱$، نتیجه با استفاده از استقرا ثابت می‌شود. □

این لم نشان می‌دهد که چگونه اعداد $A(n,d,w)$ را می‌توان تخمین زد. این اعداد می‌توانند برای تخمین $A(n,d)$ به کار روند، آن‌چنان که در تعمیم زیر از کران همینگ به‌کار رفته‌اند، که به کران جانسون[۱۵] معروف است.

قضیه ۱۹.۵.۲. فرض کنید $q=۲$، $n,e\in\mathbb{N}$ و $d=۲e+۱$؛ در این‌صورت:

$$A(n,d)\leq \frac{۲^n}{\sum_{i=۰}^{e}\binom{n}{i}+\frac{\binom{n}{e+۱}-\binom{d}{e}A(n,d,d)}{\lfloor \frac{n}{e+۱}\rfloor}}$$

[۱۵] Johnson

اثبات. ایده اثبات مشابه اثبات کران همینگ است. فرض کنید N_{e+1} کلمه در $\{0,1\}^n$ وجود دارد که دارای فاصله $e+1$ تا کد C که یک کد (n,M,d) است، می‌باشند؛ بنابراین:

$$M\sum_{i=0}^{e}\binom{n}{i}+N_{e+1}\leq 2^n.$$

به‌منظور تخمین N_{e+1}، کدکلمه دلخواه $\mathbf{c}$ را درنظر می‌گیریم که می‌توانیم آن را صفر قرار دهیم (بدون از دست دادن کلیت)؛ بنابراین، آشکارا دیده می‌شود که تعداد کدکلمات C با وزن d حداکثر $A(n,d,d)$ است. هر یک از این کلمات دارای فاصله e تا $\binom{d}{e}$ کلمه به وزن $e+1$ است. چون $\binom{n}{e+1}$ کلمه با وزن $e+1$ وجود دارد، حداقل $\binom{n}{e+1}-\binom{d}{e}A(n,d,d)$ آنها دارای فاصله $e+1$ تا C می‌باشند. با تغییر دادن $\mathbf{c}$، $M\{\binom{n}{e+1}-\binom{d}{e}A(n,d,d)\}$ کلمه در $\{0,1\}^n$ را می‌شماریم که دارای فاصله $e+1$ تا کد مذکور هستند. هر یک از این کلمات چندبار شمارش شده‌اند؟ یکی از آنها را درنظر بگیرید؛ مجدداً آن‌را ۰ می‌نامیم. کدکلمات با فاصله $e+1$ تا ۰ دارای فاصله متقابل بزرگتر یا مساوی $2e+1$ هستند اگر و تنهااگر آنها دارای عناصر ۱ در مکان‌های متفاوت باشند؛ بنابراین، حداکثر $\lfloor n/(e+1)\rfloor$ از چنین کدکلماتی وجود دارد. این مطلب به ما تخمین موردنظر برای N_{e+1} را می‌دهد. □

از لم ۱۸.۵.۲، با درنظر گرفتن $k=e+1$ و $w=2e+1$، داریم:

$$\binom{d}{e}A(n,d,d)\leq\binom{n}{e}\lfloor\frac{n-e}{e+1}\rfloor.$$

با جانشینی در قضیه ۱۹.۵.۲، می‌توان نشان داد که کد C در رابطه زیر صدق می‌کند:

$$|c|\{\sum_{i=0}^{e}\binom{n}{i}+\frac{\binom{n}{e}}{\lfloor\frac{n}{e+1}\rfloor}(\frac{n-e}{e+1}-\lfloor\frac{n-e}{e+1}\rfloor)\}\leq 2^n, \qquad (3)$$

که شکل اصلی کران جانسون است.

مثال ۲۰.۵.۲. فرض کنید $q=2$، $n=13$ و $d=5$؛ یعنی $e=2$؛ در این‌صورت:

$$A(13,5,5)\leq\lfloor\frac{13}{5}\lfloor\frac{12}{4}\lfloor\frac{11}{3}\rfloor\rfloor\rfloor=23$$

و کران جانسون باعث می‌شود تا:

$$A(13,5)\leq\lfloor\frac{2^{13}}{1+13+78+\frac{286-10.23}{4}}\rfloor=77.$$

برای $n=13$، $q=2$ و $d=5$ این کران تاکنون بهترین بوده است. تنها، روش‌های موثر در بخش بعد برای تولید مقدار صحیح $A(13,5)$ کافی هستند.

۵.۳ کران برنامه‌ریزی خطی

بسیاری از بهترین کران‌ها برای اعداد $A(n,d)$ که تا به‌حال شناخته شده‌اند، بر پایه روشی هستند که توسط دلسارت[۱۶] (۱۹۷۳) توسعه داده شد. ایده کار، به‌دست آوردن نامساوی‌هایی بود که رابطه نزدیکی با نامساوی مک‌ویلیامز دارند (قضیه ۲.۳.۵) و سپس استفاده از تکنیک‌های برنامه‌ریزی برای تجزیه و تحلیل این نامساوی‌ها. در این بخش، مجبور خواهیم بود که به‌شدت به خواص چندجمله‌ای‌های کراچوک تکیه کنیم.

به‌منظور اجتناب از نمادگذاری‌های پرزحمت، فرض می‌کنیم که q و n انتخاب شده و ثابت هستند. سپس تعریف می‌کنیم:

$$K_k(x) := \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j},$$

که در آن:

$$\binom{x}{j} := \frac{x(x-1)\cdots(x-j+1)}{j!}, \quad (x \in \mathbb{R})$$

برای بحث درباره این چندجمله‌ای‌ها و خواصی که به آن نیاز داریم، خواننده را به بخش ۱.۲ ارجاع می‌دهیم.

در ادامه، فرض می‌کنیم که الفبای Q همان حلقه $\mathbb{Z}/q\mathbb{Z}$ است؛ در این‌صورت، به‌طور معمول، $< x, y >$ نمایش ضرب داخلی $\sum_{i=1}^{n} x_i y_i$ برای $x, y \in Q^n$ می‌باشد.

لم ۱.۵.۳. فرض کنید ω یک qامین ریشه واحد در $\mathbb{C}$ باشد و $x \in Q^n$ یک کلمه مشخص با وزن i باشد؛ در این صورت:

$$\sum_{\substack{y \in Q^n \\ w(y)=k}} \omega^{<x,y>} = K_k(i).$$

اثبات. ممکن است فرض کنیم $x = (x_1, x_2, \cdots, x_i, 0, 0, \cdots, 0)$ که در آن مختصات x_1 تا x_i برابر ۰ نمی‌باشد. k موقعیت را انتخاب کنید، h_1، h_2، $\cdots$، h_k؛ به‌طوری که $0 < h_1 < h_2 < \cdots < h_j \leq i < h_{j+1} < \cdots < h_k \leq n$. فرض کنید D مجموعه تمام کلمات (باوزن

[۱۶] P. Delsarte

k) باشد که مختصات ناصفر آنها در این مکان‌ها می‌باشد؛ در این‌صورت با استفاده از لم ۲۷.۱.۱ داریم:

$$\sum_{y\in D} w^{<x,y>} = \sum_{y_{h_1}\in Q\setminus\{0\}} \cdots \sum_{y_{h_k}\in Q\setminus\{0\}} w^{x_{h_1}y_{h_1}+\cdots+x_{h_k}y_{h_k}}$$

$$= (q-1)^{k-j}\prod_{l=1}^{j}\sum_{y\in Q\setminus\{0\}} w^{x_{h_i}y} = (-1)^j(q-1)^{k-j}.$$

چون به تعداد $\binom{i}{j}\binom{n-i}{k-j}$ انتخاب برای D وجود دارد، نتیجه حاصل می‌گردد. □

به منظور توانایی برای بررسی کدهای دلخواه، یعنی نه لزوماً خطی، تعریف ۱.۳.۵ را تعمیم می‌دهیم.

تعریف ۲.۵.۳. فرض کنید $C\subset Q^n$ کدی با M کدکلمه باشد؛ تعریف می‌کنیم:

$$A_i := M^{-1}\,|\{(x,y)\,|\,x\in C, y\in C, d(x,y)=i\}|\,.$$

دنباله $(A_i)_{i=0}^n$، توزیع فاصله[۱۷] یا توزیع داخلی[۱۸] C نامیده می‌شود.

دقت کنید که اگر C خطی‌پایا یا فاصله‌پایا باشد، آن‌گاه توزیع فاصله یک توزیع وزنی است.

لم زیر اساس کران برنامه‌ریزی خطی (قضیه ۴.۵.۳) می‌باشد.

لم ۳.۵.۳. فرض کنید $(A_i)_{i=0}^n$ توزیع فاصله یک کد $C\subseteq Q^n$ باشد؛ آن‌گاه:

$$\sum_{i=0}^{n} A_i K_k(i) \geq 0,$$

برای $k\in\{0,1,\cdots,n\}$.

اثبات. با توجه به لم ۱.۵.۳ داریم:

$$M\sum_{i=0}^{n} A_i K_k(i) = \sum_{i=0}^{n} \sum_{\substack{(x,y)\in C^2\\ d(x,y)=i}} \sum_{\substack{\mathbf{z}\in Q^n\\ w(\mathbf{z})=k}} w^{<x-y,z>}$$

$$= \sum_{\substack{\mathbf{z}\in Q^n\\ w(\mathbf{z})=k}} |\sum_{x\in C} w^{<x,y>}|^2 \geq 0.$$

□

[۱۷] distance distribution

[۱۸] inner distribution

قضیه ۴.۵.۳. فرض کنید $q \geq ۲$ و $q, n, d \in \mathbb{N}$؛ در این‌صورت:

$$A(n,d) \leq \max\{\sum_{i=۰}^{n} A_i \,|\, A_۰ = ۱, A_i = ۰ \quad ۱ \leq i < d \text{ برای},$$
$$A_i \geq ۰, \sum_{i=۰}^{n} A_i K_k(i) \geq ۰ \quad k \in \{۰, ۱, \cdots, n\} \text{ برای}\}.$$

اگر $q = ۲$ و d زوج باشد، آن‌گاه ممکن است برای iی زوج، فرض کنیم $A_i = ۰$.

اثبات. با به‌کارگیری لم ۳.۵.۳، توزیع فاصله یک کد (n, M, d) در نامساوی $\sum_{i=۰}^{n} A_i K_k(i) \geq ۰$ صدق می‌کند. به‌وضوح A_iها نامنفی هستند و $A_۰ = ۱$، $A_i = ۰$ برای $۱ \leq i < d$. علاوه‌براین با استفاده از لم ۳.۵.۳ داریم $\sum_{i=۰}^{n} A_i = M^{-۱}|c^{۲}| = M$. □

ادعای آخر در مساله ۶.۴.۸ آمده است.

مثال ۵.۵.۳. همانند چند مثال قبل، می‌خواهیم تا $A(۱۳,۵) = A(۱۴,۶)$ را برای $q = ۲$ تخمین بزنیم. برای توزیع فاصله یک کد $(۱۴, M, ۶)$، ممکن است فرض کنیم:

$$A_۰ = ۱, A_۱ = A_۲ = A_۳ = A_۴ = A_۵ = A_۷ = A_۹ = A_{۱۱} = A_{۱۳} = ۰,$$

$$A_۶ \geq ۰, A_۸ \geq ۰, A_{۱۰} \geq ۰, A_{۱۲} \geq ۰, A_{۱۴} \geq ۰.$$

برای اینها، نامساوی‌های زیر از لم ۳.۵.۳ را داریم (مقادیر $K_k(i)$ با به‌کارگیری رابطه ۱۴ یافت شده‌اند).

$$۱۴ + ۲A_۶ - ۲A_۸ - ۶A_{۱۰} - ۱۰A_{۱۲} - ۱۴A_{۱۴} \geq ۰;$$

$$۹۱ - ۵A_۶ - ۵A_۸ + ۱۱A_{۱۰} + ۴۳A_{۱۲} + ۹۱A_{۱۴} \geq ۰;$$

$$۳۶۴ - ۱۲A_۶ + ۱۲A_۸ + ۴A_{۱۰} - ۱۰۰A_{۱۲} - ۳۶۴A_{۱۴} \geq ۰;$$

$$۱۰۰۱ + ۹A_۶ + ۹A_۸ - ۳۹A_{۱۰} + ۱۲۱A_{۱۲} - ۱۰۰۱A_{۱۴} \geq ۰;$$

$$۲۰۰۲ + ۳۰A_۶ - ۳۰A_۸ + ۳۸A_{۱۰} - ۲۲A_{۱۲} - ۲۰۰۲A_{۱۴} \geq ۰;$$

$$۲۰۰۳ - ۵A_۶ - ۵A_۸ + ۲۷A_{۱۰} - ۱۶۵A_{۱۲} + ۳۰۰۳A_{۱۴} \geq ۰;$$

$$۳۴۳۲ - ۴۰A_۶ + ۴۰A_۸ - ۷۲A_{۱۰} + ۲۶۴A_{۱۲} - ۳۴۳۲A_{۱۴} \geq ۰.$$

حال باید یک کران بالا برای $M = ۱ + A_۶ + A_۸ + A_{۱۰} + A_{۱۲} + A_{۱۴}$ بیابیم. ثابت می‌شود که این

مساله برنامه‌ریزی خطی دارای جواب یکتاست؛ یعنی:

$$A_۶ = ۴۲, A_۸ = ۷, A_{۱۰} = ۱۴, A_{۱۲} = A_{۱۴} = ۰.$$

بنابراین، $M \leq ۶۴$. در بخش ۴.۴ یک کد $(۱۳, ۶۴, ۵)$ به نام Y را ساختیم؛ بنابراین، اینک ثابت نموده‌ایم که $A(۱۳, ۵) = ۶۴$.

حال قضیه ۴.۵.۳ را به‌صورت دیگری تبدیل می‌کنیم که نسبت به فرم اصلی، دارای مزیت‌هایی است. خوانندهٔ آشنا با برنامه‌ریزی خطی تصدیق می‌کند که ما داریم از قضیه دوگانگی[۱۹] استفاده می‌کنیم (ر.ک. مرجع [۳۲]).

قضیه ۶.۵.۳. فرض کنید $\beta(x) = ۱ + \sum_{k=۱}^{n} \beta_k K_k(x)$ یک چندجمله‌ای با $\beta_k \geq ۰$ $(۱ \leq k \leq n)$ باشد؛ به‌طوری که برای $j = d, d+۱, \cdots, n$ داریم $\beta(j) \leq ۰$؛ در این صورت $A(n, d) \leq \beta(۰)$.

اثبات. فرض کنید $A_۰, A_۱, \cdots, A_n$ در شرایط قضیه ۴.۵.۳ صدق کند؛ یعنی:

$$K_k(۰) + \sum_{i=d}^{n} A_i K_k(i) \geq ۰. \quad (k = ۰, ۱, \cdots, n; A_i \geq ۰, \quad i = d, d+۱, \cdots, n \text{ برای})$$

بنابراین، شرطی که روی β قرار دادیم، باعث می‌گردد تا $\sum_{i=d}^{n} A_i \beta(i) \leq ۰$؛ یعنی:

$$-\sum_{i=d}^{n} A_i \geq \sum_{k=۱}^{n} \sum_{i=d}^{n} A_i K_k(i) \geq -\sum_{k=۱}^{n} \beta_k K_k(۰) = ۱ - \beta(۰),$$

بنابراین:

$$۱ + \sum_{i=d}^{n} A_i \leq \beta(۰).$$

□

مزیت قضیه ۶.۵.۳ این است که هر چندجمله‌ای β صادق در شرایط قضیه، کرانی برای $A(n, d)$ را القا می‌کند که برای به‌دست آوردن این کران، باید در قضیه ۴.۵.۳ جواب بهینه برای دستگاه نامعادلات را یافت.

مثال ۷.۵.۳. فرض کنید $q = ۲$، $n = ۲l + ۱$ و $d = l + ۱$. سعی می‌کنیم تا کرانی برای $A(n, d)$ با درنظر گرفتن $\beta(x) = ۱ + \beta_۱ K_۱(x) + \beta_۲ K_۲(x) = ۱ + \beta_۱(n - ۲x) + \beta_۲(۲x^۲ - ۲nx + \frac{۱}{۲}n(n-۱))$ بیابیم. $\beta_۱$ و $\beta_۲$ را طوری انتخاب کنید که در آن $\beta(d) = \beta(n) = ۰$. داریم $\beta_۱ = (n+۱)/۲n$، $\beta_۲ = ۱/n$؛ بنابراین،

[۱۹] duality theorem

شرایط قضیه ۶.۵.۳ برقرار است؛ بنابراین، داریم $A(2l+1,l+1) \le \beta(0) = 1+\beta_1 n+\beta_2\binom{n}{2} = 2l+2$.
این مطلب، مشابه کران پلاتکین ۴.۵.۲ است.

بهترین کران برای $\alpha(\delta)$ که درحال حاضر مشهور است، توسط مک‌الیس، ردمیچ[۲۰]، رامسی[۲۱]، و ولچ[۲۲] (۱۹۷۷؛ مرجع [۵۰]) مطرح شده است. در اینجا این بهترین کران را مطرح نمی‌کنیم، اما یک نتیجه کمی ضعیف‌تر (که درواقع برای $\delta > 0.273$ برابر است) را که مجدداً توسط همین نویسندگان مطرح شده، ارائه می‌کنیم. اثبات آن بر پایه کاربردی از قضیه ۶.۵.۳ است.

قضیه ۸.۵.۳ فرض کنید $q = 2$؛ در این صورت:

$$\alpha(\delta) \le H_2(\frac{1}{2} - \sqrt{\delta(1-\delta)}).$$

اثبات. عدد صحیح t با شرط $1 \le t \le \frac{1}{2}n$ و عدد حقیقی a در بازه $[0,n]$ را درنظر می‌گیریم. چندجمله‌ای $\alpha(x)$ را به‌صورت زیر تعریف کنید:

$$\alpha(x) := (a-x)^{-1}\{K_t(a)K_{t+1}(x) - K_{t+1}(a)K_t(x)\}^2.$$

با به‌کارگیری رابطه ۱۶ از فصل ۱ داریم:

$$\alpha(x) = \frac{2}{t+1}\binom{n}{t}\{K_t(a)K_{t+1}(x) - K_{t+1}(a)K_t(x)\}\sum_{k=0}^{t}\frac{K_k(a)K_k(x)}{\binom{n}{k}}. \qquad (۴)$$

فرض کنید $\alpha(x) = \sum_{k=0}^{2t+1}\alpha_k K_k(x)$ توسیع کراچوک $\alpha(x)$ باشد. می‌خواهیم a و t را طوری بیابیم که $\beta(x) := \alpha(x)/\alpha_0$ در شرایط قضیه ۶.۵.۳ صدق کند. اگر قرار دهیم $a \le d$، آن‌گاه تنها چیزی که باید چک کنیم این است که آیا $\alpha_i \ge 0$ $(i = 1,\cdots,n)$، $a_0 > 0$. اگر $x_1^{(k)}$ نمایش کوچکترین صفر K_k باشد، آن‌گاه می‌دانیم که $0 < x_1^{(t+1)} < x_1^{(t)}$ (با رابطه ۱۷ از فصل ۱ مقایسه کنید).

به منظور ساده‌کردن محاسبات زیر، t را طوری انتخاب می‌کنیم که $x_1^{(t)} < d$ و a را مابین $x_1^{(t)}$ و $x_1^{(t+1)}$ طوری انتخاب می‌کنیم که $K_t(a) = -K_{l+1}(a) > 0$. نتیجه ۴ بیان می‌کند که $\alpha(x)$ به‌شکل $\sum_{c_{kl}} K_k(x)K_l(x)$ است؛ که در آن تمامی ضرایب c_{kl} ناصفر می‌باشند. از ۱۸ نتیجه می‌شود که تمامی α_i ناصفر می‌باشند. علاوه‌براین، $\alpha_0 = -[2/(t+1)] \times \binom{n}{t}K_t(a)K_{t+1}(a) > 0$. پس درحقیقت می‌توانیم

[۲۰] E. R. Rodemich
[۲۱] H. C .Rumsey
[۲۲] L. R. Welch

قضیه ۶.۵.۳ را به‌کار ببریم؛ داریم:

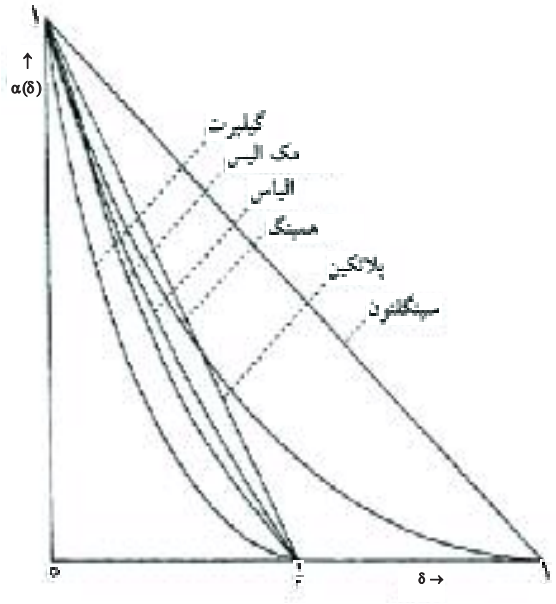
$$A(n,d) \le \beta(0) = \frac{\alpha(0)}{\alpha_0} = \frac{(n+1)^2}{2a(t+1)}\binom{n}{t}. \qquad (5)$$

برای تکمیل اثبات، نیاز داریم درباره مکان صفرهای $x_1^{(t)}$ مطالب بیشتری بدانیم. می‌توان دید که اگر $0 < \tau < \frac{1}{2}$، $n \to \infty$ و $t/n \to \tau$، آن‌گاه $x_1^{(t)}/n \to \frac{1}{2} - \sqrt{\tau(1-\tau)}$. در نتیجه می‌توانیم رابطه ۵ را برای $n \to \infty$، $d/n \to \delta$ با دنباله‌ای از مقادیر t که $t/n \to \frac{1}{2} - \sqrt{\delta(1-\delta)}$ به‌کار بگیریم. با گرفتن لگاریتم در رابطه ۵ و تقسیم بر n، ادعای قضیه به‌دست می‌آید (برای مشاهده اثبات حکمی درباره $x_1^{(t)}$ خواننده را به یکی از منابع درباره چندجمله‌ای‌های متعامد [۴۶] یا [۵۰] ارجاع می‌دهیم). □

۵.۴ پیشنهادها

برای مشاهده مطالبی درباره کدهای تعریف‌شده با استفاده از هندسه جبری و برای بهبود کران گیلبرت، به مرجع [۷۳] ارجاع می‌دهیم. برای نمونه بخش ۶.۸ را ببنید.

در شکل ۵.۱، کران‌های مجانبیِ به‌دست آمده در این بخش را مقایسه نموده‌ایم.



شکل ۵.۱: مقایسه برخی کران‌های مجانبی معروف با یکدیگر.

این شکل، کران‌های مطرح‌شده توسط لون‌اشتین[۲۳] (۱۹۷۹؛ مرجع [۴۰]) و سیدل‌نیکف[۲۴] (۱۹۷۵؛ مرجع [۶۳]) را شامل نمی‌شود؛ زیرا این کران‌ها به اندازه نتایج به‌دست آمده توسط مک‌الیس در مرجع

[۲۳] V. I. Levenshtein
[۲۴] M. Sidelnikov

[۵۰] خوب نیستند و به‌دست آوردن آنها نسبتاً مشکل می‌باشد. بهترین کران ذکرشده در فوق به صورت زیر است:

$$\alpha(\delta) \leq \min\{۱ + g(u^۲) - g(u^۲ + ۲\delta u + ۲\delta) \mid ۰ \leq u \leq ۱ - ۲\delta\}, \qquad (٦)$$

که در آن:

$$g(x) := H_۲(\frac{۱ - \sqrt{۱ - x}}{۲}).$$

برای مشاهده اثباتی از آن، خواننده را به منابع [۵۰] یا [۵۲] ارجاع می‌دهیم. برای مقادیر بسیار کوچک δ، کران الیاس بهتر از کران موجود در قضیه ۸.۵.۳ است، اما به‌خوبی کران ٦ نمی‌باشد.

در مقاله‌ای توسط بست (۱۹۷۷؛ مرجع [٦])، با استفاده از مطالب زیر، کران‌های موجود در لم ۳.۵.۳ و قضیه ۴.۵.۳ تعمیم داده شده‌اند:

۱) با مشاهده این‌که اگر $|c|$ فرد باشد، آن‌گاه نامساوی ۳.۵.۳ قوی‌تر است و

۲) با اضافه‌نمودن نامساوی‌هایی (نظیر نامساوی بدیهی $A_{n-۱} + A_n \leq ۱$) به قضیه ۴.۵.۳. این مطلب چندین کران بسیار خوب را نتیجه می‌دهد (مساله ۱۲.۵.۵ را مشاهده کنید).

۵.۵ مسائل

۱.۵.۵. از این مطلب که یک کد خطی می‌تواند توسط ماتریس بررسی‌توازن خود تعریف شود، استفاده نموده و نشان دهید که یک کد $[n, k, d]$ روی $\mathbb{F}_q$ وجود دارد، اگر $V_q(n - ۱, d - ۲) < q^{n-k}$. این مطلب را با قضیه ٦.۵.۱ مقایسه کنید.

۲.۵.۵. $A(۱۰, ۵)$ را برای $q = ۲$ تعیین کنید.

۳.۵.۵. فرض کنید $q = ۲$. نشان دهید اگر در قضیه ۴.۵.۲ طرف راست عدد صحیح فرد l باشد، آن‌گاه $A(n, d) \leq l - ۱$.

۴.۵.۵. اگر $q = ۲$، آن‌گاه کران‌هایی برای $A(۱۷, ۸)$ بیابید.

۵.۵.۵. ماتریس مولدی برای دوگان کد $[۳۱, ۵]$ همینگ دوتایی درنظر بگیرید. نشان دهید که می‌توان از تعدادی از ستون‌های این ماتریس به‌گونه‌ای صرف نظر نمود که کد حاصل دارای $d = ۱۰$ باشد و به کران گریسمر دست یابد.

۶.۵.۵. فرض کنید C یک کد دوتایی با طول n و کمترین —فاصله $d = ۲k$ باشد و تمامی کدکلمات C دارای وزن w باشند. هم‌چنین فرض کنید $|c| = [n(n-۱)/w(w-۱)] \times A(n-۲, ۲k, w-۲)$. نشان دهید که کدکلمات C بلوک‌های یک ۲—طرح هستند.

۷.۵.۵. نشان دهید که یک کد همینگ دوتایی کوتاه‌شده بهینه است.

۸.۵.۵. فرض کنید $w \in \mathbb{N}$ و $w > ۴$. هم‌چنین فرض کنید $C_۱$ یک کد دوتایی با طول n تعریف شده به‌صورت زیر باشد:

$$C_l := \{(c_۰, c_۱, \cdots, c_{n-۱}) \mid \sum_{i=۰}^{n-۱} c_i = w, \sum_{i=۰}^{n} ic_i \equiv l \bmod n\},$$

که در آن اعمال جمع روی $\mathbb{Z}$ انجام گرفته‌اند. نشان دهید:

$$A(n, ۴, w) \sim \frac{n^{w-۱}}{w!}, \quad (n \to \infty).$$

۹.۵.۵. فرض کنید $q = ۲$. نشان دهید: $\binom{n}{w} A(n, ۲k) \leq ۲^n A(n, ۲k, w)$.

۱۰.۵.۵.

۱) نشان دهید $A(n, ۲k, w) \leq (۱ - \frac{w}{k}(۱ - \frac{w}{k}))^{-۱}$، اگر طرف راست مثبت باشد.

۲) با استفاده از (۱) و مساله ۹.۵.۵، کران الیاس را به‌دست آورید.

۱۱.۵.۵. فرض کنید C یک کد (n, M, d) دوتایی با $n - \sqrt{n} < ۲d \leq n$ باشد. فرض کنید C دارای این خاصیت باشد که اگر $x \in C$، آن‌گاه $x + ۱ \in C$. نشان دهید قرار دادن $k = ۲$ در رابطه ۳.۵.۳، کران زیر را نتیجه می‌دهد:

$$M \leq \frac{۸d(n-d)}{n - (n - ۲d)^۲}.$$

(این کران با نام کران گری[۲۵] شناخته می‌شود).

۱۲.۵.۵. نشان دهید کد $(۸, ۲۰, ۳)$ از بخش ۴.۴، بهینه است (اثبات مشکل است؛ بخش ۵.۴ را ببینید).

[۲۵] Grey bound

فصل ٦

کدهای دوری

٦.١ تعاریف

در بخش ۴.۵، گروه خودریختی $Aut(C)$ از کد C را تعریف نمودیم. متناظر با این گروه، گروه ماتریس‌های جای‌گشتی وجود دارد. برخی اوقات، تعریف $Aut(C)$ با جای‌گزین نمودن ماتریس‌های جای‌گشتی با ماتریس‌های تک‌جمله‌ای گسترش می‌یابد؛ یعنی ماتریس‌هایی که عناصر ناصفر آنها متناظر با یک ماتریس جای‌گشتی باشد. در هر دو حالت، ما به گروه جای‌گشت‌ها علاقه‌مند می‌باشیم. در این فصل، آن دسته از کدهای خطی را مورد مطالعه قرار می‌دهیم که گروه خودریختی آنها شامل گروه دوری مرتبه n باشد که در آن n طول کلمه کد می‌باشد.

تعریف ۱.٦.١. یک کد خطی C دوری نامیده می‌شود، اگر:

$$\forall_{(c_0,c_1,\cdots,c_{n-1})\in C}[(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C].$$

این تعریف با به‌کارگیری ماتریس‌های تک‌جمله‌ای به‌جای جای‌گشت‌ها، هم‌چنان که در ادامه می‌آید، گسترش می‌یابد. اگر برای هر کدکلمه $(c_0,c_1,\cdots,c_{n-1})$، کلمه $(\lambda c_{n-1},c_0,\cdots,c_{n-2})$ (در اینجا λ مقداری ثابت است) نیز در C باشد، آن‌گاه این کد، یک کد پایادوری[1] (و نادوری[2] اگر $\lambda=-1$) نامیده

[1] constacyclic
[2] negacyclic

می‌شود. در اینجا، نظریه کدهای دوری را معرفی خواهیم نمود؛ تعمیم کدهای پایادوری برای خواننده یک تمرین آسان می‌باشد.

مهم‌ترین ابزار در توصیف ما از کدهای دوری، یک‌ریختی زیر، بین $\mathbb{F}_q^n$ و یک گروه از چندجمله‌ای‌ها می‌باشد. مضارب $x^n - ۱$ تشکیل یک ایده‌آل اصلی در حلقه چندجمله‌ای $\mathbb{F}_q[x]$ می‌دهد. حلقه کلاس باقی‌مانده $\mathbb{F}_q[x]/(x^n - ۱)$ شامل مجموعه‌ای از چندجمله‌ای‌های:

$$\{a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱} \mid a_i \in \mathbb{F}_q, ۰ \leq i < n\},$$

به‌عنوان یک دستگاه نماینده‌ها است. به‌وضوح، $\mathbb{F}_q^n$ با این حلقه یک‌ریخت می‌باشد (تنها به‌عنوان یک گروه جمعی درنظر گرفته شده است). در ادامه، هم‌چنین ساختار ضربی را که اینک معرفی کردیم؛ یعنی حاصل‌ضرب چندجمله‌ای‌ها در پیمانه $(x^n - ۱)$، به‌کار خواهیم برد. از اینجا به‌بعد، از همسانی زیر استفاده خواهیم کرد:

$$(a_۰, a_۱, \cdots, a_{n-۱}) \in \mathbb{F}_q^n \rightleftarrows a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱} \in \mathbb{F}_q[x]/(x^n - ۱), \qquad (۱)$$

و اغلب از کدکلمه c به‌عنوان کدکلمه $c(x)$ با به‌کارگیری رابطه ۱ صحبت خواهیم نمود. با توسیع این مطلب، یک کد خطی را به‌عنوان زیر مجموعه‌ای از $\mathbb{F}_q[x]/(x^n - ۱)$ تفسیر می‌کنیم.

قضیه ۲.۶.۱. یک کد خطی C در $\mathbb{F}_q^n$ دوری است اگر و تنها اگر C در $\mathbb{F}_q[x]/(x^n - ۱)$ یک ایده‌آل باشد.

اثبات.

۱) اگر C در $\mathbb{F}_q[x]/(x^n - ۱)$ دوری باشد و $c(x) = c_۰ + c_۱x + \cdots + c_{n-۱}x^{n-۱}$ یک کدکلمه باشد، آن‌گاه $xc(x)$ نیز یک کدکلمه خواهد بود؛ یعنی:

$$(c_{n-۱}, c_۰, \cdots, c_{n-۲}) \in C.$$

۲) برعکس، اگر C دوری باشد، آن‌گاه برای هر کدکلمه $c(x)$، کدکلمه $xc(x)$ نیز در C است؛ بنابراین، $x^ic(x)$ برای هر i در C است و چون C خطی است، $a(x)c(x)$ برای هر چندجمله‌ای $a(x)$ در C است؛ بنابراین، C یک ایده‌آل است.

□

قرارداد ۳.٦.۱. از اینجا به بعد، تنها کدهای دوری به طول n روی $\mathbb{F}_q$ با شرط $(n,q)=1$ را درنظر می‌گیریم. برای مشاهده برخی مباحث تئوری در مورد کدهای دوری دودویی با طول زوج می‌توان به بخش ٦.۱۰ مراجعه نمود.

چون $\mathbb{F}_q[x]/(x^n-1)$ یک حلقه ایده‌آل اصلی است، هر کد دوری C شامل مضارب یک چندجمله‌ای $g(x)$، چندجمله‌ای تکین با کمترین درجه (چندجمله‌ای ناصفر) در این ایده‌آل (بخش ۱.۱ را ببینید) است.

این چندجمله‌ای $g(x)$، چندجمله‌ای مولد[۳] این کد دوری نامیده می‌شود. چندجمله‌ای مولد یک عامل x^n-1 است (چون درغیر این‌صورت، ب.م.م x^n-1 و $g(x)$ چندجمله‌ای در C با درجه کمتر از درجه $g(x)$ خواهد بود). فرض کنید $x^n-1=f_1(x)f_2(x)\cdots f_t(x)$ تجزیه x^n-1 به عوامل تحویل‌ناپذیر باشد. بنابر قرارداد ۳.٦.۱، این عوامل متمایز هستند. حال می‌توانیم تمامی کدهای دوری به طول n را با برداشتن (در تمامی حالات ممکن) یکی از 2^t عامل x^n-1 به‌عنوان چندجمله‌ای مولد $g(x)$ و تعریف کد متناظر به‌صورت مضارب $g(x)$ در پیمانه (x^n-1)، بیابیم.

مثال ۴.٦.۱. روی $\mathbb{F}_2$ داریم:

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1).$$

در کل هشت کد دوری به طول ۷ وجود دارد. یکی از اینها تنها دارای کدکلمه صفر می‌باشد و یکی دیگر شامل تمامی کدکلمات ممکن می‌باشد. کد با چندجمله‌ای مولد $x-1$ دارای تمامی کدکلمات با وزن زوج است. کد $[7,1]$ دوری تنها شامل کدکلمات ۰ و ۱ است. چهار کد باقی‌مانده به‌ترتیب دارای ابعاد ۳، ۳، ۴ و ۴ هستند؛ برای مثال، با درنظر گرفتن $g(x):=(x-1)(x^3+x+1)=x^4+x^3+x^2+1$، یک کد $[7,3]$ دوری داریم. این کد نمونه‌ای از یک کد دوری تحویل‌ناپذیر است که در زیر تعریف شده است.

تعریف ۵.٦.۱. کد دوری تولیدشده توسط $f_i(x)$، یک کد دوری ماکسیمال[۴] می‌باشد (چون یک ایده‌آل ماکسیمال می‌باشد) و با M_i^+ نمایش داده می‌شود. کد تولید شده توسط $(x^n-1)/f_i(x)$، کد دوری می‌نیمال[۵] نامیده می‌شود و با M_i^- نمایش داده می‌شود. کدهای دوری می‌نیمال، کدهای دوری تحویل‌ناپذیر[٦] نیز نامیده می‌شوند.

---

[۳] generator matrix

[۴] maximal cyclic code

[۵] minimal cyclic code

[٦] irreducible cyclic code

تعریف ۱.٦.۱ تضمین می‌کند که گروه خودریختی یک کد دوری C، شامل گروه دوری تولیدشده توسط جای‌گشت:

$$i \to i + 1 \bmod n,$$

است. اما، چون $a(x^q) = a(x)^q$ متعلق به همان کدی است که $a(x)$ متعلق به آن است، می‌بینیم که جای‌گشت π_q تعریف شده، به‌صورت $\pi_q(i) = qi \bmod n$، یعنی $x \to x^q$، نیز یک کد دوری را به خودش تصویر می‌کند. اگر m از مرتبه q در پیمانه n باشد، آن‌گاه دو جای‌گشت $i \to i+1$ و π_q، یک گروه با مرتبه mn مشمول در $Aut(C)$ تولید می‌کنند.

٦.۲ ماتریس مولد و چندجمله‌ای بررسی

فرض کنید $g(x)$، چندجمله‌ای مولد یک کد دوری C به‌طول n باشد. اگر $g(x)$ دارای درجه $n-k$ باشد، آن‌گاه کدکلمات $g(x)$، $xg(x)$، $\cdots$، $x^{k-1}g(x)$ به‌وضوح تشکیل یک پایه برای C می‌دهند؛ یعنی C یک کد $[n,k]$ است؛ بنابراین، اگر $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$، آن‌گاه:

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & & & & \cdots & 0 \\ 0 & 0 & \cdots & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix},$$

یک ماتریس مولد برای C است. معنای آن این است که ما یک دنباله اطلاعاتی $(a_0, a_1, \cdots, a_{k-1})$ را به‌صورت aG کد می‌کنیم که به‌شکل چندجمله‌ای:

$$(a_0 + a_1 x + \cdots + a_{k-1}x^{k-1})g(x),$$

می‌باشد. یک شکل مناسب‌تر از ماتریس مولد با تعریف $x^i = g(x)q_i(x) + r_i(x)$ (برای $i \geq n-k$) حاصل می‌شود، که در آن $r_i(x)$ چندجمله‌ای با درجه کمتر یا مساوی $n-k$ است. چندجمله‌ای‌های $x^i - r_i(x)$، کدکلماتی از C هستند و تشکیل یک پایه برای کد می‌دهند؛ در نتیجه ماتریس مولدی از C به شکل استاندارد (با I_k در ابتدا) را خواهیم داشت. در این حالت $(a_0, a_1, \cdots, a_{k-1})$ به‌صورت زیر کد می‌شود:

$(a_0, a_1, \cdots, a_{k-1})x^{n-k}$ را بر $g(x)$ تقسیم نموده و باقی‌مانده را از $(a_0, a_1, \cdots, a_{k-1})x^{n-k}$ کم نمایید که درنتیجه یک کد کلمه حاصل می‌شود. از لحاظ فنی، این یک روش خیلی آسان برای کد نمودن اطلاعات است؛ چرا که تقسیم بر یک چندجمله‌ای ثابت از نظر یک رجیستر تغییرمکان (برای دیدن تعریف آن به فصل ۱۳ مراجعه نمایید) قابل اِعمال است.

چون $g(x)$ یک عامل $x^n - ۱$ است، چندجمله‌ای $h(x) = h_۰ + h_۱x + \cdots + h_kx^k$ وجود دارد؛ به‌طوری که $g(x)h(x) = x^n - ۱$ (در $\mathbb{F}_q[x]$). در حلقه $\mathbb{F}_q[x]$، داریم $g(x)h(x) = ۰$؛ یعنی $g_۰h_i + g_۱h_{i-۱} + \cdots + g_{n-k}h_{i-n+k} = ۰$ برای $i = ۰, ۱, \cdots, n-۱$. در نتیجه:

$$H := \begin{pmatrix} ۰ & ۰ & \cdots & ۰ & h_k & \cdots & h_۱ & h_۰ \\ ۰ & ۰ & \cdots & h_k & \cdots & h_۱ & h_۰ & ۰ \\ \vdots & & & & & & & \vdots \\ h_k & ۰ & \cdots & h_۱ & h_۰ & ۰ & \cdots & ۰ \end{pmatrix},$$

یک ماتریس بررسی‌توازن برای کد C است. ما $h(x)$ را چندجمله‌ای بررسی C می‌نامیم. کد C شامل تمامی $c(x)$ هایی است که $c(x)h(x) = ۰$. با مقایسه G و H، می‌بینیم که کد با چندجمله‌ای مولد $h(x)$ هم‌ارز دوگان C می‌باشد (به دست آمده با استفاده از معکوس نمودن ترتیب سمبل‌ها). بیشتر اوقات، این کد، برای سادگی، دوگان کد C نامیده می‌شود (که ممکن است سردرگمی بسیاری را سبب شود؛ چراکه آن برابر با $C^\perp$ نمی‌باشد). توجه دارید که به این مفهوم، "دوگان" یک کد دوری ماکسیمال M_i^+، کد دوری می‌نیمال M_i^- است.

کد دوری می‌نیمال M_i^- با ماتریس مولد $g(x) = (x^n - ۱)/f_i(x)$ را درنظر بگیرید، که در آن $f_i(x)$ دارای درجه k می‌باشد. اگر $a(x)$ و $b(x)$، دو کدکلمه در M_i^- باشند به‌طوری که $a(x)b(x) = ۰$، آن‌گاه یکی از آنها باید بر $f_i(x)$ بخش‌پذیر باشد؛ بنابراین، برابر با ۰ است. چون M_i^- دارای هیچ عامل صفری نیست، یک میدان است؛ یعنی یک‌ریخت با $\mathbb{F}_q^k$. مخصوصاً، اگر قرار دهیم $n = ۲^k - ۱$ و $f_i(x)$ یک چندجمله‌ای اولیه از درجه k باشد، یک مثال جالب به‌دست می‌آید. در این‌حالت، n شیفت دوری چندجمله‌ای مولد $g(x)$ ظاهراً تمامی کدکلمات ناصفر M_i^- می‌باشد. این بدان معناست که این کد هم‌فاصله است (ارجاع به بخش ۵.۲)؛ بنابراین، این فاصله برابر با $۲^{k-۱}$ است (با استفاده از ۵.۳.۸). به‌عنوان یک نتیجه، می‌بینیم که برای هر عامل اولیه $f(x)$ از $x^n - ۱$ (که در آن $n = ۲^k - ۱$)، چندجمله‌ای $(x^n - ۱)/f(x)$ دارای دقیقاً $۲^{k-۱}$ ضریب مساوی با ۱ است. یک نمونه با $k = ۳$ در مثال ۴.٦.۱ آورده شده است.

٦.۳ صفرهای یک کد دوری

فرض کنید $x^n - ۱ = f_۱(x) \cdots f_t(x)$ و β_i یک صفر از $f_i(x)$ در میدان گسترش‌یافته‌ای از $\mathbb{F}_q$ باشد. از این‌رو $f_i(x)$ چندجمله‌ای—می‌نیمال β_i است؛ بنابراین، کد ماکسیمال M_i^+ چیزی نیست جز مجموعه چندجمله‌ای های $c(x)$ به‌طوری که $c(\beta_i) = ۰$. بنابراین، در حالت کلی، یک کد دوری می‌تواند با استفاده از این شرط این‌که تمامی کدکلمات دارای صفرهای مشخص‌شده‌ای هستند، تعیین شود. در

واقع، کافی است تا یک صفر β_i از هر عامل تحویل‌ناپذیر f_i از چندجمله‌ای مولد $g(x)$ را گرفته و تمامی کلماتی که این نقاط را به‌عنوان صفر (ریشه) دارند (تمامی متعلق به یک میدان مناسب گسترش‌یافته از $\mathbb{F}_q$ هستند)، به دست آوریم. اگر با هر مجموعه α_1، α_2، $\cdots$، α_s شروع کنیم و یک کد C را به این‌صورت تعریف کنیم که $c(x) \in C$ اگر و تنها اگر $c(\alpha_i) = 0$، برای $i = 1, 2, \cdots, s$، در این‌صورت C دوری است و چندجمله‌ای مولد C، کوچک‌ترین مضرب مشترک چندجمله‌ای‌های—می‌نیمال α_0، α_1، $\cdots$، α_s است. فرض کنید که تمامی این صفرها متعلق به $\mathbb{F}_{q^m}$ است (که می‌توانیم آن‌را به‌صورت یک فضای برداری $\mathbb{F}_q^m$ نمایش دهیم). برای هر i، می‌توانیم ماتریس m در n را با نمایش‌های برداری ۱، α_i، α_i^2، $\cdots$، $(\alpha_i)^{n-1}$ به‌عنوان ستون‌ها درنظر بگیریم و تمامی اینها را با یکدیگر قرار داده تا ماتریس sm در n، H را تشکیل داده که درایه‌های آن متعلق به $\mathbb{F}_q$ هستند. به‌وضوح $cH^t = 0$، که در آن $c = (c_0, c_1, \cdots, c_{n-1})$ بدان معنی است که $c(\alpha_i) = 0$، برای $i = 1, 2, \cdots, s$. سطرهای H لزوماً مستقل نمی‌باشند. ممکن است یک ماتریس بررسی‌توازن را از H با حذف برخی سطرها به‌دست آوریم. به‌عنوان توصیفی از این روش در توصیف کدهای دوری، اثبات خواهیم نمود که کدهای دودویی (و بسیاری از سایر کدهای) همینگ برابر (هم‌ارز با) کدهای دوری هستند.

قضیه ۱.۶.۳. فرض کنید $n := (q^m - 1)/(q - 1)$ و β را یک ریشه nام واحد در $\mathbb{F}_{q^m}$ درنظر بگیرید. علاوه‌براین، فرض کنید $(m, q - 1) = 1$. در این‌صورت کد دوری:

$$C := \{c(x) : c(\beta) = 0\},$$

هم‌ارز با یک کد همینگ $[n, n - m]$ روی $\mathbb{F}_q$ است.

اثبات. چون:

$$n = (q - 1)(q^{m-2} + 2q^{m-3} + \cdots + m - 1) + m,$$

داریم $(n, q - 1) = (m, q - 1) = 1$؛ بنابراین، $\beta^{i(q-1)} \neq 1$، برای $i = 1, 2, \cdots, n - 1$؛ یعنی $\beta^i \notin \mathbb{F}_q$ برای $i = 1, 2, \cdots, n - 1$. درنتیجه ستون‌های ماتریس H، که در آن نمایش‌های ۱، β، β^2، $\cdots$، β^{n-1} به‌صورت بردارهایی در $\mathbb{F}_q^m$ می‌باشند، دو به‌دو روی $\mathbb{F}_q$ مستقل خطی هستند. بنابراین، H ماتریس بررسی‌توازن یک کد همینگ $[n, n - m]$ است. □

در اینجا آنچه را که تاکنون درباره ساختن کدهای دوری دودویی به‌طول ۹ آموخته‌ایم، تشریح می‌کنیم.

مثال ۲.۶.۳. کوچک‌ترین میدان گسترش‌یافته از $\mathbb{F}_2$ که شامل ۹ امین ریشه اولیه واحد می‌باشد، برابر با $\mathbb{F}_{2^6}$ است. اگر α یک عضو اولیه در این میدان باشد، آن‌گاه $\alpha^{63} = 1$ و $\beta := \alpha^7$ یک ریشه ۹ام اولیه

واحد می‌باشد. با استفاده از قضیه ۱۸.۱.۱ چندجمله‌ای—می‌نیمال β دارای ریشه‌های β، $\beta^{۲}$، $\beta^{۴}$، $\beta^{۸}$، $\beta^{۱۶}=\beta^{۷}$ و $\beta^{۱۴}=\beta^{۵}$ است. این چندجمله‌ای باید $(x^{۹}-۱)/(x^{۳}-۱)=x^{۶}+x^{۳}+۱$ باشد (ارجاع به رابطه ۲۴.۱.۱)؛ بنابراین:

$$(x^{۹}-۱)=(x-۱)(x^{۲}+x+۱)(x^{۶}+x^{۳}+۱)=f_{۱}(x)f_{۲}(x)f_{۳}(x).$$

کد $M_{۳}^{+}$ دارای ستون‌های دوبه‌دو مستقل در H می‌باشد؛ یعنی کمترین—فاصله بزرگ‌تر یا مساوی ۳ است. چون M_{i}^{+} به‌وضوح شامل کدکلمات:

$$(\,c_{۰}c_{۱}c_{۲}\quad c_{۰}c_{۱}c_{۲}\quad c_{۰}c_{۱}c_{۲}\,),$$

است، فوراً می‌بینیم که $d=۳$. کد M_{i}^{-} دارای چندجمله‌ای توازن $x^{۶}+x^{۳}+۱$ است، بنابراین، یک کد $[۹,۶]$ است. چون $x^{۳}-۱$ یک کدکلمه است، این فاصله برابر با ۲ است. اگر ما $\mathbb{F}_{۲^{۶}}$ را با چندجمله‌ای $x^{۶}+x+۱$ بسازیم و سپس ماتریس H با ابعاد ۱۲ در ۹ را برای کد $M_{۳}^{-}$، با استفاده از روشی که قبلاً آن را در قضیه ۱.٦.۳ تشریح نمودیم، تشکیل دهیم، آنگاه این ماتریس تنها دارای ٦ سطر به صورت یک سطر تمام صفر، یک سطر تمام ۱، سطر $(۱۱۰\quad ۱۱۰\quad ۱۱۰)$ و چهار سطر $(۰۱۱\quad ۰۱۱\quad ۰۱۱)$ خواهد بود؛ بنابراین، با توجه به آن، یک ماتریس بررسی‌توازن ۳ در ۹ داریم. البته از $x^{۶}+x^{۳}+۱$ یک ماتریس بررسی‌توازن هم‌ارز با $(I\quad I\quad I)$ داریم. خواننده می‌تواند مثال‌های با وضوح کمتر را به روشی مشابه حل نماید.

مثال ۳.٦.۳. چندجمله‌ای $x^{۸}-۱$ روی $\mathbb{F}_{۳}$ را درنظر بگیرید. اگر β یک ۸ امین ریشه واحد باشد، آن‌گاه $\beta=\beta^{۹}$؛ بنابراین، $x^{۸}-۱$ باید حاصل‌ضرب $(x-۱)$، $(x+۱)$ و سه چندجمله‌ای تحویل‌ناپذیر از درجه ۲ باشد. با جای‌گذاری $x=۰,۱,۲$ در $x^{۲}+ax+b$، می‌بینیم که تنها چندجمله‌ای‌های تحویل‌ناپذیر از درجه ۲ در $\mathbb{F}_{۳}[x]$ به صورت $x^{۲}+۱$، $x^{۲}+x+۱$ و $x^{۲}+۲x+۲$ هستند؛ بنابراین، تجزیه $x^{۸}-۱$ را می‌دانیم. کد دوری با ماتریس مولد $g(x):=(x^{۲}+۱)(x^{۲}+x+۲)$ دارای کمترین—فاصله کمتر یا مساوی ۴ است، چون $g(x)$ دارای وزن ۴ است. در بخش ٦.٦، روشی آسان برای اثبات این‌که ۴ کمترین—فاصله این کد است، ارائه خواهیم داد.

٦.۴ خودتوان یک کد دوری

در بسیاری از کاربردها، مزیت جای‌گزین کردن چندجمله‌ای مولد یک کد دوری با یک چندجمله‌ای $c(x)$ که خودتوان[۷] نام دارد، اثبات شده است. قضیه زیر، این تعریف را دربر گرفته است.

[۷] idempotent

قضیه ۱.۶.۴. فرض کنید C یک کد دوری باشد؛ در این‌صورت یک کدکلمه منحصر به‌فرد $c(x)$ وجود دارد که یک عضو همانی برای C است.

اثبات. فرض کنید $g(x)$ چندجمله‌ای مولد کد C باشد و $h(x)$ چندجمله‌ای توازن، یعنی $g(x)h(x) = x^n - ۱$ در $\mathbb{F}_q[x]$. چون $x^n - ۱$ دارای هیچ ریشه مضاعفی نمی‌باشد، داریم $(g(x), h(x)) = ۱$؛ بنابراین، چندجمله‌ای‌های $a(x)$ و $b(x)$ وجود دارند؛ به‌طوری که $a(x)g(x) + b(x)h(x) = ۱$. حال تعریف کنید:

$$c(x) := a(x)g(x) = ۱ - b(x)h(x).$$

به‌وضوح $c(x)$ یک کدکلمه در C می‌باشد. علاوه‌بر این، اگر $p(x)g(x)$ یک کدکلمه در C باشد، آن‌گاه:

$$\begin{aligned} c(x)p(x)g(x) &= p(x)g(x) - b(x)h(x)p(x)g(x) \\ &\equiv p(x)g(x) \bmod (x^n - ۱). \end{aligned}$$

چون $c(x)$ یک عضو همانی برای C می‌باشد، بنابراین، یکتاست. □

چون $c^۲(x) = c(x)$، این کدکلمه خودتوان[۸] می‌باشد. البته، عناصر دیگری در C می‌توانند وجود داشته باشند به‌طوری که با مربع خودشان برابر باشند، اما تنها یکی از اینها عضو همانی کد است. چون هر کدکلمه می‌تواند به‌صورت $v(x)c(x)$ نوشته شود؛ یعنی مضربی از $c(x)$، می‌بینیم که $c(x)$ ایده‌آل C را تولید می‌کند.

بیایید تجزیه $x^n - ۱ = f_۱(x) \cdots f_t(x)$ را یک‌بار دیگر درنظر بگیریم. حال قرار می‌دهیم $q = ۲$. از قضیه ۱.۱.۱۸ می‌دانیم که این عوامل متناظر با افراز مجموعه $\{۰, ۱, \cdots, n-۱\}$ به هم‌مجموعه‌های دایره‌بر[۹] : $\{۰\}$، $\{۱, ۲, ۴, \cdots, ۲^r\}$، ...، $\{a, ۲a, \cdots, ۲^s a\}$ می‌باشند که در آن s کمترین توانی است که $a(۲^{s+۱} - ۱) \equiv ۰ \bmod n$. در مثال ۲.۶.۳ این تجزیه برابر $\{۰\}$، $\{۱, ۲, ۴, ۸, ۷, ۵\}$ و $\{۳, ۶\}$ با $n = ۹$ است. از طرف دیگر، واضح است که اگر یک خودتوان $c(x)$ شامل جمله x^i باشد، آن‌گاه شامل جمله $x^{۲i}$ نیز هست؛ بنابراین، یک خودتوان باید مجموعی از خودتوان‌ها به‌شکل $x^a + x^{۲a} + \cdots + x^{۲^s a}$ باشد، که در آن $\{a, ۲a, \cdots, ۲^s a\}$ یکی از هم‌مجموعه‌های دایره‌بر است. چون دقیقاً ۲^t تا از این مجموع‌ها وجود دارد، می‌بینیم که یافتن تمامی خودتوان‌های ممکن آسان است و بنابراین، می‌توانیم تمامی کدهای دوری دودویی از یک طول داده شده را بدون نیاز به تجزیه $x^n - ۱$ تولید کنیم.

---

[۸] idempotent

[۹] cyclotomic cosets

کمی جلوتر، این نظریه را تعمیم می‌دهیم. مجدداً خود را روی $q = ۲$ محدود می‌کنیم. درابتدا مشاهده می‌کنید که از اثبات قضیه ۱.٦.۴ نتیجه می‌شود که اگر $c(x)$ یک خودتوان از کد C، با مولد $g(x)$ و چندجمله‌ای بررسی $h(x)$، باشد، آن‌گاه $1 + c(x)$ خودتوان کد با مولد $h(x)$ است؛ بنابراین، $1 + x^n c(x^{-1})$ خودتوان کد دوگان است.

تعریف ۲.٦.۴. خودتوان یک کد دوری تحویل‌ناپذیر M_i^-، یک خوتوان اولیه[۱۰] نامیده شده و با $\theta_i(x)$ نشان داده می‌شود؛ برای مثال، در ۴.٦.۱ چندجمله‌ای $g(x) = x^6 + x^5 + x^3 + 1 = (x^2 + 1)$ یک خودتوان اولیه است.

فرض کنید α یک n امین ریشه اولیه واحد در یک میدان گسترش‌یافته $\mathbb{F}_2$ باشد. اگر چندجمله‌ای $c(x)$ خودتوان باشد، آن‌گاه برای تمامی مقادیر i داریم $c(\alpha^i) = 0$ یا $c(\alpha^i) = 1$ و عکس مطلب نیز به‌وضوح درست می‌باشد. اگر $c(x)$ یک خودتوان اولیه باشد، آن‌گاه یک عامل تحویل‌ناپذیر $f(x)$ از $x^n - 1$ وجود دارد، به‌طوری که $c(\alpha^i) = 1$ اگر و تنها اگر $f(\alpha^i) = 0$؛ یعنی $c(\alpha^i) = 1$ اگر و تنها اگر i متعلق به یکی از هم‌مجموعه‌های دایره‌بر $\{a, 2a, \cdots\}$ باشد. چنین خودتوان اولیه‌ای اغلب با θ_a نمایش داده می‌شود؛ یعنی در تعریف ۲.٦.۴ اندیس i از نماینده‌های هم‌مجموعه‌های دایره‌بر متفاوت انتخاب شده است؛ برای مثال، درنظر بگیرید $n = 15$ و α را ریشه‌ای از $x^4 + x + 1$ درنظر بگیرید؛ در این‌صورت، خودتوان اولیه متعلق به کد دوری می‌نیمال با چندجمله‌ای بررسی $x^4 + x + 1$ با θ_1 نمایش داده می‌شود و در این حالت θ_{-1} متناظر با عناصر ناصفر α^{-1}، α^{-2}، α^{-4}، α^{-8} است؛ یعنی با چندجمله‌ای بررسی $x^4 + x^3 + 1$. در ادامه، اگر چنین αای را ثابت فرض نکرده باشیم، آن‌گاه برای سادگی کدهای دوری تحویل‌ناپذیر را به صورت M_1^-، M_2^-، $\cdots$، M_t^- می‌شماریم.

قضیه ۳.٦.۴. اگر C_1 و C_2 کدهای دوری با خودتوان‌های $c_1(x)$ و $c_2(x)$ باشند، آن‌گاه:

۱) $C_1 \cap C_2$ دارای خودتوان $c_1(x)c_2(x)$ می‌باشد؛

۲) $C_1 + C_2$، یعنی مجموعه تمامی کلمات $a + b$ با $a \in C_1$ و $b \in C_2$، دارای خودتوان $c_1(x) + c_2(x) + c_1(x)c_2(x)$ است.

اثبات.

۱) یک نتیجه بدیهی از قضیه ۱.٦.۴ است.

[۱۰] primitive idempotent

۲) به طریق مشابه نتیجه می‌شود، چرا که به‌وضوح $c_1(x)+c_2(x)+c_1(x)c_2(x)$ در C_1+C_2 است و مجدداً به‌آسانی دیده می‌شود که این یک عضو همانی برای کد است؛ چرا که تمامی کدکلمات، به‌فرم $a(x)c_1(x)+b(x)c_2(x)$ هستند.

□

قضیه ۴.۶.۴. برای خودتوان‌های اولیه داریم:

۱) $\theta_i(x)\theta_j(x)=0$ اگر $i\neq j$؛

۲) $\sum_{i=1}^{t}\theta_i(x)=1$؛

۳) $1+\theta_{i_1}(x)+\theta_{i_2}(x)+\cdots+\theta_{i_r}(x)$ خودتوان کد با مولد $f_{i_1}(x)f_{i_2}(x)\cdots f_{i_r}(x)$ است.

اثبات.

۱) از قضیه ۳.۶.۴ قسمت (۱) نتیجه می‌شود؛ زیرا $M_i^-\cap M_j^-=\{0\}$؛

۲) از قضیه ۳.۶.۴ قسمت (۲) و قضیه ۴.۶.۴ قسمت (۱) نتیجه می‌شود؛ زیرا $M_1^-+M_2^-+\cdots+M_t^-$ مجموعه تمامی کلمات به طول n است؛ و سرانجام:

۳) با مشاهده این‌که چندجمله‌ای توازن $M_{i_1}^-+\cdots+M_{i_r}^-$ برابر با $f_{i_1}(x)f_{i_2}(x)\cdots f_{i_r}(x)$ است، نتیجه می‌شود.

□

با به‌کارگیری این قضایا، یافتن خودتوان‌های اولیه کار زیاد سختی نیست؛ در این‌صورت فرد روش آسانی برای یافتن خودتوان‌های یک کد دارد، اگر مولد کد به‌صورت $f_{i_1}f_{i_2}\cdots f_{i_t}$ داده شده باشد.

در موضوعات مختلف پیشرفته‌تر در نظریه کدگذاری، می‌توان به تکنیک‌های اثبات شامل خودتوان‌ها دسترسی یافت. در این کتاب، ما به آن مرحله نخواهیم رسید، اما می‌خواهیم تا کمی بیشتر درباره خودتوان‌ها بدانیم. خواننده‌ای که می‌خواهد این مطلب را مطالعه نماید، ملاحظات زیر را مفید خواهد یافت.

کد دوری C به طول n با مولد $g(x)$ را درنظر بگیرید. فرض کنید $x^n-1=g(x)h(x)$. از دو طرف مشتق صوری می‌گیریم (ارجاع به بخش ۱.۱)؛ داریم:

$$x^{n-1}=g'(x)h(x)+g(x)h'(x).$$

در اینجا درجه $g'(x)h(x)$ برابر با $n-1$ است، اگر و تنها اگر درجه $h(x)$ فرد باشد. با ضرب طرفین در x و کاهش دادن در پیمانه x^n-1 داریم:

$$1 = xg'(x)h(x) + xg(x)h'(x) + (x^n - 1),$$

که در آن جمله آخر، جمله x^n را که در یکی از دو چندجمله‌ای دیگر رخ می‌دهد، از بین می‌برد. می‌بینیم که خودتوان C برابر با $xg(x)h'(x) + \delta(x^n-1)$ است که در آن $\delta = 1$، اگر درجه $h(x)$ فرد باشد و در غیر این‌صورت برابر با 0 است. به‌عنوان یک مثال؛ کد کمترین به‌طول ۱۵ با چندجمله‌ای توازن $x^4 + x + 1$ را درنظر بگیرید. خودتوان θ_1 برابر با $xg(x) = x(x^{15}-1)/(x^4+x+1)$ است.

تناظر زیر بین خودتوان‌ها، تمرین مفید دیگری است. مثال بالا می‌تواند به‌عنوان یک توصیف به‌کار رود. فرض کنید $f(x)$ یک مقسوم‌علیه x^n-1 باشد که در آن $n = 2^k - 1$. فرض کنید α یک عضو اولیه از $\mathbb{F}_{2^k}$ طوری باشد که $f(\alpha) = 0$. خودتوان‌های اولیه θ_1، به‌ترتیب θ_{-1}، متناظر با هم‌مجموعه‌های دایره‌بر $\{1, 2, \cdots, 2^{k-1}\}$، به‌ترتیب $\{-1, -2, \cdots, -2^{k-1}\}$ می‌باشند. ادعا می‌کنیم:

$$\theta_{-1}(x) = \varphi(x) = \sum_{i=0}^{n-1} Tr(\alpha^i)x^i,$$

که در آن Tr تابع اثر (ارجاع به ۲۵.۱.۱) می‌باشد. به منظور نشان دادن آن، باید $\varphi(\alpha^l)$ برای $l = 0, 1, \cdots, n-1$ را محاسبه کنیم؛ داریم:

$$\varphi(\alpha^l) = \sum_{i=0}^{n-1} (\alpha^l)^i \sum_{j=0}^{k-1} (\alpha^i)^{2^j} = \sum_{j=0}^{k-1} \sum_{i=0}^{n-1} (\alpha^{l+2^j})^i.$$

این حاصل‌ضرب داخلی برابر با 0 است، مگر این‌که $\alpha^{l+2^j} = 1$؛ بنابراین، $\varphi(\alpha^l) = 1$ اگر برای یک مقدار j داشته باشیم $l = -2^j$ و در غیر این‌صورت $\varphi(\alpha^l) = 0$. این مطلب، ادعا را ثابت می‌کند.

خودتوان‌ها در بسیاری جاها به‌کار رفته‌اند، به‌طور نمونه در شمارنده‌های وزنی. ما در این موضوع وارد نشده، اما خواننده را به مراجع [۴۲] و [۴٦] ارجاع می‌دهیم. نظریه‌ای که در این بخش به آن پرداختیم، به‌طور خاص قضیه ۴.٦.۴، حالت خاصی از نظریه عمومی خودتوان‌ها برای جبرهای شبه—ساده است. خواننده را به مرجع [۱٦] ارجاع می‌دهیم.

٦.۵ نمایش‌های دیگر کدهای دوری

چندین روش دیگر برای نمایش کدهای دوری به‌غیر از روش استاندارد که در بخش ٦.۱ به آن پرداختیم، وجود دارد. برخی اوقات، یک اثبات زمانی که از یکی از این نمایش‌های دیگر استفاده شود، آسان‌تر خواهد بود. اولین آنها، که در اینجا به آن می‌پردازیم، تابع اثر را به‌کار می‌گیرد (ارجاع به تعریف ۲۵.۱.۱).

قضیه ۱.٦.۵. فرض کنید k رتبه ضربی p در پیمانه n باشد؛ یعنی $q = p^k$ و β یک nامین ریشه اولیه واحد باشد، آن‌گاه مجموعه:

$$V := \{c(\xi) := (Tr(\xi), Tr(\xi\beta), \cdots, Tr(\xi\beta^{n-1})) \,|\, \xi \in \mathbb{F}_q\},$$

یک کد دوری تحویل‌ناپذیر $[n,k]$ روی $\mathbb{F}_p$ است.

اثبات. با به‌کارگیری قضیه ۲٦.۱.۱، V یک کد خطی است. سپس، مشاهده می‌کنید که $c(\xi\beta^{-1})$ یک شیفت دوری $c(\xi)$ می‌باشد. بنابراین، V یک کد دوری است. چون β متعلق به هیچ زیرمیدانی از $\mathbb{F}_q$ نیست، می‌دانیم که β یک ریشه از یک چندجمله‌ای تحویل‌ناپذیر $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ از درجه k است. اگر $c(\xi) = (c_0, c_1, \cdots, c_{n-1})$، آن‌گاه:

$$\sum_{i=0}^{k} c_i h_i = Tr(\xi h(\beta)) = Tr(0) = 0,$$

یعنی، یک معادله‌بررسی‌توازن برای کد V داریم.

چون $h(x)$ تحویل‌ناپذیر است، می‌بینیم که $x^k h(x^{-1})$ چندجمله‌ای بررسی برای V است؛ بنابراین، V یک کد $[n,k]$ دوری تحویل‌ناپذیر است. □

حال یک نمونه گسسته از تبدیل فوریه را معرفی خواهیم نمود که در نظریه کدگذاری همیشه از آن به‌عنوان چندجمله‌ای ماتسون—سولومن[11] تعبیر می‌شود. فرض کنید β یک nامین ریشه اولیه واحد در میدان گسترش‌یافته $\mathcal{F}$ از $\mathbb{F}_q$ باشد. فرض کنید T مجموعه چندجمله‌ای‌های روی $\mathcal{F}$ با درجه حداکثر $n-1$ باشد. نگاشت $\Phi : T \to T$ را به‌صورت زیر تعریف می‌کنیم. فرض کنید $a(x) \in T$. در این‌صورت $A(X) = (\Phi a)(X)$ به‌صورت زیر تعریف شده است:

$$A(X) := \sum_{j=1}^{n} a(\beta^j) X^{n-j}. \qquad (۲)$$

اگر $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$، آن‌گاه چندجمله‌ای $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$، چندجمله‌ای ماتسون—سولومن بردار $\mathbf{a}$ نامیده می‌شود.

لم ۲.٦.۵. معکوس Φ برابر با:

$$a(x) = n^{-1}(\Phi A)(x^{-1}) \bmod x^n - 1,$$

است.

[11] Mattson-Solomon polynomial

اثبات.

$$A(\beta^k) = \sum_{j=1}^{n} \sum_{i=0}^{n-1} a_i \beta^{ij} \beta^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=1}^{n} \beta^{(i-k)j} = n a_k.$$

□

فرض کنید ∘ حاصل‌ضرب چندجمله‌ای‌ها در پیمانه $x^n - 1$ باشد و $*$ به‌صورت زیر تعریف شده باشد:

$$(\sum a_i x^i) * (\sum b_i x^i) := \sum a_i b_i x^i.$$

در این‌صورت به‌آسانی دیده می‌شود که Φ یک یک‌ریختی از حلقه $(T, +, \circ)$ به روی حلقه $(T, +, *)$ می‌باشد.

حال بیایید این چندجمله‌ای‌ها را برای مطالعه کدهای دوری به‌کار گیریم.

لم ۳.٦.۵. فرض کنید V یک کد دوری روی $\mathbb{F}_q$ تولیدشده توسط:

$$g(x) = \prod_{k \in K} (x - \beta^k),$$

باشد. فرض کنید $\{1, 2, \cdots, d-1\} \subset K$ و $\mathbf{a} \in V$؛ در این‌صورت درجه چندجمله‌ای ماتسون–سولومن A از $\mathbf{a}$ حداکثر برابر با $n - d$ است.

اثبات. $a(\beta^j) = 0$، برای $1 \leq j \leq d-1$؛ چون $a(x)$ توسط $g(x)$ عاد می‌شود. حال با توجه به رابطه ۲ نتیجه حاصل می‌شود. □

قضیه ۴.٦.۵. اگر r تا nامین ریشه واحد وجود داشته باشند که ریشه‌های چندجمله‌ای ماتسون–سولومن A از یک کلمه $\mathbf{a}$ باشند، آن‌گاه $w(\mathbf{a}) = n - r$.

اثبات. این یک نتیجه فوری از لم ۲.٦.۵ است. □

هم‌چنین می‌توانیم ارتباطی بین کدهای دوری و نظریه دنباله‌های بازگشتی خطی[۱۲] که مطالب گسترده‌ای درباره آن وجود دارد (ر.ک. مرجع [٦١])، برقرار سازیم. یک دنباله بازگشتی خطی با عناصر در $\mathbb{F}_q$ توسط یک دنباله اولیه $a_0, a_1, \cdots, a_{k-1}$ و یک رابطه بازگشتی:

$$a_l + \sum_{i=1}^{k} b_i a_{l-i} = 0, \qquad (l \geq k), \tag{۳}$$

[۱۲] linear recurring sequences

تعریف شده است. تکنیک استاندارد برای یافتن یک جواب، امتحان $a_l = \beta^l$ است. این یک جواب از رابطه ۳ است، اگر β یک ریشه از $h(x)$ باشد که در آن $h(x) := x^k + \sum_{i=1}^{k} b_i x^{k-i}$. بیاییم فرض کنیم که معادله $h(x) = 0$ دارای k ریشه متمایز $\beta_1, \beta_2, \cdots, \beta_k$ در یک میدان گسترش‌یافته $\mathbb{F}_q$ است؛ در این‌صورت اگر $c_1, c_2, \cdots, c_k$ دلخواه باشند، آن‌گاه دنباله $a_l = \sum_{i=1}^{k} c_i \beta_i^l$ جوابی از رابطه ۳ می‌باشد. ما باید c_i را به‌گونه‌ای انتخاب نماییم که $a_0, a_1, \cdots, a_{k-1}$ دارای مقادیر مشخص شده باشند. این مقادیر برای حل یک دستگاه با k معادله خطی کاربرد دارد، که در آن دترمینان ضرایب، دترمینان واندرموند:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_k \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_k^2 \\ \cdots & \cdots & \cdots & \cdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \cdots & \beta_k^{k-1} \end{pmatrix} = \prod_{i>j} (\beta_i - \beta_j) \neq 0. \qquad (۴)$$

است؛ بنابراین، می‌توانیم درواقع دنباله مورد نیاز را بیابیم.

فرض کنید $h(x)$ یک عامل $x^n - 1$ است (مجدداً $(n, q) = 1$)؛ در این‌صورت دنباله بازگشتی خطی، متناوب با دوره تناوب عاملی از n است. حال تمامی دنباله‌های جزیی $(a_0, a_1, \cdots, a_{n-1})$ را درنظر بگیرید، که در آن $(a_0, a_1, \cdots, a_{n-1})$ متعلق به $\mathbb{F}_q^k$ می‌باشد؛ در این‌صورت ما یک کد $[n, k]$ دوری با $x^k h(x^{-1})$ به‌عنوان چندجمله‌ای بررسی داریم؛ بنابراین:

$$C = \{(a_0, \cdots, c_{n-1}) \,|\, a_l = \sum_{i=1}^{k} c_i \beta_i^l (0 \leq l < n), (c_1, c_2, \cdots, c_k) \in \mathbb{F}_q^k\},$$

نمایش دیگری از یک کد دوری می‌باشد.

۶.۶ کدهای BCH

یک کلاس مهم از کدهای دوری، که هنوز در عمل بسیار به‌کار می‌رود، توسط بویس[۱۳] و چادوری[۱۴] (۱۹۶۰) و به‌طور مستقل توسط هُکنگِم[۱۵] کشف شد. این کدها به کدهای BCH معروف هستند.

تعریف ۱.۶.۶. یک کد دوری به‌طول n روی $\mathbb{F}_q$، کد BCH با فاصله طراحی‌شده[۱۶] δ می‌باشد، اگر مولد آن $g(x)$ کوچک‌ترین مضرب مشترک چندجمله‌ای‌های $\beta^l, \beta^{l+1}, \cdots, \beta^{l+\delta-2}$ برای یک l باشد که در آن β یک nامین ریشه اولیه واحد است. معمولاً قرار می‌دهیم $l = 1$ (برخی اوقات به آن، یک کد BCH

[۱۳] R. C. Bose
[۱۴] D. K. Ray-Chaudhuri
[۱۵] Hocquenghem
[۱۶] designed distance

با مفهوم کم‌عرض[۱۷] اطلاق می‌شود). اگر $n = q^m - ۱$، یعنی β یک عضو اولیه $\mathbb{F}_{q^m}$ باشد، آن‌گاه کد BCH، اولیه نامیده می‌شود.

اصطلاح "فاصله طراحی‌شده" توسط قضیه زیر تشریح شده است.

قضیه ۲.٦.٦. کمترین —فاصله یک کد BCH با فاصله طراحی‌شده d حداقل برابر با d است.

اثبات اول. به روشی مشابه با بخش ٦.٣، ماتریس $m(d-۱)$ در n، H را تشکیل می‌دهیم:

$$H := \begin{pmatrix} ۱ & \beta^{l} & \beta^{۲l} & \dots & \beta^{(n-۱)l} \\ ۱ & \beta^{l+۱} & \beta^{۲(l+۱)} & \dots & \beta^{(n-۱)(l+۱)} \\ \dots & \dots & \dots & \dots & \dots \\ ۱ & \beta^{l+d-۲} & \beta^{۲(l+d-۲)} & \dots & \beta^{(n-۱)(l+d-۲)} \end{pmatrix},$$

که در آن هر درایه به‌عنوان یک بردار ستونی به‌طول m روی $\mathbb{F}_q$ تعبیر می‌شود. کلمه c در کد BCH قرار دارد اگر و تنها اگر $cH^T = ۰$. $m(d-۱)$ سطر H لزوماً مستقل نیستند. $d-۱$ ستون دلخواه از H را درنظر گرفته و فرض کنید $\beta^{i_۱ l}$، ...، $\beta^{i_{d-۱} l}$ عناصر بالای این ستون‌ها باشند. دترمینان زیرماتریس H، به‌دست آمده در این روش، مجدداً یک دترمینان واندرموند (ارجاع به رابطه ۴) با مقدار $\beta^{(i_۱+\dots+i_{d-۱})l} \prod_{r>s}(\beta^{i_r} - \beta^{i_s})$ است، چون β یک nامین ریشه واحد است. بنابراین، هر $d-۱$ ستون H به‌طور خطی مستقل می‌باشند؛ بنابراین، یک کدکلمه $c \neq ۰$ دارای وزن بزرگ‌تر یا مساوی d است.

اثبات دوم. قرار می‌دهیم $l = ۱$. با به‌کارگیری لم ٣.٦.٥، درجه چندجمله‌ای ماتسون—سولومن کدکلمه c، حداکثر $n-d$ است؛ بنابراین، در قضیه ۴.٦.٥ داریم $r \leq n-d$؛ یعنی $w(c) \geq d$.

□

تذکر ۳.٦.٦. معمولاً قضیه ۲.٦.٦، کران BCH نامیده می‌شود. از اینجا به‌بعد، معمولاً کدهای BCH با مفهوم کم‌عرض را درنظر می‌گیریم. اگر با $l = ۰$ به‌جای $l = ۱$ شروع کنیم، آن‌گاه زیرکد با وزن زوج از کد با مفهوم کم‌عرض را درنظر گرفته‌ایم.

[۱۷] a narrow-sense BCH code

مثال ۴.۶.۶. فرض کنید $n = ۳۱$، $m = ۵$، $q = ۲$ و $d = ۸$. فرض کنید α یک عضو اولیه از $\mathbb{F}_{۳۲}$ باشد. چندجمله‌ای—می‌نیمال α برابراست با:

$$(x-\alpha)(x-\alpha^{۲})(x-\alpha^{۴})(x-\alpha^{۸})(x-\alpha^{۱۶}).$$

به‌روش مشابه چندجمله‌ای—می‌نیمال $m_{۳}(x)$ را داریم؛ اما:

$$m_{۵}(x) = (x-\alpha^{۵})(x-\alpha^{۱۰})(x-\alpha^{۲۰})(x-\alpha^{۹})(x-\alpha^{۱۸}) = m_{۹}(x).$$

ثابت می‌شود $g(x)$ کوچک‌ترین مضرب مشترک $m_{۱}(x)$، $m_{۳}(x)$، $m_{۵}(x)$، $m_{۷}(x)$ و $m_{۹}(x)$ است؛ بنابراین، کمترین—فاصله کد BCH اولیه با فاصله طراحی‌شده ۸ (که به‌وضوح برابر ۹ بود) در واقع برابر ۱۱ است.

چندین تعمیم کران BCH ثابت شده است. در اینجا روش تخمین کمترین—فاصله یک کد دوری را بیان می‌کنیم. این روش توسط ون‌لینت[۱۸] و ویلسن[۱۹] در مرجع [۷۶] آمده است. بهبودهای اخیر قضیه ۲.۶.۶ نتیجه این روش می‌باشد.

اگر $A = \{\alpha^{i_{۱}}, \cdots, \alpha^{i_{l}}\}$ مجموعه nامین ریشه‌های واحد باشد؛ به‌طوری که برای یک کد دوری به‌طول n داشته باشیم:

$$c(x) \in C \Leftrightarrow \forall_{\xi \in A}[c(\xi) = ۰],$$

آن‌گاه خواهیم گفت A یک مجموعه تعریف[۲۰] برای C است. اگر A بزرگ‌ترین مجموعه تعریف برای C باشد، آن‌گاه A را کامل[۲۱] می‌نامیم.

تعریف ۵.۶.۶. $M(A)$ یا $M(\alpha^{i_{۱}}, \cdots, \alpha^{i_{l}})$ را ماتریسی با اندازه l در n تعریف می‌کنیم که سطر kام آن به‌صورت $۱, \alpha^{i_k}, \alpha^{۲i_k}, \cdots, \alpha^{(n-۱)i_k}$ باشد؛ یعنی:

$$M(\alpha^{i_{۱}}, \ldots, \alpha^{i_{l}}) = \begin{pmatrix} ۱ & \alpha^{i_{۱}} & \alpha^{۲i_{۱}} & \cdots & \alpha^{(n-۱)i_{۱}} \\ ۱ & \alpha^{i_{۲}} & \alpha^{۲i_{۲}} & \cdots & \alpha^{(n-۱)i_{۲}} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ ۱ & \alpha^{i_{l}} & \alpha^{۲i_{l}} & \cdots & \alpha^{(n-۱)i_{l}} \end{pmatrix}.$$

$M(A)$ را ماتریس بررسی‌توازن متناظر با A می‌نامیم. این نمادگذاری مشابه با قضیه ۲.۶.۶ است (دقت کنید که روی $\mathbb{F}_q$، ماتریس $M(A)$ دارای سطرهایی است که لزوماً مستقل نیستند).

---

[۱۸] J. H. van Lint

[۱۹] R. M. Wilson

[۲۰] defining set

[۲۱] complete

تعریف ٦.٦.٦. مجموعه $A = \{\alpha^{i_1}, \cdots, \alpha^{i_l}\}$، مجموعه متوالی[۲۲] به‌طول n نامیده می‌شود، اگر nامین ریشه واحد β و توان i وجود داشته باشد، به‌طوری که $A = \{\beta^i, \beta^{i+1}, \cdots, \beta^{i+l-1}\}$.

بنابراین، قضیه ٢.٦.٦ بیان می‌کند که اگر یک مجموعه تعریف A برای یک کد دوری شامل یک مجموعه متوالی به‌طول $d-1$ باشد، آن‌گاه کمترین—فاصله حداقل برابر با d است. یک نتیجه از اثبات قضیه ٢.٦.٦، لم زیر است.

لم ٧.٦.٦. اگر A یک مجموعه متوالی به طول l باشد، آن‌گاه زیرماتریس $M(A)$، حاصل از درنظر گرفتن l ستون دلخواه، دارای رتبه l است.

در ادامه نتیجه زیر از این لم را به‌کار خواهیم برد.

نتیجه‌گیری ٨.٦.٦ اگر β یک nامین ریشه اولیه واحد باشد و

$$i_1 < i_2 < \cdots < i_k = i_1 + t - 1,$$

آن‌گاه اگر هر t ستون $M(\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_k})$ را درنظر بگیریم، ماتریس به‌دست آمده دارای رتبه k می‌باشد.

حال نماد زیر را معرفی می‌کنیم:

$$AB := \{\xi\eta \,|\, \xi \in A, \eta \in B\}$$

درادامه، عمل‌گر حاصل‌ضربی برای ماتریس‌ها درنظر می‌گیریم که در موقعیت خاصی که این ماتریس‌ها، ماتریس بررسی‌توازن به‌شکل $M(A)$ تعریف شده در ٥.٦.٦ هستند، به‌کار خواهد رفت.

تعریف ٩.٦.٦. ماتریس $A * B$ ماتریسی است که سطرهای آن تمامی حاصل‌ضرب‌های ab است که a متعلق به سطرهای A و b متعلق به سطرهای B است.

لم (تقریباً بدیهی) زیر، پایه روشی است که توصیف شد. ماتریس‌های A و B با n ستون را درنظر بگیرید.

لم ١٠.٦.٦. اگر یک ترکیب خطی از تمام ستون های $A * B$ با ضرایب ناصفر برابر با ٠ باشد، آن‌گاه:

$$rank(A) + rank(B) \leq n.$$

[۲۲] consecutive set

اثبات. اگر ضرایب موجود در این ترکیب خطی برابر با λ_j $(j = ۱, \ldots, n)$ باشند، آن‌گاه ستون jام B را در λ_j ضرب کنید. این کار، ماتریس B' با رتبه مشابه با رتبه B را تولید خواهد کرد. شرط لم بیان می‌کند که هر سطر A دارای ضرب داخلی صفر با هر سطر B' است. چون این مطلب ایجاب می‌کند $rank(A) + rank(B') \leq n$، آنچه را می‌خواستیم، انجام داده‌ایم. □

حال در موقعیتی هستیم که قضیه‌ای را بیان کنیم که ما را قادر به یافتن کمترین—فاصله تعداد زیادی از کدهای دوری می‌سازد. اگر c یک کدکلمه در یک کد دوری باشد، آن‌گاه محمل[۲۳] I از c، مجموعه مکان‌های مختصات i است؛ به‌طوری که $c_i \neq ۰$. اگر A یک ماتریس باشد، آن‌گاه A_I معرف زیرماتریس حاصل از حذف مکان‌هایی است که متعلق به I نیستند.

قضیه ۱۱.۶.۶. فرض کنید A و B ماتریس‌هایی با درایه‌هایی از یک میدان $\mathbb{F}$ باشند. فرض کنید $A * B$ یک ماتریس بررسی‌توازن برای کد C روی $\mathbb{F}$ باشد. اگر I محمل کدکلمه‌ای در C باشد، آن‌گاه:

$$rank(A_I) + rank(B_I) \leq |I|.$$

اثبات. این مطلب نتیجه فوری از لم ۱۰.۶.۶ است. □

این قضیه را به‌صورت زیر به‌کار خواهیم برد. لم ۷.۶.۶ به ما اجازه خواهد داد تا درباره رتبه ماتریس‌های مناسب از نوع A_I، به‌ترتیب B_I، چیزی بگوییم. اگر مجموع این رتبه‌ها بیشتر از $|I|$، برای هر زیرمجموعه I از $\{۱, ۲, \cdots, n\}$ با اندازه کمتر از δ، باشد، آن‌گاه این کد دارای کمترین—فاصله حداقل δ است.

مثال ۱۲.۶.۶. دراینجا روشی را با استفاده از اثبات کران معروف به روس[۲۴] تشریح می‌کنیم. این کران بیان می‌کند که اگر A یک مجموعه تعریف برای یک کد دوری با کمترین—فاصله d_A باشد و اگر B مجموعه ریشه‌های nام واحد باشد، به‌طوری که کوچک‌ترین مجموعه متوالی که شامل B است دارای اندازه کمتر یا مساوی $|B| + d_A - ۲$ باشد، آن‌گاه کد با مجموعه تعریف AB دارای کمترین—فاصله $d \geq |B| + d_A - ۱$ است.

برای اثبات این مطلب، در ابتدا مشاهده می‌کنید که:

$$rank(M(A)_I) = \begin{cases} |I|, & |I| < d_A \text{ برای} \\ \geq d_A - ۱, & |I| \geq d_A \text{ برای.} \end{cases}$$

[۲۳] support
[۲۴] Roos bound

نتیجه ۸.٦.٦ اطلاعاتی در مورد رتبه زیرماتریس‌های $M(A)$ به ما ارایه می‌دهد؛ یعنی:

$$rank(M(B)_I) \geq \begin{cases} ۱, & \text{برای } |I| < d_A \\ |I| - d_A + ۲, & d_A \geq |I| \geq |B| + d_A - ۲ \text{ برای.} \end{cases}$$

حال قضیه ۱۱.٦.٦ را به‌کار می‌بریم. از مطلب بالا داریم:

$$rank(M(A)_I) + rank(M(B)_I) > |I|. \quad \text{برای } |I| < |B| + d_A - ۲$$

بنابراین، به ازای این مقادیر $|I|$، مجموعه I نمی‌تواند محمل کدکلمه‌ای در یک کد با مجموعه تعریف AB باشد بنابراین، از این مطلب استفاده می‌کنیم که سطرهای $M(A) * M(B)$ یکسان با سطرهای $M(AB)$ هستند).

تذکر ۱۳.٦.٦. این کران توسط روس[۲۵] [۸۰] معرفی شده است. حالت خاصی که B یک مجموعه متوالی است، توسط هارتمن[۲٦] و تزینگ[۲۷] در سال ۱۹۷۲، مرجع [۳۳]، اثبات شده است.

مثال ۱۴.٦.٦. کد دوری C به‌طول ۳۵ با مولد:

$$g(x) = m_۱(x)m_۵(x)m_۷(x),$$

را درنظر بگیرید. اگر α یک ۳۵امین ریشه اولیه واحد باشد، آن‌گاه مجموعه تعریف C شامل مجموعه $\{\alpha^i \,|\, i = ۷, ۸, ۹, ۱۰, ۱۱, ۲۰, ۲۱, ۲۲, ۲۳\}$ را درنظر بگیرید. این مجموعه می‌تواند به‌صورت AB نوشته شود، که در آن $A = \{\alpha^i \,|\, i = ۷, ۸, ۹, ۱۰\}$ و $B = \{\beta^j \,|\, j = ۰, ۳, ۴\}$ با $\beta = \alpha^{۱۲}$ (نیز یک ۳۵امین ریشه اولیه واحد). مجموعه A، مجموعه تعریف یک کد دوری با کمترین —فاصله $d_A = ۵$ است. مجموعه B مشمول در مجموعه متوالی با اندازه ۵ است. شرط روی $|B|$ از مثال ۱۲.٦.٦ برقرار است. درنتیجه C دارای کمترین —فاصله حداقل $۷ = ۱ - ۵ + ۳$ است. این مقدار درواقع کمترین —فاصله این کد است. توجه دارید که کران BCH تنها نشان می‌دهد که کمترین —فاصله حداقل برابر ٦ است.

قبل از ارایه یکی از زیباترین مثال‌ها از روش خود، حالت خاصی از یک قضیه را که توسط مک‌الیس[۲۸] بیان شده است، اثبات می‌کنیم.

---

[۲۵] C. Roos
[۲٦] C. R. P. Hartmann
[۲۷] K. K. Tzeng
[۲۸] R. J. McEliece

لم ۱۵.۶.۶. فرض کنید C یک کد دودویی دوری به‌طول n با مجموعه تعریف کامل R باشد. فرض کنید حاصل‌ضرب هر دو ریشه nام واحدی که در R نباشند، برابر با ۱ نباشد؛ در این‌صورت وزن هر کدکلمه در C بر ۴ بخش‌پذیر است.

اثبات. واضح است که $1 \in R$ و برای هر ریشه nام واحد γ داریم $\gamma \in R$ یا $\gamma^{-1} \in R$. فرض کنید $c(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_k}$ یک کدکلمه باشد. چون $1 \in R$، k باید زوج باشد. از آنجا که $c(x)c(x^{-1})$ برای هر nامین ریشه واحد، صفر است نتیجه می‌گیریم که آن برابر با چندجمله‌ای صفر است. اگر $x^{i-j} = x^{l-m}$، آن‌گاه $x^{j-i} = x^{m-l}$؛ یعنی در حاصل‌ضرب $c(x)c(x^{-1})$، هربار چهار جمله حذف می‌شوند. k جمله برابر با ۱ وجود دارد؛ بنابراین، $k(k-1) \equiv 0 \bmod 4$. بنابراین، $4 \mid k$. □

نتیجه‌ای از لم ۱۵.۶.۶ این است که دوگان کد C از کد BCH اولیه با طول ۱۲۷ و فاصله طراحی‌شده ۱۱ دارای کمترین—فاصله بخش‌پذیر بر ۴ است. با استفاده از کران BCH، کد C دارای کمترین—فاصله حداقل ۱۶ است. با استفاده از کران روس، فاصله حداقل برابر ۲۲ است، بنابراین، در واقع از لم ۱۵.۶.۶، حداقل برابر ۲۴ است. چون این کد شامل کوتاه‌شده کد رید—مولر $\mathcal{R}(2,7)$ است، کمترین فاصله آن حداکثر برابر ۳۲ می‌باشد. حال نشان خواهیم داد که روش بیان شده در بالا نشان می‌دهد $d \geq 30$، بنابراین، با اثبات این مطلب در واقع نشان داده‌ایم که $d = 32$.

مثال ۱۶.۶.۶. فرض کنید R مجموعه تعریف C باشد. توجه دارید که R شامل مجموعه‌های $\{\alpha^i \mid 81 \leq i \leq 95\}$، $\{\alpha^i \mid 98 \leq i \leq 111\}$ و $\{\alpha^i \mid 113 \leq i \leq 127\}$ است که در آن α یک ریشه ۱۲۷ام اولیه واحد است. فرض کنید:

$$A = \{\alpha^i \mid 83 \leq i \leq 95\} \cup \{\alpha^i \mid 98 \leq i \leq 111\},$$

$$B = \{\beta^j \mid j = -7, 0, 1\}, \qquad \beta = \alpha^{16}.$$

در این‌صورت $R \supseteq AB$. مجموعه A شامل ۱۴ توان متوالی α است؛ بنابراین، زیرمجموعه‌ای از یک مجموعه از ۲۹ توان متوالی α است، با توان‌های α^{96} و α^{97} که از دست رفته‌اند؛ بنابراین، از لم ۷.۶.۶ و نتیجه ۸.۶.۶ داریم:

$$rank(M(A)_I) \geq \begin{cases} |I|, & 1 \leq |I| \leq 14 \text{ برای}, \\ 14, & 14 \leq |I| \leq 16 \text{ برای}, \\ |I| - 2, & 17 \leq |I| \leq 29 \text{ برای}. \end{cases}$$

با روشی مشابه، داریم:

$$rank(M(B)_I) \geq \begin{cases} |I|, & ۱ \leq |I| \leq ۲ \text{ برای}, \\ ۲, & ۲ \leq |I| \leq ۸ \text{ برای}, \\ ۳, & |I| \geq ۹ \text{ برای}. \end{cases}$$

با به‌کارگیری قضیه ۱۱.٦.٦ مجموعه I با شرط $|I| < ۳۰$ می‌تواند محمل یک کدکلمه در C باشد.

این مطلب توسط ون‌لینت و ویلسن در مرجع [٧٦] نشان داده شده است که روش تشریح شده در بالا، کمترین—فاصله دقیق برای تمامی کدهای دوری دودویی با طول کمتر از ٦٣، با تنها دومورد استثنا، را می‌دهد.

یافتن کمترین—فاصله واقعی یک کد BCH در حالت کلی یک مساله مشکل است. اما، مطلبی در اینجا می‌تواند بیان شود. برای تشریح این مطلب، ما خود را به کدهای BCH اولیه دودویی محدود خواهیم نمود. در ابتدا باید یک لم را ثابت کنیم. $\mathbb{F}_{۲^k}$ را به‌عنوان فضای $\mathbb{F}_۲^k$ و U را زیرفضایی با بعد l درنظر بگیرید. تعریف می‌کنیم $\sum_i(U) := \sum_{x \in U} x^i$.

لم ۱۷.٦.٦. اگر i دارای کمتر از l یک در بسط دودویی خود باشد، آن‌گاه $\sum_i(U) = ۰$.

اثبات. استقراء را به‌کار می‌گیریم. حالت $l = ۱$ بدیهی است. فرض کنید ادعا برای یک مقادیر l درست باشد و فرض کنید V دارای بعد $l+۱$ باشد و $V = U \cup (U+b)$ که در آن U دارای بعد l است؛ در این صورت:

$$\sum_i(V) = \sum_i(U) + \sum_{x \in U}(x+b)^i = \sum_{v=۰}^{i-۱} \binom{i}{v} b^{i-v} \sum_v(U).$$

اگر بسط دودویی i دارای حداکثر l یک باشد، آن‌گاه با استفاده از قضیه ۱.۴.۵، ضریب دوجمله‌ای $\binom{i}{v}$، که $v < i$، برابر با ۰ است، مگر آن که در آن بسط دودویی v دارای کمتر از l تا ۱ باشد، در چنین حالتی $\sum_v(U)$ با استفاده از فرض استقرا برابر با ۰ است. □

قضیه ۱۸.٦.٦. کد BCH دودویی اولیه C با طول $n = ۲^m - ۱$ و فاصله طراحی‌شده $\delta = ۲^l - ۱$ دارای کمترین—فاصله δ است.

اثبات. فرض کنید U یک زیرفضای l بعدی از $\mathbb{F}_{۲^m}$ باشد. بردار c را که دارای یک‌هایی دقیقاً در مکان‌های متناظر با عناصر ناصفر U است، درنظر بگیرید؛ یعنی:

$$c(x) = \sum_{j:\alpha^j \in U \setminus \{۰\}} x^j.$$

فرض کنید $۱ \leq i \leq ۲^l - ۱$؛ در این‌صورت بسط دودویی i دارای کمتر از l عدد یک می‌باشد. علاوه‌براین $c(\alpha^i) = \sum_i(U)$؛ بنابراین، با استفاده از لم ۱۷.۶.۶ داریم $c(\alpha^i) = ۰$ برای $۱ \leq i < ۲^l - ۱$؛ یعنی $c(x)$ کدکلمه‌ای در C است. □

نتیجه‌گیری ۱۹.۶.۶. یک کد BCH اولیه با فاصله طراحی‌شده δ دارای فاصله $d \leq ۲\delta - ۱$ است.

اثبات. در قضیه ۱۸.۶.۶، مقدار l را طوری درنظر بگیرید که $۲^{l-۱} \leq \delta \leq ۲^l - ۱$. کد موجود در قضیه ۱۸.۶.۶ زیرکدی از این با فاصله طراحی‌شده δ است. □

اگرچه این مطلب خیلی مشکل نیست، زمان بسیار زیادی از ما می‌گیرد تا تخمین‌های قابل قبولی برای بعد واقعی یک کد BCH ارایه دهیم. در حالت دودویی، تخمین $۲^m - ۱ - mt$ در حالت $\delta = ۲t + ۱$ را داریم که به‌وضوح برای مقادیر به‌اندازه کافی بزرگ t ضعیف می‌باشد، اگرچه این تخمین برای مقادیر کوچک t (نسبت به m)، دقیق می‌باشد؛ خواننده علاقه‌مند را به مرجع [۴۶] ارجاع می‌دهیم. با ترکیب این تخمین‌ها، می‌توان به‌آسانی نشان داد که کدهای BCH اولیه با طول بزرگ، در مفهوم فصل ۵ کدهای بدی می‌باشند؛ یعنی اگر C_v یک کد BCH اولیه $[n_v, k_v, d_v]$ برای $v = ۱, ۲, \cdots$ باشد و $n_v \to \infty$، آن‌گاه $k_v/n_v \to ۰$ یا $d_v/n_v \to ۰$.

در بخش ۶.۱ اشاره کردیم که گروه خودریختی یک کد دوری به طول n روی $\mathbb{F}_q$ نه تنها شامل جای‌گشت‌های دوری است، بلکه شامل π_q نیز می‌باشد. برای کدهای BCH می‌توانیم بیشتر از این اثبات نماییم. یک کد BCH اولیه C با طول $n = q^m - ۱$ روی $\mathbb{F}_q$ با فاصله طراحی‌شده d را درنظر بگیرید، یعنی α، $\alpha^۲$، $\cdots$، $\alpha^{d-۱}$ صفرهای تعیین‌شده کدکلمات هستند که α یک عضو اولیه از $\mathbb{F}_{q^m}$ است.

مکان‌های سمبل‌های موجود در کدکلمات را با X_i $(i = ۰, ۱, \cdots, n-۱)$ نشان می‌دهیم که $X_i = \alpha^i$. این کد را با $\bar{C}$ با اضافه نمودن یک بررسی‌توازن سراسری توسعه می‌دهیم. این مکان اضافی را با ∞ نشان می‌دهیم و قراردادهای قبلی درباره قواعد حساب با سمبل ∞ را درنظر می‌گیریم. کدکلمه $(c_۰, c_۱, \cdots, c_\infty)$ را با $c_۰ + c_۱x + \cdots + c_{n-۱}x^{n-۱} + c_\infty x^\infty$ معرفی می‌کنیم و قراردادهای بیشتر $۱ \cdot ۱^\infty := ۰$، $(\alpha^i)^\infty := ۰$ برای $i \not\equiv ۰ \bmod n$ را درنظر می‌گیریم.

حال نشان خواهیم داد که $\bar{C}$ تحت جای‌گشت‌های گروه جای‌گشتی آفین[۲۹] $AGL(۱, q^m)$، عمل‌کننده روی مکان‌ها، پایاست (بخش ۱.۱ را نیز ببینید). این گروه شامل جای‌گشت‌های:

$$P_{u,v}(X) := uX + v, \qquad (u \in \mathbb{F}_{q^m}, v \in \mathbb{F}_{q^m}, u \neq ۰)$$

[۲۹] affine permutation group

است. این گروه، ۲–ترایا[۳۰] است. درابتدا مشاهده می‌کنید که $P_{\alpha,0}$ شیفت دوری روی مکان‌های C است و ∞ را ثابت نگه می‌دارد. فرض کنید $(c_0, c_1, \cdots, c_{n-1}, c_\infty) \in \bar{C}$ و $P_{u,v}$ کلمه جای‌گشتی $(c'_0, c'_1, \cdots, c'_\infty)$ را به‌دست دهد؛ در این‌صورت برای $0 \leq k \leq d-1$ داریم:

$$\sum_i c'_i \alpha^{ik} = \sum_i c_i (u\alpha^i + v)^k = \sum_i c_i \sum_{l=0}^{k} \binom{k}{l} u^l \alpha^{il} v^{k-l}$$

$$= \sum_{l=0}^{k} \binom{k}{l} u^l v^{k-l} \sum_i c_i (\alpha^l)^i = 0$$

زیرا مجموع داخلی برای $0 \leq l \leq d-1$ برابر با 0 است؛ چراکه $c \in \bar{C}$؛ بنابراین، قضیه زیر را داریم.

قضیه ۲۰.٦.٦. هر کد BCH اولیه گسترش‌یافته با طول $n+1 = q^m$ روی $\mathbb{F}_q$ شامل $AGL(1, q^m)$ به‌عنوان گروهی از خودریختی‌ها می‌باشد.

نتیجه‌گیری ۲۱.٦.٦. کمترین–وزن از یک کد BCH دودویی، عددی فرد است.

اثبات. فرض کنید C چنین کدی باشد. نشان داده‌ایم که $Aut(\bar{C})$ روی مکان‌ها پایاست. این مطلب مشابه با این است که ما تنها کلمات با کمترین–وزن در $\bar{C}$ را درنظر بگیریم؛ بنابراین، $\bar{C}$ دارای کلمات با کمترین–وزن با یک ۱ در آخرین مکان بررسی است. □

٦.٧ کدگشایی کدهای BCH

مجدداً یک کد BCH با طول n روی $\mathbb{F}_q$ با فاصله طراحی‌شده $\delta = 2t+1$ را درنظر بگیرید و β را یک ریشه nام واحد در $\mathbb{F}_{q^m}$ فرض کنید. کدکلمه $C(x)$ را درنظر گرفته و فرض کنید کلمه دریافتی برابر با:

$$R(x) = R_0 + R_1 x + \cdots + R_{n-1} x^{n-1},$$

باشد. فرض کنید $E(x) := R(x) - C(x) = E_0 + E_1 x + \cdots + E_{n-1} x^{n-1}$ بردار خطا باشد. تعریف می‌کنیم:

مکان‌هایی که یک خطا رخ می‌دهد $M := \{i \mid E_i \neq 0\}$,

تعداد خطاها $e := |M|$,

که ما آن را چندجمله‌ای تشخیص–خطا می‌نامیم $\sigma(z) := \prod_{i \in M}(1 - \beta^i z)$,

$\omega(z) := \sum_{i \in M} E_i \beta^i z \prod_{j \in M \setminus \{i\}} (1 - \beta^i z)$.

[۳۰] 2-transitive

واضح است که اگر بتوانیم $\sigma(z)$ و $\omega(z)$ را بیابیم، آن‌گاه خطاها می‌توانند تصحیح شوند. درواقع یک خطا در مکان i رخ می‌دهد اگر و تنها اگر $\sigma(\beta^{-i}) = ۰$ و در آن حالت، خطا برابر است با $E_i = -\omega(\beta^{-i})\beta^i/\sigma'(\beta^{-i})$. از اینجا به‌بعد فرض می‌کنیم $e \le t$ (اگر $e > t$ ما انتظار نداریم که بتوان خطاها را تصحیح نمود). مشاهده می‌کنید که:

$$\begin{aligned}\frac{\omega(z)}{\sigma(z)} &= \sum_{i\in M} \frac{E_i\beta^i z}{۱-\beta^i z} = \sum_{i\in M} E_i \sum_{l=۱}^{\infty} (\beta^i z)^l \\ &= \sum_{l=۱}^{\infty} z^l \sum_{i\in M} E_i\beta^{li} = \sum_{l=۱}^{\infty} z^l E(\beta^l),\end{aligned}$$

که در آن تمامی محاسبات با سری‌های توانی روی $\mathbb{F}_{q^m}$ می‌باشد. برای $۱ \le l \le ۲t$ داریم $E(\beta^l) = R(\beta^l)$؛ یعنی گیرنده $۲t$ مختصات اول در طرف راست را می‌داند؛ بنابراین، $\omega(z)/\sigma(z)$ در پیمانه $z^{۲t+۱}$ معلوم است. ادعا می‌کنیم که گیرنده باید چندجمله‌ای‌های $\sigma(z)$ و $\omega(z)$ را به‌گونه‌ای تعیین نماید که $\deg\omega(z) \le \deg\sigma(z)$ و $\deg\sigma(z)$ به‌اندازه کافی تحت شرط زیر کوچک باشد:

$$\frac{\omega(z)}{\sigma(z)} = \sum_{l=۱}^{۲t} z^l R(\beta^l) \bmod z^{۲t+۱}. \qquad (۵)$$

فرض کنید $S_l := R(\beta^l)$ برای $l = ۱, \ldots, ۲l$ و $\sigma(z) = \sum_{i=۰}^{e} \sigma_i z^i$؛ در این‌صورت:

$$\omega(z) \equiv (\sum_{l=۱}^{۲t} S_l z^l)(\sum_{i=۰}^{e} \sigma_i z^i) = \sum_k (\sum_{i+l=k} S_l\sigma_i) \bmod z^{۲t+۱}.$$

ازآنجایی که $\omega(z)$ دارای درجه کمتر یا مساوی e است؛ داریم:

$$\sum_{i+l=k} S_l\sigma_i = ۰, \quad e+۱ \le k \le ۲t \text{ برای } .$$

این یک دستگاه با $۲t-e$ معادله خطی برای متغیرهای نامعین $\sigma_۱$، ...، σ_e (می‌دانیم $\sigma_۰ = ۱$) است. فرض کنید $\tilde{\sigma}(z) = \sum_{i=۰}^{e} \tilde{\sigma}_i z^i$ (که در آن $\tilde{\sigma}_۰ = ۱$) چندجمله‌ای با کمترین درجه یافت‌شده توسط حل این معادلات باشد (می‌دانیم حداقل جواب $\sigma(z)$ وجود دارد). برای $e+۱ \le k \le ۲t$ داریم:

$$۰ = \sum_l S_{k-l}\tilde{\sigma}_l = \sum_{i\in M}\sum_l E_i\beta^{(k-l)i}\tilde{\sigma}_l = \sum_{i\in M} E_i\beta^{ik}\tilde{\sigma}(\beta^{-i}).$$

می‌توانیم طرف راست را به‌عنوان دستگاهی از معادلات خطی برحسب $E_i\tilde{\sigma}(\beta^{-i})$ با ضرایب β^{ik} تعبیر کنیم. بنابراین، دترمینان ضرایب مجدداً واندرموند است، پس مخالف صفر است؛ بنابراین، $E_i\tilde{\sigma}(\beta^{-i}) = ۰$ برای $i \in M$. چون $E_i \ne ۰$ برای $i \in M$ می‌بینیم که $\tilde{\sigma}(z)$ عاد می‌کند $\sigma(z)$ را؛ یعنی $\tilde{\sigma}(z) = \sigma(z)$؛ بنابراین، درواقع جواب $\tilde{\sigma}(z)$ با کمترین درجه، مساله ما را حل می‌کند و دیده‌ایم که یافتن آن، حل یک دستگاه معادلات خطی را منجر می‌شود. مزیت این تقریب این است که کدگشا دارای یک الگوریتم است

که به e وابسته نیست. البته، در عمل یافتن یک الگوریتم سریع مهم‌تر از آنچه که در واقع ما تنها از یک دیدگاه تئوری درنظر گرفته‌ایم، می‌باشد. چنین الگوریتمی (با کاربرد) توسط برلیکمپ[۳۱] (مراجع [۲] و [۲۴]) طراحی شد و اغلب به‌عنوان کدگشای برلیکمپ[۳۲] از آن یاد می‌شود.

اگر ما چندجمله‌ای (معلوم) طرف راست رابطه ۵ را $S(z)$ بنامیم و تعریف کنیم $G(z) := z^{۲t+۱}$، آن‌گاه این رابطه به‌صورت زیر در می‌آید:

$$S(z)\sigma(z) \equiv \omega(z) \bmod G(z). \qquad (٦)$$

نیاز داریم تا جوابی از این هم‌نهشتی با σ از درجه کمتر یا مساوی t و ω از درجه کمتر از درجه σ را بیابیم. این جواب (یکتا)، احتمال تصحیح خطا را تعیین می‌کند. در بخش ۹.۵، با هم‌نهشتی مشابهی مواجه می‌شویم.

٦.٨ کدهای رید–سولومن

یکی از ساده‌ترین مثال‌های کدهای BCH، یعنی حالت $n = q - ۱$، ثابت شده که دارای کاربردهای بسیاری است.

تعریف ۱.٦.٨. یک کد رید–سولومن[۳۳] (کد RS) یک کد BCH اولیه با طول $n = q - ۱$ روی $\mathbb{F}_q$ است. مولد چنین کدی دارای شکلی به‌صورت $g(x) = \prod_{i=۱}^{d-۱}(x - \alpha^i)$ است که در آن α یک عضو اولیه از $\mathbb{F}_q$ است.

با استفاده از کران BCH (قضیه ۲.٦.٦)، کمترین–فاصله یک کد RS با این مولد $g(x)$ حداقل برابر d می‌باشد. با مراجعه به بخش ٦.۲، این کد دارای بعد $k = n - d + ۱$ است؛ بنابراین، نتیجه ۱.۵.۲ ایجاب می‌کند تا کمترین–فاصله برابر d باشد و کد RS یک کد تفکیک‌پذیر با بیشترین فاصله باشد.

فرض کنید به کدی برای یک کانال نیاز داریم که دارای خطاهای تصادفی نباشد (شبیه کانال BSC)، اما به‌جای آن دارای خطاهایی باشد که به‌صورت گروهی[۳۴] رخ دهند (یعنی چندین خطای نزدیک به‌هم). این حالت اغلب در عمل رخ می‌دهد (مخابرات، نوارهای ضبط صوت، دیسک فشرده). برای چنین کانالی، کدهای RS اغلب به‌کار می‌رود. این روش را تشریح می‌کنیم. فرض کنید اطلاعات دودویی به‌صورت رشته‌های با m سمبل، که به‌عنوان عناصر $\mathbb{F}_{۲^m}$ تعبیر شده‌اند، رخ داده‌اند. اگر اینها با استفاده از

[۳۱] E. R. Berlekamp
[۳۲] Berlekamp-decoder
[۳۳] Reed-solomon
[۳۴] bursts

کد RS کد شوند، آن‌گاه یک دسته پشت سر هم از خطاها (به‌صورت دنباله‌هایی از ۰ و ۱) تنها روی تعداد کمی سمبل متوالی در یک کدکلمه از کد RS تاثیر خواهد گذاشت. البته این موضوع می‌تواند برای هر کدی رخ دهد، اما چون کدهای RS، MDS هستند، آنها در عمل مفید هستند. یک کاربرد مهم‌تر در بخش ۱۱.۲ رخ خواهد داد. در ارتباط با این کاربرد، تقریب اساسی رید و سولومن را بیان می‌کنیم. فرض کنید $n = q - 1$ و α یک عضو اولیه از $\mathbb{F}_q$ باشد. به‌طور معمول، $a = (a_0, a_1, \cdots, a_{k-1})$ را با $a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} = a(x)$ یکی درنظر می‌گیریم؛ در این‌صورت:

$$C = \{(c_0, c_1, \cdots, c_{n-1}) | c_i = a(\alpha^i), 0 \leq i < n, a \in \mathbb{F}_q^k\},$$

یک کد RS با $d = n - k + 1$ است. برای دیدن این مطلب، ابتدا مشاهده کنید که C به‌وضوح دوری است. تعریف C و لم ۲.۶.۵، کدکلمه c که دارای $na(x)$ به‌عنوان چندجمله‌ای ماتسون—سولومن است را ایجاب می‌کند. چون درجه $a(x)$ کمتر یا مساوی $k - 1$ است، این مطلب بدان معناست که $c(\alpha^i) = 0$ برای $i = 1, 2, \cdots, n - k$؛ بنابراین، C یک کد RS است. این نمایش، روش کدگذاری بسیار کارایی برای کدهای RS هرچند آن متقارن نباشد، ارایه می‌دهد.

اگر کدکلمات C را با اضافه نمودن سمبل $c_n = a(0)$ بسط دهیم، آن‌گاه $\sum_{i=0}^{n} c_i = a_0 q = 0$؛ بنابراین، در واقع $\bar{C}$ را به‌دست می‌آوریم. اگر $c_n = 0$، یعنی $c(1) = 0$، آن‌گاه این کلمه دارای وزن بیشتر یا مساوی $n - k + 2$ است و به‌وضوح اگر $c_n \neq 0$، آن‌گاه این مطلب باز درست است؛ بنابراین، کد $\bar{C}$ نیز یک کد MDS است.

نمایش دوم یک کد رید—سولومن به ما اجازه می‌دهد تا این ایده را گسترش دهیم. دراینجا $\mathbb{F}_{q^m}$ را به‌عنوان الفبا درنظر گرفته و n عضو متمایز را از این میدان اختیار می‌کنیم؛ گیریم α_1، α_2، $\cdots$، α_n. فرض کنید $v = (v_1, v_2, \cdots, v_n)$ برداری از $\mathbb{F}_{q^m}^n$ با درایه‌های ناصفر باشد و می‌نویسیم $a := (\alpha_1, \alpha_2, \cdots, \alpha_n)$.

تعریف ۲.۶.۸. کد رید—سولومن گسترش‌یافته[۳۵] $GRS_k(a, v)$ شامل تمامی $(v_1 f(\alpha_1), v_2 f(\alpha_2), \cdots, v_n f(\alpha_n))$ به‌عنوان کدکلمات است که در آن f متعلق به چندجمله‌ای‌های با درجه کمتر از k در $\mathbb{F}_{q^m}[x]$ می‌باشد.

با روشی مشابه با روش فوق، می‌بینیم که یک کد رید—سولومن گسترش‌یافته و دوگان آن کدهای MDS هستند.

توصیف دوم ما از کدهای RS نیز به ما اجازه می‌دهد تا یک ایده محکم از کدهایی که با استفاده از هندسه جبری تعریف شده‌اند را ارایه دهیم. در تعریف ۴.۱.۳ دیدیم که خط تصویری از مرتبه q می‌تواند با معرفی مولفه‌های نقاط (x, y) توصیف شود که در آن (x, y) و (cx, cy) نقطه یکسانی هستند

[۳۵] generalized Reed-Solomon code

($c \in \mathbb{F}_q$). اگر $a(x,y)$ و $b(x,y)$ چندجمله‌ای‌های همگنی با درجه یکسان باشند، آن‌گاه مطالعه کسر گویای $a(x,y)/b(x,y)$ روی خط تصویر، بامعناست (چون یک تغییر در مولفه‌ها مقدار کسر را تغییر نمی‌دهد). نقطه $Q := (۱, ۰)$ را به‌عنوان نقطه خاصی بر روی این خط برمی‌داریم. نقاط باقی‌مانده شامل $(۰, ۱)$ و $(\alpha^i, ۱)$ $(۰ \leq i < q-۱)$ به‌عنوان مختصات می‌باشند که در آن α مجدداً یک عضو اولیه از $\mathbb{F}_q$ را نمایش می‌دهد. حال آن دسته از کسرهای گویای $a(x,y)/y^l$ را که $l < k$، درنظر می‌گیریم (و البته $a(x,y)$ همگن از درجه l می‌باشد). این یک فضای برداری با بعد k است (گوییم K) و فوراً دیده می‌شود که این توصیف از کدهای RS که در بالا داده شده، با شماره‌گذاری نقاط خط با یک ترتیب ثابت (گیریم $P_۰$، $P_۱$، $\cdots$، $P_{q-۱}$) و درنظر گرفتن آن به‌صورت کدکلمات $(f(P_۰)$، $\cdots$، $f(P_{q-۱})$ که در آن f متعلق به فضای K است، معادل است. این توابع به‌صورتی انتخاب شده‌اند که درواقع می‌توان مقادیر آنها را در تمامی نقاط P_i محاسبه نمود؛ این مطلب برای Q برقرار نیست. به زبان آنالیز، نقطه Q برای توابع متعلق به K، قطب[۳۶] با مرتبه حداکثر $k-۱$ است.

ساده‌ترین مثال‌های کدهای هندسه‌جبری این ساختار را با جانشین نمودن خط تصویری با منحنی تصویری در یک فضای تصویری تعمیم می‌دهد. کدهای هندسه‌جبری را در فصل ۱۰ مطالعه می‌کنیم.

حال نگاهی به کدهای MDS به‌طور کلی می‌اندازیم. اگر C یک کد $[n,k]$ با کمترین—فاصله $d = n-k+۱$ باشد، آن‌گاه C بر روی هر k مکانی متقارن است (ارجاع به مساله ۲.۳.۸).

قضیه ۳.٦.۸. دوگان یک کد MDS نیز یک کد MDS است.

اثبات. فرض کنید $G = (\, I_k \quad P\,)$ ماتریس مولد کد C باشد. چون C دارای کمترین—فاصله d است، هر مجموعه از $d-۱ = n-k$ ستون ماتریس بررسی‌توازن $H := (\, -P^T \quad I_{n-k}\,)$ به‌طور خطی مستقل است؛ بنابراین، هر زیرماتریس مربعی از H نامنفرد است؛ یعنی هیچ کدکلمه از $C^\perp$ دارای $n-k$ صفر نمی‌باشد؛ بنابراین، $C^\perp$ یک کد $[n, n-k, k+۱]$ است؛ یعنی یک کد MDS. □

فرض کنید C یک کد $[n,k,d]$ با $d = n-k+۱$ باشد. اگر مجموعه‌ای از d مکان را درنظر بگیریم و به زیرکد C با صفرهایی در سایر مکان‌ها، نگاه کنیم، این زیرکد دارای بعدی بزرگ‌تر یا مساوی $k-(n-d) = ۱$ است. چون این زیرکد دارای کمترین—فاصله d است، باید دارای بعدی دقیقاً برابر با ۱ باشد. درنتیجه برای $n \geq d' > d$ با تخصیص مجموعه‌ای از d' مکان و درنظر گرفتن کدکلمات به‌صورتی که در سایر مکان‌ها برابر با صفر باشند، زیرکدی از C با بعد $d'-d+۱$ تعریف خواهد شد. این نتیجه را به‌صورت یک لم فرمول‌بندی می‌کنیم.

---

[۳۶] pole

لم ۴.۶.۸. برای $n \geq d' \geq d = n - k + ۱$، زیرکد یک کد MDS با پارامترهای n، k و d، شامل تمامی کدکلماتی که خارج از یک مجموعه از d' مکان، صفر می‌باشند دارای بعد $d' - d + ۱$ است.

ما این لم و یک فرم مشابه از فرمول معکوس موبیوس ۴.۱.۱ را برای یافتن شمارنده وزنی یک کد MDS به‌کار خواهیم برد. درابتدا یک فرم مشابه از فرمول معکوس موبیوس را اثبات می‌کنیم.

تعریف ۵.۶.۸. اگر N یک مجموعه تعریف باشد و $S \subset T \subset N$، آن‌گاه تعریف می‌کنیم:

$$\mu(S,T) := (-۱)^{|T|-|S|}.$$

قضیه ۶.۶.۸. فرض کنید N یک مجموعه تعریف باشد و فرض کنید f یک تابع تعریف‌شده روی یک زیرمجموعه از N باشد. اگر:

$$g(S) := \sum_{R \subset S} f(R),$$

آن‌گاه:

$$f(T) = \sum_{S \subset T} \mu(S,T) g(S).$$

اثبات.

$$\begin{aligned} \textstyle\sum_{S \subset T} \mu(S,T) g(S) &= \textstyle\sum_{S \subset T} \mu(S,T) \sum_{R \subset S} f(R) \\ &= \textstyle\sum_{R \subset T} f(R) \sum_{R \subset S \subset T} \mu(S,T), \end{aligned}$$

و نتیجه از تساوی زیر حاصل می‌شود:

$$\sum_{R \subset S \subset T} \mu(S,T) = \sum_{j=۰}^{|T|-|R|} \binom{|T| - |R|}{j} (-۱)^j = (۱ - ۱)^{|T|-|R|} = \begin{cases} ۰, & \text{اگر } R \neq T \\ ۱, & \text{اگر } R = T \end{cases}$$

□

حال نشان می‌دهیم که شمارنده وزنی یک کد MDS توسط پارامترهایش تعیین می‌شود.

قضیه ۷.۶.۸. فرض کنید C یک کد $[n,k]$ با فاصله $d = n - k + ۱$ باشد. اگر شمارنده وزنی C برابر با $۱ + \sum_{i=d}^{n} A_i z^i$ باشد، آن‌گاه:

$$A_i = \binom{n}{i} (q-۱) \sum_{j=۰}^{i-d} (-۱)^j \binom{i-۱}{j} q^{i-j-d} \qquad (i = d, d+۱, \cdots, n).$$

اثبات. اگر R زیرمجموعه‌ای از $N := \{۰, ۱, \cdots, n-۱\}$ باشد، $f(R)$ را تعداد کدکلمات $(c_۰, c_۱, \cdots, c_{n-۱})$ تعریف کنید به‌طوری‌که $c_i \neq ۰ \Leftrightarrow i \in R$. اگر g را مانند قضیه ٦.٦.٨ تعریف کنیم، آن‌گاه با استفاده از لم ۴.٦.٨ داریم:

$$g(S) = \begin{cases} ۱, & \text{اگر } |S| \leq d-۱ \\ q^{|S|-d+۱}, & \text{اگر } n \geq |S| \geq d \end{cases}$$

با به‌کارگیری تعریف f، داریم $A_i = \sum_{R \subset N, |R|=i} f(R)$؛ بنابراین، کاربردِ قضیه ٦.٦.٨ نتیجه می‌دهد:

$$\begin{aligned} A_i &= \sum_{R \subset N, |R|=i} \sum_{S \subset R} \mu(S,R) g(S) \\ &= \binom{n}{i} \{\sum_{j=۰}^{d-۱} \binom{i}{j} (-۱)^{i-j} + \sum_{j=d}^{i} \binom{i}{j} (-۱)^{i-j} q^{j-d+۱}\} \\ &= \binom{n}{i} \sum_{j=d}^{i} \binom{i}{j} (-۱)^{i-j} (q^{j-d+۱} - ۱). \end{aligned}$$

حال اگر ما j را با $i-j$ جای‌گزین نموده، سپس تساوی $\binom{i}{j} = \binom{i-۱}{j-۱} + \binom{i-۱}{j}$ را به‌کار بریم، نتیجه حاصل می‌شود. □

قضیه ۷.٦.٨، محدودیت زیر را روی اندازه الفبای یک کد MDS مطرح می‌کند.

قضیه ۸.٦.٨ اگر یک کد MDS روی $\mathbb{F}_q$ به طول n و بعد k وجود داشته باشد، آن‌گاه $q \geq n-k+۱$ یا $k \leq ۱$.

اثبات. فرض کنید $d = n-k+۱$. با استفاده از قضیه ۷.٦.٨ برای $d < n$ داریم $۰ \leq A_{d+۱} = \binom{n}{d+۱}(q-۱)(q-d)$. □

چون دوگان یک کد MDS نیز MDS است (قضیه ۳.٦.٨)، نتیجه زیر را داریم:

نتیجه‌گیری ۹.٦.٨. اگر یک کد MDS روی $\mathbb{F}_q$ با طول n و بعد k وجود داشته باشد، آن‌گاه $q \geq k+۱$ یا $d = n-k+۱ \leq ۲$.

٦.٩ کدهای باقی‌مانده مربعی

در این بخش، کدهایی را درنظر خواهیم گرفت که طول کلمه n یک عدد اولِ فرد باشد. الفبای $\mathbb{F}_q$ باید در این شرط صدق کند: q یک باقی‌مانده مربعی در پیمانه n باشد؛ یعنی $q^{(n-۱)/۲} \equiv ۱ \bmod n$. به‌طور

معمول α یک ریشه nام اولیه واحد را در یک توسیع میدان $\mathbb{F}_q$ نشان خواهد داد. بعداً ثابت می‌شود که نیاز داریم تا α در یک شرط اضافی صدق کند. تعریف می‌کنیم:

$$R_0 := \{i^2 \bmod n \mid i \in \mathbb{F}_n, i \neq 0\}, \qquad \text{مانده‌های مربعی در } \mathbb{F}_n,$$

$$R_1 := \mathbb{F}_n^* \setminus R_0, \qquad \text{مجموعه عناصر غیرمربعی در } \mathbb{F}_n,$$

$$g_0(x) := \prod_{r \in R_0}(x - \alpha^r), \qquad g_1(x) := \prod_{r \in R_1}(x - \alpha^r).$$

چون شرط کرده‌ایم که $q \bmod n$ در R_0 باشد، چندجمله‌ای‌های $g_0(x)$ و $g_1(x)$ هردو دارای ضرایبی در $\mathbb{F}_q$ هستند (مراجعه به قضیه ۱۸.۱.۱)؛ علاوه‌براین:

$$x^n - 1 = (x-1)g_0(x)g_1(x).$$

تعریف ۱.۶.۹. کدهای دوری به طول n روی $\mathbb{F}_q$ با مولدهای $g_0(x)$، به‌ترتیب $(x-1)g_0(x)$ هردو کدهای باقی‌مانده مربعی[۳۷] (کدهای QR) نامیده می‌شوند.

ما تنها کدهای QR گسترش‌یافته در حالت دودویی را درنظر خواهیم گرفت که تعریف آن مشابه تعریف ۶.۳.۲ است. چنین کدی با اضافه‌نمودن یک بررسی‌توازن سراسری به کد با مولد $g_0(x)$ به دست می‌آید.

درمورد سایر میدان‌ها، تعریف کد گسترش‌یافته معمولاً به صورتی است که اگر $n \equiv -1 \bmod 4$، آن‌گاه کد گسترش‌یافته خوددوگان باشد، و به ترتیب، اگر $n \equiv 1 \bmod 4$، آن‌گاه دوگانِ توسیع کد با مولد $g_1(x)$ باشد (ر.ک. مرجع [۴۶]). در حالت دودویی، کد با مولد $(x-1)g_0(x)$ زیرکد با وزن زوج از یک کد QR دیگر است. اگر G ماتریس مولد برای اولین این کدها باشد، آن‌گاه ماتریس مولدی برای کد بعدی با اضافه‌نمودن یک سطر تماماً ۱ به G به‌دست می‌آوریم. اگر چنین کاری را پس از اضافه‌نمودن یک ستون تمام صفر به G انجام دهیم، ماتریس مولدی برای کد گسترش‌یافته به‌دست می‌آوریم.

در حالت دودویی این شرط که q باقی‌مانده مربعی در پیمانه n باشد، به‌معنی $n \equiv \pm 1 \bmod 8$ می‌باشد (ارجاع به بخش ۱.۱). جای‌گشت $\pi_j : i \to ij \bmod n$ با عمل کردن روی مکان‌های کدکلمات، کد با مولد $g_0(x)$ را به خودش تصویر می‌کند، اگر $j \in R_0$ و به کد با مولد $g_1(x)$ تبدیل می‌کند، اگر $j \in R_1$؛ بنابراین، کدهای با مولدهای $g_0(x)$، به‌ترتیب $g_1(x)$، هم ارز می‌باشند. اگر $n \equiv -1 \bmod 4$، آن‌گاه $-1 \in R_1$ و در آن حالت تبدیل $x \to x^{-1}$، کدکلمه‌ای از کد با مولد $g_0(x)$ را به کدکلمه‌ای از کد با مولد $g_1(x)$ تصویر می‌کند.

[۳۷] quadratic residue codes

قضیه ۲.٦.۹. اگر $c = c(x)$ کدکلمه‌ای در کد QR با مولد $g_0(x)$ بوده و $c(1) \neq 0$ و $w(c) = d$، آن‌گاه:

۱) $n \geq d^2$؛

۲) اگر $n \equiv -1 \bmod 4$، آن‌گاه $n \geq d^2 - d + 1$؛

۳) اگر $n \equiv -1 \bmod 8$ و $q = 2$، آن‌گاه $d \equiv 3 \bmod 4$.

اثبات.

۱) چون $c(1) \neq 0$، چندجمله‌ای $c(x)$ بر $(x-1)$ بخش‌پذیر نیست. با استفاده از جای‌گشت مناسب π_j می‌توانیم $c(x)$ را به یک چندجمله‌ای $\hat{c}(x)$ که بر $g_1(x)$ بخش‌پذیر است تبدیل کنیم و البته مجدداً بر $(x-1)$ بخش‌پذیر نمی‌باشد. این مطلب ایجاب می‌کند تا $c(x)\hat{c}(x)$ مضربی از $1 + x + x^2 + \cdots + x^{n-1}$ باشد. چون چندجمله‌ای $c(x)\hat{c}(x)$ دارای حداکثر d^2 ضریب ناصفر می‌باشد، ادعای اول را اثبات نموده‌ایم.

۲) در اثبات بالا ممکن است فرض کنیم $j = -1$. در این حالت واضح است که $c(x)\hat{c}(x)$ دارای حداکثر $d^2 - d + 1$ ضریب ناصفر است.

۳) فرض کنید $c(x) = \sum_{i=1}^{d} x^{l_i}$ و $\bar{c}(x) = \sum_{i=1}^{d} x^{-l_i}$. اگر $l_i - l_j = l_k - l_l$، آن‌گاه $l_j - l_i = l_l - l_k$؛ بنابراین، اگر جملاتی در حاصل‌ضرب $c(x)\hat{c}(x)$ حذف شوند، آنها چهارتایی حذف می‌شوند. از این‌رو برای یک $a \geq 0$ داریم $n = d^2 - d + 1 - 4a$. □

ثابت خواهد شد که خودتوان یک کد دوری، معرفی شده در بخش ٦.۴، ابزار نیرومندی در تجزیه و تحلیل کدهای QR است.

قضیه ۳.٦.۹. برای انتخاب مناسبی از ریشه nام اولیه واحد α، چندجمله‌ای:

$$\theta(x) := \sum_{r \in R_0} x^r,$$

خودتوان کد دودویی QR با مولد $(x-1)g_0(x)$ است، اگر $n \equiv 1 \bmod 8$ و خودتوان کد QR با مولد $g_0(x)$ است، اگر $n \equiv -1 \bmod 8$.

اثبات. به‌وضوح $\theta(x)$ یک چندجمله‌ای خودتوان است؛ بنابراین، $\theta(\alpha) = \{\theta(\alpha)\}^{۲}$؛ یعنی $\theta(\alpha) = ۰$ یا $\theta(\alpha) = ۱$. با اثباتی مشابه داریم $\theta(\alpha^i) = \theta(\alpha)$، اگر $i \in R_۰$ و $\theta(\alpha^i) + \theta(\alpha) = ۱$، اگر $i \in R_۱$. "انتخاب مناسب" α طوری است که $\theta(\alpha) = ۰$ (خواننده باید خود را قانع کند که این‌که تمامی عناصر اولیه $\mathbb{F}_q$ در رابطه $\theta(\alpha) = ۰$ صدق کنند، غیرممکن می‌باشد). انتخاب ما ایجاب می‌کند تا $\theta(\alpha^i) = ۰$، اگر $i \in R_۰$ و $\theta(\alpha^i) = ۱$، اگر $i \in R_۱$. سرانجام داریم $\theta(\alpha^۰) = (n-۱)/۲$. به این ترتیب، حکم ثابت می‌شود. □

با کمک θ، اکنون ماتریس C با درایه‌های ۰ و ۱ را (معروف به ماتریس گردشی[۳۸])، با درنظر گرفتن کلمه θ به‌عنوان سطر اول و تمامی شیفت‌های دوری به‌عنوان سایر سطرها، می‌سازیم. فرض کنید $c := (۰۰\cdots۰)$، اگر $n \equiv ۱ \bmod ۸$ و $c := (۱۱\cdots۱)$، اگر $n \equiv -۱ \bmod ۸$؛ داریم:

$$G := \begin{pmatrix} ۱ & ۱ & \cdots & ۱ \\ c^T & & C & \end{pmatrix}.$$

از قضیه ۳.۶.۹ نتیجه می‌شود که سطرهای G (که به‌وضوح مستقل نمی‌باشند)، کد QR دودویی گسترش‌یافته با طول $n+۱$ را تولید می‌کنند. حال مکان‌های مختصات کدکلمات این کد را با نقاط خط تصویری مرتبه n، یعنی ∞، ۱، $\cdots$، $n-۱$ شماره‌گذاری می‌کنیم. بررسی‌توازن سراسری در ابتدا و دارای شماره ∞ است. قراردادهای معمول را درباره عمل‌گرهای ریاضی شامل ∞ درنظر می‌گیریم. گروه $PSL(۲,n)$ شامل تمامی تبدیل‌های $x \to (ax+b)/(cx+d)$ با a، b، c، d متعلق به $\mathbb{F}_n$ و $ad-bc = ۱$ است. بررسی این‌که این گروه، تولید شده توسط تبدیلات $S : x \to x+۱$ و $T : x \to -x^{-۱}$ است، مشکل نمی‌باشد. به‌وضوح S روی مکان‌های متفاوت از ∞ یک شیفت دوری است و ∞ را ثابت نگه می‌دارد. با استفاده از تعریف یک کد QR، S کد گسترش‌یافته را ثابت نگه می‌دارد. برای بررسی تاثیر T روی کد QR گسترش‌یافته، کافی است تا بررسی کنیم کدام T روی سطرهای G اعمال شده است. با یک تمرین آسان (و شاید تا حدی کسل‌کننده) می‌توان نشان داد که T یک سطر از G را به یک ترکیب خطی از حداکثر سه سطر از G تصویر می‌کند (خواننده‌ای که در این کار موفق نیست به مرجع [۴۲] ارجاع داده می‌شود)؛ بنابراین، هردوی S و T، کد QR گسترش‌یافته را ثابت نگه می‌دارند که این مطلب اثباتی بر قضیه زیر است.

قضیه ۴.۶.۹. گروه خودریختی کد QR دودویی گسترش‌یافته با طول $n+۱$، شامل $PSL(۲,n)$ است.

تعریف اصلاح شده از کد گسترش‌یافته که اخیراً بیان نمودیم، ما را مطمئن می‌کند که قضیه ۴.۶.۹ برای کدهای غیردودویی نیز درست است (ر.ک. مرجع [۴۶]).

---

[۳۸] circulant

نتیجه‌گیری ۵.٦.۹ یک کلمه با کمترین—وزن در یک کد QR دودویی، در شرایط قضیه ۲.٦.۹ صدق می‌کند.

اثبات. اثبات مشابه با اثبات نتیجه ۲۱.٦.٦ است. در این حالت از این واقعیت که $PSL(۲,n)$ تعدی است، استفاده می‌کنیم؛ بنابراین، کمترین—وزن، عددی فرد می‌باشد. □

مثال ٦.٦.۹. (a) فرض کنید $q=۲$ و $n=۷$؛ داریم:

$$x^۷-۱=(x-۱)(x^۳+x+۱)(x^۳+x^۲+۱).$$

$g_۰(x)$ را به‌عنوان مولد می‌گیریم. انتخاب α صادق در قضیه ۳.٦.۹ ایجاب می‌کند که $x+x^۲+x^۴$ نیز یک مولد باشد؛ بنابراین، $g_۰(x)=۱+x+x^۳$. البته این کد، کد همینگ $[۷,۴]$ (کامل) است (بخش ۳.۳ و قضیه ۲.۳.۳ را ببینید). زیرکد با وزن زوجِ متناظر، در مثال ۴.٦.۱ بررسی شده است.

(b) فرض کنید $q=۲$ و $n=۲۳$؛ داریم:

$$\begin{aligned}x^{۲۳}-۱ = \ & (x-۱)(x^{۱۱}+x^۹+x^۷+x^٦+x^۵+x+۱)\\ & \times(x^{۱۱}+x^{۱۰}+x^٦+x^۵+x^۴+x^۲+۱).\end{aligned}$$

مجدداً $g_۰(x)$ را مضربی از $\theta(x)$ می‌گیریم که برابر است با:

$$x^{۱۱}+x^۹+x^۷+x^٦+x^۵+x+۱.$$

با استفاده از نتیجه ۵.٦.۹، کد QR متناظر C دارای کمترین—فاصله $d\geq ۷$ است.

چون $|c|=۲^{۱۲}$ و $\sum_{i=۰}^{۳}\binom{۲۳}{i}=۲^{۱۱}$، نتیجه می‌شود که d برابر با ۷ است و با استفاده از ٦.۳.۱، C یک کد کامل است. چون کد گلی دودویی از بخش ۴.۲ یکتاست، در اینجا نشان داده‌ایم که این کد در واقع یک کد QR است.

چندین مثال دیگر را به‌عنوان تمرین واگذار می‌کنیم (بخش ٦.۱۳).

٦.۱۰ کدهای دوری دودویی با طول $۲n$ (n فرد)

فرض کنید n فرد باشد و $x^n-۱=f_۱(x)f_۲(x)\cdots f_t(x)$ تجزیه $x^n-۱$ به عوامل تحویل‌ناپذیر در $\mathbb{F}_۲[x]$ باشد.

تعریف می‌کنیم $g_۱(x) = f_۱(x)\cdots f_k(x)$ و $g_۲(x) = f_{k+۱}(x)\cdots f_l(x)$ که در آن $k < l < t$. فرض کنید $r_۱ := \deg g_۱$ و $r_۲ := \deg g_۱g_۲$.

فرض کنید $C_۱$ کد دوری به‌طول n و بعد $n - r_۱$ با مولد $g_۱(x)$ باشد و فرض کنید $C_۲$ کد دوری به طول n و بعد $n - r_۲$ و با مولد $g_۱(x)g_۲(x)$ باشد. هم‌چنین فرض کنید d_i کمترین—فاصله C_i $(i = ۱, ۲)$ باشد. به‌وضوح $d_۲ \geq d_۱$.

در ادامه کد دوری C با طول $۲n$، بعد $۲n - r_۱ - r_۲$ و مولد $g(x) := g_۱^۲(x)g_۲(x)$ را مورد مطالعه قرار خواهیم داد. ادعا می‌کنیم که این کد دارای ساختار زیر است:

فرض کنید $a = (a_۰, a_۱, \cdots, a_{n-۱}) \in C_۱$ و $c = (c_۰, c_۱, \cdots, c_{n-۱}) \in C_۲$. تعریف کنید $b := a + c$. چون n فرد است، می‌توانیم کلماتی را به‌صورت:

$$w := (a_۰, b_۱, a_۲, \cdots, b_{n-۲}, a_{n-۱}, b_۰, a_۱, \cdots, a_{n-۲}, b_{n-۱})$$

تعریف کنیم که متعلق به C می‌باشند و با این روش تمامی کلمات C را می‌یابیم؛ (ادعای اخیر از مباحث بُعد نتیجه می‌شود). برای تشریح این مطلب، به‌صورت زیر عمل می‌کنیم. بنویسید:

$$\begin{aligned} a(x) &= a_۰ + a_۱x + \cdots + a_{n-۱}x^{n-۱} \\ &= (a_۰ + a_۲x^۲ + \cdots + a_{n-۱}x^{n-۱}) + x(a_۱ + \cdots + a_{n-۲}x^{n-۳}) \\ &= a_e(x^۲) + xa_۰(x^۲), \end{aligned}$$

و به‌طور مشابه برای $c(x)$ و $b(x)$؛ در این‌صورت دو نمایش (یکسان) زیر را برای چندجمله‌ای $w(x)$ متناظر با کدکلمه w داریم:

$$w(x) = \{a_e(x^۲) + x^{n+۱}a_۰(x^۲)\} + \{xb_۰(x^۲) + x^nb_e(x^۲)\}, \qquad (۷)$$

و

$$w(x) = \{a(x) + x(x^n + ۱)a_۰(x^۲)\} + \{b(x) + (x^n + ۱)b_e(x^۲)\}. \qquad (۸)$$

هر دو جمله در رابطه ۸، بر $g_۱(x)$ بخش‌پذیر هستند. از رابطه ۷ می‌بینیم که اولین جمله تنها شامل توان‌های زوج x و دومی تنها شامل توان‌های فرد x می‌باشد. چون $g_۱(x)$ شامل عوامل تکراری نمی‌باشد، هر دو جمله درواقع بر $g_۱^۲(x)$ بخش‌پذیر هستند.

از رابطه ۸ داریم:

$$w(x) = (x^n + ۱)a(x) + c(x) + (x^n + ۱)c_e(x^۲),$$

به‌طوری که هر جمله بر $g_۲(x)$ بخش‌پذیر است.

چون $b = a + c$، کلمه w، جای‌گشتی از کلمه $|a\,|\,a+c|$ است (ارجاع به رابطه ۳). پس قضیه زیر را اثبات کرده‌ایم:

قضیه ۱.٦.۱۰. فرض کنید $C_۱$ یک کد دوری دودویی با طول n (فرد) با مولد $g_۱(x)$ باشد و فرض کنید $C_۲$ یک کد دوری دودویی با طول n با مولد $g_۱(x)g_۲(x)$ باشد؛ در این‌صورت کد دوری دودویی C با طول $۲n$ با مولد $g_۱^۲(x)g_۲(x)$ هم‌ارز با مجموع $|u\,|\,u+v|$ از $C_۱$ و $C_۲$ می‌باشد؛ بنابراین، C دارای کمترین —فاصله $\min\{۲d_۱, d_۲\}$ می‌باشد.

کدهای دودویی دوری خوب زیادی با طول زوج وجود ندارند. اما، قضیه زیر وجود کلاسی از مثال‌های بهینه را نشان می‌دهد.

قضیه ۲.٦.۱۰. زیرکد با وزن زوج از یک کد همینگ دودویی کوتاه‌شده، دوری است (تحت یک ترتیب مناسب از سمبل‌ها).

اثبات. دیدن این امر مشکل نمی‌باشد که تفاوتی در این‌که کد روی چه مکانی کوتاه‌شده، نیست (تمامی کدهای حاصل، هم‌ارز می‌باشند). فرض کنید $n = ۲^s - ۱$. هم‌چنین فرض کنید که $m_۱(x)$ معرف چندجمله‌ای مینیمال یک عضو اولیه α از $\mathbb{F}_۲$ باشد؛ در این‌صورت $m_۱(x)$ چندجمله‌ای مولد یک کد همینگ $[n, n-s]$ دودویی است و $(x+۱)m_۱(x)$ چندجمله‌ای مولد زیرکد با وزن زوج از آن است. در قضیه ۱.٦.۱۰ قرار دهیم $g_۱(x) = (x+۱)$ و $g_۲(x) = m_۱(x)$؛ در این‌صورت ما یک کد دوری C با طول $۲n$، بعد $۲n-s-۲$ و کمترین—فاصله ۴ می‌یابیم. از ساختار $|u\,|\,u+v|$ نتیجه می‌شود که تمام وزن‌های C زوج هستند؛ بنابراین، C شامل یک ماتریس بررسی‌توازن با یک سطر بالایی تماماً ۱ و ستون‌های مجزا می‌باشد. از این‌رو C هم‌ارز با زیرکد با وزن زوج از یک کد همینگ کوتاه شده است. □

مشاهده می‌کنیم که روش‌های متفاوتی برای اثبات قضیه قبل وجود دارد. ما مشتق هسه[۳۹] (فصل ۱ را ببینید) را به‌کار خواهیم برد. مولد C شامل ۱ به‌عنوان یک ریشه با تکرار ۲ و α یک ریشه با تکرار ۱ است. این بدان معناست که اگر $c(x) = \sum c_i x^i$ یک کدکلمه باشد، آن‌گاه:

$$\sum c_i = ۰, \quad \sum i c_i = ۰, \quad \sum c_i \alpha^i = ۰;$$

یعنی:

$$H_۱ := \begin{pmatrix} ۱ & ۱ & ۱ & \cdots & ۱ & ۱ & ۱ & \cdots & ۱ & ۱ \\ ۰ & ۱ & ۰ & \cdots & ۰ & ۱ & ۰ & \cdots & ۰ & ۱ \\ ۱ & \alpha & \alpha^۲ & \cdots & \alpha^{n-۱} & \alpha^n & \alpha^{n+۱} & \cdots & \alpha^{۲n-۲} & \alpha^{۲n-۱} \end{pmatrix},$$

[۳۹] Hasse

یک ماتریس بررسی‌توازن برای C است؛ دراینجا سطر دوم با به‌کارگیری خاصیت مشتق هسه و ریشه‌های مضاعف به‌دست آمده است. دقت کنید که $\alpha^n = ۱$. دراینجا ماتریس $H_۱$ شامل تمامی ستون‌های ممکن با یک ۱ در بالا، به‌جز $(۱۰۰۰۰\cdots۰)^T$ و $(۱۱۰۰\cdots۰)^T$ است؛ یعنی این کد درواقع هم‌ارز با زیرکد با وزن زوج از یک کد همینگ کوتاه‌شده است.

۶.۱۱ کدهای رید–مولر گسترش‌یافته

ما کلاسی از کدهای دوری (گسترش‌یافته) روی $\mathbb{F}_q$ را تعریف خواهیم نمود که هم‌ارز با کدهای رید–مولر در حالت $q = ۲$ هستند. درابتدا ایده وزن همینگ را به اعداد صحیحی که به‌صورت دستگاه اعداد qتایی نوشته می‌شوند، تعمیم می‌دهیم.

تعریف ۱.۶.۱۱. اگر q یک عدد صحیح بزرگ‌تر یا مساوی ۲ باشد و برای $۰ \le \xi_i < q$ و $i = ۰, ۱, \cdots, m-۱$ داشته‌باشیم $j = \sum_{i=۰}^{m-۱} \xi_i q^i$، در این‌صورت تعریف می‌کنیم $w_q(j) := \sum_{i=۰}^{m-۱} \xi_i$.

دقت کنید که این مجموع در $\mathbb{Z}$ رخ داده است. کلاس جدیدی از این کدها به‌صورت زیر تعریف شده است.

تعریف ۲.۶.۱۱. کد کوتاه‌شده رید–مولر گسترش‌یافته (کد GRM) از مرتبه rام با طول $n = q^m - ۱$ روی $\mathbb{F}_q$، کد دوری با مولد زیر است:

$$g(x) := \prod^{(r)} (x - \alpha^j),$$

که در آن α یک عضو اولیه در $\mathbb{F}_{q^m}$ است و اندیس بالایی (r) نشان می‌دهد که حاصل‌ضرب بر روی اعداد صحیح j می‌باشد که درآن $۰ \le j < q^m - ۱$ و $۰ \le w_q(j) < (q-۱)m - r$.

کد GRM از مرتبه rام با طول q^m دارای ماتریس مولد G^* است که از ماتریس مولد G از کد GRM کوتاه‌شده با الحاق یک ستون تماماً صفر و سپس یک سطر تماماً یک، به‌دست آمده است.

دقت کنید که مجموعه توان‌ها در این تعریف از کدهای GRM کوتاه‌شده، درواقع تحت ضرب بر q بسته است. فرض کنید $h(x)$ چندجمله‌ای بررسی کد کوتاه‌شده GRM از مرتبه r باشد؛ در این‌صورت دوگان این کد شامل چندجمله‌ای $h^*(x)$ به‌عنوان مولد است، که در آن $h^*(x)$ از $h(x)$ با تخصیص مرتبه توان‌های x به‌دست آمده است. آن با روشی مشابه با $g(x)$، دراینجا با شرط $۰ < w_q(j) \le r$، تعریف شده است.

تعمیم زیر از قضیه ۸.۴.۵ را داریم.

قضیه ۳.٦.۱۱. دوگان کد GRM مرتبه rام با طول q^m، هم‌ارز با یک کد GRM با مرتبه $(q-1)m-r-1$ است.

اثبات. در بالا دیدیم که $(x-1)h^*(x)$ مولد کد کوتاه‌شده GRM با مرتبه $(q-1)m-r-1$ است. حال اگر کدهای دوری را تا رسیدن به کدهای GRM افزایش طول دهیم، باید تعامد سطرهای ماتریس مولد را نشان دهیم. تنها چیزی که باعث می‌شود تا این مطلب، نتیجه‌ای از دوگانگی کدهای کوتاه‌شده نباشد، سطرهای تماماً ۱ است. در مورد این سطرها، عامل $(x-1)$ در مولدها و این واقعیت که طول، برابر با q^m است، دلیل تعامد است. چون جمع بعدهای این دو کد برابر با q^m است، آنچه را به دنبال آن بودیم، انجام داده‌ایم. □

برای دست‌یابی به حالت دودویی، نیاز به یک لم داریم.

لم ۴.٦.۱۱. فرض کنید C_1 و C_2 کدهای دوری به‌طول n روی $\mathbb{F}_q$ با چندجمله‌ای‌های بررسی $f_1(x) := \prod_{i=1}^{k_1}(x-\alpha_i)$، به‌ترتیب، $\prod_{j=1}^{k_2}(x-\beta_j)$ باشند. فرض کنید C کد دوری با همان طول باشد به‌طوری که چندجمله‌ای بررسی آن شامل تمامی حاصل‌ضرب‌های $\alpha_i\beta_j$ به‌عنوان ریشه‌های خود باشد؛ در این‌صورت C شامل تمامی کلمات ab است که $a \in C_1$ و $b \in C_2$.

اثبات. ما نمایش کدهای دوری را با دنباله‌های بازگشتی خطی، داده شده در انتهای بخش ٦.۵، به‌کار می‌بریم. می‌دانیم که مختص‌های a و b می‌توانند به‌صورت مجموع‌های $a_l = \sum_{i=1}^{k_1} c_i\alpha_i^{-l}$ و $b_l = \sum_{j=1}^{k_2} c'_j\beta_j^{-l}$ نمایش داده شوند. نتیجه فوراً با توجه به این نمایش و تعریف ab حاصل می‌گردد. □

قضیه زیر، اصطلاح به‌کار رفته در این بخش را توجیه می‌کند.

قضیه ۵.٦.۱۱. کد GRM دودویی مرتبه r با طول 2^m هم‌ارز با کد رید—مولر مرتبه r با طول 2^m است.

اثبات. اثبات برپایه استقراست. برای $r=0$، کدهای تعریف شده توسط تعاریف ٦.۴.۵ و ۲.٦.۱۱، هر دو کدهای تکرار هستند. می‌دانیم که کد همینگ دودویی، دوری است؛ بنابراین، برای $r=1$ اثبات با توجه به نتیجه قضیه ۸.۴.۵ واضح است. فرض کنید که ادعا برای یک مقدار r درست باشد. چندجمله‌ای بررسی $h^*(x)$ از کد GRM کوتاه‌شده دارای ریشه‌های α^j است که $w_2(j) \le r$. ریشه‌های چندجمله‌ای بررسی کد کوتاه‌شده RM از مرتبه ۱، شامل توان‌های α^j با شرط $w_2(j)=1$ هستند. حال قضیه با توجه به فرض استقرا، تعریف ٦.۴.۵ و لم ۴.٦.۱۱ اثبات می‌شود. □

ما این بخش را با قضیه‌ای درباره وزن‌های کدهای RM تمام می‌کنیم. این، کاربرد دیگری از قضیه ۵.٦.۸ است.

قضیه ٦.٦.۱۱. فرض کنید $F = F(x_۱, x_۲, \cdots, x_m)$ چندجمله‌ای با درجه r تعریف شده روی $\mathbb{F}_۲^m$ باشد. اگر تک‌جمله‌ای‌های G تشکیل زیرمجموعه‌ای از تک‌جمله‌ای‌های F را دهند، می‌نویسیم $G \subset F$. $v(G)$ را تعداد متغیرهایی تعریف می‌کنیم که مشمول در G نباشند و تعداد تک‌جمله‌ای‌های در G را با $|G|$ نمایش می‌دهیم. اگر $N(f)$ تعداد ریشه‌های F در $\mathbb{F}_۲^m$ باشند، آن‌گاه:

$$N(F) = ۲^{m-۱} + \sum_{G \subset F} (-۱)^{|G|}\, ۲^{|G|+v(G)-۱}.$$

اثبات. برای هر $G \subset F$، $f(G)$ را تعداد نقاطی در $\mathbb{F}_۲^m$ تعریف می‌کنیم که تمامی تک‌جمله‌ای‌های G، دارای مقدار صفر باشند و سایر تک‌جمله‌ای‌های F دارای مقدار ۱. به‌وضوح داریم:

$$\sum_{H \subset G} f(H) = ۲^{v(F-G)}$$

(زیرا این مقدار برابر با تعداد نقاطی از زیرفضای آفین $\mathbb{F}_۲^m$ تعریف شده به‌صورت $x_{i_۱} = x_{i_۲} = \cdots = x_{i_v} = ۱$ است، که‌در آن x_{i_k}ها متغیرهایی واقع در $F - G$ هستند). از قضیه ٦.٦.۸ نتیجه می‌شود:

$$f(G) = \sum_{H \subset G} \mu(H, G)\, ۲^{v(F-G)}.$$

علاوه‌براین:

$$N(F) = \sum_{G \subset F,\, |F-G| \equiv ۰ \bmod ۲} f(G).$$

چون $\sum_{G \subset F} f(G) = ۲^m$ داریم:

$$\begin{aligned}
N(F) &= ۲^{m-۱} + \tfrac{۱}{۲} \textstyle\sum_{G \subset F} (-۱)^{|F-G|} f(G) \\
&= ۲^{m-۱} + \tfrac{۱}{۲} \textstyle\sum_{G \subset F} (-۱)^{|F-G|} \sum_{H \subset G} \mu(H, G)\, ۲^{v(F-H)} \\
&= ۲^{m-۱} + \tfrac{۱}{۲} \textstyle\sum_{H \subset F} (-۱)^{|F-G|}\, ۲^{v(F-H)} \sum_{H \subset G \subset F} ۱ \\
&= ۲^{m-۱} + \tfrac{۱}{۲} \textstyle\sum_{H \subset F} (-۱)^{|F-G|}\, ۲^{v(F-H)}\, ۲^{|F-H|} \\
&= ۲^{m-۱} + \tfrac{۱}{۲} \textstyle\sum_{G \subset F} (-۱)^{|G|}\, ۲^{v(G)+|G|}.
\end{aligned}$$

□

حال این مطلب را روی کدهای RM به‌کار می‌بریم.

قضیه ۷.٦.۱۱. وزن‌های کدکلمات در $\mathcal{R}(r,m)$ بر $۲^{\lceil m/r \rceil -۱}$ بخش‌پذیر می‌باشند.

اثبات. کد $\mathcal{R}(r,m)$ شامل دنباله‌هایی از مقادیر داده‌شده توسط چندجمله‌ای‌های با درجه حداکثر r با m متغیر دودویی است. کدکلمه متناظر با یک چندجمله‌ای F، دارای وزن $۲^m - N(F)$ است. اگر $G \subset F$ و G دارای درجه d باشد، آن‌گاه $d \mid |G|$. $v(G) \geq m - \lceil \frac{m-v(G)}{d} \rceil \geq |G|$؛ یعنی چون:

$$v(G) + \lceil \frac{m - v(G)}{d} \rceil \geq \lceil \frac{m}{d} \rceil,$$

نتیجه با توجه به قضیه ٦.٦.۱۱ حاصل می‌شود. □

٦.۱۲ پیشنهادها

خواننده‌ای که علاقه‌مند به مشاهده تابع اثر و خودتوان‌های با وزن زیاد، به‌کاررفته در اثبات‌ها است، باید فصل ۱۵ مرجع [٤٦] را مطالعه نماید.

تعمیمی از کدهای BCH در فصل ۹ مورد بررسی قرار خواهد گرفت. مطالب زیادی درباره وزن‌ها، بعد، شعاع پوششی و غیره از کدهای BCH وجود دارد. ما کران کارلیتز–آچیاما[۴۰] را یادآوری می‌کنیم که به یک قضیه عمیق در نظریه اعداد توسط ویل[۴۱] بستگی دارد. برای مشاهده این کران، به مرجع [۴۲] ارجاع می‌دهیم. برای تعمیمی از کدهای QR به کلمات با طول n که توانی از یک عدد اول است، در حالتی که قضیه مشابه با بخش ٦.۹ است، خواننده را به مقاله‌ای توسط ون‌لینت[۴۲] و مک‌ویلیامز[۴۳] (۱۹۷۸؛ مرجع [۴۵]) ارجاع می‌دهیم.

٦.۱۳ مسائل

۱.٦.۱۳. نشان دهید که کد همینگ $[۴, ۲]$ سه‌تایی، یک کد نادوری می‌باشد.

۲.٦.۱۳. خودتوان یک کد همینگ $[۱۵, ۱۱]$ دودویی را تعیین کنید.

[۴۰] Carlitz-Uchiyama
[۴۱] A. Weil
[۴۲] J. H. van Lint
[۴۳] F. J. MacWilliams

۳.۶.۱۳. نشان دهید کد رید—مولر دودویی با مرتبه r در تعریف ۳.۴.۶ هم‌ارز با یک کد دوری گسترش‌یافته است.

۴.۶.۱۳. یک کد BCH سه‌تایی با طول ۲۶ و فاصله طراحی‌شده ۵ را بسازید.

۵.۶.۱۳. فرض کنید α یک عضو اولیه از $\mathbb{F}_{2^6}$، صادق در رابطه $\alpha^5 = \alpha^2 + 1$، باشد. یک کد BCH کم‌عرض با طول ۳۱ با فاصله طراحی‌شده ۵، مورداستفاده قرار گرفته است. بردار زیر را دریافت کرده‌ایم:

$$(1001 \quad 0110 \quad 1111 \quad 0000 \quad 1101 \quad 0101 \quad 0111 \quad 111)$$

این پیام را با استفاده از روش موجود در بخش ۶.۷ کدگشایی کنید.

۶.۶.۱۳. فرض کنید m عددی فرد باشد و β یک عضو اولیه از $\mathbb{F}_{2^m}$. یک کد دوری دودویی C با طول $n = 2^m - 1$ و با مولد $g(x)$ را بسازید به‌طوری که $g(\beta) = g(\beta^{-1}) = 0$. نشان دهید که کمترین—فاصله d برای C حداقل برابر ۵ است.

۷.۶.۱۳. فرض کنید C یک کد $[q+1, 2, d]$ روی $\mathbb{F}_q$ (q فرد) است. نشان دهید $d < q$؛ یعنی C متعلق به یک کد MDS نمی‌باشد، به نتیجه ۱.۵.۲ رجوع کنید.

۸.۶.۱۳. نشان دهید که کد $[11, 6]$ سه‌تایی QR، کامل است (این کد هم‌ارز با کد موجود در بخش ۴.۳ است).

۹.۶.۱۳. کمترین—فاصله کد QR دودویی با طول ۴۷ را تعیین کنید.

۱۰.۶.۱۳. تمامی کدهای QR کامل و تصحیح‌کننده ۱ خطا را تعیین کنید.

۱۱.۶.۱۳. ایده‌های موجود در بخش ۶.۹ را به‌معنای زیر توسعه دهید. فرض کنید $e > 2$، n یک عدد اول باشد به‌طوری که $e \mid (n-1)$ و q توانی از یک عدد اول باشد و $q^{(n-1)/e} \equiv 1 \bmod n$. به‌جای به‌کارگیری عناصر مربعی در $\mathbb{F}_n$، توان‌های eام را به‌کار ببرید. نشان دهید که قضیه ۲.۶.۹ قسمت (۱) می‌تواند به $d^e > n$ توسعه داده شود. کمترین—فاصله کد باقی‌مانده مکعبی با طول ۳۱ را تعیین کنید.

۱۲.٦.۱۳. فرض کنید m یک عدد فرد باشد، $n = ۲^m - ۱$ و α یک عضو اولیه از $\mathbb{F}_{۲^m}$ باشد. فرض کنید $g(x)$ یک مقسوم‌علیه از $x^n - ۱$ باشد، به‌طوری که $g(\alpha) = g(\alpha^۵) = ۰$. به دو روش زیر ثابت کنید که کد دوری دودویی با مولد $g(x)$ دارای کمترین —فاصله بزرگ‌تر یا مساوی ۴ است:

الف) با به‌کارگیری یک قضیه از این فصل.

ب) با نشان دادن این‌که روابط $۰ = \eta + \xi + ۱$ و $۰ = \eta^۵ + \xi^۵ + ۱$ وقتی‌که ξ و η متعلق به $\mathbb{F}_{۲^m}$ هستند، غیرممکن است.

ج) با به‌کارگیری ایده موجود در (ب) نشان دهید که درواقع داریم $d \geq ۵$.

۱۳.٦.۱۳. نشان دهید که کد گلی سه‌تایی دارای یک نمایش نادوری است.

۱۴.٦.۱۳. با استفاده از قضیه ۲.٦.۹، کد QR $[۳۱, ۱٦]$ دارای $d \geq ۷$ است درحالی‌که کران BCH تنها ایجاب می‌کند که $d \geq ۵$. نشان دهید که روش AB از بخش ٦.٦ نیز ایجاب می‌کند که $d \geq ۷$.

فصل ۷

کدهای کامل و کدهای به‌طور یکنواخت بسته‌بندی‌شده

۷.۱ قضیه لوید

در این فصل، توجه خود را به‌روی کدهای دودویی محدود خواهیم کرد. برای به‌دست آوردن یک دیدگاه روی روش‌ها و قضایای این بخش از نظریه کدگذاری، این محدودیت، کافی است. اخیراً هرچیزی می‌تواند برای میدان‌های دلخواه $\mathbb{F}_q$ (با مقدار کمی کار بیشتر) انجام پذیرد. در این دوره زمانی، بسیاری از روش‌های مطالعه کدهای کامل و مسائل مربوطه، پیش‌رفت کرده است. روی‌کرد جبری که ما در بخش بعدی بحث خواهیم نمود شاید یکی از زیباترین آنها باشد. ما با یک روش کاملاً متفاوت شروع می‌کنیم. ما یک اثبات واقعاً مقدماتی از یک شرط لازم قوی برای وجود کدهای کامل دودویی e–تصحیح‌کننده خطا ارایه خواهیم داد. قضیه مربوطه در ابتدا توسط لوید[۱] (۱۹۵۷) (درواقع برای $q = ۲$) با به‌کارگیری روش‌های تحلیلی اثبات شد. از آن روز به‌بعد توسط بسیاری از مولفین (به [۴۴] رجوع شود) تعمیم داده شد، اما هنوز به قضیه لوید ارجاع داده می‌شود. اثبات موجود در این بخش توسط سِتکُویک[۲] و ون‌لینت[۳] (۱۹۷۷؛ مرجع [۱۷]) ارایه شده است.

---

[۱] S. P. Lloyd

[۲] D. M. Cvetković

[۳] J. H. van Lint

تعریف ۱.۷.۱. ماتریس مربعی A_k با اندازه 2^k به‌صورت زیر تعریف شده است. سطرها و ستون‌ها را با نمایش دودویی از ۰ تا $2^k - 1$ شماره‌گذاری کنید. درایه $A_k(i,j)$ برابر ۱ است اگر نمایش‌های i و j دارای فاصله همینگ ۱ باشد، درغیر این‌صورت $A_k(i,j) = 0$.

از تعریف ۱.۷.۱ فوراً می‌بینیم که:

$$A_{k+1} = \begin{pmatrix} A_k & I \\ I & A_k \end{pmatrix}. \qquad (1)$$

لم ۲.۷.۱. مقادیر ویژه A_k برابر با $-k + 2j$ $(0 \le j \le k)$ با تکرار $\binom{k}{j}$ هستند.

اثبات. اثبات برپایه استقراست. برای $k = 1$ به‌آسانی حکم ثابت می‌شود. فرض کنید بردار ستونی x بردار ویژه A_k متناظر با مقدار ویژه λ باشد؛ در این‌صورت با توجه به تعریف ۱ داریم:

$$A_{k+1}\binom{x}{x} = (\lambda + 1)\binom{x}{x},$$

$$A_{k+1}\binom{x}{-x} = (\lambda - 1)\binom{x}{-x},$$

حال اثبات با توجه به خواص شناخته‌شده از ضرایب دوجمله‌ای، نتیجه می‌شود. □

مهم‌ترین قسمت مشکل این بخش از نظر تکنیکی، تعیین مقادیر ویژه ماتریس‌های سه‌قطری [۴] است که در اثبات قضیه رخ می‌دهد. برای کاهش نمادگذاری، تعریف زیر را به کار می‌بریم.

تعریف ۳.۷.۱. ماتریس $Q_e = Q_e(a,b)$ ماتریسی سه‌قطری به‌صورت زیر است:

$$(Q_e)_{i,i} := a, \quad 0 \le i \le e,$$

$$(Q_e)_{i,i+1} := b - i, \quad 0 \le i \le e-1,$$

$$(Q_e)_{i,i-1} := i, \quad 1 \le i \le e,$$

علاوه‌براین تعریف می‌کنیم:

$$P_e := P_e(a,b) := \left(\begin{array}{cc} & 1 \\ & 1 \\ Q_{e-1}(a,b) & \vdots \\ & 1 \\ \hline 0\,0\cdots 0 \quad e & 1 \end{array}\right).$$

[۴] tridiagonal matrices

دترمینان این ماتریس‌ها با $\bar{Q}_e$، به‌ترتیب $\bar{P}_e$ نمایش داده می‌شود.

لم ۴.۷.۱. فرض کنید $\Psi_e(x)$ چندجمله‌ای کراچوک $K_e(x-۱;n-۱,۲)$ تعریف شده در تعریف ۱.۱.۲ (فصل ۱) و رابطه ۱۹ (فصل ۱) باشد؛ در این‌صورت:

$$\bar{P}_e(۲y-n,n)=(-۱)^e e!\Psi_e(y).$$

اثبات. با اضافه‌نمودن تمام ستون‌ها به ستون آخر و سپس توسیع نسبت به سطر آخر داریم:

$$\bar{Q}_e=(a+e)\bar{Q}_{e-۱}-e(a+b)\bar{P}_{e-۱}.$$

با بسط $\bar{P}_e$ نسبت به سطر آخر داریم:

$$\bar{P}_e=\bar{Q}_{e-۱}-e\bar{P}_{e-۱}.$$

با ترکیب این روابط، رابطه بازگشتی زیر برای $\bar{P}_e$ ایجاد می‌شود:

$$\bar{P}_{e+۱}=(a-۱)\bar{P}_e-e(b-a)\bar{P}_{e-۱}. \qquad (۲)$$

بررسی این ادعا که این لم برای $e=۱$ و $e=۲$ درست است، آسان می‌باشد. از رابطه ۱۳ (فصل ۱) و رابطه ۲ نتیجه می‌شود که در این ادعا دو چندجمله‌ای مذکور در رابطه بازگشتی یکسانی صدق می‌کنند. این مطلب، لم را اثبات می‌کند. □

ما نیاز به یک لم آسان‌تر در مورد مقادیر ویژه داریم.

لم ۵.۷.۱. فرض کنید A ماتریسی با اندازه m در m باشد که به شکل زیر است:

$$A=\begin{pmatrix} A_{۱۱} & A_{۱۲} & \cdots & A_{۱k} \\ A_{۲۱} & A_{۲۲} & \cdots & A_{۲k} \\ \cdots & \cdots & \cdots & \cdots \\ A_{k۱} & A_{k۲} & \cdots & A_{kk} \end{pmatrix},$$

که در آن A_{ij} دارای اندازه m_i در m_j، $i=۱,۲,\cdots,k$، $j=۱,۲,\cdots,k$، است. فرض کنید که برای هر i و j، ماتریس A_{ij} دارای مجموع سطری ثابت b_{ij} است. فرض کنید B ماتریس با درایه‌های b_{ij} باشد؛ در این‌صورت هر مقدار ویژه B نیز یک مقدار ویژه A می‌باشد.

اثبات. فرض کنید $Bx = \lambda x$ که در آن $x = (x_1, x_2, \cdots, x_k)^T$. y را به‌صورت زیر تعریف کنید:

$$y^T := (x_1, x_1, \cdots, x_1, x_2, x_2, \cdots, x_2, \cdots, x_k, x_k, \cdots, x_k),$$

که در آن هر x_i به‌اندازه m_i بار تکرار می‌شود. با استفاده از تعریف B، واضح است که $Ay = \lambda y$. □

حال به سراغ قضیه‌ای اساسی می‌رویم که نتایج مهمی را دربر دارد.

قضیه ۶.۷.۱. اگر یک کد کامل دودویی $e-$تصحیح‌کننده خطا با طول n وجود داشته باشد، آن‌گاه $\Psi_e(x)$ دارای e ریشه متمایز در میان اعداد صحیح ۱، ۲، $\cdots$، n است.

اثبات. این واقعیت که ریشه‌ها متمایز هستند، یک خاصیت معروف از چندجمله‌ای‌های کراچوک است (ارجاع به رابطه ۱۷). برای نشان دادن این‌که آنها مقادیر صحیح هستند، فرض می‌کنیم که C کد خواسته‌شده در قضیه باشد. ماتریس A_n را درنظر بگیرید (ارجاع به تعریف ۱.۷.۱). سطرها و ستون‌های آن را به‌صورت زیر ثبت کنید. در ابتدا سطرها و ستون‌ها را با یک عدد متناظر با یک کدکلمه درنظر بگیرید. سپس آنها را به‌طور متوالی با اعداد متناظر با کلمات موجود در $C_i := \{x \in \mathbb{F}_2^n \mid d(x, c) = i\}$، $1 \le i \le e$، درنظر بگیرید. چون C کامل است، این باعث ایجاد افرازی از A_n به بلوک‌هایی مانند آنچه در لم ۵.۷.۱ آمد، می‌گردد. اکنون داریم:

$$B = \begin{pmatrix} 0 & n & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & n-1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots \\ 0 & 2 & 0 & n-2 & 0 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & e-1 & 0 & n-e+1 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 & e & n-e \end{pmatrix}.$$

با جانشینی $x = n - 2y$ در $\det(B - xI_{e+1})$، داریم:

$$\det(B - xI_{e+1}) = 2y\bar{P}_e(2y - n, n).$$

حال نتیجه با توجه به لم‌های ۲.۷.۱، ۴.۷.۱ و ۵.۷.۱ حاصل می‌گردد. □

اثبات داده‌شده در این بخش، هیچ دیدی درباره ادامه کار نمی‌دهد (برای مثال آیا ریشه‌های Ψ_e دارای یک معنای ترکیبیاتی است؟)، اما دارای این مزیت است که کاملاً مقدماتی می‌باشد (به‌جز برای اطلاعات اجتناب‌ناپذیری از خواص چندجمله‌ای‌های کراچوک). در بخش ۷.۵، قضیه ۶.۷.۱ را برای یافتن تمامی کدهای کامل به‌کار می‌بریم.

۷.۲ چندجمله‌ای مشخصه یک کد

کد دودویی C با طول n را درنظر می‌گیریم. در تعریف ۱.۳.۵، توزیع وزنی یک کد را تعریف کردیم و در تعریف ۲.۵.۳ آن را به توزیع فاصله یا توزیع داخلی $(A_i)_{i=0}^n$ تعمیم دادیم. متناظر با این دنباله، شمارنده فاصله[۵] را به‌صورت زیر داریم:

$$A_C(z) := \sum_{i=0}^{n} A_i z^i = |c|^{-1} \sum_{u,v \in C} z^{d(u,v)}. \qquad (۳)$$

حتی برای به‌دست آوردن اطلاعات بیشتر درباره فاصله‌ها، در اینجا توزیع خارجی[۶] را ماتریسی مانند B تعریف می‌کنیم (سطرها با عناصر $\mathcal{R} = \mathbb{F}_2^n$ و ستون‌ها با $0, 1, \cdots, n$ اندیس‌گذاری شده‌اند)، به‌طوری که:

$$B(x,i) := |\{c \in c | d(x,c) = i\}|. \qquad (۴)$$

سطری از B که با x اندیس‌گذاری شده، با $B(x)$ نمایش داده می‌شود. مشاهده می‌کنید که:

$$(A_0, A_1, \cdots, A_n) = |c|^{-1} \sum_{x \in C} B(x), \qquad (۵)$$

و

$$x \in C \Leftrightarrow B(x,0) = 1. \qquad (۶)$$

تعریف ۱.۷.۲. کد C یک کدمنظم[۷] نامیده می‌شود، اگر تمامی سطرهای B دارای یک ۱ در مکان ۰ برابر باشند. این کد کاملاًمنظم[۸] نامیده می‌شود، اگر:

$$\forall_{x \in \mathcal{R}} \forall_{y \in \mathcal{R}} [(\rho(x,C) = \rho(y,C)) \Leftrightarrow (B(x) = B(y))],$$

که در آن $\rho(x,C)$، فاصله x تا کد است.

مشاهده می‌کنید که اگر کد C منظم باشد و $0 \in C$، آن‌گاه شمارنده وزنی C برابر $A_C(z)$ می‌باشد.

به‌منظور مطالعه ماتریس B، در ابتدا تعدادی جبر معرفی می‌کنیم (به تعریف ۱۱.۱.۱ مراجعه شود).

---

[۵] distance enumerator
[۶] outer distribution
[۷] regular code
[۸] completely regualr

تعریف ۲.۷.۲. اگر G یک گروه جمعی باشد و $\mathbb{F}$ یک میدان باشد، آن‌گاه جبر گروهی[۹] $\mathbb{F}G$ (یا بهتر $(\mathbb{F}G, \oplus, *)$) یک فضای برداری روی $\mathbb{F}$ با عناصر G به‌عنوان پایه است که در آن جمع $\oplus$ و ضرب $*$ به‌صورت زیر تعریف شده‌اند:

$$\sum_{g\in G}\alpha(g)g * \sum_{h\in G}\beta(h)h := \sum_{k\in G}(\sum_{g+h=k}\alpha(g)\beta(h))k.$$

برخی مولفین، معرفی یک سمبل اضافی z و به‌کارگیری ضرب صوری به‌صورت زیر را ترجیح می‌دهند:

$$\sum_{g\in G}\alpha(g)z^g * \sum_{h\in G}\beta(h)z^h := \sum_{k\in G}(\sum_{g+h=k}\alpha(g)\beta(h))z^k.$$

ما G را طوری خواهیم گرفت که برابر با $\mathcal{R} = \mathbb{F}_2^n$ و $\mathbb{F} = \mathbb{C}$ باشد. این جبر را با $\mathcal{A}$ نمایش می‌دهیم. برای گیج نشدن درباره جمع در G با جمع عناصر $\mathcal{A}$، عناصر جمع گروهی را به‌صورت $\sum_{x\in\mathcal{R}}\alpha(x)x$ می‌نویسیم. اگر S زیرمجموعه‌ای از $\mathcal{R}$ باشد، آن‌گاه این زیرمجموعه را با عنصر $\sum_{x\in S}x$ در $\mathcal{A}$ هم‌سان درنظر می‌گیریم (ما آن را نیز با S نمایش می‌دهیم). در اینجا نمادهای زیر را برای مجموعه کلمات با وزن ثابت، به‌ترتیب گوی‌های حول صفر، تعریف می‌کنیم:

$$Y_i := \{x \in \mathcal{R} \,|\, w(x) = i\}, \tag{۷}$$

$$S_j := \{x \in \mathcal{R} \,|\, w(x) \le j\}. \tag{۸}$$

اگر C کدی با توزیع خارجی B باشد، آن‌گاه قراردادی که در بالا مطرح کردیم، ایجاب می‌کند که:

$$Y_i * C := \sum_{x\in\mathcal{R}} B(x,i)x. \tag{۹}$$

اگر $D(x,j)$ تعداد کدکلمات با فاصله حداکثر j تا x را نشان دهد $(D(x,j) = \sum_{i\le j} B(x,i))$، آن‌گاه داریم:

$$S_j * C := \sum_{x\in\mathcal{R}} D(x,i)x. \tag{۱۰}$$

فرض کنید χ سرشت $\mathbb{F}_2$ با $\chi(1) = -1$ باشد. برای هر $u \in \mathcal{R}$، نگاشت $\chi_u : \mathcal{R} \to \mathbb{C}$ را به‌صورت:

$$\forall_{v\in\mathcal{R}}[\chi_u(v) := \chi(< u, v >) = (-1)^{<u,v>}], \tag{۱۱}$$

[۹] group algebra

تعریف می‌کنیم؛ یعنی $\chi_u(v) = ۱$ اگر $u \perp v$ و -۱ درغیر این‌صورت.

این نگاشت را به تابع خطی بر روی جبر گروهی A به‌صورت زیر گسترش می‌دهیم.

$$\chi_u(\sum \alpha(x)x) := \sum \alpha(x)\chi_u(x). \qquad (۱۲)$$

دو ادعای زیر، فوراً از تعریف ما نتیجه می‌شوند. اثبات آنها را به‌صورت تمرین‌هایی آسان برعهده خواننده می‌گذاریم.

$$\forall_{u\in\mathcal{R}}\forall_{A\in\mathcal{R}}\forall_{B\in\mathcal{R}}[\chi_u(A * B) := \chi(A)\chi_u(B)], \qquad (۱۳)$$

$$(\chi_۰(S) = ۲^n, \quad \forall_{u\neq ۰}[\chi_u(S) = ۰]) \Leftrightarrow S = S_n. \qquad (۱۴)$$

نتیجه لم ۱.۵.۳ (دراینجا داریم $q = ۲$) می‌تواند به‌صورت زیر نوشته شود:

$$\chi_u(Y_k) = K_k(w(u)). \qquad (۱۵)$$

از این نتیجه می‌شود که اگر $w(u) = x$، آن‌گاه:

$$\chi_u(S_j) = \sum_{k=۰}^{j} K_k(x) = \Psi_j(x). \qquad (۱۶)$$

(به رابطه ۱۹ مراجعه شود).

فرض کنید C یک کد باشد. اعداد زیر را درنظر می‌گیریم.

$$C_j := |c|^{-۱} \sum_{u\in Y_j} \chi_u(C).$$

این اعداد را قبلاً دیده‌ایم. اگر C یک کد خطی باشد، آن‌گاه اثبات قضیه ۲.۳.۵ به ما نشان می‌هد که C_j، تعداد کلمات به‌وزن j در $C^\perp$ است. اگر C خطی نباشد، آن‌گاه هنوز می‌توانیم اعداد C_j را درنظر بگیریم و اثبات قضیه ۲.۳.۵ را ادامه دهیم تا دریابیم که $۲^{-n}|c|\sum_{j=۰}^{n} C_j(۱-z)^j(۱+z)^{n-j}$ شمارنده وزنی کد C است. این رابطه مابین شمارنده وزنی و اعداد C_j، تعریف شده با کمک χ، یک شکل غیرخطی از رابطه مک‌ویلیمز است.

در اینجا دنباله دومی از اعداد را مجدداً با به‌کارگیری سرشت χ تعریف می‌کنیم.

تعریف ۳.۷.۲. اعداد مشخصه[۱۰] B_j $(۰ \leq j \leq n)$ از کد C به‌صورت زیر تعریف شده‌اند:

$$B_j := |c|^{-۲} \sum_{u\in Y_j} |\chi_u(C)|^۲.$$

[۱۰] characteristic numbers

همان‌طور که قبلاً دیدیم، B_j تعداد کلمات به وزن j در کد $C^\perp$ است، اگر C یک کد خطی باشد. فرض کنید $N(C) := \{j \mid ۱ \le j \le n, B_j \neq ۰\}$. چندجمله‌ای مشخصه F_C از کد C به‌صورت زیر تعریف شده است:

$$F_C(x) := ۲^n|c|^{-۱} \prod_{j \in N(C)} (۱ - \frac{x}{j}). \qquad (۱۷)$$

قضیه ۴.۷.۲. فرض کنید $\alpha_۰$، $\alpha_۱$، $\cdots$، α_n ضرایب موجود در توسیع کراچوک F_C باشند؛ در این‌صورت در $\mathcal{A}$ داریم:

$$\chi_u(\bigotimes \alpha_i Y_i * C) = S_n.$$

اثبات. فرض کنید $u \in \mathcal{R}$، $w(u) = j$. با استفاده از روابط ۱۳ و ۱۵ داریم:

$$\chi_u(\bigotimes \alpha_i Y_i * C) = \chi_u(\bigotimes \alpha_i Y_i)\chi_u(C) = \chi_u(C) \sum \alpha_i K_i(j) = \chi_u(C) F_C(j).$$

اگر $u \neq ۰$، آن‌گاه طرف راست معادله فوق با استفاده از تعریف F_C برابر با صفر است. اگر $u = ۰$، آن‌گاه طرف راست برابر با ۲^n است. حال، حکم با توجه به رابطه ۱۴ اثبات می‌شود. □

نتیجه‌گیری ۵.۷.۲. اگر $\alpha_۰$، $\alpha_۱$، $\cdots$، α_n ضرایب موجود در توسیع کراچوک F_C باشند و $u \in \mathcal{R}$، آن‌گاه:

$$\sum_{i=۰}^{n} \alpha_i B(u,i) = ۱.$$

اثبات. رابطه ۹ را به‌کار ببرید. □

تعریف ۶.۷.۲. عدد $s := |N(C)|$، فاصله بیرونی[۱۱] C نامیده می‌شود.

توجه دارید که اگر C خطی باشد، آن‌گاه s تعداد وزن‌های ناصفر واقع در $C^\perp$ است. این نام که تاحدی عجیب است، توسط نتیجه ۵.۷.۲ که نشان می‌دهد شعاع پوششی $\rho(C)$ از یک کد (بخش ۳.۴ را ببینید) حداکثر برابر با s است، تا اندازه کمی توجیه می‌شود.

[۱۱] external distance

۷.۳ کدهای به‌طور یکنواخت بسته‌بندی‌شده

در این بخش، کدهایی را درنظر می‌گیریم که تعمیم کدهای کامل هستند (به رابطه ۲ مراجعه شود). توجه دارید که اگر C یک کد کامل e–تصحیح‌کننده خطا باشد، آن‌گاه در $\mathcal{A}$ داریم $S_e * C = S_n$. حال کدهای C با $d \geq 2e+1$ و $\rho(C) = e+1$ را درنظر می‌گیریم (اگر $d = 2e+3$، آن‌گاه این بدان معناست که C کامل است). این گوی های به شعاع $e-1$ و به مرکز کدکلمات، مجزا هستند و هر کلمه‌ای که در یکی از این گوی‌ها نباشد، دارای فاصله e یا $e+1$ تا حداقل یک کدکلمه است.

تعریف ۱.۷.۳. کد C با $\rho(C) = e+1$ و $g \geq 2e+1$ به‌طور یکنواخت بسته‌بندی‌شده[۱۲] با پارامتر r نامیده می‌شود، اگر هر کلمه u با $\rho(u, C) \geq e$ دارای فاصله e یا $e+1$ تا دقیقاً r کدکلمه باشد.

توجه دارید که اگر $r = 1$، آن‌گاه C یک کد کامل e–تصحیح‌کننده خطاست. البته یک کلمه u با $\rho(u, C) = e$ دارای فاصله e تا دقیقاً یک کدکلمه است. فرض کنید $\rho(u, C) = e+1$ و نیز فرض کنید $u = 0$؛ در این‌صورت کدکلمات با فاصله $e+1$ تا u، دارای وزن $e+1$ می‌باشند. چون آنها باید دارای فاصله‌های متقابلِ بزرگ‌تر یا مساوی $2e+1$ باشند؛ در نتیجه:

$$r \leq \frac{n}{e+1}. \qquad (18)$$

حال فرض کنیم $e+1$، $n+1$ را عاد نکند. کدی که در آن $r = \lfloor n/(e+1) \rfloor$، تقریباً کامل[۱۳] نامیده می‌شود. به‌آسانی می‌توان چک نمود که این بدان معناست که C در کران جانسون (۳) در حالت تساوی صدق می‌کند. در مقاله‌ای که توسط گوتالز[۱۴] و ون تیلبرگ[۱۵] مرجع [۲۵] آمده است، تعریف ۱.۷.۳ با جانشینی r با دو عدد، وابسته به این‌که $\rho(u, C) = e$ یا $e+1$، تعمیم داده شده است.

قضیه ۲.۷.۳. کد C با $\rho(C) = e+1$ و $d \geq 2e+1$ به‌طور یکنواخت بسته‌بندی‌شده با پارامتر r است اگر و تنها اگر در $\mathcal{A}$ داشته باشیم:

$$\{Y_0 \oplus Y_1 \oplus \cdots \oplus Y_{e-1} \oplus \frac{1}{r}(Y_e \oplus Y_{e+1})\} * C = S_n.$$

اثبات. این مطلب با توجه به روابط ۳، ۹ و تعریف ۱.۷.۳ نتیجه می‌شود. □

---

[۱۲] uniformly packed
[۱۳] nearly perfect
[۱۴] J. M. Goethals
[۱۵] H. C. A. van Tilborg

قضیه ۳.۷.۳. کد C با $\rho(C) = e+1$ و $d \geq 2e+1$ به‌طور یکنواخت بسته‌بندی‌شده با پارامتر r است اگر و تنها اگر چندجمله‌ای مشخصه دارای درجه $s = e+1$ و ضرایب کراچوک:

$$\alpha_0 = \alpha_1 = \cdots = \alpha_{e-1} = 1, \qquad \alpha_e = \alpha_{e+1} = \frac{1}{r},$$

باشد.

اثبات.

۱) قسمت اگر با توجه به قضیه ۴.۷.۲ و قضیه ۲.۷.۳ نتیجه می‌شود.

۲) فرض کنید C به‌طور یکنواخت بسته‌بندی‌شده باشد. می‌دانیم که F_C دارای درجه $s \geq e+1$ است. فرض کنید $F(x) := \sum_{i=0}^{e+1} \alpha_i K_i(x)$ با $\alpha_0 = \alpha_1 = \cdots = \alpha_{e-1} = 1$، $\alpha_e = \alpha_{e+1} = 1/r$. اگر $u \in \mathcal{R}$، $w(u) = j \neq 0$ و $\chi_u(C) \neq 0$؛ در این‌صورت با استفاده از روابط ۱۳ و ۱۴ و ۱۵ و قضیه ۲.۷.۳ داریم $F(j) = 0$. حال با استفاده از رابطه ۱۷ نتیجه می‌شود که $F_C(x)$، $F(x)$ را عاد می‌کند؛ بنابراین، $s = e+1$ و $F(x) = aF_C(x)$ برای یک مقدار a. با جانشینی $x = 0$ داریم $a = 1$ (مجدداً با به‌کارگیری قضیه ۲.۷.۳). □

قضیه زیر فرمول‌بندی متفاوتی از قضیه ۳.۷.۳ است.

قضیه ۴.۷.۳. اگر کد به‌طور یکنواخت بسته‌بندی‌شده C با $\rho(C) = e+1$ و $d \geq 2e+1$ موجود باشد، آن‌گاه چندجمله‌ای:

$$F(x) := \sum_{i=0}^{e-1} K_i(x) + \frac{1}{r}[K_e(x) + K_{e+1}(x)]$$

دارای $e+1$ ریشه صحیح مجزا در بازه $[1, n]$ می‌باشد و $F(0) = 2^n |c|^{-1}$.

درابتدا مشاهده می‌کنید که C یک کد کامل است؛ یعنی $d = 2e+3$؛ در این‌صورت با استفاده از رابطه ۱۹ داریم $r = 1$ و $F(x) = \Psi_{e+1}(x)$ و قضیه ۴.۷.۳ همان قضیه لوید (قضیه ۶.۷.۱) است.

پس از آن توجه داریم که شرط لازم درباره $F(0)$ می‌تواند به‌صورت زیر نوشته شود:

$$|c|\{\sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r}\binom{n+1}{e+1}\} = 2^n, \qquad (۱۹)$$

رابطه ۱۹، در حالتی که $r = 1$، همان رابطه ۶.۳.۱ (فصل ۳) و در حالتی که $r = \lfloor n/(e+1) \rfloor$، همان رابطه ۳ (فصل ۵) است.

درواقع رابطه ۱۹ در حالت کلی درست است، اگر r را به‌عنوان مقدار متوسط کدکلمات با فاصله e یا $e+1$ نسبت به کلمه u برای $\rho(u,C) \geq e$ تفسیر نماییم.

در حالت کلی چک نمودن این‌که یک کد داده‌شده با استفاده از این تعریف به‌طور یکنواخت بسته‌بندی‌شده است، کار آسانی نیست.

در اینجا حالت خاصی را درنظر می‌گیریم؛ یعنی یک کد خطی با $e = ۱$. برای این‌که C به‌طور یکنواخت فشرده باشد، چندجمله‌ای مشخصه باید دارای درجه ۲ باشد (با استفاده از قضیه ۳.۷.۳). از قبل توجه داریم که این بدان معناست که در $C^\perp$ تنها دو وزن ناصفر $w_۱$ و $w_۲$ رخ می‌دهد. حال فرض کنید که $C^\perp$ چنین کد دو—وزنی با شمارنده وزنی:

$$A_{C^\perp}(z) = ۱ + N_۱ z^{w_۱} + N_۲ z^{w_۲},$$

باشد. رابطه مک‌ویلیامز (ارجاع به بخش ۷.۲) را درنظر بگیرید و برای $(۱+z)^{n-x}(۱-z)^x$ (ارجاع به رابطه ۷) رابطه زیر را جانشین کنید:

$$\sum_{k=۰}^{\infty} K_k(x) z^k.$$

چون فرض کرده‌ایم که C دارای کمترین—فاصله $d \geq ۳$ است، با به دست آوردن ضرایب $z^۰$، $z^۱$ و $z^۲$، سه معادله به‌صورت زیر داریم:

$$۱ + N_۱ + N_۲ = ۲^n |c|^{-۱},$$

$$K_k(۰) + N_۱ K_k(\omega_۱) + N_۲ K_k(\omega_۲) = ۰, \qquad (k = ۱, ۲).$$

با استفاده از تعریف داریم $F_C(w_۱) = F_C(w_۲) = ۰$ و $F_C(۰) = ۲^n |c|^{-۱}$؛ در این‌صورت برای ضرایب $\alpha_۰$، $\alpha_۱$ و $\alpha_۲$ در توسیع کراچوک $F_C(x)$ با استفاده از رابطه ۱۱ داریم:

$$\alpha_۰ + \alpha_۱ n + \alpha_۲ \binom{n}{۲} = ۲^n |c|^{-۱},$$

$$\alpha_۰ + \alpha_۱ (n - ۲\omega_i) + \alpha_۲ \{۲\omega_i^۲ - ۲n\omega_i + \binom{n}{۲}\} = ۰, \qquad (i = ۱, ۲).$$

ما این معادلات را با معادلات متناظر با $N_۱$ و $N_۲$ مقایسه می‌کنیم. این مطلب نشان می‌دهد که $\alpha_۰ = ۱$. تعریف می‌کنیم:

$$r := ۲(n+۱)\omega_۱ - ۲\omega_۱^۲ - \frac{۱}{۲} n(n+۱).$$

در این‌صورت نتیجه می‌شود که $\alpha_۱ = \alpha_۲ = ۱/r$ اگر $w_۱ + w_۲ = n + ۱$؛ بنابراین، مشخصه‌سازی زیر را از کدهای ۱—تصحیح‌کننده خطای به‌طور یکنواخت بسته‌بندی‌شده داریم:

قضیه ۵.۷.۳ کد خطی C با $\rho(C) = ۲$ و $d \geq ۳$ به‌طور یکنواخت بسته‌بندی‌شده است اگر و تنها اگر $C^{\perp}$ یک کد دو–وزنی با وزن‌های $w_۱$ و $w_۲$ صادق در رابطه $w_۱ + w_۲ = n + ۱$ باشد.

در مرجع [۲۵] نشان داده شده است که اگر ما تعریف کلی‌تر کدهای به‌طور یکنواخت بسته‌بندی‌شده را بپذیریم، آن‌گاه می‌توانیم محدودیت $w_۱ + w_۲ = n + ۱$ را حذف کنیم. این قضیه نیز برای $e > ۱$ با $e + ۱$ وزن در $C^{\perp}$ به‌جای دو تا، درست است.

۷.۴ مثال‌هایی از کدهای به‌طور یکنواخت بسته‌بندی‌شده

۱.۷.۴. یک کد هادامارد (ارجاع به بخش ۴.۱)

کد هادامارد C (۱۱, ۲۴, ۵) پنچر کنید. واضح است که هر کلمه z می‌تواند دارای فاصله ۲ یا ۳ تا حداکثر چهار کدکلمه باشد و اگر این رخ دهد، آن‌گاه وضعیت زیر را داریم (پس از تغییر علامت به نماد $\pm$ و ضرب مناسب ستون‌ها در -۱):

$$z = \quad -- \quad +++ \quad +++ \quad +++,$$

$$x_۱ = \quad ++ \quad +++ \quad +++ \quad +++,$$

$$x_۲ = \quad -- \quad --- \quad +++ \quad +++,$$

$$x_۳ = \quad -- \quad +++ \quad --- \quad +++,$$

$$x_۴ = \quad -- \quad +++ \quad +++ \quad ---,$$

این بدان معناست که ماتریس هادامارد اصلی از مرتبه ۱۲ دارای چهار سطر $(+, x_۱)$، $(-, x_۲)$، $(-, x_۳)$، $(-, x_۴)$ است. بردار سطری $(-۴, -۴, -۴, ۰, ۰, \cdots, ۰)$ ترکیب خطی از این چهار سطر است؛ بنابراین، باید به سطرهای باقی‌مانده ماتریس هادامارد عمود باشد که به‌وضوح غیرممکن است. از این نتیجه می‌شود که کلمه z دارای فاصله ۲ یا ۳ تا حداکثر سه کدکلمه است. از رابطه ۱۹ نتیجه می‌شود که مقدار متوسط کدکلمات با فاصله ۲ یا ۳ تا کدکلمه z با $\rho(z, C) > ۱$، برابر سه است؛ بنابراین، این تعداد همواره برابر با سه است. از این‌رو C به‌طور یکنواخت بسته‌بندی‌شده با $r = ۳$ است. در این مثال، C غیرخطی است.

توجه دارید که در این مثال، $e + ۱$، $n + ۱$ را عاد می‌کند؛ بنابراین، رابطه ۱۹ برقرار است، اما برابر با ۳ نیست. این کد یک کد تقریباً کامل نمی‌باشد.

۲.۷.۴. یک کد RM پنچرشده

فرض کنید V فضای برداری با ۶ بعدی روی $\mathbb{F}_2$ باشد. فرض کنید W مجموعه با ۳۵ نقطه x در $V\backslash\{0\}$ روی فرم درجه ۲ با معادله $x_1x_2 + x_3x_4 + x_5x_6 = 0$ باشد. این بردارها را به‌عنوان ستون‌هایی از یک ماتریس ۶ در ۳۵، G درنظر بگیرید. مانند بخش ۴.۵، می‌بینیم که iامین سطر G، تابع مشخصه اشتراک W و ابرصفحه‌هایی با معادله $x_i = 1$ $(1 \le i \le 6)$ است؛ بنابراین، وزن یک ترکیب خطی a^TG $(a \in V)$، تعداد جواب‌های:

$$x_1x_2 + x_3x_4 + x_5x_6 = 0, \quad \sum_{i=1}^{6} \alpha_i x_i = 1,$$

است. بدون کاستن از کلیت فرض می‌کنیم $a_1 = 1$ (مگر این‌که $a = 0$). با جانشین‌کردن و استفاده از تبدیل آفین:

$$y_2 = x_2, \quad y_3 = x_3 + a_4x_2, \quad y_4 = x_4 + a_3x_2,$$

$$y_5 = x_5 + a_6x_2, \quad y_6 = x_6 + a_5x_2,$$

(که معکوس‌پذیر است) می‌بینیم که باید تعداد جواب‌های معادله زیر را بشماریم:

$$(1 + a_2 + a_3a_4 + a_5a_6)y_2 + y_3y_4 + y_5y_6 = 0.$$

اگر ضریب y_2 برابر با ۱ باشد، آن‌گاه این تعداد برابر با ۱۶ است؛ اگر آن برابر ۰ باشد، آن‌گاه تعداد جواب‌ها برابر با ۲۰ است؛ بنابراین، کد C که شامل G به‌عنوان ماتریس بررسی‌توازن است، دارای دوگان $C^\perp$، یک کد دو–وزنی با وزن‌های ۱۶ و ۲۰، است. چون کد C تصویری است، داریم $d \ge 3$. با استفاده از ملاحظه زیر (رابطه ۶.۷.۲) داریم $\rho(C) = 2$؛ بنابراین، با استفاده از ۵.۷.۳، C به‌طور یکنواخت بسته‌بندی‌شده با $r = 10$ است (با استفاده از ۱۹). روش مشابه در ابعاد بالاتر کار می‌کند.

۳.۷.۴. کدهای پرپاراتا

در سال ۱۹۶۸، پرپاراتا[16] مرجع [۵۷] کلاسی از کدهای غیرخطی ۲–تصحیح‌کننده خطا را طراحی نمود که ثابت شده است آنها دارای خواص بسیار جالبی هستند. تعریف او برپایه ترکیبی از کدهای همینگ و کدهای BCH ۲–تصحیح‌کننده خطاست. تحلیل این کدها شامل محاسبات وحشتناکی است (ر.ک. مرجع [۱۱]). توصیف زیر از کدهای پرپاراتا توسط باکر[17] و ویلسن[18] و مولف این کتاب (ر.ک. مرجع [۷۲]) است.

[16] F. P. Preparata
[17] R. D. Baker
[18] R. M. Wilson

در زیر، m ($m \geq ۳$) فرد است و $n = ۲^m - ۱$. ما کد $\bar{\mathcal{T}}$ با طول $۲n + ۲ = ۲^{m+۱}$ را تعریف خواهیم کرد. کلمات، توسط زوج‌های (X, Y) توصیف می‌شوند که در آن $X \subset \mathbb{F}_{۲^m}$ و $Y \subset \mathbb{F}_{۲^m}$. به‌طور معمول، زوج (X, Y) را به‌عنوان تابع مشخصه متناظر تفسیر می‌کنیم که یک $(۰, ۱)$–بردار با طول $۲^{m+۱}$ است.

تعریف ۴.۷.۴. کد پرپاراتای گسترش‌یافته $\bar{\mathcal{T}}$ با طول $۲^{m+۱}$، شامل کدکلمات توصیف شده توسط تمامی زوج‌های (X, Y) صادق در روابط زیر است:

۱) $|X|$ زوج است، $|Y|$ زوج است.

۲) $\sum_{x \in X} x = \sum_{y \in Y} y$.

۳) $\sum_{x \in X} x^۳ + (\sum_{x \in X} x)^۳ = \sum_{y \in X} y^۳$.

کد $\mathcal{T}$ با صرف‌نظر کردن از مختصات متناظر با مکان‌های صفر در اولین نیمه، به‌دست آمده است.

در ابتدا نشان می‌دهیم که $\mathcal{T}$ دارای $۲^{۲n-۲m}$ کلمه است. می‌توانیم X صادق در شرط (۱) را به ۲^n طریق انتخاب کنیم. سپس مشاهده می‌کنیم که چون m فرد است، چندجمله‌ای مینیمال $m_۳(x)$ برای $\mathbb{F}_{۲^m}$ دارای درجه m است. بنابراین، کد BCH با طول n و فاصله طراحی‌شده ۵ دارای بعد $n - ۲m$ است. این مطلب در ادامه ایجاب می‌کند که برای X داده شده، معادلات (۲) و (۳) دارای $۲^{n-۲m}$ جواب $Y \subset \mathbb{F}^*_{۲^m}$ باشند. می‌توانیم، اگر لازم باشد، عضو صفر را به این Y اضافه کنیم تا در شرط (۱) صدق کند. این مطلب، ادعا را ثابت می‌کند.

ادعای بعدی این است که $\bar{\mathcal{T}}$ دارای کمترین–فاصله ۶ است. از تعریف ۴.۷.۴ قسمت (۱) می‌بینیم که کمترین–فاصله، زوج است و هم‌چنین این‌که اگر (X, Y) در دو شرط فوق صدق کند، آن‌گاه (Y, X) نیز چنین است. فرض کنید دو کلمه $(X, Y_۱)$ و $(X, Y_۲)$ را داریم و قرار دهید $Y := Y_۱ \Delta Y_۲$؛ در این‌صورت از تعریف ۴.۷.۴ قسمت (۲) داریم:

$$\sum_{y \in Y} y = \sum_{y \in Y} y^۳ = ۰,$$

یعنی با استفاده از کران BCH داریم $|Y| \geq ۵$؛ بنابراین، در این حالت دو کلمه دارای فاصله بزرگ‌تر یا مساوی ۶ هستند. تنها مطلبی که باقی می‌ماند این است که احتمال $(X_۱, Y_۱)$ و $(X_۲, Y_۲)$ را به شرط زیر درنظر بگیریم:

$$|X_۱ \Delta X_۲| = |Y_۱ \Delta Y_۲| = ۲.$$

فرض کنید $X_۱ \Delta X_۲ = \{\alpha, \beta\}$ و $Y_۱ \Delta Y_۲ = \{\gamma, \delta\}$ و فرض کنید $s + \alpha$ مجموع عناصر در $X_۱$ باشد. در

این‌صورت، قسمت (۲) و (۳) از ۴.۷.۴ ایجاب می‌کنند:

$$\alpha + \beta = \gamma + \delta,$$

$$s^{۲}(\alpha + \beta) + s(\alpha + \beta)^{۲} = \gamma^{۳} + \delta^{۳}.$$

از اینها داریم $(s+\gamma)^{۳} + (s+\delta)^{۳} = ۰$؛ یعنی $\gamma = \delta$ که یک تناقض است. این مطلب ادعای ما را ثابت می‌کند. پس قضیه زیر را ثابت کرده‌ایم:

قضیه ۵.۷.۴. در کد پرپاراتای $\mathcal{T}$ با طول $۲^{m+۱} - ۱$ ($m \geq ۳$ فرد است) $|\mathcal{T}| = ۲^{k}$ که در آن $k = ۲^{m+۱} - ۲m - ۲$ و کمترین—فاصله برابر با ۵ است.

از رابطه ۱۹ در می‌یابیم که مقدار متوسط r برای کد $\mathcal{T}$ برابر $۳/(۱ - ۲^{m+۱})$ است و سپس رابطه ۱۸ ایجاب می‌کند که r ثابت بوده و برابر $۳/(۱ - ۲^{m+۱})$ است؛ یعنی $\mathcal{T}$ تقریباً کامل است.

اگر در تعریف ۴.۷.۴ درنظر بگیریم $m = ۳$، آن‌گاه کد نرداستروم—رابینسن را داریم که در بخش ۴.۴ معرفی شد.

تذکر ۶.۷.۴. توان‌های ۳ در تعریف ۴.۷.۴ قسمت (۳) ضروری نمی‌باشند. می‌توانیم ۳ را با $s := ۲^{t} + ۱$ جای‌گزین کنیم که در آن نیاز داریم $x \to x^{s}$ و $x \to x^{s-۲}$ نگاشت‌های ۱—۱ از $\mathbb{F}_m$ به خودش باشند؛ در این‌صورت قسمت اول استدلال مربوط به کمترین—فاصله با استدلال مربوط به قضیه ۵.۶.۶ جای‌گزین می‌شود. این مطلب را به‌صورت یک تمرین آسان به خواننده واگذار می‌کنیم.

مشاهده می‌کنید که کد صادق در روابط (۱) و (۲) تعریف ۴.۷.۴، کد همینگ گسترش‌یافته با طول $۲^{m+۱}$ است. با توجه به این مطلب و یک استدلال شمارشی نتیجه می‌گیریم که اگر ما $\mathcal{T}$ را درنظر بگیریم و آن را به تمامی کلمات با فاصله ۳ تا $\mathcal{T}$ اضافه کنیم، کد همینگ با طول $۲^{m+۱} - ۱$ را به‌دست می‌آوریم. در قضیه ۷.۷.۴ یک ساختار مستقیم ارائه می‌دهیم.

قضیه ۷.۷.۴. اجتماع کد پرپاراتای $\mathcal{T}$ با طول $n = ۲^{m+۱} - ۱$ (m فرد) و مجموعه کلمات دارای فاصله ۳ با $\mathcal{T}$، برابر کد همینگ با طول n است.

اثبات. چون $\mathcal{T}$ در رابطه ۳ صدق می‌کند، می‌دانیم که $|\mathcal{T}|.\frac{n-۱}{۲}$ کلمه دارای فاصله ۳ با $\mathcal{T}$ وجود دارد. بنابراین، اجتماع C شامل $۲^{n-m-۱}$ کلمه است که به اندازه کد همینگ با طول n است.

حال تعریف می‌کنیم $C_۰ := \bar{\mathcal{T}}$ و برای $\alpha \in \mathbb{F}_{۲^m}^{*}$، C_α را کد به‌دست آمده توسط اضافه‌نمودن کلمه متناظر با $(\{۰, \alpha\}, \{۰, \alpha\})$ به کلمات $C_۰$ تعریف می‌کنیم. به‌وضوح هر C_α تنها شامل بردارهای با وزن زوج است. اگر وزن ۲ رخ دهد، آن‌گاه $C_۰$ شامل کلمه‌ای متناظر با $X = \{۰, \alpha\}$، $Y = \{۰, \alpha, \beta, \gamma\}$

خواهد بود که با تعریف ۴.۷.۴ قسمت (۲) در تناقض است. بنابراین، هر C_α دارای کمترین—فاصله ۴ است. از اثبات قضیه ۲۲ نتیجه می‌شود که C_αها دوبه‌دو مجزا هستند ($\alpha \in \mathbb{F} := \mathbb{F}_{2^m}$). ادعا می‌کنیم که $\bar{H} := \cup_{\alpha\in\mathbb{F}} C_\alpha$ خطی است. نشان دادن این مطلب، با استفاده از تعریف ۴.۷.۴ قسمت (۳)، به حل معادله‌ای از نوع $x^3 = \alpha$ منجر می‌گردد که امکان‌پذیر است، زیرا m فرد است. از این پارامترها و خطی بودن، نتیجه می‌گیریم که $\bar{H}$، کد همینگ گسترش‌یافته با طول $n+1$ است. این مطلب، ادعا درباره C را اثبات می‌کند. □

توجه دارید که از قضیه ۷.۷.۴ نتیجه می‌شود که ترکیبات خطی کدکلماتِ کد پرپاراتا، مشمول در کد همینگ است.

۷.۵ قضایای عدم وجود

این مطلب توسط تیتاواینن[۱۹] [۶۸] و ون‌لینت[۲۰] [۴۱] نشان داده شده است که کدهای گلی تنها کدهای کامل غیربدیهی $e-$ تصحیح‌کننده خطا با $e > 1$ روی الفبای دلخواه Q هستند، به‌طوری که $|Q|$ توانی از یک عدد اول است. برای $e > 2$، محدودویت روی Q می‌تواند به‌صورتی که توسط بست[۲۱] [۷] و هونگ[۲۲] [۷۴] نشان داده شده است، حذف گردد، اما اثبات آن بسیار مشکل‌تر می‌باشد. برای $e = 1$، کدهای همینگ را دیده‌ایم. هم‌چنین مثال‌هایی از کدهای کامل غیرخطی با $e = 1$ وجود دارد (ارجاع به مساله ۴.۷.۷).

در سال ۱۹۷۰، تیلبرگ[۲۳] [۶۹] نشان داد که کدهای به‌طور یکنواخت بسته‌بندی‌شده $e-$تصحیح‌کننده خطا با $e > 3$ وجود ندارند و آنهایی که $e \le 3$ همگی شناخته شده‌اند. در این بخش، برخی ایده‌ها مربوط به روش به‌کار رفته برای اثبات این نتایج را ارائه خواهیم داد. کافی‌است تا حالت دودویی را درنظر بگیریم.

قضیه ۱.۷.۵. اگر C یک کد دودویی کامل $e-$ تصحیح کننده خطا با $e > 1$ باشد، آن‌گاه C یک کد تکرار یا یک کد گلی دودویی است.

اثبات. با استفاده از قضیه لوید (۶.۷.۱)، چندجمله‌ای Ψ_e دارای ریشه‌های $x_1 < x_2 < \cdots < x_e$ می‌باشد که اعداد صحیحی در بازه $[1, n]$ هستند. با استفاده از تعریف Ψ_e و رابطه (۱۲)، توابع متقارن

[۱۹] A. Tietäväinen
[۲۰] j. H. van Lint
[۲۱] M. R. Best
[۲۲] Y. Hong
[۲۳] van Tilborg

مقدماتی از درجه ۱ و ۲ از ریشه‌ها شناخته‌شده هستند:

$$\sum_{i=1}^{e} x_i = \frac{1}{2}e(n+1), \tag{۲۰}$$

$$\sum_{i<j} x_i x_j = \frac{1}{24}e(e-1)\{3n^2+3n+2e+2\}. \tag{۲۱}$$

مشاهده می‌کنید که رابطه ۲۰ نیز از رابطه ٦ نتیجه می‌شود که نشان می‌دهد:

$$x_{e-i+1} = n+1-x_i. \tag{۲۲}$$

از روابط ۲۰ و ۲۱ داریم:

$$\sum_{i=1}^{e}\sum_{j=1}^{e}(x_i-x_j)^2 = \frac{1}{2}e^2(e-1)\{n-\frac{2e-1}{3}\}. \tag{۲۳}$$

برای یافتن حاصل‌ضرب ریشه‌ها، $\Psi_e(0)$ را محاسبه می‌کنیم. از تعریف ۱.۱.۲ داریم $\Psi_e(0)=\sum_{j=0}^{e}\binom{n}{j}$. با ترکیب این تعریف با رابطه ٦.۳.۱ با رابطه ۱۲ (فصل ۱) داریم:

$$\prod_{i=1}^{e} x_i = e!2^l, \qquad \text{برای یک مقدار صحیح } l. \tag{۲۴}$$

در روشی مشابه، $\Psi_e(1)$ و $\Psi_e(2)$ را محاسبه می‌کنیم که به روابط زیر منجر می‌شود:

$$\prod_{i=1}^{e}(x_i-1) = 2^{-e}(n-1)(n-2)\cdots(n-e), \tag{۲۵}$$

$$\prod_{i=1}^{e}(x_i-2) = 2^{-e}(n-1-2e)(n-2)\cdots(n-e). \tag{۲٦}$$

حال نتیجه درباره x_1، x_2، ...، x_e را از این روابط استخراج می‌کنیم. فرض کنید $A(x)$ بزرگ‌ترین مقسوم‌علیه فرد x باشد. در این‌صورت رابطه ۲۴ نشان می‌دهد که:

$$\prod_{i=1}^{e} A(x_i) = A(e!) < e!.$$

این مطلب ایجاب می‌کند که باید دو صفر x_i و x_j وجود داشته باشند به‌طوری که $A(x_i)=A(x_j)$ $(i<j)$؛ بنابراین، $2x_i \le 2x_j$ و از این‌رو $2x_1 \le x_e$. حال رابطه ۲۳ ایجاب می‌کند:

$$x_e - x_1 \ge \frac{1}{3}(n+1). \tag{۲۷}$$

اگر ما x_1 و x_e را ثابت نگه داریم، آن‌گاه سمت چپ رابطه ۲۳ دارای کمترین مقدار است، اگر:

$$x_2 = x_3 = \cdots = x_{e-1} = \frac{1}{2}(x_1+x_e).$$

با جانشین نمودن این مقادیر در رابطه ۲۳، داریم:

$$(x_e - x_1)^2 \leq \frac{1}{2}e(e-1)(n - \frac{2e-1}{3}), \tag{۲۸}$$

که ما آن را با رابطه ۲۷ ترکیب می‌کنیم. نتیجه به‌صورت زیر است:

$$n + 1 \leq \frac{9}{2}e(e-1). \tag{۲۹}$$

حال روابط ۲۵ و ۲۶ را درنظر بگیرید. چون اگر $x \in \mathbb{N}$، آن‌گاه $(x-1)(x-2)$ همواره زوج است، داریم:

$$(n-1-2e)(n-1)(n-2)^2(n-3)^2 \cdots (n-e)^2 \equiv 0 \bmod 2^{3e}. \tag{۳۰}$$

اگر $e = \frac{1}{2}(n-1)$، آن‌گاه این مطلب بدیهی است؛ یعنی C کد تکراری است. فرض کنید $e < \frac{1}{2}(n-1)$. نیز 2^α را بزرگ‌ترین توان ۲ در هر عامل $n-j$ در طرف چپ رابطه ۳۰ درنظر بگیرید که شامل $n-1-2e$ باشد؛ در این‌صورت بزرگ‌ترین توان ۲ که طرف چپ رابطه ۳۰ را عاد می‌کند حداکثر برابر با $2^{3\alpha+2e-3}$ است که ایجاب می‌کند $\alpha \geq \frac{1}{3}e + 1$.

بنابراین:

$$n > 2^{1+(1/3)e}. \tag{۳۱}$$

اگر e بزرگ باشد، آن‌گاه رابطه ۳۱ متناقض با رابطه ۲۹ است. مقادیر کوچک e که به‌واسطه رابطه ۲۹، مقادیر کوچک n را ایجاب می‌کند، به آسانی بررسی می‌شوند. درواقع، اگر در تخمین n کمی دقیق‌تر عمل کنیم، آن‌گاه تنها حالات بسیار کمی وجود دارند که نیاز به بررسی دارند. ثابت می‌شود که $e = 3$ تنها حالت ممکن است. درواقع، $e = 3$ می‌تواند حتی کاملاً بدون استفاده از قضیه لوید مورد بحث واقع شود. این مطلب در مساله ۱.۷.۷ نشان داده شده است. □

دلیل به‌کار رفته برای نشان دادن این‌که تمامی کدهای به‌طور یکنواخت بسته‌بندی‌شده، شناخته شده‌اند (یعنی؛ تمامی آنهایی که در رابطه ۱.۷.۳ صدق می‌کنند)، روند مشابهی را به کار می‌گیرد، اما به دلیل وقوع پارامتر r در آن، تعداد کمی ترفند اضافی لازم است.

قضیه ۲.۷.۵. جدول ۷.۱، تمامی کدهای به‌طور یکنواخت بسته‌بندی‌شده را لیست می‌کند.

اثبات. با تعمیم قضیه لوید شروع می‌کنیم؛ یعنی قضیه ۴.۷.۳. در روندی دقیقاً مشابه با روشی که رابطه ۲۸، به‌ترتیب رابطه ۳۱، را ثابت کردیم، داریم:

$$x_{e+1} - x_1 \leq (e+1)(\frac{n+1}{2})^{1/2}, \tag{۳۲}$$

$$n > 2^{e/7}. \tag{۳۳}$$

دلیلی که منجر به رابطه ۲۷ گردد باید تغییر کند. در روشی متفاوت، ریشه‌ها را به‌صورت y_1، y_2، $\cdots$، y_{e+1} شماره‌گذاری می‌کنیم که در آن $y_j = A(y_j)2^{\alpha_j}$ و $\alpha_1 \leq \alpha_2 \leq \cdots \alpha_{e+1}$. از طرف دیگر داریم (با نوشتن (a,b) برای ب.م.م a و b):

$$\begin{aligned}\prod_{i=1}^{e} \frac{|y_i - y_{i+1}|}{y_i} &\geq \prod_{i=1}^{e} \frac{(y_i, y_{i+1})}{y_i} = \prod_i \frac{(A(y_i), A(y_{i+1}))2^{\alpha_i}}{y_i} \\ &\geq \prod_{i=1}^{e} \frac{1}{A(y_i)} \geq \frac{1}{A(y_1, \cdots, y_{e+1})} = \frac{A(|c|)}{A(r)A((e+1)!)} \\ &\geq \frac{1}{rA((e+1)!)}.\end{aligned}$$

در اینجا، معادله آخر از رابطه ۱۹ نتیجه می‌شود. از طرف دیگر، داریم:

$$\begin{aligned}\prod_{i=1}^{e} \frac{|y_i - y_{i+1}|}{y_i} &\leq \frac{(x_{e+1} - x_1)^e}{y_1 \cdots y_e} \leq \frac{n(x_{e+1} - x_1)^e}{x_1 x_2 \cdots x_{e+1}} \\ &= \frac{1}{n(x_{e+1} - x_1)^e} r(e+1)!. \frac{2^{e+1}|c|}{2^n}.\end{aligned}$$

با ترکیب این دو نامساوی داریم:

$$\begin{aligned}(x_{e+1} - x_1)^e &\geq \frac{(e+1)!}{A((e+1)!)} \frac{1}{2^{e+1}} \cdot \frac{2^n}{n|c|} \\ &\geq \frac{(e+1)!}{A((e+1)!)} \frac{1}{2^{e+1}} \cdot \frac{1}{n} \sum_{i=0}^{e} \binom{n}{i} \geq \frac{(e+1)!}{A((e+1)!)} \frac{1}{2^{e+1}} \frac{1}{n} \binom{n}{e};\end{aligned}$$

بنابراین:

$$(x_{e+1} - x_1)^e \geq \frac{(e+1)}{A((e+1)!)} \frac{1}{2^{e+1}} (n-1)(n-2)\cdots(n-e+1). \tag{۳۴}$$

حال روابط ۳۲ و ۳۳ را با رابطه ۳۴ مقایسه کنید. اگر $e \geq 3$، آن‌گاه تنها تعداد متناهی از زوج‌های (e,n) در تمامی این سه نامساوی صدق می‌کنند. حالات $e = 1$ و $e = 2$ به‌آسانی و به‌طور مستقیم توسط قضیه ۴.۷.۳ می‌توانند مورد بحث قرار گیرند. به‌عنوان یک نتیجه، حالات متناهی بسیاری به‌طور مجزا بررسی شده‌اند. ما جزییات (ر.ک. مرجع [۶۹]) را حذف می‌کنیم. به‌عنوان یک نتیجه، کدهای لیست‌شده در جدول زیر را داریم. □

(در اینجا عناصر "کد همینگ" و "کد پرپاراتا" به‌صورت تمامی کدهای با پارامترهای یکسان از این کدها تعبیر می‌شوند).

جدول ۷.۱: جدول تمامی کدهای کامل، تقریباً کامل و به‌طور یکنواخت بسته‌بندی‌شده.

توصیف	نوع	$\|c\|$	n	e
$\{۰,۱\}^n$	کامل	۲^n	n	۰
کد همینگ (و سایر کدها)	کامل	۲^{n-m}	$۲^m-۱$	۱
کد همینگ کوتاه‌شده	تقریبا کامل	۲^{n-m}	$۲^m-۲$	۱
رجوع به ۱.۷.۷				
رجوع به ۲.۷.۴	به‌طور یکنواخت فشرده	$۲^{n-۲m}$	$۲^{۲m-۱}\pm۲^{m-۱}-۱$	۱
کد پرپاراتا	تقریبا کامل	$۲^{n+۱-۴m}$	$۲^{۲m}-۱$	۲
کد BCH(رجوع به ۲.۷.۷)	به‌طور یکنواخت فشرده	$۲^{n-۴m-۲}$	$۲^{۲m+۱}-۲$	۲
رجوع به ۱.۷.۴)	به‌طور یکنواخت فشرده	۲۴	۱۱	۲
کد گلی	کامل	$۲^{۱۲}$	۲۳	۳
کد تکرار	کامل	۲	$۲e+۱$	e
$\{۰\}$	کامل	۱	e	e

۷.۶ پیشنهادها

کدهای کامل به چندین روش تعمیم یافته‌اند (برای مثال متریک‌های دیگری به‌جز فاصله همینگ، الفباهای ترکیب‌شده). برای یک بررسی (شامل بسیاری از منابع) خواننده باید به مرجع [۴۴] مراجعه کند.

نسخه تغییر یافته‌ای از اثبات عدم وجودِ تیتاواینن می‌تواند در منبع [۴۶] و نیز بسیاری از منابع دیگر یافت شود.

کامل‌ترین اطلاعات درباره کدهای به‌طور یکنواخت بسته‌بندی‌شده می‌تواند در مرجع [۶۹] یافت شود. برای مشاهده ارتباط با نظریه طرح[۲۴] ، به مراجع [۱۱] و [۴۶] ارجاع می‌دهیم.

مساله امکان وجود کدهای ۲—تصحیح‌کننده خطای شناخته نشده بر روی الفباهای Q، در حالتی که $|Q|$ توانی از یک عدد اول نباشد، به‌نظر بسیار مشکل می آید، اما غیرممکن نیست. حالت $e=۱$ امیدوارکننده به‌نظر می‌رسد.

بسیاری از ایده‌ها و روش‌هایی که در این بخش به‌کار رفته‌اند (برای مثال بخش ۷.۲) توسط دلسارت[۲۵] مطرح شده‌اند.

[۲۴] design theory
[۲۵] P. Delsarte

۷.۷ مسائل

۱.۷.۷. نشان دهید کد همینگ دودویی کوتاه‌شده $[۲^m - ۲, ۲^m - m - ۲]$ تقریباً کامل است.

۲.۷.۷. فرض کنید C کد BCH دودویی با طول $n = ۲^{۲m+۱} - ۱$ و با فاصله طراحی‌شده ۵ باشد. با استفاده از محاسبه صریح تعداد کدکلمات با فاصله ۳ تا کدکلمه u با $\rho(u, C) \geq ۲$، نشان دهید C به‌طور یکنواخت بسته‌بندی‌شده با پارامتر $r = \frac{۱}{۹}(n - ۱)$ است.

۳.۷.۷. نشان دهید که یک کد تقریباً کامل C وجود دارد به‌طوری که $\bar{C}$ کد نرد—استروم است.

۴.۷.۷. فرض کنید H، کد همینگ $[۷, ۴]$ دودویی باشد. f را روی H با $f(۰) = ۰$ و $f(c) = ۱$ اگر $c \neq ۰$ تعریف کنید. فرض کنید C کد با طول ۱۵ با کدکلمات:

$$(x, x + c, \sum_{i=۱}^{۷} x_i + f(c)), \quad c \in H, x \in \mathbb{F}_۲^۷ \text{ . که در آن}$$

باشد. نشان دهید C کامل است و C هم‌ارز با یک کد خطی نیست.

۵.۷.۷. نشان دهید که یک کد کامل دودویی ۲—تصحیح‌کننده خطا بدیهی است.

۶.۷.۷. فرض کنید C یک کد به‌طور یکنواخت بسته‌بندی‌شده با طول n، $e = ۱$ و $r = ۶$ باشد. نشان دهید $n = ۲۷$ و یک ساختار از C را ارائه دهید.

۷.۷.۷. در مثال ۳.۳.۳ دیدیم که خطوط $PG(۲, ۲)$، کد همینگ $[۷, ۴]$ را تولید می‌کنند. کد گسترش‌یافته برابر یک کد $[۸, ۴, ۴]$ است. یک نفر ممکن است امید داشته باشد که با به‌کارگیری $PG(۲, q)$، می‌توان کد C روی $\mathbb{F}_q$ را با طول $q^۲ + q + ۲$، $d = ۴$ و $|c| = q^{n-۴}$، بیابد. این درواقع مثالی از یک کد به‌طور یکنواخت بسته‌بندی‌شده در حالت کلی‌تر است (ر.ک. مرجع [۲۵]). حالت $q = ۳$ و $|c| = ۳^{۱۰}$ را درنظر بگیرید. نشان دهید چنین کدی وجود ندارد.
راهنمایی: زوج‌های (x, c) را به دو روش با $x \in \mathbb{F}_۳^{۱۴}$، $c \in C$ و $d(x, c) = ۲$ شمارش کنید. $A_۴$ و سپس $A_۵$ را محاسبه کنید.

۸.۷.۷. الفبای $\mathbb{Z}_m$ (m فرد) با فاصله لی را درنظر بگیرید. یک کد کامل تصحیح‌کننده یک خطا با طول $n = \frac{۱}{۲}(m^۲ - ۱)$ بسازید.

فصل ۸

کدهای روی $\mathbb{Z}_4$

۸.۱ کدهای چهارتایی

در سال ۱۹۹۴ (مرجع [۸۸] را به‌عنوان راهنمایی برای این فصل مشاهده کنید) نشان داده شد که چندین کد دودویی معروف را با ساختِ یک کد روی الفبای $\mathbb{Z}_4$ و سپس تصویر کردن مختصات آن به $\mathbb{Z}_2^2$، می‌توان ساخت. درابتدا کدهای روی $\mathbb{Z}_4$ را در حالت کلی مطالعه می‌کنیم.

تعریف ۱.۸.۱. اگر C یک زیرگروه جمعی از $\mathbb{Z}_4^n$ باشد، آن‌گاه C را یک کد بلوکی خطی به طول n روی $\mathbb{Z}_4$ یا یک کد چهارتایی[۱] می‌نامیم.

اگرچه C یک $\mathbb{Z}_4$—مدول است ویک فضای برداری نیست، ما اصطلاح نظریه کدگذاری را دنبال کرده و از کلمه "خطی" به‌صورت نامناسب استفاده می‌کنیم.

ضرب داخلی $< \mathbf{a}, \mathbf{b} >$ از دو کلمه $\mathbb{Z}_4^n$، به‌طور معمول تعریف می‌شود. می‌توانیم کد دوگان $C^\perp$ را به‌شکل مشابه با تعریف ۴.۳.۲، معرفی نماییم.

به‌طور معمول، ما دو کد را هم‌ارز[۲] می‌نامیم، اگر یکی را از دیگری بتوان با جای‌گشت مکان‌های مختصات به‌دست آورد. برخی اوقات این تعریف با تغییر مجاز علامت‌ها در بعضی مکان‌ها، تعمیم داده می‌شود؛ (این تغییر، سمبل ۱ را به‌جای ۳ جای‌گزین می‌کند و برعکس).

---

[۱] quaternary

[۲] equivalent

در تعمیم مفهوم ماتریس مولد، باید دقت کنیم. درابتدا یک مثال می‌آوریم.

مثال ۲.۸.۱. زیرگروه جمعی از $\mathbb{Z}_۴^۳$ را که شامل تمامی کلمات (x,x,x) و $(y,y+۲,y+۲)$ $(x,y\in\mathbb{Z}_۴)$ باشد، درنظر بگیرید. می‌توانیم این کد چهارتایی را به‌عنوان مجموعه ترکیبات خطی $a(۱,۱,۱)+b(۰,۲,۲)$ درنظر بگیریم که در آن $a\in\mathbb{Z}_۴$ و $b\in\mathbb{Z}_۲$ (جمع به پیمانه ۴).

در حالت کلی، یک کد چهارتایی، حاصل‌ضرب مستقیم زیرکدهای با مرتبه ۴ یا ۲ است (گروه‌های دوری جمعی از مرتبه ۴ یا ۲). این مطلب نشان‌دهنده آن است که یک کد هم‌ارز با ماتریس مولد به‌شکل زیر است:

$$G:=\begin{pmatrix} I_{k_۱} & A & B \\ ۰ & ۲I_{k_۲} & ۲C \end{pmatrix} \qquad (۱)$$

که در آن درایه‌های A و C برابر با ۰ و ۱ و درایه‌های B متعلق به $\mathbb{Z}_۴$ هستند. یک کدکلمه، به‌شکل aG می‌باشد که در آن $a_۱$ تا $a_{k_۱}$ متعلق به $\mathbb{Z}_۴$ و $a_{k_۱+۱}$ تا $a_{k_۱+k_۲}$ متعلق به $\mathbb{Z}_۲$ می‌باشند. کد دوگان $C^\perp$ دارای ماتریس مولدی به‌شکل زیر است:

$$H:=\begin{pmatrix} -B^\top-C^\top A^\top & C^\top & I_{n-k_۱-k_۲} \\ ۲A^\top & ۲I_{k_۲} & ۰ \end{pmatrix} \qquad (۲)$$

با دنبال کردن بحث کدهای خطی از فصل ۳، اکنون باید به شمارنده‌های وزنی نگاهی بیندازیم. به‌عنوان مقدمه‌ای بر این فصل، این مطالب در بخش ۳.۶ مورد بحث قرار گرفته‌اند. شمارنده وزنی متقارن یک کد در $\mathbb{Z}_۴^n$ و شمارنده وزن لی را تعریف نمودیم. نتیجه مهم، این واقعیت بود که شمارنده‌های وزن لی یک کد و دوگان آن در روابط مک‌ویلیامز صدق می‌کنند.

۸.۲ کدهای دودویی به‌دست آمده از کدهای روی $\mathbb{Z}_۴$

یک نگاشت طبیعی ϕ از $\mathbb{Z}_۴$ به $\mathbb{Z}_۲^۲$ وجود دارد که فاصله لی در $\mathbb{Z}_۴$ را به فاصله همینگ تصویر می‌کند و به‌صورت زیر است:

$$\phi(۰)=(۰,۰),\quad \phi(۱)=(۰,۱),\quad \phi(۲)=(۱,۱),\quad \phi(۳)=(۱,۰)$$

در اینجا این نگاشت را به کدهای متعلق به $\mathbb{Z}_4^n$ تعمیم می‌دهیم. برای سادگی در نمادگذاری، در ادامه سه تابع از $\mathbb{Z}_4$ به $\mathbb{Z}_2$ را به‌صورت زیر معرفی می‌کنیم:

$i \in \mathbb{Z}_4$	$\alpha(i)$	$\beta(i)$	$\gamma(i)$
۰	۰	۰	۰
۱	۱	۰	۱
۲	۰	۱	۱
۳	۱	۱	۰

توجه کنید که نمایش دودویی عدد i با بیشترین ارزش در رقم نخست، به‌صورت $(\beta(i)),\alpha(i))$ است. به‌علاوه $\gamma(i) = \alpha(i) + \beta(i)$. نگاشت ϕ تعریف شده در بالا، به‌طور بدیهی به $\mathbb{Z}_4^n$ تعمیم داده می‌شود.

تعریف ۱.۸.۲.

$$\phi(C) := (\beta(c), \gamma(c)), \quad (c \in \mathbb{Z}_4^n).$$

این نگاشت، نگاشت گری[۳] نامیده می‌شود و برای کد چهارتایی C، کد $C' := \phi(c)$، تصویر دودویی C نامیده می‌شود. چنین کد دودویی، $\mathbb{Z}_4$—خطی نامیده می‌شود. درادامه، همیشه C' معرف تصویر دودویی کد چهارتایی C می‌باشد.

مثال ۲.۸.۲. کد چهارتایی C با طول ۳ تولید شده توسط (۳ ,۱ ,۱) و (۰ ,۲ ,۲) را درنظر بگیرید (اینها سطرهای G در رابطه ۱ با $k_1 = k_2 = 1$ هستند). سهم سطراول در تصویر دودویی، ترکیبات خطی (۰۰۱۱۱۰) و (۱۱۰۰۰۱) می‌باشد. سطر دوم فقط (۰۱۱۰۱۱) را شرکت می‌دهد. سرانجام ما ترکیبات خطی اینها را داریم؛ بنابراین، در این حالت، تصویر دودویی C' یک کد خطی با ماتریس مولد به شکل زیر است:

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

با مقایسه با این مثال، خواننده می‌تواند بررسی کند که اگر C' یک کد چهارتایی با ماتریس مولدی همانند ۱ بوده و تصویر دودویی C'، یک کد دودویی خطی باشد، آن‌گاه C' دارای ماتریس مولدی به‌شکل

[۳] Gray map

زیر است:

$$G' := \begin{pmatrix} I_{k_1} & A & \alpha(B) & I_{k_1} & A & \alpha(B) \\ 0 & I_{k_2} & C & 0 & I_{k_2} & C \\ 0 & 0 & \beta(B) & I_{k_1} & A & \gamma(B) \end{pmatrix}. \quad (۳)$$

در حالت کلی، C' خطی نمی‌باشد، زیرا ϕ یک نگاشت خطی نیست. مهم‌ترین مساله برای ما این است که نگاشت ϕ حافظ فاصله است؛ یعنی فاصله لی دو کدکلمه در C مساوی فاصله همینگ تصویرهای آنان است.

یکی از دلایل توجه به کدهای روی $\mathbb{Z}_4$، این مطلب است که آنها توجیهی برای یک "انطباق" قابل توجه را ارائه می‌دهند. یک کد کرداک و یک کد پرپاراتا[۴] با طول مشابه، هر دو غیرخطی هستند. شمارنده‌های فاصله آنها در روابط مک‌ویلیامز صدق می‌کنند. به بیان دیگر، آنها تلاش می‌کنند تا دوگان هم باشند، اگرچه این مفهوم برای کدهای غیرخطی بی‌معناست، ما روی روش خود برای توصیف این کدها هم‌چنان مصمم هستیم. هر دوی این کدها تصویرهای دودویی کدهای چهارتایی هستند که درواقع دوگان یکدیگر هستند؛ بنابراین، ما $\mathbb{Z}_4$—دوگانگی را به‌صورت زیر تعریف می‌کنیم:

تعریف ۳.۸.۲. اگر C یک کد چهارتایی و $C^\perp$ کد دوگان آن باشد، آن‌گاه $C' = \phi(C)$ و $(C^\perp)' := \phi(C^\perp))$، کدهای $\mathbb{Z}_4$—دوگان نامیده می‌شوند.

از این‌که C خطی است، نتیجه می‌شود که تصویر دودویی آن، یعنی C'، تحت فاصله پایاست.

قضیه ۴.۸.۲. اگر C و $C^\perp$ کدهای چهارتایی و دوگان هم باشند، آن‌گاه توزیع‌های وزنی متناظر با تصویرهای دودویی C' و $(c^\perp)'$ از این کدها، در روابط مک‌ویلیامز از قضیه ۲.۳.۵ صدق می‌کنند.

اثبات. ملاحظه کردیم که وزن همینگ $\phi(C)$ مساوی $w_L(C)$ است. اگر طول C برابر با n باشد، آن‌گاه طول کد C' برابر $2n$ است. بنابراین، از رابطه ۳.۳.٦ و قضیه ۴.۳.٦، داریم:

$$Ham_{(C^\perp)'}(x,y) = \frac{1}{|c'|} Ham_{C'}(x+y, x-y).$$

□

دراینجا شرایط لازم و کافی را برای این‌که یک کد دودویی، تصویر دودویی یک کد چهارتایی باشد، اثبات خواهیم نمود. در ابتدا مشاهده می کنید که $\phi(-C) = (\gamma(C), \beta(C))$. این مطلب نتیجه می‌دهد که یک کد $\mathbb{Z}_4$—خطی توسط جای‌گشت σ به‌صورت $(1.n+1)(2, n+2).....(n, 2n)$، ثابت می‌باشد. این جای‌گشت، دو نیمه هر کدکلمه را با یکدیگر جابه‌جا می‌کند.

[۴] Preparata

لم ۵.۸.۲ برای تمامی $a, b \in \mathbb{Z}_4^n$، داریم:

$$\phi(a+b) = \phi(a) + \phi(b) + (\phi(a) + \sigma(\phi(a)))(\phi(b) + \sigma(\phi(b))).$$

اثبات. اثبات با توجه به مطالب زیر نتیجه می‌شود:

۱) $\alpha(a) + \beta(a) + \gamma(a) = 0$؛

۲) $\alpha(a)\alpha(b) = 1$ اگر وفقط اگر a و b فرد باشند؛

۳) $\beta(a+b) = \beta(a) + \beta(b) + \epsilon$ که در آن $\epsilon = 1$ اگر و فقط اگر a و b هر دو فرد باشند (درغیر این‌صورت $\epsilon = 0$) و γ نیز به‌طور مشابه در این رابطه صدق می‌کند.

□

قضیه ۶.۸.۲. یک کد دودویی با طول زوج که لزوماً خطی نمی‌باشد، $\mathbb{Z}_4$—خطی است اگر و تنها اگر با یک کد C معادل باشد، به‌طوری که:

$$a, b \in C \Rightarrow a + b + (a + \sigma(a))(b + \sigma(b)) \in C.$$

اثبات. این اثبات فوراً از لم ۵.۸.۲ نتیجه می‌شود. □

مثال ۷.۸.۲. کد رید—مولر مرتبه اول $\mathcal{R}(1, m)$ با طول 2^m را درنظر بگیرید. هر کدکلمه، دارای فرم $a = (x, x + \epsilon)$ است که در آن $\varepsilon = 0$ یا $\varepsilon = 1$ (از طول $1 - 2^m$). اگر $b = (y, y + \epsilon)$ دومین کدکلمه باشد، آن‌گاه $(a + \sigma(a))(b + \sigma(b)) = 0$ یا $(a + \sigma(a))(b + \sigma(b)) = 1$؛ بنابراین، با استفاده از قضیه ۶.۸.۲، کد $\mathcal{R}(1, m)$، $\mathbb{Z}_4$—خطی است. اگر حالت $m = 3$ را درنظر بگیریم، آن‌گاه کد چهارتایی متناظر، دارای ماتریس مولدی به‌شکل زیر است:

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

از G و ماتریس ۱، بردارهای پایه استاندارد برای $\mathcal{R}(۱,m)$ را پیدا می‌کنیم.
اکنون کدهای خطی دودویی را درنظر می‌گیریم که تصاویری از کدهای چهارتایی هستند. مبحث زیر، نتیجه مستقیمی از قضیه ۶.۸.۲ است.

نتیجه‌گیری ۸.۸.۲ تصویر دودویی $\phi(C)$ از یک کد چهارتایی C، خطی است اگر و تنها اگر:

$$a,b \in C \Rightarrow ۲(\alpha(a)\alpha(b)) \in C.$$

اثبات. با دو بار به‌کار بردن لم ۵.۸.۲ داریم:

$$\phi(a+b+۲(\alpha(a)\alpha(b))) = \phi(a)+\phi(b).$$

□

این به معنی وجود کلمه‌ای در کد است که در مکان‌هایی که هر دوی **a** و **b** درایه‌های فرد دارند، دارای مقدار ۲ است و در مکان‌های دیگر دارای مقدار صفر است.

در اینجا نشان خواهیم داد که کد همینگ گسترش‌یافته به‌طول $n = ۲^m$ برای $m \geq ۵$، $\mathbb{Z}_۴$—خطی نیست.

قضیه ۹.۸.۲. کد $\mathcal{R}(m-۲,m)$ برای $m \geq ۵$، $\mathbb{Z}_۴$—خطی نیست.

اثبات. فرض کنید C یک کد چهارتایی به‌طول $۲^{m-۱}$ باشد که تصویر دودویی آن شامل کد همینگ دودویی گسترش‌یافته H_m به طول $n = ۲^m$ است. فرض کنید G از رابطه ۱، ماتریس مولد C باشد. بخش بالایی را $G_{k_۱}$ و بخش پایینی را $۲G_{k_۲}$ می‌نامیم. چون H_m یک کد با وزن زوج است، $G_{k_۱}$ سطرهایی با تعدادی زوج از درایه‌های فرد دارد؛ تعریف می‌کنیم:

$$G'_{k_۱} := (\, I_{k_۱} \quad A \quad \alpha(B)\,).$$

کد دودویی H' که توسط $G'_{k_۱}$ تولید شده را مطالعه می‌کنیم. توجه کنید که $۲G'_{k_۱}$ و $۲G_{k_۲}$ زیرکدی از C را که تنها شامل کلمات با مختصات زوج است، تولید می‌کند. به‌وضوح $k_۱ + k_۲ \leq ۲^{m-۱} - ۱$. چون $۲k_۱ + k_۲ = ۲^m - m - ۱$، می‌بینیم که H' دارای بعد حداقل $۲^{m-۱} - m$ می‌باشد.

از نتیجه ۸.۸.۲ در می‌یابیم که اگر H' شامل کلماتی با وزن ۲ باشد، آن‌گاه مکان‌های ناصفر این کلمات، مجزا هستند. ما می‌توانیم این کلمات را به عنوان بردارهای پایه کد درنظر گرفته و ممکن است

فرض کنیم که سایر بردارهای پایه، دارای مکان‌های ناصفری مجزا از مکان‌های ناصفرِ بردارهای وزن ۲ هستند (زیرا اشتراک مکان‌های ناصفر نمی‌تواند در یک مکان باشد). اگر a کلمه با وزن ۲ وجود داشته باشد، آن‌گاه اینها را از G'_{k-1} حذف کرده و در مکان‌های این کلمات پنچر می‌کنیم. ما مولد یک کد دودویی به‌طول $2^{m-1}-2a$ با بعد حداقل $2^{m-1}-m-a$ و کمترین—فاصله ۴ را پیدا کردیم. این مطلب با کران همینگ تناقض دارد، مگر این‌که $a=0$؛ بنابراین، نشان داده‌ایم که H' خودش یک کد گسترش‌یافته همینگ است. چون کدهای همینگ کامل هستند، به‌آسانی دیده می‌شود که کلمات با وزن ۴ در یک کد گسترش‌یافته همینگ تشکیل یک طرح $(2^m-3, 4, 1)$ می‌دهند. برای $m \geq 4$، این طرح بلوک‌هایی دارد که در یک نقطه به هم‌دیگر می‌رسند (با یک محاسبه آسان). این مطلب توسط نتیجه ۸.۸.۲ مستثنی شده است، پس ما یک تناقض داریم. این اثبات را کامل می‌کند. □

۸.۳ حلقه‌های گالوا روی $\mathbb{Z}_4$

می‌خواهیم مفهوم کدهای دوری را برای کدهای روی $\mathbb{Z}_4$ تعمیم دهیم. برای این‌کار، به اندکی از جبر نیاز داریم. برای کدهای دوری به طول n روی $\mathbb{F}_2$، به یک میدان گسترش‌یافته که شامل ریشه nام واحد باشد نیاز داریم. موقعیت فعلی مشابه است. ما باید یک توسیع از $\mathbb{Z}_4$ را به‌واسطه ریشه nام واحد درنظر بگیریم. چنین توسیعی را حلقه گالوا[5] می‌نامیم.

ما نیاز به برخی پیش زمینه‌ها درمورد چندجمله‌ای‌های تحویل‌ناپذیر در $\mathbb{Z}_4[x]$ داریم. چندجمله‌ای $f(x)$ در $\mathbb{Z}_2[x]$ را درنظر بگیرید و آن‌را به‌صورت $f(x)=a(x^2)-xb(x^2)$ بنویسید (که در آن ما علامت منفی را به‌کار می‌بریم، زیرا محاسبات مختصری را روی $\mathbb{Z}_4$ انجام خواهیم داد). نگاشت ϕ را به‌صورت:

$$\phi(f)(x)=F(X):=\pm(a(x)^2-xb(x)^2)\in\mathbb{Z}_4[x],$$

تعریف می‌کنیم که در آن علامت $\pm$ را طوری انتخاب کرده‌ایم که ضریب بالاترین توان x برابر با ۱ است. توجه کنید که $\phi(x^n-1)=x^n-1$ اگر n فرد باشد. به‌وضوح نگاشت معکوس، همان $f(x)\equiv F(x) \bmod 2$ می‌باشد.

با انجام یک محاسبه جزیی می‌توان چک نمود که $\phi(fg)=\phi(f)\phi(g)$. چون هم ϕ و هم معکوس آن، درجه چندجمله‌ای و ضریب بزرگ‌ترین توان x را تغییر نمی‌دهند، چندجمله‌ای‌های تحویل‌ناپذیر به چندجمله‌ای‌های تحویل‌ناپذیر متناظر می‌شوند. این مطلب نتیجه می‌دهد که اگر x^n-1 (که در آن $n=2^m-1$) را بتوان به‌صورت حاصل‌ضرب $f_1(x)f_2(x)\cdots f_l(x)$ از چندجمله‌ای‌های تحویل ناپذیر

[5] Galois Ring

در $\mathbb{Z}_۲[x]$ نوشت، آن‌گاه $F_۱(x)F_۲(x)\cdots F_l(x)$ که در آن $F_i := \phi(f_i)$، تجزیه منحصربه‌فرد $x^n - ۱$ در $\mathbb{Z}_۴[x]$ می‌باشد. عامل تحویل‌ناپذیر $h(x)$ از درجه m، چندجمله‌ای ابتدایی پایه[۶] در $\mathbb{Z}_۴[x]$ نامیده می‌شود.

این روش توسعه دادن[۷] یک چندجمله‌ای تحویل‌ناپذیر در $Z_۲[x]$ به یک چندجمله‌ای تحویل‌ناپذیر در $\mathbb{Z}_۴[x]$ (با نگاشت ϕ) به روش گرائف[۸] معروف است (ر.ک. مرجع [۹۹]). این مطلب یک مورد خاص از یک نتیجه، معروف به لم هنسل[۹] است (ر.ک. مرجع [۹۳]).

مثال ۱.۸.۳. چندجمله‌ای اولیه $f(x) = x^۳ + x + ۱$ به عنوان عاملی از $x^۷ - ۱$ را درنظر بگیرید. با نمادگذاری به‌کار رفته در بالا، داریم $a(x) = ۱$ و $b(x) = -۱ - x$، بنابراین، $F(x) = x^۳ + ۲x^۲ + x - ۱ \equiv x^۳ + x + ۱ \bmod ۲$. در این روش، تجزیه زیر را داریم:

$$x^۷ - ۱ = (x^۳ + ۲x^۲ + x - ۱)(x^۳ - x^۲ + ۲x - ۱)(x - ۱),$$

که دو عامل اول، چندجمله‌ای‌های اولیه پایه در $\mathbb{Z}_۴[x]$ هستند.

تعریف ۲.۸.۳. حلقه گالوا $GR(۴, m)$ به‌صورت $\mathbb{Z}_۴[\xi]$ تعریف شده است که در آن ξ ریشه‌ای از $h(x)$ است (چون ξ nام ریشه واحد است؛ داریم $(Z_۴[\xi] = \frac{\mathbb{Z}_۴[x]}{(h(x))})$).

دقت می‌کنید که مجدداً داریم:

$$h(x) = x^۳ + ۲x^۲ + x - ۱ = (x - \xi)(x - \xi^۲)(x - \xi^۴).$$

مشابه مثال ۱۹.۱.۱، می‌توان عناصر $GR(۴, m)$ را به‌صورت چندجمله‌ای‌های با درجه کمتر از m برحسب ξ با ضرایب در $\mathbb{Z}_۴$، نشان داد.

مثال ۳.۸.۳. برای $GR(۴, m)$، تولید شده توسط $x^۳ + ۲x^۲ + x - ۱$، جدول زیر را برای مجموعه $\{۰, ۱, \xi, \xi^۲, \xi^۳, ..., \xi^۶\}$ داریم. دراینجا:

$$C = \sum_{i=۰}^{۲} a_i \xi^i, \qquad (\xi^۳ = ۱ + ۳\xi + ۲\xi^۲).$$

چنین جدولی به ما نمی‌گوید که چگونه عناصری از $GR(۴, m)$ را که در مجموعه:

---

[۶] basic primitive polynomial

[۷] lifting

[۸] Graeff's method

[۹] Hensel

c	a_0	a_1	a_2
۰	۰	۰	۰
۱	۱	۰	۰
ξ	۰	۱	۰
ξ^2	۰	۰	۱
ξ^3	۱	۳	۲
ξ^4	۲	۳	۳
ξ^5	۳	۳	۱
ξ^6	۱	۲	۱

$$\tau := \{0, 1, \xi, \xi^2, ..., \xi^{n-1}\},$$

نیستند، بیان کنیم. با مشاهده نمایش ξ^i به‌صورت چندجمله‌ای با درجه کمتر از m نسبت به ξ، می‌بینیم که $2\xi^i = 2$ نتیجه می‌دهد که $\xi^i = 1$؛ یعنی $\xi = 1$. ازاین رو اگر t در τ تغییر کند، آن‌گاه همه عناصر $2t$ متمایز هستند.

4^m مجموع به‌شکل $a + 2b$ را درنظر بگیرید که a و b در مجموعه τ قرار دارند. اگر $a + 2b = a' + 2b'$، آن‌گاه $2a = 2a'$؛ بنابراین، $a = a'$ و از این‌رو $b = b'$؛ پس، مجموع‌های $a + 2b$ همگی متفاوت هستند؛ بنابراین، آنها تمامی عناصر $GR(4, m)$ را نمایش می‌دهند. مجموعه τ، مجموعه مربع‌های عناصر $GR(4, m)$ است.

برای یافتن نمایش یک عنصر داده‌شده، از لم زیر استفاده می‌کنیم.

لم ۴.۸.۳. داریم:

$$(x + y)^{2^k} \equiv x^{2^k} + 2x^{2^{k-1}} y^{2^{k-1}} + y^{2^k} \bmod 4.$$

اثبات. برای $k = 1$ اثبات بدیهی است. با مربع کردن هر دو طرف، نتیجه با استقرا اثبات می‌شود. □

بنابراین، اگر $b \in \tau$، $a \in \tau$ و $c = a + 2b$، آن‌گاه:

$$c^{2^m} = a^{2^m} = a.$$

از این‌رو، نگاشت $\tau : c \longmapsto a$ با ضابطه:

$$\tau(c) = c^{2^m}, \quad (c \in GR(4, m), n = 2^m - 1), \tag{۴}$$

داده شده است. همین که a معرفی شد، b از $c = a + ۲b$ نتیجه می‌شود.

به‌وضوح $\tau(cd) = \tau(c)\tau(d)$ و با استفاده از لم ۴.۸.۳ داریم:

$$\tau(c+d) = \tau(c) + \tau(d) + ۲(cd)^{۲^{m-۱}}.$$

اکنون می‌توانیم ساختار حلقه $R := GR(۴, m)$ را تشریح کنیم. ایده‌آل ماکسیمال منحصربه‌فرد در R، مجموعه ۲τ است. حاصل‌ضرب هر دو عنصر در این مجموعه برابر با صفر است (بنابراین، در R مقسوم علیه‌های صفر وجود دارد). مجموعه باقی‌مانده، $R^* := \frac{R}{(۲\tau)}$، از عناصر معکوس پذیر تشکیل شده است. آنها تشکیل یک گروه ضربی از مرتبه $۲^m(۲^m - ۱)$ می‌دهند. این گروه، یک حاصل‌ضرب مستقیم از گروه دوری H از مرتبه n است که توسط ξ تولید شده و گروه ε که شامل عناصری به‌شکل $۱ + ۲t, t \in \tau$ است، می‌باشد؛ (اینها یکه‌های اصلی R هستند).

برای دانستن ساختار ε، توجه کنید که اگر t_i و t_j در τ باشند، آن‌گاه $t_i + t_j = a_{ij} + ۲b_{ij}$ که در آن $a_{ij}, b_{ij} \in \tau$؛ بنابراین، $(۱ + ۲t_i)(۱ + ۲t_j) = ۱ + ۲a_{ij}$. علاوه‌براین، نمایش جمعی a_{ij} (مانند جدول مثال ۳.۸.۳)، در پیمانه ۲ با مجموع نمایش‌هایی از t_j و t_i برابر است. در پیمانه ۲، عناصر موجود در این جدول، گروه جمعی $F_{۲^m}$ هستند؛ بنابراین، ε با این گروه یک‌ریخت است. هر عضو R^* دارای یک نمایش منحصربه‌فرد به‌شکل $\xi^r(۱ + ۲t)$ که $۰ \le r < n, t \in \tau$، است. عناصر با r ثابت، یک کلاس باقی‌مانده از حلقه $\frac{R}{(۲R)} = \frac{R}{(۲\tau)}$ را تشکیل می‌دهند و ۲τ کلاس متناظر با صفر است. فرض کنید θ یک ریشه از $h_۲(x)$ باشد؛ یعنی یک عنصر اولیه از $F_{۲^m}$. قبلاً دیده‌ایم که این جدول برای مقادیر ξ^r؛ به پیمانه ۲، یک جدول جمعی برای $F_{۲^m}$ با مولد θ است. درنتیجه، نگاشت μ که τ^r را به θ^r و صفر را به صفر تصویر می‌کند، یک یک‌ریختی از حلقه کلاسی باقی‌مانده $\frac{R}{(۲\tau)}$ روی میدان $F_{۲^m}$ است.

در زیر، به این یک‌ریختی و به این مطلب که $۲\xi^r = ۲\xi^s$ نتیجه می‌دهد $r = s$ را، نیاز خواهیم داشت. همچنین، به تعدادی از نتایج وابستگی میان توان‌های ξ^r نیاز پیدا می‌کنیم. این مطالب را در قالب یک لم بیان می‌کنیم.

لم ۵.۸.۳ فرض کنید $m \ge ۲$. در نظر بگیرید $GR(۴, m) = \mathbb{Z}_۴[\xi]$ با $\xi^n = ۱$ (برای $n = ۲^m - ۱$)؛ داریم:

۱) $\pm\xi^j \pm \xi^k$ برای $۰ \le j < k < n$، معکوس پذیر است.

۲) برای i, j, k متمایز در بازه $[۰, n-۱]$ داریم $\xi^j - \xi^j \ne \pm\xi^l$.

۳) اگر $m \geq 3$ و $i \neq j, k \neq l$ در بازه $[0, n-1]$، آن‌گاه:

$$\xi^i - \xi^j = \xi^k - \xi^l \Rightarrow i = k, j = l.$$

۴) اگر $m \geq 3$ و m فرد باشد، آن‌گاه:

$$\xi^i + \xi^j + \xi^k + \xi^l = 0 \Rightarrow i = j = k = l.$$

اثبات.

۱) اگر $\pm\xi^j \pm \xi^k = 2\lambda$ برای یک $\lambda \in R$، آن‌گاه با مربع نمودن دو طرف معادله $\pm\xi^j = \pm\xi^k + 2\lambda$ داریم $j = k$.

۲) یک معادله از این نوع می‌تواند به $\xi^a = \xi^b + 1$ تقلیل یابد. دو طرف را به توان 2^m رسانده و لم ۴.۸.۳ را به‌کار می‌بریم. داریم $2\xi^{a.2^{m-1}} = 0$ که یک تناقض است.

۳) یک معادله از این نوع می‌تواند به $\xi^a = \xi^b + \xi^c + 1$ تقلیل یابد. با به‌کار بردن لم ۴.۸.۳، داریم $2(\xi^a)^{2^{m-1}} = 2(\xi^{b+c})^{2^{m-1}}$؛ بنابراین، $\xi^a = \xi^{b+c}$. این معادله به‌صورت $2(\xi^b - 1)(\xi^c - 1) = 0$ در می‌آید و ما این حالت را در مرحله (۱) انجام داده‌ایم.

۴) در اینجا، لازم است که با F_{2^m} کار کنیم. ما یک‌ریختی μ را به‌کار می‌بریم. اگر چهار توان ξ جمع شود و صفر گردند، رابطه مشابهی وجود دارد که یکی از توان‌ها برابر با ۱ است. علاوه‌براین، چون $\xi^n = 1$ ممکن است فرض کنیم که بقیه توان‌ها زوج هستند. پس داریم:

$$\xi^{2a} + \xi^{2b} = -\xi^{2c} - 1.$$

با رساندن دو طرف به توان 2^m وبه‌کار بردن لم ۴.۸.۳، داریم:

$$2(\xi^{2a} + \xi^{a+b} + \xi^{2b}) = 2\xi^c.$$

از این معادله نمی‌توانیم نتیجه‌ای را در R به‌دست آوریم، اما این مطلب مفهومی در F_{2^m} دارد. نگاشت μ را به‌کار برده و می‌نویسیم $x := \theta^a$، $y := \theta^b$ و $z := \theta^c$. از معادله آخر نتیجه می‌گیریم که $x^2 + xy + y^2 = z$. معادله اصلی ایجاب می‌کند که $x^2 + y^2 + z^2 + 1 = 0$؛ بنابراین،

$x+y=z+1$. از این دو، داریم $x^2+y^2=(x+1)(y+1)$. باید نشان دهیم که این مطلب ایجاب می‌کند که $x=y=z$؛ زیرا که آن نشان می‌دهد $a=b=c=0$.

فرض کنید $x\neq 1$. می‌نویسیم $x=u+1$، $y=ut+1$. معادله $u^2(t^2+t+1)=0$ را داریم. چون $u\neq 0$، باید داشته باشیم $t^2+t+1=0$، که این مطلب با این‌که m فرد است در تناقض است.

□

۸.۴ کدهای دوری روی $\mathbb{Z}_4$

در روشی مشابه با آنچه که در حالت $\mathbb{F}_q$ انجام دادیم، اینک کدهای دوری روی $\mathbb{Z}_4$ را بررسی می‌کنیم. مجدداً، کلمه $c=(c_0,c_1,\cdots,c_{n-1})$ را با چندجمله‌ای $c(x):=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ از حلقه $\mathcal{R}=\mathbb{Z}_4[x]/(x^n-1)$ همسان درنظر می‌گیریم. هر چیزی تعمیم نمی‌یابد! $\mathcal{R}$ دامنه تجزیه یکتا نمی‌باشد؛ یعنی برخی از چندجمله‌ای‌ها در $\mathcal{R}$ را می‌توان به‌صورت حاصل‌ضرب عوامل تحویل‌ناپذیر به بیشتر از یک صورت نوشت. این مطلب روی بحث ما تاثیری نخواهد داشت.

به‌طور معمول، کدها را با معرفی ماتریس مولد یا ماتریس بررسی‌توازن تعریف می‌کنیم. این مطالب دارای شکلی فشرده‌تر از مطالبی است که در بخش ۸.۱ بیان کردیم (مانند همیشه در مورد کدهای دوری؛ در اینجا عناصر R با بردارهای ستونی، متناظر با نمایش آنها با گونه مثال ۳.۸.۳، جای‌گزین می‌شوند). اگر ما به توسیع یک کد علاقه‌مند باشیم، آن‌گاه در ابتدا یک ستون تماماً صفر و سپس یک سطر تماماً یک به ماتریس بررسی‌توازن آن اضافه می‌کنیم. این کار، به طول $\mathbb{Z}_4$–کد یک عدد اضافه می‌کند، اما تصویر دودویی آن به اندازه دو سمبل طولانی‌تر می‌شود.

مثال ۱.۸.۴. کد دوری چهارتایی C به‌طول $n=2^m-1$ با مولد $(2\ \ 2\xi\ \ \cdots\ \ 2\xi^{n-1})$ را درنظر بگیرید. این کد یک کد بدیهی است، یک کد دودویی درون آن پنهان است. تمامی کدکلمات تصویر دودویی آن به‌شکل (c,c) می‌باشند که در آن c در دوگان کد همینگ $[2^m-1,2^m-m-1,3]$ قرار دارد.

مرحله بعد، $\mathbb{Z}_4$–کد با ماتریس مولد به‌صورت زیر را درنظر بگیرید:

$$G:=\begin{pmatrix}1 & 1 & 1 & \cdots & 1\\ 0 & 2 & 2\xi & \cdots & 2\xi^{n-1}\end{pmatrix}.$$

هر دوی C و C' دارای 2^{m+2} کدکلمه هستند. تصاویر دودویی آنها دارای طول 2^{m+1} بوده و به‌وضوح کد رید–مولر مرتبه اول $\mathcal{R}(1, m+1)$ است. قبلاً در مثال ۷.۸.۲ دیدیم که این کد $\mathbb{Z}_4$–خطی است.

حال به سراغ کدهایی می‌آییم که باعث ایجاد یک جرقه ناگهانی در علاقه به کدهای روی $\mathbb{Z}_4$ گردید. $\mathbb{Z}_4$–کد C_m با طول $n+1 = 2^m$ (m فرد) با ماتریس بررسی‌توازن زیر را درنظر بگیرید:

$$H := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \cdots & \xi^{n-1} \end{pmatrix},$$

که درآن ξ یک nامین ریشه اولیه واحد در $GR(4, m)$ است.

لم ۲.۸.۴. C_m دارای فاصله لی $d \leq 6$ است.

اثبات. اولین سطر H ایجاب می‌کند که هر کدکلمه در C_m دارای تعدادی زوج از درایه‌های با مقدار فرد است؛ بنابراین، دارای وزن لی زوج می‌باشد؛ پس d زوج است. در چهار حالت زیر، ما کدکلمات احتمالی با مختصات ناصفر، نه در مکان‌های اولیه، را درنظر می‌گیریم. برای موقعیت‌های متناظر که در آن یک مختصات ناصفر در خط اول وجود دارد، معادلات مشابه با یک جمله کم‌تر باید درنظر گرفته شوند و آن را به خواننده واگذار می‌کنیم.

۱) اگر کدکلمه‌ای در C_m دارای وزن لی ۲ باشد، آن‌گاه دو مولفه ناصفر برابر با ۱ و ۱− می‌باشند؛ در این‌صورت سطر دوم از H، وجود i و j را که $\xi^i = \xi^j$، نتیجه می‌دهد و این نادرست است.

۲) اگر کدکلمه‌ای در C_m دارای وزن لی ۴ باشد و مولفه‌های ناصفر برابر با ۱، ۱ و ۲ (یا ۳، ۳ و ۲) باشند، آن‌گاه داریم $\xi^i + \xi^j = \pm 2\xi^k$ برای برخی i, j, k. بااستفاده از لم ۵.۸.۳ قسمت (۱)، این امر غیرممکن می‌باشد.

۳) اگر کدکلمه‌ای در C_m دارای وزن لی ۴ با دو مولفه ۱ و دو مولفه ۳ باشد، آن‌گاه اندیس‌های i, j, k, l وجود خواهند داشت به‌طوری که $\xi^i - \xi^j = \xi^k - \xi^l$. با استفاده از لم ۵.۸.۳ قسمت (۳)، این امر غیرممکن می‌باشد.

۴) اگر کدکلمه‌ای با وزن ۴ با چهار مولفه ناصفر و برابر موجود باشد، آن‌گاه با لم ۵.۸.۳ قسمت (۴) به تناقض بر می‌خوریم.

حال خواننده می‌تواند به آسانی چهار حالت دیگر را بررسی کند. این مطلب اثبات را کامل می‌کند. □

از ماتریس H و رابطه ۲، می‌بینیم که C_m دارای $۴^{n-m-۱}$ کدکلمه است. حال نگاهی به تصویر دودویی C_m می‌اندازیم. آن یک کد دودویی باطول $۲^{m+۱}$ است، با تعداد ۲^k عضو که در آن $k = ۲^{m+۱} - ۲m - ۲$ و کمترین—فاصله آن حداقل ٦ است. از بخش ۷.۴ می‌بینیم که اگر ما این کد دودویی را کوتاه کنیم، آن‌گاه یک کد با طول $۲^{m+۱} - ۱$ با پارامترهای یکسان با یک کد پرپاراتا به‌دست می‌آوریم! بنابراین، یک کد تقریبا کامل است و از این‌رو دارای شمارنده وزنی مشابه با کد پرپاراتا با طول یکسان است. مولفین در مرجع [۸۸]، C'_m را یک کد "پرپاراتا" نامیده‌اند، چرا که آن با کد موجود در بخش ۷.۴ هم‌ارز نمی‌باشد.

حال بیایید دوگان کد $C_m^{\perp}$ را درنظر بگیریم. این کد، ماتریس H را به‌عنوان ماتریس مولد خود داراست. با استفاده از قضیه ۴.۸.۲، شمارنده وزنی دو تصویر دودویی در روابط مک‌ویلیامز صدق می‌کنند. می‌دانستیم که شمارنده‌های وزنی کد کرداک و کد پرپاراتای گسترش‌یافته با طول مشابه، در روابط مک‌ویلیامز صدق می‌کنند؛ (این یک "انطباق" بود که نظریه‌پردازان کدگذاری را سال‌ها سردرگم کرده بود). برای مشاهده اثبات آن می‌توانید مرجع [۴٦] را ببینید. حال می‌دانیم که کد دودویی که تصویر کد روی $\mathbb{Z}_۴$ با ماتریس مولد H است، باید دارای شمارنده وزنی همانند کد کرداک با همان طول باشد. در مرجع [۸۸] نشان داده شده است که کدهای تعریف شده توسط کرداک در [۷۵] در واقع تصویر دودویی $\mathbb{Z}_۴$–کدها هستند که ما آن‌را در اینجا مورد بحث قرار دادیم.

مثالی از یک کد دودویی خوب می‌آوریم که تصویر دودویی $\mathbb{Z}_۴$–کدی است که دوری بوده، اما خطی نیست.

مثال ۳.۸.۴. به بردار (۱۱۱۰۰) و شیفت‌های دوری آن نگاهی بیندازید. هنگامی که ما دوتا از اینها را با هم مقایسه می‌کنیم، سه احتمال را متوجه می‌شویم: (۱) سه جفت فرد—فرد یا دو جفت زوج—زوج، (۲) چهارجفت زوج—فرد و یک جفت فرد—فرد، (۳) دو جفت زوج—فرد، دو جفت فرد—فرد و یک جفت زوج—زوج. حال این بردار و سه‌تای دیگر را به‌همراه سه‌تای دیگر که توسط جای‌گذاری ۱۱۱ با ۱۱۳ یا برخی جای‌گشت‌ها و ۰۰ با ۰۲، ۲۰ یا ۲۲ به‌دست آمده‌اند، می‌گیریم. ادعا می‌کنیم که انتخاب ۱۱۱۲۰، ۳۱۱۰۰، ۱۳۱۰۲، ۱۱۳۲۲ دارای این خاصیت است که این چهار بردار، منفی آنها و تمامی شیفت‌های دوری تشکیل یک $\mathbb{Z}_۴$–کد با فاصله لی ۴ را می‌دهند. هنگام محاسبه فاصله لی، یک جفت زوج—فرد، یک وزن لی را می‌شمرد، یک زوج با بررسی یکسان، ۰ یا ۲ را تشکیل می‌دهند. جای‌گذاری ما تضمین می‌کند که اگر دو ترکیب زوج—زوج وجود داشته باشد، آن‌گاه یک ۲ تادر این فاصله شمرده می‌شود یا مختصات دیگر فاصله ٦ را به‌دست می‌دهد. یک زوج ۳—۱ نیز به اندازه ۲ تا در این فاصله شرکت می‌کند. دو کدکلمه با فاصله لی کمتر از ۴ چگونه وجود خواهد داشت؟ این تنها زمانی رخ

خواهد داد که ما دو کلمه $(o_1, o_2, o_3, e_1, e_2)$ و $(e'_1, o'_2, o'_3, o'_1, e'_2)$ (o فرد، e زوج) که در آن $o_2 = o'_2$، $o_3 = o'_3$ و $e_2 = e'_2$، داشته باشیم. در انتخاب خود، دیدن این امر آسان است که تنها شش زوج از کلمات باید چک شوند تا نشان دهیم که این حالت رخ نمی‌دهد.

حال تصویر دودویی این کد را درنظر بگیرید. این تصویر شامل ۴۰ کلمه به طول ۱۰ و کمترین–فاصله ۴ است. چون این مطلب معلوم شده که بهترین کد از بخش ۴.۴ یکتاست، این کد باید با بهترین کد معادل باشد. این ساختار (ر.ک. مرجع [۸۳]) دارای این مزیت است که فاصله تعداد خیلی کمی از کلمات باید دستی چک شوند.

۸.۵ مسائل

۱.۸.۵. یک کد چهارتایی خوددوگان به طول ٦ بسازید. نشان دهید چنین کدی باید شامل کلمه (۲۲۲۲۲۲) باشد. آیا تصویر دودویی این کد، خطی است؟ آیا آن نیز خوددوگان است؟

۲.۸.۵. ثابت کنید کد رید–مولر $\mathcal{R}(۲, m)$ یک کد $\mathbb{Z}_4$–خطی است.

۳.۸.۵. فرض کنید $c = \xi^i + ۲\xi^j$ عنصری از $GR(۴, m)$ باشد. معکوس آن را بیابید.

۴.۸.۵. شمارنده وزنی کد نرداستروم–رابینسن را درنظر بگیرید. نشان دهید که آن با تبدیل مک‌ویلیامز خود برابر است.

۵.۸.۵. کد پرپاراتا $\mathcal{P}$ از قضیه ۵.۷.۴ را درنظر بگیرید. تعداد کلمات با وزن ۵ و ٦ را تعیین کنید. از این استفاده نموده، شمارنده وزنی کد پرپاراتای گسترش‌یافته به طول ١٦ را بیابید.

٦.۸.۵. نشان دهید کد رید–مولر مرتبه اول، زیرکدی از تصویر دودویی کد دوگان C_m در بخش ۸.۴ است.

۷.۸.۵. نشان دهید کد C'_m و کد ۵.۷.۴ برای $m \geq ۵$ معادل نمی‌باشند (راهنمایی: نشان دهید که ترکیبات خطی C'_m شامل کلمات به وزن ۲ است).

فصل ۹

کدهای گاپا

۹.۱ انگیزه

یک بار دیگر ماتریس بررسی‌توازن یک کد BCH (کم عرض) را آن‌چنان که در اثبات قضیه ۲.۶.۶ آمده است، درنظر بگیرید؛ یعنی:

$$H = \begin{pmatrix} ۱ & \beta & \beta^۲ & \dots & \beta^{n-۱} \\ ۱ & \beta^۲ & \beta^۴ & \dots & \beta^{۲(n-۱)} \\ \dots & \dots & \dots & \dots & \dots \\ ۱ & \beta^{d-۱} & \beta^{۲(d-۱)} & \dots & \beta^{(d-۱)(n-۱)} \end{pmatrix},$$

که در آن β یک nامین ریشه اولیه واحد در $\mathbb{F}_{q^m}$ است و هر درایه به‌صورت برداری ستونی با طول n روی $\mathbb{F}_q$ تفسیر می‌شود؛ وجود β نتیجه می‌دهد $n \mid (q^m - ۱)$.

با به‌کارگیری این واقعیت که هر زیرماتریس H تشکیل‌شده با درنظر گرفتن $d-۱$ ستون، یک ماتریس واندرموند است؛ بنابراین، دارای دترمینان مخالف صفر است، در قضیه ۲.۶.۶ ثابت کردیم که کمترین—فاصله، حداقل برابر d است. بسیاری از مولفین توجه داشته‌اند که اگر ما H را با ماتریس زیر جای‌گزین کنیم، هنوز هم دلیل مشابهی می‌تواند کارساز باشد:

$$\hat{H} = \begin{pmatrix} h_۰\beta_۰ & h_۱\beta_۱ & \dots & h_{n-۱}\beta_{n-۱} \\ \vdots & \vdots & & \vdots \\ h_۰\beta_۰^{d-۱} & h_۱\beta_۱^{d-۱} & \dots & h_{n-۱}\beta_{n-۱}^{d-۱} \end{pmatrix},$$

که در آن $h_j \in \mathbb{F}_{q^m}^*$ و β_iها عناصر متفاوتی از $\mathbb{F}_{q^m}^*$ باشند. اگر $h_j \in \mathbb{F}_q$ $(0 \leq j \leq n-1)$، آن‌گاه عوامل h_j هیچ تاثیر مهمی ندارند؛ این کد با یک کد هم‌ارز جای‌گزین می‌شود. اما اگر h_j عناصری از $\mathbb{F}_{q^m}$ باشند، آن‌گاه جملات $h_j\beta_j^i$ به‌عنوان بردارهای ستونی روی $\mathbb{F}_q$ می‌توانند با درایه‌های اولیه تفاوت بسیار داشته باشند.

دو روش در تعمیم کدهای BCH به این طریق را درنظر خواهیم گرفت. آنچه که ما را درواقع بیشتر علاقه‌مند می‌کند از این واقعیت ناشی می‌شود که این کلاس‌های جدید از کدها شامل دنباله‌هایی از کدها است که به کران گیلبرت دست می‌یابند؛ در حالی‌که ثابت شده است کدهای BCH با طول بزرگ، بد هستند.

۹.۲ کدهای گاپا

فرض کنید $(c_0, c_1, \ldots, c_{n-1})$ کدکلمه‌ای در یک کد BCH با فاصله طراحی‌شده d (طول کلمه n، β یک ریشه اولیه nام واحد) باشد؛ در این‌صورت با استفاده از تعریف داریم $\sum_{i=0}^{n-1} c_i(\beta^j)^i = 0$ برای $1 \leq j \leq d$. می‌خواهیم تا این شرط را به‌روش دیگری بنویسیم. مشاهده می‌کنید که:

$$\frac{z^n - 1}{z - \beta^{-i}} = \sum_{k=0}^{n-1} z^k(\beta^{-i})^{n-1-k} = \sum_{k=0}^{n-1} \beta^{i(k+1)}z^k. \qquad (1)$$

این نتیجه می‌دهد که برای یک چندجمله‌ای $p(z)$ داریم:

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \beta^{-i}} = \frac{z^{d-1}p(z)}{z^n - 1}. \qquad (2)$$

اگر $g(z)$ چندجمله‌ای دلخواه باشد و $g(\gamma) \neq 0$، آن‌گاه $1/(z-\gamma)$ را چندجمله‌ای یکتایی در پیمانه $g(z)$ تعریف می‌کنیم، به‌طوری که $(z-\gamma).1/(z-\gamma) \equiv 1 \bmod g(z)$؛ یعنی:

$$\frac{1}{z-\gamma} = \frac{-1}{g(\gamma)}.(\frac{g(z)-g(\gamma)}{z-\gamma}). \qquad (3)$$

این مشاهدات به‌عنوان یک آمادگی برای تعریف زیر به‌کار می‌روند.

تعریف ۱.۹.۲. فرض کنید $g(z)$ چندجمله‌ای (تکین) با درجه t روی $\mathbb{F}_{q^m}$ باشد. فرض کنید $L = \{\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\}$ به‌طوری که $|L| = n$ و $g(\gamma_i) \neq 0$ برای $0 \leq i \leq n-1$. کد گاپای[1]

[1] Goppa code

$\Gamma(L,g)$ را با چندجمله‌ای گاپای[۲] $g(z)$ به‌صورت مجموعه کدکلمات $c=(c_0,c_1,\cdots,c_{n-1})$ روی $\mathbb{F}_q$ تعریف می‌کنیم، به‌طوری که:

$$\sum_{i=0}^{n-1}\frac{c_i}{z-\gamma_i}\equiv 0 \bmod g(z). \qquad (۴)$$

مشاهده می‌کنید که کدهای گاپا، خطی هستند.

مثال ۲.۹.۲. با توجه به ملاحظات مقدماتی، می‌بینیم که اگر ما چندجمله‌ای گاپای $g(z)=z^{d-1}$ و $L:=\{\beta^{-i}\mid 0\le i\le n-1\}$ را درنظر بگیریم که در آن β یک ریشه nام اولیه واحد در $\mathbb{F}_{q^m}$ است، کد گاپای $\Gamma(L,g)$ حاصل شده، یک کد BCH کم‌عرض با فاصله طراحی‌شده d است (ارجاع به مسأله ۲.۹.۸).

به منظور برقراری رابطه با بخش ۹.۱، سعی می‌کنیم تا یک ماتریس بررسی‌توازن مناسب برای $\Gamma(L,g)$ بیابیم. از روابط ۴ و ۳ می‌بینیم که:

$$\left(\ \frac{1}{g(\gamma_0)}\cdot\frac{g(z)-g(\gamma_0)}{(z-\gamma_0)},\ldots,\frac{1}{g(\gamma_{n-1})}\frac{g(z)-g(\gamma_{n-1})}{(z-\gamma_{n-1})}\ \right),$$

که در آن هر درایه به‌صورت یک بردار ستونی تعبیر می‌شود، به یک معنا، یک ماتریس بررسی‌توازن است. فرض کنید $h_j:=g(\gamma_j)^{-1}$ و بنابراین، $h_j\neq 0$. اگر $g(z)=\sum_{i=0}^{t}g_iz^i$، آن‌گاه در روشی مشابه با رابطه ۱ داریم:

$$\frac{g(z)-g(x)}{z-x}=\sum_{i+j\le t-1}g_{i+j+1}x^jz^i.$$

با صرف‌نظر کردن از عوامل z^i، به‌عنوان ماتریس بررسی‌توازن برای $\Gamma(L,g)$ داریم:

$$\begin{pmatrix} h_0g_t & \cdots & h_{n-1}g_t\\ h_0(g_{t-1}+g_t\gamma_0) & \cdots & h_{n-1}(g_{t-1}+g_t\gamma_{n-1})\\ \vdots & \cdots & \vdots\\ h_0(g_1+g_2\gamma_0+\cdots+g_t\gamma_0^{t-1}) & \cdots & h_{n-1}(g_1+g_2\gamma_{n-1}+\cdots+g_t\gamma_{n-1}^{t-1}) \end{pmatrix}.$$

با استفاده از یک تبدیل خطی، ماتریسی را که می‌خواستیم، می‌یابیم؛ یعنی:

$$H=\begin{pmatrix} h_0 & \cdots & h_{n-1}\\ h_0\gamma_0 & \cdots & h_{n-1}\gamma_{n-1}\\ \vdots & & \vdots\\ h_0\gamma_0^{t-1} & \cdots & h_{n-1}\gamma_{n-1}^{t-1} \end{pmatrix}.$$

[۲] Goppa polynomial

(در اینجا این واقعیت را به‌کار برده‌ایم که $g_t \neq 0$).

این ماتریس، عمومیت کامل ماتریس $\hat{H}$ از بخش ۹.۱ را ندارد؛ زیرا آنجا h_j دلخواه بود، اما در اینجا داریم $h_j = g(\gamma_j)^{-1}$.

قضیه ۳.۹.۲. کد گاپای $\Gamma(L,g)$ تعریف شده در ۱.۹.۲ دارای بعدی بزرگ‌تر یا مساوی $n - mt$ و کمترین—فاصله بزرگ‌تر یا مساوی $t + 1.5$ است.

اثبات. این مطلب با توجه به ماتریس بررسی‌توازن H با روشی دقیقاً مشابه با کدهای BCH، نتیجه می‌شود. □

مثال داده‌شده ۲.۹.۲ نشان می‌دهد که کران BCH (برای کدهای BCH کم‌عرض) حالت خاصی از قضیه ۳.۹.۲ است.

به‌منظور داشتن آمادگی برای تعمیم این کدها به کدهای روی منحنی‌های جبری (فصل ۱۰ را ببینید)، ما تعریف کدهای گاپا را مجدداً فرمول‌بندی می‌کنیم. با میدان $\mathbb{F}_{q^m}$ شروع کنید. فضای برداری تمام توابع گویای $f(z)$ با خواص زیر را درنظر بگیرید:

۱) $f(z)$ دارای ریشه در تمامی نقاطی است که $g(z)$ ریشه داشته باشد، هر یک با حداقل تکرار یکسان با آن ریشه در $g(z)$.

۲) $f(z)$ دارای هیچ قطبی نمی‌باشد، مگر احتمالاً در برخی نقاط γ_0، γ_1، $\cdots$، γ_{n-1} و در آن حالت قطب‌ها مرتبه ۱ می‌باشند.

یک کد روی $\mathbb{F}_{q^m}$ با درنظرگرفتن کدکلمات به‌صورت n—تایی:

$$(\mathrm{Res}_{\gamma_0} f, \mathrm{Res}_{\gamma_1} f, \cdots, \mathrm{Res}_{\gamma_{n-1}} f)$$

تعریف شده است که در آن باقی‌مانده $f(z)$ در نقطه γ_i به‌صورت معمول تعریف شده است. کد گاپای $\Gamma(L,g)$ زیرمیدان زیرکد (روی $\mathbb{F}_q$) این کد است.

ماتریس بررسی‌توازن H تعریف‌شده در بالا را درنظر بگیرید. این موقعیت را با تعریف ۲.۶.۸ مقایسه کنید که در آن درنظر گرفته‌ایم $v := (h_0, h_1, \cdots, h_{n-1})$ و $a := (\gamma_0, g_1, \cdots, \gamma_{n-1})$، $k = t$. می‌بینیم که H ماتریس مولد کد $GRS_k(a,v)$ است. بنابراین، کد گاپای $\Gamma(L,g)$ زیرمیدان زیرکد دوگان یک کد رید—سولومن گسترش‌یافته است.

بنابراین، تا اینجا دیده‌ایم که کدهای تعریف شده به‌وسیله چندجمله‌ای‌ها مانند تعریف ۲.۶.۸ و کدهایی که با استفاده از باقی‌مانده ها در قطب‌های مرتبه اول در اینجا تعریف کرده‌ایم، دوگان هستند. در فصل مربوط به کدهای هندسه جبری، با پدیده مشابهی برخورد خواهیم کرد.

۹.۳ کمترین–فاصله کدهای گاپا

اگر ما دیدگاه خود را کمی تغییر دهیم، ممکن است قضیه ۳.۹.۲ و نیز برخی تعمیم‌ها را به روش دیگری به‌دست آوریم. مانند قبل، فرض کنید $\mathcal{R}$ معرف $(\mathbb{F}_q)^n$ با فاصله همینگ باشد. فرض کنید L مانند تعریف ۱.۹.۲ باشد؛ تعریف می‌کنیم:

$$\mathcal{R}^* := \{\xi(z) = \sum_{i=0}^{n-1} \frac{b_i}{z-\gamma_i} \mid (b_0, b_1, \cdots, b_{n-1}) \in \mathcal{R}\},$$

و فاصله دو تابع گویای $\xi(z)$ و $\eta(z)$ را به‌صورت زیر تعریف می‌کنیم:

$$d(\xi(z), \eta(z)) := || \xi(z) - \eta(z) ||,$$

که در آن $|| \xi(z) ||$ معرف درجه مخرج است و $\xi(z)$ به‌صورت $n(z)/d(z)$ با $(n(z), d(z)) = 1$ است. به‌آسانی دیده می‌شود که این تابع فاصله است و درواقع نگاشت $(b_0, \cdots, b_{n-1}) \to \sum_{i=0}^{n-1} b_i/(z-\gamma_i)$ یک یک‌ریختی از $\mathcal{R}$ به $\mathcal{R}^*$ است. ما این اصطلاح را برای مطالعه کدهای گاپا با درنظر گرفتن سمت چپ رابطه ۴ به‌عنوان عضوی از $\mathcal{R}^*$ به‌کار خواهیم برد؛ یعنی رابطه ۳ را به‌کار نخواهیم برد. اگر $\xi(z) = n(z)/d(z)$ متناظر با یک کدکلمه ناصفر باشد، آن‌گاه $\deg d(z) \geq \deg n(z) + 1$. شرط $\xi(z) \equiv 0 \bmod g(z)$ ایجاب می‌کند که $g(z)$ عاد کند $n(z)$ را؛ یعنی $\deg d(z) \geq t+1$. بنابراین، داریم $|| \xi(z) || \geq t+1$ که نتیجه‌ای از قضیه ۳.۹.۲ است.

اگر ما $\xi(z)$ را به‌صورت $n(z)/d(z)$ بنویسیم که در آن $d(z)$ برابر با حاصل‌ضرب تمام n عامل‌های $(z-\gamma_i)$ است، آن‌گاه می‌توانیم تخمین خود درمورد کمترین–فاصله را بهبود بخشیم، اگر درجه $n(z)$ و $d(z)$ در بیشتر از یک عدد اختلاف داشته باشند. ضریب z^{n-1} در $n(z)$ برابر با $\sum_{i=0}^{n-1} b_i$ است. نتیجه می‌شود که اگر ما یک معادله بررسی‌توازن اضافی $\sum_{i=0}^{n-1} b_i = 0$ را اضافه کنیم، آن‌گاه تخمین درباره کمترین–فاصله، یکی اضافه خواهد شد و در مورد بعد کد، حداکثر یکی کم خواهد شد. می‌توانیم ایده مشابهی را در مورد سایر ضرایب به‌کار بریم. ضریب z^{n-s-1} در مخرج $n(z)$ برابر با $(-1)^s \sum_{i=0}^{n-1} b_i \sum'_{j_1, j_2, \cdots, j_s} \gamma_{j_1}\gamma_{j_2}\cdots\gamma_{j_s}$ است (که در آن $\sum'$ نشان می‌دهد که $j_v \neq i$ برای $v = 1, 2, \cdots, s$). این ضریب یک ترکیب خطی از مجموع‌های $\sum_{i=0}^{n-1} b_i\gamma_i^r$ $(0 \leq r \leq s)$ است. نتیجه می‌شود که اگر ما $s+1$ معادله بررسی‌توازن، یعنی $\sum_{i=0}^{n-1} b_i\gamma_i^r = 0$ $(0 \leq r \leq s)$ را اضافه نماییم، آن‌گاه کدی با بعد حداقل $n - tm - (1+sm)$ و کمترین–فاصله حداقل $t+s+2$ را داریم. چگونه این حالت با زمانی‌که $g(z)$ را با چندجمله‌ای گاپای دیگری با درجه $t+s$ جای‌گزین می‌کنیم، مقایسه می‌گردد؟ اولین روش، دارای این مزیت است که $\sum_{i=0}^{n-1} = 0$ ایجاب می‌کند $\sum_{i=0}^{n-1} b_i\gamma_i^q = 0$؛ بنابراین، در q مرحله ما مطمئن هستیم که بعد کاهش نمی‌یابد.

قضیه ۱.۹.۳. فرض کنید $q = ۲$ و فرض کنید $g(z)$ دارای هیچ ریشه تکراری نباشد؛ در این‌صورت $\Gamma(L, g)$ دارای کمترین —فاصله حداقل $۲t + ۱$ است (که در آن $t = \deg g(z)$).

اثبات. فرض کنید $(c_۰, c_۱, \cdots, c_{n-۱})$ یک کدکلمه باشد؛ تعریف کنید $f(z) = \prod_{i=۰}^{n-۱}(z - \gamma_i)^{c_i}$؛ در این‌صورت $\xi(z) = \sum_{i=۰}^{n-۱} c_i/(z - \gamma_i) = f'(z)/f(z)$ که در آن $f'(z)$ مشتق صوری است. در $f'(z)$ تنها توان‌های زوج z رخ می‌دهند؛ یعنی $f'(z)$ یک مربع کامل است. چون نیاز داریم که $g(z)$ عاد کند $f'(z)$ را، باید درواقع داشته باشیم $g^۲(z)$ عاد کند $f'(z)$ را؛ بنابراین، استدلال قبلی ایجاب می‌کند که $d \geq ۲t + ۱$. □

البته می‌توان قضیه ۱.۹.۳ را با موضوع مشترک با یک کد BCH ترکیب نمود.

۹.۴ رفتار مجانبی کدهای گاپا

در بخش ٦.٦ اشاره کردیم که کدهای BCH اولیه با طول بزرگ، بد هستند. این واقعیت با قضیه ۹.٦.٦ در ارتباط است. کازامی[۳] (۱۹٦۹؛ مرجع [۳۹]) نشان داد که خانواده‌ای از کدهای دوری که در مورد آنها کدهای توسیع‌یافته تحت گروه آفین پایا هستند در مفهوم مشابه، بد می‌باشند. در زیردنباله‌ای از کدهای C_i با طول n_i، بعد k_i و فاصله d_i باید $\liminf(k_i/n_i) = ۰$ یا $\liminf(d_i/n_i) = ۰$. اینک نشان خواهیم داد که کلاس گاپا به‌طور قابل توجهی بزرگ‌تر است.

قضیه ۱.۹.۴. دنباله‌ای از کدهای گاپا روی $\mathbb{F}_q$ وجود دارد که به کران گیلبرت دست می‌یابد.

اثبات. درابتدا پارامترهای $n = q^m$، t و d را برمی‌داریم، $L = \mathbb{F}_{q^m}$ را انتخاب می‌کنیم و سعی می‌کنیم تا چندجمله‌ای تحویل‌ناپذیر $g(z)$ از درجه d روی $\mathbb{F}_{q^m}$ را به‌گونه‌ای بیابیم که $\Gamma(L, g)$ دارای کمترین —فاصله حداقل d باشد. فرض کنید $c = (c_۰, c_۱, \cdots, c_{n-۱})$ کلمه دلخواهی با وزن $d > j$ باشد؛ یعنی کلمه‌ای که نمی‌خواهیم در $\Gamma(L, g)$ باشد. چون $\sum_{i=۰}^{n-۱} c_i/(z - \gamma_i)$ دارای شمارنده با درجه حداکثر $j - ۱$ است، حداکثر $\lfloor (j-۱)/t \rfloor$ چندجمله‌ای $g(z)$ وجود دارند که در آن $\Gamma(L, g)$ شامل c نیست. این بدان معناست که به منظور اطمینان از فاصله d، باید حداکثر $\sum_{j=۱}^{d-۱} \lfloor (j-۱)/t \rfloor (q-۱)^j \binom{n}{j}$ چندجمله‌ای تحویل‌ناپذیر با درجه t را خارج کنیم. این تعداد کمتر از $(d/t)V_q(n, d-۱)$ است (ارجاع به رابطه ۱). با استفاده از رابطه ۴، تعداد چندجمله‌ای‌های تحویل‌ناپذیر با درجه t روی $\mathbb{F}_{q^m}$ از $(۱/t)q^{mt}(۱ - q^{-(۱/۲)mt+m})$

[۳] T. Kasami

تجاوز می‌کند؛ بنابراین، یک شرط کافی برای وجود کد $\Gamma(L,g)$ که ما به دنبال آن هستیم این است که:

$$\frac{d}{t}V_q(n,d-1) < \frac{1}{t}q^{mt}(1-q^{-(1/2)mt+m}). \tag{۵}$$

با استفاده از قضیه ۳.۹.۲، این کد شامل حداقل q^{n-mt} کلمه است. از دو طرف رابطه ۵ لگاریتم در پایه q می‌گیریم و بر n تقسیم می‌کنیم. فرض کنید n متغیر باشد، $n \to \infty$، و $d/n \to \infty$. با به‌کارگیری لم ۴.۵.۱ داریم:

$$H_q(\delta) + o(1) < \frac{mt}{n} + o(1).$$

نرخ اطلاعات کد $\Gamma(L,g)$ بزرگ‌تر یا مساوی $1 - mt/n$ است. در نتیجه می‌توانیم دنباله‌ای از چندجمله‌ای‌های $g(z)$ را بیابیم که کدهای گاپای متناظر، دارای نرخ اطلاعات مایل به $1 - H_q(\delta)$ باشند. این همان کران گیلبرت (قضیه ۸.۵.۱) است. □

۹.۵ کدگشایی کدهای گاپا

کدگشای برلیکمپ برای کدهای BCH که آن‌را در انتهای بخش ٦.٧ بیان کردیم، نیز می‌تواند کدهای گاپا را کدگشایی نماید. برای نشان دادن این مطلب، در روشی مشابه با بخش ٦.٧ پیش خواهیم رفت.

فرض کنید $(C_0, C_1, \cdots, C_{n-1})$ کدکلمه‌ای در $\Gamma(L,g)$، آن‌چنان که در تعریف ۱.۹.۲ آمد، باشد و فرض کنید بردار $(R_0, R_1, \cdots, R_{n-1})$ را دریافت کنیم. ما بردار خطا را با $(E_0, E_1, \cdots, E_{n-1}) = R - C$ نشان می‌دهیم. فرض کنید $M := \{i \mid E_i \neq 0\}$. درجه $g(x)$ را با t نشان می‌دهیم و فرض کنیم که $|M| = e < \frac{1}{2}t$. مجدداً با به‌کارگیری قرارداد ۳، چندجمله‌ای $S(x)$ که هم‌رفت نامیده می‌شود، به‌صورت زیر تعریف می‌گردد:

$$S(x) \equiv \sum_{i=0}^{n-1} \frac{E_i}{x-\gamma_i} \bmod g(x). \tag{٦}$$

مشاهده می‌کنید که $S(x)$ می‌تواند توسط گیرنده با به‌کارگیری R و رابطه ۴ محاسبه شود. حال ما چندجمله‌ای تشخیص–خطا[۴] $\sigma(z)$ و یک چندجمله‌ای همراه $\omega(z)$ را به‌روشی مشابه با بخش ٦.٧ تعریف می‌کنیم (اما در این لحظه با به‌کارگیری خود مکان‌ها به‌جای معکوس آنها).

$$\sigma(z) := \prod_{i \in M}(z-\gamma_i), \tag{٧}$$

$$\omega(z) := \sum_{i \in M} E_i \prod_{j \in M \setminus \{i\}}(z-\gamma_i). \tag{٨}$$

[۴] error-locator polynomial

با توجه به این تعریف نتیجه می‌شود که $\sigma(z)$ و $\omega(z)$ هیچ عامل مشترکی ندارند، $\sigma(z)$ دارای درجه e است و $\omega(z)$ دارای درجه کمتر از e است. محاسبه $\omega(z)/\sigma(z)$ از بخش ۶.۷ با استفاده از استدلال زیر جای‌گزین می‌شود.

$$\begin{aligned} S(z)\sigma(z) &\equiv \sum_{i=0}^{n-1} \frac{E_i}{z-\gamma_i} \prod_{i\in M}(z-\gamma_i) \\ &\equiv \omega(z) \bmod g(z). \end{aligned} \tag{۹}$$

حال فرض کنید لگاریتمی داریم که چندجمله‌ای تکین $\sigma_1(z)$ با کمترین درجه ($\sigma_1(z) \neq 0$) و یک چندجمله‌ای $\omega_1(z)$ با درجه کمتر را می‌یابد، به‌طوری که:

$$S(z)\sigma_1(z) \equiv \omega_1(z) \bmod g(z). \tag{۱۰}$$

این نتیجه می‌دهد که:

$$\omega_1(z)\sigma(z) - \omega(z)\sigma_1(z) \equiv 0 \bmod g(z).$$

چون درجه سمت چپ معادله فوق کمتر از درجه $g(z)$ است، می‌فهمیم که سمت چپ برابر با صفر است؛ بنابراین، $(\sigma(z), \omega(z)) = 1$ ایجاب می‌کند که $\sigma(z)$ عاد می‌کند $\sigma_1(z)$ را؛ بنابراین، باید داشته باشیم $\sigma_1(z) = \sigma(z)$. همین‌که $\sigma(z)$ و $\omega(z)$ را یافتیم، واضح است که E را می‌شناسیم. الگوریتم برلیکمپ یک روش کارا در محاسبه $\sigma_1(z)$ است. روش‌های دیگری، برپایه الگوریتم اقلیدسی برای یافتن ب.م.م دو چندجمله‌ای وجود دارد (ر.ک. مرجع [۵۱]).

۹.۶ کدهای BCH گسترش‌یافته

بیایید نگاه دیگری به کدهای گاپا بیندازیم. درنظر بگیرید $L = \{1, \beta, \beta^2, \cdots, \beta^{n-1}\}$ که در آن β یک ریشه nام اولیه واحد در $\mathbb{F}_{2^m}$ و $g(z)$ یک چندجمله‌ای مناسب است. فرض کنید $(a_0, a_1, \cdots, a_{n-1}) \in \Gamma(L, g)$. مشابه رابطه ۲، چندجمله‌ای ماتسون–سولومن $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ را با $A(X)$ نشان می‌دهیم. چندجمله‌ای:

$$(X^n - 1)\sum_{i=0}^{n-1} \frac{A(\beta^i)}{X - \beta^i} = (X^n - 1)n \sum_{i=0}^{n-1} \frac{a_i}{X - \beta^i},$$

را درنظر بگیرید (با استفاده از لم ۲.۶.۵). طرف چپ معادله، یک چندجمله‌ای با درجه کمتر یا مساوی $n-1$ است که برای $X = \beta^i$ ($0 \leq i \leq n-1$) مقدار $n\beta^{-i}A(\beta^i)$ را می‌پذیرد. می‌توانیم n را با ۱ جای‌گزین نماییم، چون روی $\mathbb{F}_2$ کار می‌کنیم؛ بنابراین، سمت چپ برابر با چندجمله‌ای $A(X) \circ X^{n-1}$

است (با به‌کارگیری نماد موجود در بخش ٦.٥)؛ زیرا این چندجمله‌ای نیز دارای درجه کمتر یا مساوی $n-1$ است و همان مقادیر را در ریشه‌های nام واحد می‌پذیرد؛ بنابراین، قضیه زیر را اثبات کرده‌ایم.

قضیه ۱.۹.٦. اگر $L=\{1,\beta,\cdots,\beta^{n-1}\}$ که در آن β یک ریشه nام اولیه واحد در $\mathbb{F}_{2^m}$ است و $(g(z),z^n-1)=1$، آن‌گاه کد گاپای دودویی $\Gamma(L,g)$ شامل کلمات $(a_0,a_1,\cdots,a_{n-1})$ است که در آن چندجمله‌ای ماتسون—سولومن $A(X)$ از $a(x)$ در رابطه زیر صدق می‌کند:

$$X^{n-1}\circ A(X)\equiv 0 \bmod g(X).$$

در قضیه ۲.٦.٦، کران BCH را با کمک قضیه ۴.٦.٥ و با به‌کارگیری این واقعیت که چندجمله‌ای ماتسون—سولومن یک کدکلمه دارای درجه به‌اندازه کافی کوچک است، ثابت کردیم. برای کدهای گاپا، استدلال مشابهی کار می‌کند. چندجمله‌ای $g(X)$ دارای درجه t است و $(g(X),X^n-1)=1$؛ بنابراین، از قضیه ۱.۹.٦ نتیجه می‌شود که حداکثر $n-1-t$ تا ریشه‌های nام واحد، ریشه‌های $A(X)$ هستند. معنای آن این است که a دارای وزن حداقل $t+1$ است که اثبات دومی برای قضیه ۳.۹.۲ را نتیجه می‌دهد.

دلیل بالا چگونگی تعمیم این کدها را نشان می‌دهد. ترفند به‌کار رفته، ما را مطمئن می‌سازد که چندجمله‌ای ماتسون—سولومن یک کدکلمه شامل تعداد کمی ریشه‌های nام واحد به‌عنوان ریشه‌های خود است. این ایده، توسط چِین[5] و چُی[6] (۱۹۷۵؛ مرجع [۱۳]) به‌روش زیر به‌کار رفته است.

تعریف ۲.۹.٦. فرض کنید $(T,+,\circ)$ همان باشد که در بخش ٦.٥ با $\mathcal{F}=\mathbb{F}_{q^m}$ و $S=\mathbb{F}_q[x] \bmod x^n-1$ آورده شد. فرض کنید $P(X)$ و $G(X)$ دو چندجمله‌ای در T باشند، به‌طوری که $(P(X),X^n-1)=(G(X),X^n-1)=1$. کد BCH گسترش‌یافته (GBCH کد) با طول n روی $\mathbb{F}_q$ با زوج چندجمله‌ای $(P(X),G(X))$ به‌صورت زیر تعریف می‌شود:

$$\{a(x)\in S \mid P(X)\circ(\Phi a)(X)\equiv 0 \bmod G(X)\}.$$

یک GBCH به‌وضوح خطی است.

قضیه ۳.۹.٦. کمترین—فاصله یک کد GBCH در تعریف ۲.۹.٦ حداقل برابر با $1+\deg G(X)$ می‌باشد.

---

[5] R. T. Chien

[6] D. M. Choy

اثبات. قضیه ۴.٦.۵ را به‌کار می‌بریم. عامل مشترک $f(X)$ از Φa و $X^n - ۱$، عاملی از $P(X) \circ (\Phi a)(X)$ هم هست. اما $(G(x), f(X)) = ۱$؛ بنابراین، درجه $f(X)$ باید حداکثر برابر با $n - ۱ - \deg G(X)$ باشد. □

توجه دارید که کدهای گاپای خاصی که در قضیه ۱.۹.٦ مطرح شدند، مثال‌هایی از کدهای GBCH هستند. اگر درنظر بگیریم $P(X) = X^{n-۱}$ و $G(X) = X^{d-۱}$، آن‌گاه یک کد BCH به‌دست می‌آوریم.

کدهای GBCH شامل یک ماتریس بررسی‌توازن شبیه $\hat{H}$ از بخش ۸.۱ هستند. برای نشان دادن این مطلب، چندجمله‌ای‌های $p(x) = (\Phi^{-۱}P)(x) = \sum_{i=۰}^{n-۱} p_i x^i$ و $g(x) = (\Phi^{-۱}G)(x) = \sum_{i=۰}^{n-۱} g_i x^i$ را درنظر می‌گیریم. با استفاده از لم ۲.٦.۵، تمامی ضرایب $p(x)$ و $g(x)$، ناصفر هستند، چون ریشه‌های nام واحد، ریشه‌های $P(X)$ یا $G(X)$ نمی‌باشند. فرض کنید $a(x)$ یک کدکلمه باشد و $A(X) = (\Phi a)(X)$. با استفاده از تعریف ۲.۹.٦، چندجمله‌ای $B(X)$ با درجه حداکثر $n - ۱ - \deg G(X)$ وجود دارد، به‌طوری که:

$$P(X) \circ A(X) = B(X)G(X) = B(X) \circ G(X).$$

تعریف کنید $b(x) := (\Phi^{-۱}B)(x) = \sum_{i=۰}^{n-۱} b_i x^i$؛ در این‌صورت داریم:

$$p(x) * a(x) = b(x) * g(x),$$

یعنی:

$$\sum_{i=۰}^{n-۱} p_i a_i x^i = \sum_{i=۰}^{n-۱} b_i g_i x^i.$$

بنابراین، به‌دست آورده‌ایم $b_i = p_i g_i^{-۱} a_i$ $(۰ \le i \le n-۱)$. فرض کنید $h_i := p_i g_i^{-۱}$ و تعریف کنید:

$$H := \begin{pmatrix} h_۰ & h_۱\beta & \cdots & h_{n-۱}\beta^{n-۱} \\ h_۰ & h_۱\beta^{۲} & \cdots & h_{n-۱}\beta^{۲(n-۱)} \\ \vdots & \vdots & & \vdots \\ h_۰ & h_۱\beta^{t} & \cdots & h_{n-۱}\beta^{t(n-۱)} \end{pmatrix}.$$

فرض کنید $۱ \le j \le t = \deg G(X)$؛ در این‌صورت $B_{n-j} = ۰$. با به‌کارگیری رابطه ۲ داریم:

$$B_{n-j} = b(\beta^j) = \sum_{i=۰}^{n-۱} b_i \beta^{ij} = \sum_{i=۰}^{n-۱} h_i a_i \beta^{ij}.$$

بنابراین، $aH^T = ۰$. برعکس، اگر $aH^T = ۰$، آن‌گاه داریم که درجه $B(X)$ حداکثر برابر $n - ۱ - t$ است؛ بنابراین، $B(X)G(X) = B(X) \circ G(X) = P(X) \circ A(X)$؛ یعنی a در کد GBCH است.

۹.۷ پیشنهادها

کدهای توصیف شده در بخش ۹.۱ کدهای متناوب[۷] نامیده می‌شوند. این کدها که در این فصل مورد بحث قرار گرفتند، موارد خاصی، وابسته به انتخاب h_i و β_i، هستند. اولین زیرکلاس جالب، به‌نظر می‌رسد که کلاس کدهای اسریواستاوا[۸] که توسط اسریواستاوا[۹] در سال ۱۹۶۷ (منتشرنشده) معرفی شده است، باشد. برلیکمپ[۱۰] [۲] امکان آنها را تشخیص داد و مطالعه بیشتر در این زمینه را پیشنهاد داد. کدهای متناوب توسط هلگرت[۱۱] (۱۹۷۴؛ مرجع [۳۵]) معرفی شد. جالب‌ترین مطلبی که در مورد کدهای گاپا ثابت شد، توسط خود گاپا[۱۲] [۲۷] در سال ۱۹۷۰ مطرح گردید (ر.ک. مرجع [۴]).

کدهای BCH، تنها کدهای گاپای دوری هستند (ارجاع به مساله ۲.۹.۸)، اما برلیکمپ و مرنو [۵] نشان دادند که کدهای گاپای دودویی گسترش‌یافته ۲—تصحیح‌کننده خطا، دوری هستند. بعداً زینگ[۱۳] و زیمرمن[۱۴] [۷۱] نتیجه مشابهی را برای سایر کدهای گاپا ثابت نمودند و همان مولفین، ایده کدهای گاپا را تعمیم دادند.

۹.۸ مسائل

۱.۹.۸. فرض کنید L شامل ریشه‌های ۱۵ام اولیه واحد در $\mathbb{F}_{۲^۴}$ باشد (فرض کنید $\alpha^۴ + \alpha + ۱ = ۰$). فرض کنید $g(z) := z^۲ + ۱$. کد دودویی گاپای $\Gamma(L, g)$ را بررسی کنید.

۲.۹.۸. فرض کنید α یک ریشه nام اولیه واحد در $\mathbb{F}_{۲^m}$ باشد و فرض کنید $L := \{۱, \alpha, \alpha^۲, \cdots, \alpha^{n-۱}\}$. هم‌چنین فرض کنید کد گاپای دودویی $C = \Gamma(L, g)$ یک کد دوری باشد. نشان دهید $g(z) = z^t$ برای برخی مقادیر یک مقدار t، یعنی C یک کد BCH است.

۳.۹.۸. فرض کنید $n = q^m - ۱$، $L = \mathbb{F}_{q^m} \setminus \{۰\}$. فرض کنید $C_۱$ کد BCH با طول n روی $\mathbb{F}_q$ به‌دست آمده با درنظر گرفتن $\delta = d_۱$ در تعریف ۱.۶.۶ باشد. هم‌چنین فرض کنید $C_۲$ یک کد گاپای $\Gamma(L, g)$ باشد. نشان دهید $C_۱ \cap C_۲$ دارای کمترین—فاصله $d \geq d_۱ + d_۲ - ۱$ است که در آن $d_۲ := ۱ + degg$.

---

[۷] alternate codes
[۸] Srivistava codes
[۹] J. N. Srivistava
[۱۰] E. R. Berlekamp
[۱۱] H. J. Helgert
[۱۲] V. D. Goppa
[۱۳] K. K. Tzeng
[۱۴] K. P. Zimmerman

۴.۹.۸. کد GBCH با زوج چندجمله‌ای $(P(X), G(X))$ را درنظر بگیرید که $G(X)$ دارای درجه t باشد. نشان دهید که چندجمله‌ای $\hat{P}(X)$ وجود دارد به‌طوری که زوج $(\hat{P}(X), X^t)$ همان کد را تعریف می‌کند.

۵.۹.۸. فرض کنید C کد دوری دودویی با طول ۱۵ با مولد $x^۲ + x + ۱$ باشد. نشان دهید C یک کد BCH است، اما یک کد گاپا نیست.

فصل ۱۰

کدهای هندسه جبری

یکی از مهم‌ترین پیشرفت‌ها در نظریه کدهای تصحیح‌کننده خطا در دهه ۸۰، معرفی روش‌های هندسه جبری برای ساخت کدهای خوب بود. این موضوع برپایه تعمیم کدهای گاپا از فصل قبل می‌باشد. کدهای هندسه جبری نیز از ایده گاپا الهام پذیرفته‌اند. درواقع، کدهای فصل ۹ در برخی اوقات، کدهای گاپای "کلاسیک" و آنهایی که مربوط به این فصل می‌شوند، کدهای گاپای "هندسی" نامیده می‌شوند.

یکی از پیشرفت‌های زیرکانه، مقاله‌ای توسط فسمن[۱] ، ولادوت[۲] و زینک[۳] [۹۸] بود. با استفاده از کدهایی از خم‌های جبری و نتایج عمیق از هندسه جبری، دنباله‌ای از کدهای تصحیح‌کننده خطا ساخته شد که منجر به کران پایینی جدیدی بر روی نرخ اطلاعاتی کدهای خوب گردید. این کران توسط کران گیلبرت—ورشامو ۸.۵.۱ بهبود داده شد. این اولین بهبود از این کران، طی سی سال بود.

این فصل برپایه سخنرانی‌های توضیحی ارائه شده توسط مولف در سال ۱۹۸۷ (ر.ک. مرجع [۷۳]) و درس ارائه شده توسط ون‌درگیر[۴] و مولف در سال ۱۹۸۷ است (ر.ک. مرجع [۷۳]). ما تنها مطالب لازم هندسه جبری را به‌طور سطحی مرور خواهیم کرد که در آن، اغلب اثبات‌ها حذف شده‌اند. در بعضی از مواقع، اشاره خواهیم نمود که پیش‌زمینه جبری بیشتری نسبت به آنچه در فصل ۱ مرور گردید، لازم است. بیشتر کارهای اخیر در مورد این کدها مربوط به روش‌های کدگشایی است. در این کتاب، ما با

---

[۱] Tsfasman
[۲] Vlăduţ
[۳] Zink
[۴] G. van der Geer

کدگشایی سروکار زیادی نخواهیم داشت، بنابراین، در این روش‌ها وارد نمی‌شویم. درواقع، تنها روش کدگشایی که به طور گسترده در عمل به‌کار رفت (برای کدهای بلوکی)، یکی از روش‌هایی است که در بخش ٦.٧ آمده بود. مشخص نیست که چه زمانی کدهای هندسه جبری، اهمیت عملی پیدا خواهند کرد.

اشاره کردیم که بسیاری از نتایج مربوط به این کدها بدون استفاده از دستگاه‌های سنگین هندسه جبری به‌دست می‌آید. برای مشاهده شرحی درباره این روی‌کرد، خواننده را به مرجع [۹۰] ارجاع می‌دهیم.

در بخش ٦.٩ دیدیم که ممکن است کدهای رید–سولومن را با درنظر گرفتن نقاط با مختص‌های متعلق به $\mathbb{F}_q$ روی خط تصویری (شاید روی بستار جبری $\mathbb{F}_q$) تعریف نماییم. کدکلمات، با درنظر گرفتن توابع گویا با یک قطب از مرتبه محدود در یک نقطه خاص و به دست آوردن مقادیر این توابع در نقاط داده‌شده به‌صورت مختص‌ها، تعریف شده‌اند. در بخش ۹.۲، کدهای گاپا را با محاسبه باقی‌مانده های توابع معین در نقاط داده‌شده تعریف کردیم. این مجموعه از توابع توسط شرط‌هایی بر روی ریشه‌ها و قطب‌های آنان محدود شده‌اند. این دو رویکرد همان چیزی است که آن‌را در این فصل توسعه خواهیم داد. ما باید خم‌های جبری را مطالعه کنیم، روشی برای توصیف این محدودیت‌ها بر روی مجموعه توابعی که به‌کار می‌بریم، پیدا کنیم و مفهوم باقی‌مانده را گسترش دهیم. دو کلاس از این کدها را که دوگان هستند، تشریح می‌کنیم.

۱۰.۱ خم‌های جبری

در ادامه، k یک میدان بسته جبری است. در کاربردهای ما، k بستار جبری $\mathbb{F}_q$ خواهد بود (در این بخش، در صورتی که کار آسان شود خواننده می‌تواند k را همان میدان $\mathbb{C}$ در نظر بگیرد، اما او باید این کار را با دقت انجام دهد، چرا که در برخی از مواقع با توجه به میدان‌هایی که درنظر می‌گیریم، نتیجه کاملاً متفاوت خواهد بود). فرض کنید $\mathbb{A}^n$ معرف فضای آفین n–بعدی باشد (با مختص‌های x_1، x_2، $\cdots$، x_n). به‌طور مشابه، $\mathbb{P}^n$ فضای تصویری n–بعدی خواهد بود (با مختص‌های همگن x_1، x_2، $\cdots$، x_n). درابتدا ما حالت آفین را مورد بحث قرار می‌دهیم. این موقعیت برای فضاهای تصویری، کمی پیچیده‌تر است.

در فضای $\mathbb{A}^n$، یک توپولوژی معرفی می‌کنیم که به توپولوژی زاریسکی[۵] معروف است. مجموعه‌های بسته[٦]، مجموعه‌هایی با ریشه‌های ایده‌آل‌های a از $k[x_1, x_2, \cdots, x_n]$ هستند؛ یعنی:

$$B = V(a) := \{(x_1, x_2, \cdots, x_n) \in \mathbb{A}^n | f(x_1, x_2, \cdots, x_n) = 0, \quad f \in a \text{ برای تمامی}\}.$$

[۵] Zariski topology

[٦] closed set

همواره فرض می‌کنیم a رادیکال[۷] است؛ یعنی a شامل تمامی چندجمله‌ای‌هایی است که روی B صفر می‌شوند (یک ایده‌آل a، رادیکال نامیده می‌شود، اگر برای هر $n \in \mathbb{N}$، $f^n \in a$ نتیجه دهد $f \in a$). یک زیرمجموعه بسته B، تحویل‌ناپذیر[۸] نامیده می‌شود، اگر B را نتوان به‌صورت اجتماع دو زیرمجموعه بسته سره از B نوشت. مجموعه $V(a)$ تحویل‌ناپذیر است، اگر و تنهااگر a یک ایده‌آل اول باشد. یک مجموعه باز[۹] مکمل یک مجموعه بسته است.

مثال ۱.۱۰.۱. در صفحه آفین، ایده‌آل اصلی تولید شده توسط $x^2 - y^2$ را درنظر بگیرید. مجموعه بسته متناظر، اجتماع دو خط با معادلات $y = x$، به‌ترتیب $y = -x$، است. هر یک از این خطها یک مجموعه تحویل‌ناپذیر در صفحه $\mathbb{A}^2$ است.

تمامی خم‌ها در فضای آفین یا تصویری در این پاراگراف نیاز است که تحویل‌ناپذیر باشند.

ایده‌آل اول p در حلقه $k[x_1, x_2, \cdots, x_n]$ را درنظر بگیرید. مجموعه χ از ریشه‌های p یک چندگونای آفین[۱۰] نامیده می‌شود.

مثال ۲.۱۰.۱. در فضای ۳ بعدی، گوی واحد را درنظر بگیرید؛ یعنی مجموعه با معادله $x^2 + y^2 + z^2 = 1$. در اصطلاح خودمان، این یک چندگویای آفین شامل ریشه‌های ایده‌آل p تولید شده توسط چندجمله‌ای $x^2 + y^2 + z^2 - 1$ است. ما هم‌اکنون در حال استفاده از اصطلاحات جبری برای توصیف اشیاء هندسی که توسط معادلات تولید می‌شوند، هستیم.

دو چندجمله‌ای که در یک عضو p متفاوت باشند، دارای مقدار یکسانی در هر نقطه χ خواهند بود. این مطلب دلیل معرفی حلقه زیر است.

تعریف ۳.۱۰.۱. حلقه $k[x_1, x_2, \cdots, x_n]/p$، حلقه مختصات[۱۱] $k[\chi]$ از متغیر χ نامیده می‌شود.

حلقه مختصات، یک دامنه صحیح[۱۲] است، چون p یک ایده‌آل اول است؛ بنابراین، می‌توانیم تعریف زیر را بسازیم.

تعریف ۴.۱۰.۱. میدان خارج‌قسمتی حلقه $k[\chi]$ با $k(\chi)$ نمایش داده می‌شود. به آن میدان تابعی[۱۳] χ گفته می‌شود. بعد متغیر χ، درجه متعالی $k(\chi)$ روی k است. اگر این بعد برابر ۱ باشد، آن‌گاه χ یک خم

---

[۷] radical
[۸] irreducible
[۹] open set
[۱۰] affine variety
[۱۱] coordinate ring
[۱۲] integral domain
[۱۳] function field

جبری نامیده می‌شود.

مثال ۵.۱۰.۱ در صفحه آفین روی میدان k، سهمی χ با معادله $x = y^2$ را درنظر می‌گیریم. در این مثال، حلقه مختصات $k[\chi]$ شامل تمامی عبارت‌هایی به‌شکل $A + By$ می‌باشد، که در آن A و B متعلق به $k[x]$ هستند و y در رابطه $x = y^2$ صدق می‌کند. در این مثال، حلقه مختصات $k(\chi)$ شامل تمامی عبارت‌های به‌شکل $A + By$ است، که در آن A و B در $k[x]$ هستند و y در رابطه $x = y^2$ صدق می‌کند. بنابراین، $k(\chi)$ یک توسیع جبری $k(x)$ به‌وسیله عضو y است که در این معادله با درجه ۲ صدق می‌کند.

در فضای تصویری $\mathbb{P}^n$، موقعیت مذکور با این واقعیت درهم پیچیده شده است که ما باید مختص‌های همگن را به‌کار بریم. این بدان معناست که تنها مطلبی که منطقی به‌نظر می‌آید، مطالعه توابع گویاست به‌طوری که صورت و مخرج کسر، چندجمله‌ای‌های همگنی با درجه یکسان باشند. یک متغیر تصویری χ، مجموعه صفر در $\mathbb{P}^n$ از یک ایده‌آل اول همگن p در $k[x_0, x_1, \cdots, x_n]$ است. زیرحلقه $R(\chi)$ از $k(x_0, x_1, \cdots, x_n)$، شامل کسرهای f/g را درنظر بگیرید که در آن f و g چندجمله‌ای‌های همگن با درجه یکسان هستند و $g \notin p$؛ در این‌صورت $R(\chi)$ دارای ایده‌آل ماکسیمال یکتای $M(\chi)$ است که شامل تمامی f/gهایی است که در آن $f \in p$. میدان تابعی $k(\chi)$ با استفاده از تعریف برابر با $R(\chi)/M(\chi)$ است.

حال فرض کنید χ یک آفین یا یک متغیر تصویری باشد. فرض کنید P یک نقطه روی χ باشد و فرض کنید U یک همسایه از این نقطه باشد. فرض کنید f و g چندجمله‌ای‌هایی، به ترتیب چندجمله‌ای‌هایی همگن، با درجه یکسان باشند و فرض کنید $g(P) \neq 0$. در این‌صورت خارج‌قسمت $\phi = f/g$، تعریف شده روی U، منظم[۱۴] در نقطه P نامیده می‌شود. توابعی که در هر نقطه از مجموعه U منظم هستند، تشکیل یک حلقه می‌دهند که با $k[U]$ نمایش داده می‌شود. چون k از نظر جبری بسته است، اگر χ تصویری باشد، آن‌گاه هیچ تابع منظمی روی χ وجود ندارد مگر توابع ثابت.

تعریف ۶.۱۰.۱. حلقه موضعی[۱۵] O_P (که برخی اوقات با $O_P(\chi)$ نشان داده می‌شود) از نقطه P روی متغیر χ، مجموعه توابع گویا روی χ است که منظم می‌باشند.

خواننده آشنا با اصطلاح جبری، تشخیص خواهد داد که این درواقع یک "حلقه موضعی" به معنای جبری است؛ یعنی شامل یک ایده‌آل ماکسیمال است که درواقع این ایده‌ال همان مجموعه m_P از توابع در O_P است که در P صفر هستند.

یک متغیر آفین می‌تواند در یک متغیر تصویری به‌روش زیر نشانده شود. اگر $f \in k[x_1, x_2, \cdots, x_n]$،

[۱۴] regular
[۱۵] local ring

آن‌گاه ما به f تابع همگن زیر را تخصیص می‌دهیم:

$$f^*(x_0, x_1, \cdots, x_n) := x_0^l f(x_1/x_0, \cdots, x_n/x_0),$$

که در آن l از درجه f است.

فرض کنید ϕ یک متغیر آفین در $\mathbb{A}^n$ تعریف شده توسط ایده‌آل اول p است. فرض کنید p^* یک ایده‌آل اول همگن تولید شده توسط مجموعه $\{f^* \mid f \in p\}$ باشد؛ در این‌صورت p^* یک متغیر تصویری χ^* در $\mathbb{P}^n$ تعریف می‌کند. تعریف می‌کنیم $\chi_0^* := \{(x_0, x_1, \cdots, x_n) \in \chi^* \mid x_0 \neq 0\}$؛ در این‌صورت χ یک‌ریخت با χ_0^* تحت نگاشت $(x_1, \cdots, x_n) \to (1 : x_1 : \cdots : x_n)$ است. نقاط $(x_0 : x_1 : \cdots : x_n) \in \chi^*$ با $x_0 = 1$ نقاط در بی‌نهایت[16] χ نامیده می‌شوند. علاوه‌براین، میدان تابعی $k(\chi)$ و $k(\chi^*)$ تحت نگاشت $f/g \to f^* x_0^m / g^*$، که در آن m برابر با $\deg(g) - \deg(f)$ است، یک‌ریخت می‌باشند.

مثال ۷.۱۰.۱. در $\mathbb{P}^2$ با مختصات‌های $(x : y : z)$، متغیر χ تعریف شده به‌صورت $xz - y^2 = 0$ را درنظر بگیرید (این، همان سهمی مثال ۵.۱۰.۱ است، در اینجا با یک نقطه در بی‌نهایت یعنی $Q := (1 : 0 : 0)$). تابع $(2xz + z^2)/(y^2 + z^2)$ در نقطه $P = (0 : 0 : 1)$ منظم می‌باشد. با جای‌گزین نمودن y^2 با xz، می‌بینیم که این تابع برابر با $(2x + z)/(x + z)$ است؛ بنابراین، در Q نیز منظم می‌باشد.

توجه کنید که تابع $(x^3 + y^3)/z^3$ که در P برابر با صفر است، می‌تواند به‌صورت حاصل‌ضرب y^3/z^3 و $(y^3 + z^3)/z^3$ نوشته شود، که در آن دومین عامل منظم است و در P صفر نیست. اگر با توپولوژی معمولی داشته باشیم $k = \mathbb{C}$، در این‌صورت برای نقاط نزدیک P، یک تناظر یک‌به‌یک با مقدار y/z وجود دارد، اما این مطلب برای x/z درست نیست. این، نمونه‌ای از آن چیزی است که در زیر آن‌را یک پارامتر موضعی خواهیم نامید.

مثال‌های موجود در پایان این پاراگراف، آنچه را گفتیم توضیح می‌دهند، اما باید درابتدا تمامی اصطلاحاتی را که نیاز داریم، معرفی کنیم. از اینجا به‌بعد، تنها خم‌ها را درنظر می‌گیریم.

خمی در $\mathbb{A}^2$، تعریف شده به‌صورت یک معادله $F(x, y) = 0$ را درنظر بگیرید. فرض کنید $P = (a, b)$ یک نقطه روی این خم باشد. اگر حداقل یکی از مشتقات F_x یا F_y در P برابر با صفر نباشد، آن‌گاه P یک نقطه ساده[17] یا نامنفرد[18] منحنی نامیده می‌شود؛ بنابراین، منحنی دارای یک مماس بر P به معادله $F_x(P)(x - a) + F_y(P)(y - b) = 0$ است. حال تعریف می‌کنیم:

$$d_P F := F_x(a, b)(x - a) + F_y(a, b)(y - b).$$

[16] points at infinity
[17] simple
[18] nonsingular

در این‌صورت مماس T_P در P به‌صورت $d_P F = 0$ تعریف می‌شود. این نماد، شناخته‌شده است. اگر $G \in k[\chi]$، آن‌گاه معنی نمی‌دهد که $d_P(G)$ را به روش مشابه تعریف کنیم؛ زیرا G تنها به پیمانه مضارب F تعریف شده است. اما روی T_P، تابع خطی $d_P G := G_x(a,b)(x-a) + G_y(a,b)(y-b)$ خوش‌تعریف است. برای P داده شده، نگاشت d_P یک عضو $k[\chi]$ را به یک تابع خطی تعریف شده بر روی مماس T_P، یعنی یک عضو T_P^* تصویر می‌کند. این نگاشت را می‌توانیم به O_P گسترش دهیم. چون $d_P f = 0$ اگر f ثابت باشد، می‌توانیم خود را به توابع گویای f در m_P محدود کنیم؛ در این‌صورت از قاعده حاصل‌ضرب مشتق، می‌بینیم که m_P^2 هسته این نگاشت است. بدون اثبات بیان می‌کنیم که این درواقع هسته است؛ بنابراین، m_P/m_P^2 یک‌ریخت با T_P^* است و برای یک نقطه نامنفرد، آن یک فضای یک بعدی است. معنای آن این است که می‌توانیم یک نقطه ساده از یک منحنی را با الزام به این‌که فضای $k-$بعدی m_P/m_P^2 دارای بعد ۱ است، تعریف کنیم. از اینجا به‌بعد، تنها خم‌های نامنفرد (خم‌های هموار نیز نامیده می‌شوند) را درنظر می‌گیریم؛ یعنی خم‌هایی که در آن تمامی نقاط نامنفرد هستند. این محدودویت دارای نتیجه زیر است. فرض کنید P یک نقطه از χ باشد. به خواننده یادآوری می‌کنیم که ایده‌آل ماکسیمال m_P از حلقه موضعی O_P شامل "توابعی" است که در P صفر هستند. سایر عناصر O_P یک‌ها هستند. چون m_P/m_P^2 دارای بعد ۱ است، یک عضو مولد t برای این فضا وجود دارد. هم‌چنین ما سمبل t را برای یک عضو متناظر در m_P به‌کار می‌بریم؛ در این‌صورت می‌توانیم هر عضو z از O_P را به‌طور یکتا به‌صورت $z = ut^m$ بنویسیم، که در آن u یک عنصر یکه است و $m \in \mathbb{N}_0$. تابع t یک پارامتر موضعی یا پارامتر یکنواخت‌کننده[۱۹] در P نامیده می‌شود. یک تابع f یک پارامتر موضعی در P است اگر $d_P f$ روی T_P صفر نباشد.

اگر $m > 0$، آن‌گاه P یک ریشه با تکرار m از z می‌باشد (نمونه‌ای با $m = 3$ را در مثال ۷.۱۰.۱ دیدیم). می‌نویسیم $m = or d_P(z) = v_P(z)$ (برای خواننده‌هایی که با این اصطلاح آشنایی دارند، O_P یک حلقه ارزیابی گسسته[۲۰] است و عناصر $v_P(t) = 1$ پارامترهای موضعی هستند). ما این تابع مرتب را با استفاده از تعریف $v_P(f/g) := v_P(f) - v_P(g)$ به $k(\chi)$ گسترش می‌دهیم. اگر $v_P(z) = -m < 0$، آن‌گاه گوییم z در P شامل یک قطب[۲۱] مرتبه m است. اگر z یک عضو از $k(\chi)$ با $v_P(z) = m$ باشد، آن‌گاه می‌توانیم بنویسیم $z = at^m + z'$، که در آن $a \in k$، $a \neq 0$ و $v_P(z') > m$. با این روش، می‌توان نشان داد که z می‌تواند به‌صورت یک سری لوران بیان شود. بعداً ما این مطلب را برای تعریف "مانده"[۲۲] z به کار خواهیم برد.

---

[۱۹] uniformizing parameter

[۲۰] discrete valuation ring

[۲۱] pole

[۲۲] residue

مثال ۸.۱۰.۱ فرض کنید χ دایره‌ای در $\mathbb{A}^۲$ با معادله $x^۲+y^۲=۱$ باشد و فرض کنید $P=(۱,۰)$، $(char(k)\neq ۲)$. هم‌چنین فرض کنید $z=z(x,y)=۱-x$. این تابع در P صفر است؛ بنابراین، در m_P واقع است. ادعا می‌کنیم که z دارای مرتبه ۲ است. برای دیدن این مطلب، مشاهده می‌کنید که y یک پارامتر موضعی در P است. توجه دارید که $d_P x = x-۱$ روی T_P برابر صفر است، بنابراین، x یک پارامتر موضعی در P نیست. روی χ داریم $۱-x=y^۲/(۱+x)$ و تابع $۱/(۱+x)$ در O_P یکه است. در مثال ۷.۱۰.۱، یک موقعیت مشابه را برای $\mathbb{P}^۲$ می‌بینیم.

مثال ۹.۱۰.۱. یک بار دیگر سهمی موجود در مثال ۷.۱۰.۱ را درنظر بگیرید. فرض کنید Q نقطه در بی‌نهایت باشد؛ یعنی $Q=(۱:۰:۰)$. میدان $k(\chi)$ شامل کسرهای $(A_l+B_{l-۱}y)/(C_l+D_{l-۱}y)$ است که در آن، ضرایب، چندجمله‌ای‌های همگنی با درجه l (به‌ترتیب $l-۱$) نسبت به x و z هستند و y در رابطه $y^۲=xz$ صدق می‌کند. چنین تابعی در Q منظم است اگر ضریب x^l در C_l صفر نباشد. به‌آسانی دیده می‌شود که y/x نیز یک پارامتر موضعی در Q است. درباره رفتار تابع $g:=(z^۳+xyz)/x^۳$ در Q چه می‌توان گفت؟ روی χ داریم:

$$\frac{z^۳+xyz}{x^۳}=(\frac{y}{x})^۳(\frac{x^۲+yz}{x^۲}).$$

دومین عامل در طرف راست معادله فوق یک یکه در O_Q است، بنابراین، g دارای یک صفر با تکرار ۳ در Q است.

هنگامی که ما کدهایی را می‌سازیم، به نقاطی که مختصات آنها متعلق به الفبای $\mathbb{F}_q$ است، علاقه‌مند خواهیم بود. به اینها نامی خاص می‌دهیم.

تعریف ۱۰.۱۰.۱. اگر k بستار جبری $\mathbb{F}_q$ باشد و χ یک خم روی k باشد، آن‌گاه نقاط روی χ که تمام مختص‌های آنها در $\mathbb{F}_q$ است، نقاط گویا[۲۳] نامیده می‌شوند (ما تنها این اصطلاح را برای خم‌های روی k با معادلاتی که دارای تمام ضرایب در $\mathbb{F}_q$ است، به‌کار خواهیم برد).

سه مثال دیگر می‌آوریم.

مثال ۱۱.۱۰.۱. فرض کنید $\mathbb{P}$ خط تصویری روی k باشد. یک پارامتر موضعی در نقطه $P=(۱:۰)$ برابر y/x است. تابع گویای $(x^۲-y^۲)/y^۲$ شامل یک قطب مرتبه ۲ در P است. اگر k دارای مشخصه ۲ نباشد، آن‌گاه $(۱:۱)$ و $(۱:-۱)$ ریشه‌هایی با تکرار ۱ هستند.

[۲۳] rational points

مثال ۱.۱۰.۱۲. خم مسطح با معادله $x^3y + y^3z + z^3x = 0$، چهارتایی کلاین[۲۴] نامیده می‌شود. این خم را روی بستار جبری $\mathbb{F}_2$ درنظر می‌گیریم. نگاهی به چند تا از زیرمیدان‌ها بیندازید. روی $\mathbb{F}_2$، نقاط گویا برابر با $(0:0:1)$، $(0:1:0)$ و $(1:0:0)$ هستند. اگر ما به $\mathbb{F}_4$ برویم، آن‌گاه دو نقطه گویای بیشتر وجود دارند؛ یعنی $(\alpha+1:\alpha:1)$ و $(\alpha:\alpha+1:1)$ که در آن $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ و $\alpha^2 = 1 + \alpha$.

در مثال‌های بعدی، این خم روی $\mathbb{F}_8$ مطالعه خواهد شد. به‌طور معمول، این میدان را به‌صورت $\mathbb{F}_2(\xi)$ تعریف می‌کنیم، که در آن $\xi^3 = \xi + 1$. اگر یک نقطه گویا دارای مختصات صفر باشد، آن‌گاه باید یکی از نقاط روی $\mathbb{F}_2$ باشد. اگر $xyz \neq 0$، آن‌گاه ما می‌توانیم درنظر بگیریم $z = 1$. اگر $y = \xi^i$ $(0 \leq i \leq 6)$، آن‌گاه می‌نویسیم $x = \xi^{3i}\eta$. با جانشین نمودن آن در معادله، داریم $\eta^3 + \eta + 1 = 0$؛ یعنی η یکی از عناصر ξ، ξ^2 یا ξ^4 است؛ بنابراین، در مجموع ۲۴ نقطه گویا روی $\mathbb{F}_8$ داریم.

مثال ۱.۱۰.۱۳. فرض کنید χ خم مسطح با معادله $x^3 + y^3 + z^3 = 0$ روس بستار $\mathbb{F}_2$ باشد و نگاهی به زیرمیدان $\mathbb{F}_4$ بیندازید. چون توان سوم یک عضو $\mathbb{F}_4$ برابر با ۰ یا ۱ است، تمامی نقاط گویا دارای یک مختصات صفر هستند. می‌توانیم فرض کنیم که یکی از مابقی مولفه‌ها برابر ۱ و سومین آن هر عضو ناصفری از $\mathbb{F}_4$ باشد؛ بنابراین، ۹ نقطه (تصویری) داریم. در $Q = (0:1:1)$، می‌توانیم $t = x/z$ را به‌عنوان پارامتر موضعی درنظر بگیریم. مشکلی را درنظر می‌گیریم که مجدداً پیش می‌آید. عبارت $f := x/(y+z)$ به‌نظر یک تابع کاملاً منطقی به نظر می‌آید و درواقع روی بیشتر χ چنین است. اما در Q، این کسر معنی نمی‌دهد. ما باید یک شکل هم‌ارز برای f نزدیک Q بیابیم. روی χ داریم:

$$\frac{x}{y+z} = \frac{x(y^2+yz+z^2)}{y^3+z^3} = t^{-2}.\frac{y^2+yz+z^2}{z^2},$$

که در آن دومین عامل سمت راست معادله فوق، منظم است و در Q صفر نیست. بااستفاده از قراردادهای اخیرمان، گوییم f شامل یک قطب مرتبه ۲ در Q است. به‌طور مشابه، $y/(y+z)$ شامل یک قطب مرتبه ۳ در Q است.

به‌منظور ایجاد یک آمادگی برای بخش ۱۰.۵، اشتراک خم‌های مسطح را درنظر می‌گیریم. فرض می‌کنیم که خواننده با این واقعیت که یک چندجمله‌ای درجه m یک متغیره با ضرایبی در یک میدان، دارای حداکثر m ریشه است، آشنا می‌باشد. اگر این میدان از نظر جبری بسته باشد و اگر ریشه‌ها با

[۲۴] Klein quartic

تکرارها شمرده شوند، آن‌گاه تعداد ریشه‌ها برابر با m است. در اینجا قضیه‌ای، معروف به قضیه بزوت[۲۵] ، را بیان می‌کنیم که تعمیمی از این مساله به چندجمله‌ای‌های چند متغیره است. ما تنها حالت دو متغیره را درنظر می‌گیریم؛ یعنی خم‌های مسطح. مجدداً فرض کنیم که خواننده می‌داند چگونه تکرارها با نقاط مشترک دو خم‌مسطح مربوط است (اگر P یک نقطه نامنفرد از یک خم با معادله $F(x,y)=0$ باشد و خم با معادله $G(x,y)=0$ شامل P باشد، آن‌گاه تکرار اشتراک، برابر با $v_P(G)$ است). در ادامه، دو صفحه مسطح آفین تعریف شده توسط $F(x,y)=0$ و $G(x,y)=0$ از درجه l به‌ترتیب m را درنظر می‌گیریم. فرض می‌کنیم F و G شامل یک عامل مشترک غیربدیهی نباشند؛ یعنی این خم‌ها شامل یک مولفه در اشتراک خود نمی‌باشند. حالتی را درنظر می‌گیریم که ضرایب، متعلق به یک میدان می‌باشند که از نظر جبری بسته است.

قضیه ۱۴.۱۰.۱. دو خم مسطح از درجه l و m که شامل یک مولفه در اشتراک خود نباشند، دقیقاً در lm نقطه مشترک هستند (اگر با تکرار شمرده شوند و نقاط در بی‌نهایت نیز درنظر گرفته شوند).

اگر k از نظر جبری بسته نباشد، آن‌گاه خم‌ها در حداکثر lm نقطه مشترک هستند. ما این قضیه را اثبات نمی‌کنیم.

مثال ۱۵.۱۰.۱. به‌وضوح، خم مسطح آفین روی بستار $\mathbb{F}_2$ با معادله $x^3+y^3=1$ و خط با معادله $x=y$ تلاقی نمی‌کنند. اما هنگامی‌که آنها به‌طور تصویری درنظر گرفته می‌شوند، خم χ از مثال ۱۳.۱۰.۱ را داریم و خواننده به‌آسانی می‌تواند بررسی کند که χ و خط با معادله $x+y=0$ در $P:=(1:1:0)$ (در بی‌نهایت) با تکرار ۳ مشترک هستند؛ (این مطلب به روشی مشابه با مثال ۱۳.۱۰.۱ انجام گرفته است).

در اینجا ما ایده کدهای رید—سولومن تعریف شده در بخش ۶.۸ (توصیف دوم) را گسترش می‌دهیم. فرض کنید V_i فضای برداری چندجمله‌ای‌های با درجه حداکثر l با دو متغیر x، y و ضرایب در $\mathbb{F}_q$ باشد. یک عضو تحویل‌ناپذیر G با درجه m در $\mathbb{F}_q[x,y]$ را درنظر بگیرید. فرض کنید P_1، P_2، $\cdots$، P_n نقاطی روی خم مسطح تعریف شده توسط معادله $G(x,y)=0$ باشند؛ یعنی $G(P_i)=0$ برای $1\le i\le n$. کد C را به‌صورت زیر تعریف می‌کنیم.

$$C:=\{(F(P_1),F(P_2),\cdots,F(P_n))\mid F\in\mathbb{F}_q[x,y],\deg(F)\le l\}.$$

ما d را برای کمترین—فاصله این کد به‌کار خواهیم برد و (به‌طور معمول) k را بعد می‌نامیم (با میدانی که اخیراً در این بخش درنظر گرفته شد، اشتباه نگردد).

[۲۵] Bézout's

قضیه ۱۰.۱۰.۱۶. فرض کنید $lm < n$. برای کمترین —فاصله d و بعد k از C، داریم:

$$d \geq n - lm,$$

$$k = \begin{cases} \binom{l+۲}{۲} & l < m \text{ اگر} \\ lm + ۱ - \binom{m-۱}{۲} & l \geq m \text{ اگر.} \end{cases}$$

اثبات. تکین‌هایی به شکل $x^\alpha y^\beta$ با $\alpha + \beta \leq ۱$ تشکیل یک پایه از V_l می‌دهند؛ بنابراین، V_l دارای بعد $\binom{l+۲}{۲}$ است.

فرض کنید $F \in V_l$. اگر G یک عامل از F باشد، آن‌گاه کدکلمه‌ای در C که متناظر با F است، برابر با صفر است. برعکس، اگر این کدکلمه صفر باشد، آن‌گاه خم‌های با معادله $F = ۰$ و $G = ۰$ به‌ترتیب دارای درجه $l > l'$ و m هستند و آنها شامل n نقطه مشترک $P_۱$، $P_۲$، $\cdots$، P_n می‌باشند. قضیه بزوت و فرض $lm < n$ ایجاب می‌کند که F و G شامل یک عامل مشترک باشند. چون G تحویل‌ناپذیر است، F باید بر G بخش‌پذیر باشد؛ بنابراین، توابع $F \in V_l$ که کدکلمه صفر را ایجاب می‌کنند، تشکیل زیرفضای GV_{l-m} را می‌دهند. این مطلب ایجاب می‌کند که اگر $l < m$، آن‌گاه $k = \binom{l+۲}{۲}$ و اگر $l \geq m$، آن‌گاه:

$$k = \binom{l+۲}{۲} - \binom{l-m+۲}{۲} = lm + ۱ - \binom{m-۱}{۲}.$$

دلیل مشابهی با قضیه بزوت نشان می‌دهد که یک کدکلمه ناصفر شامل حداکثر lm مختصات برابر با صفر است؛ یعنی شامل وزن حداکثر $n - lm$ است؛ بنابراین، $d \geq n - lm$. □

۱۰.۲ مقسوم‌علیه‌ها

در ادامه، χ یک خم تصویری هموار روی k است.

تعریف ۱.۱۰.۲.

۱) یک مقسوم‌علیه[۲۶]، یک جمع صوری $D = \sum_{P \in \chi} n_P P$ است به‌طوری که $n_P \in \mathbb{Z}$ و برای همه به‌جز یک تعداد متناهی از نقاط P داریم $n_P = ۰$.

۲) $Div(\chi)$ یک گروه جمعی از مقسوم‌علیه‌ها با جمع صوری است (گروه آبلی آزاد روی χ)؛

[۲۶] divisor

۳) یک مقسوم‌علیه D، موثر[۲۷] نامیده می‌شود اگر تمام ضرایب n_P نامنفی باشند (نماد $D \succeq 0$)؛

۴) درجه[۲۸] $\deg(D)$ از مقسوم‌علیه D برابر با $\sum n_P$ است.

فرض کنید $v_P = ord_P$ یک ارزیابی گسسته تعریف شده برای توابع روی χ در بخش ۱۰.۱ باشد.

تعریف ۲.۱۰.۲. اگر f یک تابع گویا روی χ باشد که هم‌ارز با تابع صفر نیست، آن‌گاه مقسوم‌علیه f را به‌صورت زیر تعریف می‌کنیم:

$$(f) := \sum_{P \in \chi} v_P(f)P.$$

بنابراین، در یک معنا، مقسوم‌علیه f یک دستگاه سازمان‌دهی است که به ما می‌گوید کجا ریشه‌ها و قطب‌های f قرار دارند و تکرار و مرتبه آنها چقدر است. چون f یک تابع گویاست به‌طوری که صورت و مخرج دارای درجه یکسانی هستند و چون k از نظر جبری بسته است، به‌طور محسوس، روشن است که f شامل تعداد یکسانی ریشه به‌عنوان قطب است، اگر به درستی شمارش شود. ما اثباتی ارائه نمی‌دهیم اما نتیجه‌ای را به‌صورت قضیه بیان می‌کنیم.

قضیه ۳.۱۰.۲. درجه یک مقسوم‌علیه از یک تابع گویا برابر با صفر است.

مقسوم‌علیه یک تابع گویا یک مقسوم‌علیه اصلی[۲۹] نامیده می‌شود.

تعریف ۴.۱۰.۲. دو مقسوم‌علیه D و D' به‌طور خطی هم‌ارز[۳۰] نامیده می‌شوند اگر و تنها اگر $D - D'$ یک مقسوم‌علیه اصلی باشد؛ نماد $D \equiv D'$.

این رابطه در واقع یک رابطه هم‌ارزی است.

در بخش ۹.۲، کدهای گاپا را بر اساس یک فضای برداری از توابع با ریشه‌های تعیین‌شده و قطب‌های ممکن، تعریف کردیم. حال ساز و کاری داریم که تعمیم این مطلب به خم‌ها دست یافتنی است.

تعریف ۵.۱۰.۲. فرض کنید D یک مقسوم‌علیه روی یک خم χ باشد. یک فضای برداری $\mathcal{L}(D)$ روی k را به‌صورت زیر تعریف می‌کنیم:

$$\mathcal{L}(D) := \{f \in k(\chi)^* : (f) + D \succeq 0\} \cup \{0\}.$$

---

[۲۷] effective

[۲۸] degree

[۲۹] principal divisor

[۳۰] linearly equivalent

توجه دارید که اگر $D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$ که $n_i, m_i > 0$، آن‌گاه $\mathcal{L}(D)$ شامل صفر و تمامی توابع در یک میدان تابعی است که ریشه‌هایی با تکرار حداقل m_j در Q_j $(1 \leq j \leq s)$ داشته باشند و شامل هیچ قطبی مگر احتمالاً در نقاط P_i، با مرتبه حداکثر n_i $(1 \leq i \leq r)$، نباشند. نشان خواهیم داد که این فضای برداری شامل بعد متناهی است.

در ابتدا توجه داریم که اگر $D \equiv D'$ و g یک تابع گویا به‌صورت $(g) = D - D'$ باشد، آن‌گاه نگاشت $f \to fg$ نشان می‌دهد که $\mathcal{L}(D)$ و $\mathcal{L}(D')$ یک‌ریخت هستند.

قضیه ۲.۱۰.۶.

۱) $\mathcal{L}(D) = 0$ اگر $\deg(D) < 0$؛

۲) $l(D) := \dim_k \mathcal{L}(D) \leq 1 + \deg(D)$.

اثبات.

۱) اگر $\deg(D) < 0$، آن‌گاه برای هر تابع $f \in k(\chi)^*$ داریم $\deg((f) + D) < 0$؛ یعنی $f \notin \mathcal{L}(D)$.

۲) اگر f برابر با صفر نباشد و $f \in \mathcal{L}(D)$، آن‌گاه $D' := D + (f)$ یک مقسوم‌علیه موثر است به‌طوری که با استفاده از مشاهده فوق $\mathcal{L}(D')$ دارای بعد یکسانی با $\mathcal{L}(D)$ است؛ بنابراین، بدون کاستن از کلیت، D موثر است و فرض می‌کنیم $D = \sum_{i=1}^{r} n_i P_i$ ($n_i \geq 0$ برای $1 \leq i \leq r$). مجدداً فرض کنید f برابر با صفر نیست و $f \in \mathcal{L}(D)$. در نقطه P_i ما f را برروی عنصر متناظر از فضای برداری n_i–بعدی $(t_i^{-n_i} O_{P_i})/O_{P_i}$ تصویر کنید که در آن t_i یک پارامتر موضعی در P_i است؛ بنابراین، نگاشتی از f بر روی مجموع مستقیم فضاهای برداری به‌دست می‌آوریم؛ (تابع صفر را به صفر تصویر کنید). این یک نگاشت خطی است. فرض کنید f در هسته باشد. معنای آن این است که f شامل یک قطب در هیچ‌یک از نقاط P_i نیست؛ یعنی f یک تابع ثابت است. نتیجه می‌شود که $\dim_k \mathcal{L}(D) \leq 1 + \sum_{i=1}^{r} n_i = 1 + \deg(D)$.

□

مثال ۷.۱۰.۲. به خم موجود در مثال ۱۳.۱۰.۱ نگاهی بیندازید. دیدیم که $f = x/(y+z)$ شامل یک قطب مرتبه ۲ در $Q = (۰ : ۱ : ۰)$ است. این تابع شامل دو ریشه است، هر یک با تکرار ۱؛ یعنی $P_۱ = (۰ : \alpha : ۱)$ و $P_۲ = (۰ : ۱ + \alpha : ۱)$. از نمایش $f = (y^۲ + yz + z^۲)/x^۲$ می‌بینیم که Q تنها قطب است؛ بنابراین، برطبق قضیه ۳.۱۰.۲ داریم $(f) = P_۱ + P_۲ - ۲Q$ و $\deg((f)) = ۰$. این مطلب بدیهی نیست، اما می‌توان نشان داد که تابعی در $k(\chi)$ که شامل یک قطب مرتبه ۱ در Q بوده و دیگر قطبی نداشته باشد، نمی‌تواند وجود داشته باشد. بنابراین، در این مثال، فضای $\mathcal{L}(۲Q)$ دارای بعد ۲ است و f و تابعی که متحد با ۱ است، تشکیل یک پایه می‌دهند.

۱۰.۳ مشتق‌های روی یک منحنی

یک خم آفین هموار χ در $\mathbb{A}^۲$ تعریف شده با استفاده از معادله $F(x,y) = ۰$ را درنظر بگیرید و فرض کنید $P = (a,b)$ یک نقطه روی χ باشد. مماس T_P در نقطه P به‌صورت $d_P F = ۰$ تعریف شده است. در بخش ۱۰.۱ نگاشت d_P را تعریف کرده‌ایم که یک عضو $k[\chi]$ را به تابعی خطی روی T_P، یعنی یک عضو T_P^*، تصویر می‌کند. حال مجموعه $\Phi[\chi]$ شامل تمامی نگاشت‌هایی را که به هر عضو P از χ یک عضو T_P^* تخصیص می‌دهند، درنظر می‌گیریم.

تعریف ۱.۱۰.۳. یک عضو $\phi \in \Phi[\chi]$ یک فرم مشتق منظم[۳۱] (روی خم χ) نامیده می‌شود اگر هر نقطه P از χ شامل یک همسایه U باشد به‌طوری که در این همسایه، ϕ به‌صورت $\phi = \sum_{i=۱}^{n} f_i dg_i$ نمایش داده شود، که در آن تمامی توابع f_i و g_i در U منظم باشند.

فرم‌های مشتق منظم روی χ تشکیل یک $k[\chi]-$مدول می‌دهند که ما آن را با $\Omega[\chi]$ نشان می‌دهیم. این مدول توسط عناصر df تولید شده است، که در آن $f \in k[\chi]$، با رابطه $d(f+g) = df + dg$، $d(fg) = fdg + gdf$ و $da = ۰$ برای $a \in k$. برای گسترش به فرم‌های مشتق گویا[۳۲] باید رابطه (معروف) $d(f/g) = (gdf - fdg)/g^۲$ را اضافه کنیم. می‌خواهیم تا یک فرم مشتق گویا روی یک خم تصویری هموار χ تعریف کنیم. برای انجام دادن این کار، زوج‌های (U,ω) و (V,η) را هم‌ارز می‌نامیم اگر $\omega = \eta$ روی $U \cap V$. یک کلاس هم‌ارزی برای این رابطه یک فرم مشتق گویا نامیده می‌شود. از اینجا به‌بعد، فرم‌های مشتق گویا روی χ را مشتق‌ها[۳۳] نامیده و فضای مشتق‌ها را با $\Omega(\chi)$ نشان می‌دهیم. بدون اثبات

[۳۱] regular differential form
[۳۲] rational differential forms
[۳۳] differentials

بیان می‌کنیم:

قضیه ۲.۱۰.۳. فضای $\Omega(\chi)$ دارای بعد روی $k(\chi)$ است؛ در یک همسایگی یک نقطه P با پارامتر موضعی t، دیفرانسیل ω می‌تواند به‌صورت $\omega = f dt$ نوشته شود که در آن f یک تابع گویاست. خواننده ممکن است فکر کند که این مطلب به‌طور غیرضروری پیچیده است. چرا تنها از توابع استفاده نشد؟ مثال بعدی نشان می‌دهد که روی یک خم تصویری، می‌توان یک فرم دیفرانسیل گویای ناصفر داشت که روی تمام خم منظم باشد. این مطلب در تقابل با توابع گویاست.

مثال ۳.۱۰.۳. مجدداً نگاهی به خم χ در $\mathbb{P}^2$ داده‌شده به‌صورت $x^3 + y^3 + z^3 = 0$ می‌اندازیم ($cha(k) \neq 3$). مجموعه باز U_x را به‌صورت $U_x := \{(x : y : z) \in \chi : y \neq 0, z \neq 0\}$ و به‌طور مشابه U_y و U_z را تعریف کنید؛ در این‌صورت U_x، U_y و U_z، χ را می‌پوشانند چون هیچ نقطه روی χ وجود ندارد به‌طوری که دو تا از مختص‌های آن صفر باشد. به آسانی می‌توان بررسی نمود که سه نمایش:

$$U_x \text{ روی } \omega := (\tfrac{y}{z})^2 d(\tfrac{x}{y}), \quad U_y \text{ روی } \eta := (\tfrac{z}{x})^2 d(\tfrac{y}{z}), \quad U_z \text{ روی } \xi := (\tfrac{x}{y})^2 d(\tfrac{z}{x}) \ ,$$

یک دیفرانسیل روی χ تعریف می‌کنند. برای نمونه، برای نشان دادن این‌که η و ξ روی $U_y \cap U_z$ برابر هستند، معادله $(x/z)^3 + (y/z)^3 + 1 = 0$، دیفرانسیل‌ها را گرفته و فرمول $d(f^{-1}) = -f^{-2} df$ را برای $f := y/z$ به‌کار بریم. یک تابع منظم روی χ ثابت است، بنابراین، نمی‌توان این دیفرانسیل را به‌صورت gdf به‌طوری که f و g توابعی منظم روی χ باشند، نمایش داد.

تعریف ۴.۱۰.۳. مقسوم‌علیه (ω) از مشتق ω به‌صورت زیر تعریف می‌شود:

$$(\omega) := \sum_{P \in \chi} v_P(f_P) P,$$

که در آن $\omega = f_P dt_P$ نمایش موضعی ω بوده و v_P یک ارزیابی روی O_P است (گسترش‌یافته به $k(\chi)$).

البته باید نشان داد که این کد به انتخاب پارامتر موضعی وابسته نیست و نیز این‌که تنها تعداد متناهی از ضرایب، صفر نیستند.

فرض کنید ω یک دیفرانسیل باشد و $W = (\omega)$؛ در این‌صورت W یک مقسوم‌علیه کانونی[۳۴] نامیده می‌شود. اگر ω' دیفرانسیل ناصفر دیگری باشد، آن‌گاه برای یک تابع گویای f خواهیم داشت $\omega' = f\omega$؛

[۳۴] canonical divisor

بنابراین، $(\omega') = W' \equiv W$ و از این‌رو مقسوم‌علیه‌های کانونی، تشکیل یک کلاس هم‌ارزی می‌دهند. این کلاس هم‌چنین با W نمایش داده می‌شود. حال فضای $\mathcal{L}(W)$ را درنظر بگیرید. این فضای توابع گویا (ارجاع به تعریف ۵.۱۰.۲) می‌تواند بر روی یک فضای یک‌ریخت از فرم‌های دیفرانسیل به‌صورت $f \to f\omega$ نگاشته شود. بنابر تعریف $\mathcal{L}(W)$، تصویر f تحت این نگاشت، یک فرم دیفرانسیل منظم است؛ یعنی $\mathcal{L}(W)$ یک‌ریخت با $\Omega[\chi]$ است.

تعریف ۵.۱۰.۳. فرض کنید χ یک خم تصویری هموار روی k باشد. گونای[۳۵] g از χ را به‌صورت $g := l(W)$ تعریف می‌کنیم.

گونای یک خم، نقش مهمی در بخش‌های بعد دارد. برای مشاهده روش‌هایی که بتوان گونای یک خم را تعیین نمود باید به کتابی در زمینه هندسه جبری مراجعه نماییم. در اینجا یک فرمول بدون اثبات، معروف به فرمول پلاکر[۳۶] را بیان می‌کنیم.

قضیه ۶.۱۰.۳. اگر χ یک خم تصویری نامنفرد از درجه d در $\mathbb{P}^2$ باشد، آن‌گاه:

$$g = \frac{1}{2}(d-1)(d-2).$$

بنابراین، خم موجود در مثال ۳.۱۰.۳ شامل گونای ۱ است و با استفاده از تعریف گونا داریم $\mathcal{L}(W) = k$؛ بنابراین، دیفرانسیل‌های منظم روی χ ضرایب اسکالر از دیفرانسیل ω در مثال ۳.۱۰.۳ هستند.

برای ساختن کدها روی خم‌های جبری که کدهای گاپا را تعمیم می‌دهند، به مفهوم "مانده" یک دیفرانسیل در یک نقطه P نیاز خواهیم داشت. این مفهوم از مبحثی که درباره رفتار موضعی یک دیفرانسیل ω داشتیم، تعریف می‌شود. فرض کنید P یک نقطه روی χ، t یک پارامتر موضعی در P و $\omega = f\,dt$ نمایش موضعی ω باشند. تابع f می‌تواند به‌صورت $\sum_i a_i t^i$ نوشته شود. باقی‌مانده $Res_P(\omega)$ از ω در نقطه P را برابر با a_{-1} تعریف می‌کنیم (آن‌چنان که انتظار آن می‌رفت). می‌توان نشان داد که این تعریف جبری از باقی‌مانده، به انتخاب پارامتر موضعی t بستگی ندارد.

یکی از نتایج پایه در نظریه خم‌های جبری، به‌عنوان "قضیه باقی‌مانده[۳۷]" شناخته شده است. ما تنها قضیه را بیان می‌کنیم.

قضیه ۷.۱۰.۳. اگر ω یک دیفرانسیل روی یک خم تصویری هموار χ باشد، آن‌گاه:

$$\sum_{P \in \chi} Res_P(\omega) = 0.$$

---

[۳۵] genus

[۳۶] Plücker formula

[۳۷] residue theorem

۱۰.۴ قضیه ریمن—روچ

قضیه مشهور زیر، معروف به قضیه ریمن—روچ[۳۸] ، تنها یک نتیجه مرکزی در هندسه جبری با کاربردهایی در سایر موضوعات نیست، بلکه کلید نتایج جدید در نظریه کدگذاری هم هست.

قضیه ۱.۱۰.۴. فرض کنید D یک مقسوم‌علیه روی یک خم تصویری هموار از گونای g باشد؛ در این صورت، برای هر مقسوم‌علیه کانونی W داریم:

$$l(D) - l(W - D) = \deg(D) - g + ۱$$

ما اثبات (کاملاً پیچیده) را نمی‌آوریم. این قضیه به ما اجازه می‌دهد تا درجه مقسوم‌علیه‌های کانونی را تعیین کنیم.

نتیجه‌گیری ۲.۱۰.۴. برای یک مقسوم‌علیه کانونی W داریم $\deg(W) = ۲g - ۲$.

اثبات. همواره توابع منظم روی یک خم تصویری ثابت هستند؛ یعنی $\mathcal{L}(۰) = k$، بنابراین، $l(۰) = ۱$. $D = W$ را در قضیه ۱.۱۰.۴ جای‌گزین کنید و نتیجه از تعریف ۵.۱۰.۳ حاصل می‌گردد. □

حال واضح است که چرا در مثال ۷.۱۰.۲ فضای $\mathcal{L}(۲Q)$ تنها دارای بعد ۲ است. با استفاده از قضیه ٦.۱۰.۳، خم χ دارای گونای ۱ است، درجه $W - ۲Q$ منفی است، بنابراین، $l(W - ۲Q) = ۰$. با استفاده از قضیه ۱.۱۰.۴ داریم $l(۲Q) = ۲$.

در ابتدا، قضیه ۱.۱۰.۴ خیلی مفید به‌نظر نمی‌آید. اما نتیجه ۲.۱۰.۴ ابزاری برای به‌کارگیری موفق آن ارائه می‌دهد.

نتیجه‌گیری ۳.۱۰.۴. فرض کنید D یک مقسوم‌علیه روی یک خم تصویری هموار با گونای g باشد و فرض کنید $\deg(D) > ۲g - ۲$؛ در این صورت:

$$l(D) = \deg(D) - g + ۱.$$

[۳۸] Riemann-Roach theorem

اثبات. با استفاده از نتیجه ۲.۱۰.۴، داریم $\deg(W-D) < 0$، بنابراین، با استفاده از قضیه ٦.۱۰.۲ قسمت (۱) داریم $l(W-D) = 0$. □

مثال ۴.۱۰.۴. کد موجود در قضیه ١٦.۱۰.۱ را درنظر بگیرید. صفحه آفین را در یک صفحه تصویری بنشانید و توابع گویا روی خم تعریف شده توسط G را درنظر بگیرید. با استفاده از قضیه بزوت، این خم با خط در بی‌نهایت اشتراک دارد؛ یعنی خط تعریف شده به‌صورت $z = 0$ در m نقطه. اینها قطب‌های ممکن برای توابع گویای ما هستند، هریک با مرتبه حداکثر l؛ بنابراین، در اصطلاح موجود در تعریف ۵.۱۰.۲، فضای توابع گویا، تعریف شده توسط یک مقسوم‌علیه D از مرتبه lm، را داریم. با استفاده از فرمول پلاکر (رابطه ٦.۱۰.۳)، خم تعریف شده توسط G دارای گونای برابر با $\binom{m-1}{2}$ است. اگر $l \geq m-2$، آن‌گاه نتیجه ۳.۱۰.۴ را به‌کار می‌بریم و نتیجه مشابهی همانند قضیه ٦.۱۰.۱ را می‌یابیم. جمله $l(W-D)$ در قضیه ۱.۱۰.۴ می‌تواند برحسب دیفرانسیل‌ها تفسیر شود. تعمیمی از تعریف ۵.۱۰.۲ برای دیفرانسیل‌ها را معرفی می‌کنیم.

تعریف ۵.۱۰.۴. فرض کنید D یک مقسوم‌علیه بر روی یک خم χ باشد؛ تعریف می‌کنیم:

$$\Omega(D) := \{\omega \in \Omega(\chi) : (\omega) - D \succeq 0\},$$

و $\dim_k \Omega(D)$ را با $\delta(D)$ نشان می‌دهیم که شاخص اختصاصی[۳۹] D نامیده می‌شود.
ارتباط آن با توابع، توسط قضیه زیر برقرار می‌گردد.

قضیه ٦.۱۰.۴. $\delta(D) = l(W-D)$.

اثبات. اگر $W = (\omega)$، آن‌گاه نگاشت خطی $\phi : \mathcal{L}(W-D) \to \Omega(D)$ را به‌صورت $\phi(f) := f\omega$ تعریف می‌کنیم. این نگاشت به‌وضوح یک یک‌ریختی است. □

مثال ۷.۱۰.۴. اگر درنظر بگیریم $D = 0$، آن‌گاه با استفاده از تعریف ۵.۱۰.۳، دقیقاً g دیفرانسیل منظم به‌طور خطی مستقل روی یک خم χ وجود دارد؛ بنابراین، دیفرانسیل موجود در مثال ۲.۱۰.۳ هم‌چنان که پس از قضیه ٦.۱۰.۳ ملاحظه شد، تنها دیفرانسیل منظم روی χ (در حد یک عامل ثابت) است.

[۳۹] index of speciality

۱۰.۵ کدها از خم‌های جبری

حال به‌سراغ کاربردهایی در نظریه کدگذاری می‌آییم. الفبای ما مجدداً $\mathbb{F}_q$ می‌باشد. قضایای موجود در بخش قبل را به‌کار خواهیم برد. انطباق‌های کمی نیاز هست، چون برای مثال فضای $\mathcal{L}(D)$ روی یک میدان بسته جبری درنظر گرفته نخواهد شد؛ بلکه روی $\mathbb{F}_q$ درنظر گرفته می‌شود. تمام آن چیزی که لازم است بدانیم این است که قضیه ۱.۱۰.۴ درست باقی می‌ماند. در تعدادی از مثال‌ها، این مطلب درمورد پایه $\mathcal{L}(D)$ (پایه‌ای روی بستار k، شامل چندجمله‌ای‌های روی $\mathbb{F}_q$) واضح خواهد شد.

فرض کنید χ یک خم تصویری نامنفرد روی $\mathbb{F}_q$ باشد. دو نوع از کدهای هندسه جبری از χ را تعریف خواهیم کرد. نوع اول کدهای رید—سولومن را تعمیم می‌دهند، نوع دوم کدهای گاپا را تعمیم می‌دهند. در ادامه، P_1، P_2، ...، P_n نقاط گویا روی χ هستند و D مقسوم‌علیه $P_1 + P_2 + \cdots + P_n$ می‌باشد. علاوه‌براین G مقسوم‌علیه دیگری است که دارای محمل[۴۰] مجزا از D است. اگرچه انجام چنین کاری لازم نیست، اما ما محدودیت‌های بیشتری روی G قرار خواهیم داد؛ یعنی این‌که محمل G نیز شامل نقاط گویاست و علاوه‌براین:

$$2g - 2 < \deg(G) < n. \qquad (1)$$

تعریف ۱.۱۰.۵. کد خطی $C(D,G)$ از درجه n روی $\mathbb{F}_q$ تصویر نگاشت خطی $\alpha : \mathcal{L}(G) \to \mathbb{F}_q^n$ تعریف‌شده به‌صورت $\alpha(f) := (f(P_1), f(P_2), \cdots, f(P_n))$ است.

کدهای با این نوع "کدهای RS گسترش‌یافته هندسی[۴۱]" نامیده می‌شوند.

قضیه ۲.۱۰.۵. کد $C(D,G)$ دارای بعد $k = \deg(G) - g + 1$ و کمترین —فاصله $d \geq n - \deg(G)$ است.

اثبات.

۱) اگر f متعلق به هسته α باشد، آن‌گاه $f \in \mathcal{L}(G-D)$ و با استفاده از قضیه ۶.۱۰.۲ قسمت (۱) این مطلب ایجاب می‌کند که $f = 0$. اکنون حکم با توجه به رابطه ۱ و نتیجه ۳.۱۰.۴ حاصل می‌گردد.

[۴۰] support

[۴۱] geometric generalized RS codes

۲) اگر $\alpha(f)$ دارای وزن d باشد، آن‌گاه $n-d$ نقطه P_i، مانند P_{i_1}، P_{i_2}، $\cdots$، $P_{i_{n-d}}$، وجود دارند، به‌طوری که $f(P_i)=0$؛ بنابراین $f\in\mathcal{L}(G-E)$، که در آن $E=P_{i_1}+\cdots+P_{i_{n-d}}$. از این‌رو $\deg(G)-n+d\geq 0$.

□

به شباهتی که این اثبات با اثبات قضیه ۱.۱۰.۱۶ دارد توجه کنید.

مثال ۳.۱۰.۵. فرض کنید χ خط تصویری روی $\mathbb{F}_q$ باشد. درنظر بگیرید $G:=mQ$، که در آن Q نقطه $(1:0)$ باشد، $n=q$، $P_i=(\alpha_i:1)$ که در آن $\mathbb{F}_q=\{\alpha_1,\alpha_2,\cdots,\alpha_q\}$؛ در این‌صورت، اگر $m=k-1$، آن‌گاه می‌بینیم که $C(D,G)$ کد رید–سولومن گسترش‌یافته، آن‌چنان که در بخش ۶.۸ توصیف شد، است.

مثال ۴.۱۰.۵. فرض کنید χ خم موجود در مثال‌های ۱.۱۰.۱۳ و ۲.۱۰.۷ باشد و $G:=2Q$، که در آن $Q:=(0:1:1)$. درنظر می‌گیریم $n=8$ (بنابراین، D مجموع نقاط گویای باقی‌مانده است). این مختصات‌ها به‌صورت زیر داده شده‌اند:

	Q	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	0	0	0	1	α	$\bar{\alpha}$	1	α	$\bar{\alpha}$
y	1	α	$\bar{\alpha}$	0	0	0	1	1	1
z	1	1	1	1	1	1	0	0	0

,

که در آن $\bar{\alpha}=1+\alpha$. در مثال ۲.۱۰.۷ می‌بینیم که 1 و $x/(y+z)$ پایه‌ای از $\mathcal{L}(2Q)$ روی k و از این‌رو روی $\mathbb{F}_4$ نیز هستند. این مطلب منجر به ماتریس مولد زیر برای $C(D,G)$ می‌گردد:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & \alpha & \bar{\alpha} \end{pmatrix}.$$

با استفاده از قضیه ۱.۱۰.۵، کمترین–فاصله، حداقل برابر با ۶ است و البته از ماتریس مولد دیده می‌شود که $d=6$.

حال به سراغ دومین کلاس از کدهای هندسه جبری می‌آییم. ما این کدها را "کدهای گاپای هندسی[۴۲]" خواهیم نامید.

تعریف ۵.۱۰.۵. کد خطی $C^*(D,G)$ با طول n روی $\mathbb{F}_q$، تصویر نگاشت خطی $\alpha^*:\Omega(G-D)\to\mathbb{F}_q^n$ تعریف شده به‌صورت زیر است:

$$\alpha^*(\eta):=(Res_{P_1}(\eta),Res_{P_2}(\eta),\cdots,Res_{P_n}(\eta)).$$

[۴۲] geometric Goppa codes

پارامترها به‌صورت قضیه زیر داده شده‌اند.

قضیه ۶.۱۰.۵. کد $C^*(D,G)$ دارای بعد $k^* = n - \deg(G) + g - 1$ و کمترین-فاصله $d^* \geq \deg(G) - 2g + 2$ است.

اثبات. مانند قضیه ۲.۱۰.۵، این ادعاها نتیجه مستقیمی از قضیه ۱.۱۰.۴ (ریمن-روچ)، به‌کارگیری قضیه ۵.۱۰.۴ (برقراری ارتباط مابین بعد $\Omega(G)$ و $l(W-G)$) و نتیجه ۲.۱۰.۴ (بیان این مطلب که درجه یک مقسوم‌علیه کانونی برابر با $2g-2$ است) هستند. □

مثال ۷.۱۰.۵. خط تصویری روی $\mathbb{F}_{q^m}$ را درنظر بگیرید. فرض کنید $P_i := (\gamma_i : 1)$، که در آن γ_iها، $0 \leq i \leq n-1$، مشابه با تعریف ۱.۹.۲ هستند. تعریف می‌کنیم $D := P_0 + P_1 + \cdots + P_{n-1}$ و $G := (g)$، که در آن $g(x,y)$ یک فرم همگن از چندجمله‌ای گاپای $g(z)$ در تعریف ۱.۹.۲ است؛ در این‌صورت کد گاپای $\Gamma(L,g)$ از تعریف ۱.۹.۲ زیرکدی (روی $\mathbb{F}_q$) از کد گاپای هندسی $C^*(D,G)$ است. در بخش ۹.۲ مشاهده کردیم که این کد، زیرکدی از دوگان یک کد رید-سولومن تعمیم‌یافته است. این مطلب حالت خاصی از قضیه زیر است.

قضیه ۸.۱۰.۵. کدهای $C(D,G)$ و $C^*(D,G)$، کدهای دوگان هستند.

اثبات. از قضیه ۲.۱۰.۵ و قضیه ۶.۱۰.۵ می‌دانیم که $k + k^* = n$؛ بنابراین، کافی است تا یک کلمه از هر کد را درنظر گرفته و نشان دهیم که حاصل‌ضرب داخلی دو کلمه برابر با صفر است. فرض کنید $f \in \mathcal{L}(G)$، $\eta \in \Omega(G-D)$. با استفاده از تعریف‌های ۱.۱۰.۵ و ۵.۱۰.۵، مشتق $f\eta$ شامل هیچ قطبی مگر احتمالاً قطب‌های مرتبه ۱ در نقاط P_1، P_2، $\cdots$، P_n نمی‌باشد. باقی‌مانده $f\eta$ در P_i برابر با $f(P_i)Res_{P_i}(\eta)$ است. با استفاده از تعریف ۷.۱۰.۳، مجموع مانده‌های $f\eta$ روی روی تمامی قطب‌ها، یعنی روی نقاط P_i، برابر صفر است؛ بنابراین، داریم:

$$0 = \sum_{i=1}^{n} f(P_i)Res_{P_i}(\eta) = < \alpha(f), \alpha^*(\eta) > .$$

□

چندین مولف، کدهای $C^*(D,G)$ را نسبت به کدهای RS هندسی ترجیح می‌دهند، اما غیرمتخصص‌ها در هندسه جبری شاید احساس بهتری درباره چندجمله‌ای‌ها نسبت به مشتق‌ها داشته باشند. در مرجع [۷۳] نشان داده شده است که کدهای $C(D,G)$ برای به‌دست آوردن تمامی کدها کافی می‌باشند. اما، داشتن هر دو کلاس هنگام پرداختن به روش‌های کدگشایی مفید است. این روش‌ها ماتریس بررسی‌توازن را به‌کار می‌برند بنابراین، فرد نیاز به ماتریس مولدی برای کد دوگان دارد.

در پاراگراف بعد، چندین مثال از کدهای هندسی را مورد بحث قرار خواهیم داد. از قبل واضح است که ما برخی کدهای خوب را می‌یابیم. به‌طور مثال، از قضیه ۲.۱۰.۵ می‌بینیم که چنین کدهایی روی یک خم با گونای صفر (خط تصویری) کدهای MDS هستند (ارجاع به بخش ۵.۱). درواقع، قضیه ۲.۱۰.۵ بیان می‌کند که $d \geq n-k+1-g$، بنابراین، اگر g کوچک باشد، آن‌گاه ما نزدیک به کران سینگلتون هستیم (به نتیجه ۱.۵.۲ رجوع شود).

۱۰.۶ برخی کدهای هندسی

می‌دانیم که برای یافتن کدهای خوب، باید کدهای با طول بزرگ بیابیم. با استفاده از روش‌های هندسه جبری، لازم است تا نقاط گویا روی یک خم داده شده را بیابیم. تعداد اینها، کرانی روی طول کد است. یک مشکل اصلی در هندسه جبری، یافتن کران‌هایی برای تعداد نقاط گویا روی یک چندگونا است. به‌جهت درک برخی مثال‌های موجود در این پاراگراف، کران هسه—ویل[۴۳] را بدون اثبات بیان می‌کنیم.

قضیه ۱.۱۰.۶. فرض کنید χ یک خم با گونای g روی $\mathbb{F}_q$ باشد. اگر $N_q(\chi)$ معرف تعداد نقاط گویا روی χ باشد، آن‌گاه:

$$|\, N_q(\chi) - (q+1)\,| \leq 2g\sqrt{q}.$$

درابتدا مثالی می‌آوریم که هیچ مطلب جدیدی را نتیجه نمی‌دهد.

مثال ۲.۱۰.۶. فرض کنید χ خط تصویری روی $\mathbb{F}_{q^m}$ باشد. فرض کنید $n := q^m - 1$. تعریف می‌کنیم $P_0 := (0:1)$، $P_\infty := (1:0)$ و مقسوم‌علیه D را به‌صورت $\sum_{j=1}^{n} P_j$ تعریف می‌کنیم، که در آن $P_j := (\beta^j : 1)$، $(1 \leq j \leq n)$. تعریف می‌کنیم $G := aP_0 + bP_\infty$، $a \geq 0$، $b \geq 0$ (دراینجا β یک ریشه nام اولیه واحد است). با استفاده از قضیه ۱.۱۰.۴، $\mathcal{L}(G)$ دارای بعد $a+b+1$ است و فوراً دیده می‌شود

[۴۳] Hasse-Weil bound

که توابع $(x/y)^i$، $-a \le i \le b$، تشکیل یک پایه از $\mathcal{L}(G)$ را می‌دهند. کد $C(D,G)$ را درنظر بگیرید. یک ماتریس مولد برای این کد شامل سطرهای $(\beta^i, \beta^{۲i}, \cdots, \beta^{ni})$ برای $-a \le i \le b$ است. به‌آسانی بررسی می‌شود که $(c_۰, c_۱, \cdots, c_n)$ یک کدکلمه در $C(D,G)$ است اگر و تنها اگر $\sum_{j=۱}^{n} c_j(\beta^l)^j = ۰$ برای تمامی lهایی که $a < l < n - b$. نتیجه می‌شود که $C(D,G)$ یک کد رید–سولومن است. زیرکد زیرمیدان با مختص‌های متعلق به $\mathbb{F}_q$، یک کد BCH است.

مثال ۳.۱۰.۶. در این مثال، کدهایی را از خم‌های هرمیتی[۴۴] را درنظر می‌گیریم. فرض کنید $q = r^۲ = ۲^l$. یک خم هرمیتی χ در $\mathbb{P}^۲$ روی $\mathbb{F}_q$ با معادله زیر تعریف شده است:

$$x^{r+۱} + y^{r+۱} + z^{r+۱} = ۰. \qquad (۲)$$

با استفاده از قضیه ۳.۱۰.۶، گونای g از χ برابر با $\frac{۱}{۲}r(r-۱) = \frac{۱}{۲}(q - \sqrt{q})$ است. در ابتدا نشان خواهیم داد که χ شامل بیشترین تعداد از نقاط گویاست؛ یعنی با استفاده از قضیه ۱.۱۰.۶ دقیقاً $۱ + q\sqrt{q}$ نقطه گویا. اگر در رابطه ۴.۱۰.۶ یکی از مختصات‌ها برابر با صفر باشد، آن‌گاه بدون کاستن از کلیت، یکی دیگر از آنها برابر با ۱ است و سومی برابر با یکی از جواب‌های $\xi^{r+۱} = ۱$ است که شامل $r+۱$ جواب در $\mathbb{F}_q$ می‌باشد. این مطلب نشان می‌دهد که χ شامل $۳(r+۱)$ نقطه با شرط $xyz = ۰$ است. اگر $xyz \neq ۰$، آن‌گاه ممکن است فرض کنیم $z = ۱$ و y عضوی از $\mathbb{F}_q^*$ باشد به‌طوری که $y^{r+۱} \neq ۰$. برای هر انتخاب y، $r+۱$ جواب x وجود دارد. این مطلب $(r-۲)(r+۱)^۲$ زوج (x,y) را نتیجه می‌دهد؛ بنابراین، χ شامل $۳(r+۱) + (r-۲)(r+۱)^۲ = ۱ + q\sqrt{q}$ نقطه گویاست (ملاحظه می‌کنیم که این نتیجه برای سایر اعداد اول به‌جز ۲ می‌تواند برقرار باشد).

گیریم $G := mQ$، که در آن $Q := (۱ : ۱ : ۰)$ و $q - \sqrt{q} < m < q\sqrt{q}$. کد $C(D,G)$ روی $\mathbb{F}_q$ دارای طول $n = q\sqrt{q}$، بعد $k = m - g + ۱$ و فاصله $d \ge n - m$ است. برای دیدن این‌که این کدها چقدر خوب هستند، مثال $q = ۱۶$ را درنظر می‌گیریم. یک پایه برای $\mathcal{L}(G)$ به‌آسانی یافت می‌شود. توابع $f_{i,j}(x,y,z) := x^i y^j/(y+z)^{i+j}$، $۰ \le i \le ۴$، $۴i + ۵j \le m$، این کار را انجام می‌دهند. درابتدا، مشاهده می‌کنید که $m - ۵ = m - g + ۱$ زوج (i,j) صادق در این شرایط وجود دارد. توابع $x/(y+z)$ و $y/(y+z)$ می‌توانند در روشی دقیقاً مشابه با روش موجود در مثال ۱.۱۰.۱۳، با نشان دادن این‌که $f_{i,j}$ شامل یک قطب مرتبه $۴i + ۵j$ در Q است، رفتار نمایند؛ بنابراین، این توابع مستقل هستند. از این‌رو، این کد به‌آسانی ساخته می‌شود. کدگشایی، سوال دیگری است! بیایید سعی کنیم تا برخی ایده‌ها درباره مرغوبیت این کد را بیابیم. فرض کنید که ما مایل هستیم تا یک پیام طولانی (بگویید $۱۰^۹$ بیت) را روی

[۴۴] Hermitian curves

یک کانال با احتمال خطای $p_e = ۰.۰۱$ (یک کانال کاملاً بد) ارسال نماییم. ما کدگذاری با استفاده از یک کد رید—سولومن با نرخ $\frac{۱}{۲}$ روی $\mathbb{F}_{۱۶}$ را با کدگذاری با استفاده از $C(D,G)$ مقایسه می‌کنیم که در آن $m = ۳۷$ تا مجدداً نرخ $\frac{۱}{۲}$ را داشته باشیم. در این حالت، $C(D,G)$ دارای فاصله ۲۷ است. کد RS حاصل، دارای طول کلمه ۱۶ (پس ۶۴ بیت) و فاصله ۹ است. اگر یک کلمه نادرست دریافت شود، آن‌گاه فرض می‌کنیم که هنگامی که تعداد خطاها را شمارش می‌کنیم، تمامی بیت‌ها اشتباه هستند. برای کد RS مذکور، احتمال خطا پس از کدگشایی به‌سختی برابر با $۳.۱۰^{-۴}$ است (درواقع یک بهبود مطلوب)؛ اما برای کد $C(D,G)$، احتمال خطا پس از کدگشایی کمتر از $۲.۱۰^{-۷}$ است. در این مثال، به‌خاطر سپردن این مطلب مهم است که ما الفبا را ثابت نگه داشته‌ایم (در این حالت $\mathbb{F}_{۱۶}$). اگر ما کد $C(D,G)$ را که در آن، کلمات، رشته‌هایی ۲۵۶ بیتی هستند با یک کد کد RS با نرخ $\frac{۱}{۲}$ روی $\mathbb{F}_{۲۵}$ (کلمات دارای طول ۱۶۰ بیت هستند) مقایسه کنیم، آن‌گاه کد آخری به کارآیی (احتمال خطای $۲.۱۰^{-۶}$) نزدیک خواهد شد و یک کد RS با نرخ $\frac{۱}{۲}$ روی $\mathbb{F}_{۲۶}$ (کلمات دارای طول ۳۸۴ بیت هستند) بهتر عمل می‌کند (تقریباً $۱۰^{-۷}$).

هم‌چنین می‌توانیم کد خود را با یک کد BCH دودویی به طول ۲۵۵ و نرخ $\frac{۱}{۲}$ مقایسه کنیم. کد BCH هنگامی که ما با خطاهای تصادفی مواجه هستیم، برنده می‌شود. اگر ما در حال استفاده از یک کانال با خطای گروهی[۴۵] باشیم، آن‌گاه کد $C(D,G)$ می‌تواند خطاهای گروهی تا طول ۴۶ بیت را به‌دست گیرد (که حداکثر ۱۳ حرف یک کدکلمه را تحت تاثیر قرار می‌دهد) در حالی که کد BCH به‌طور کامل از کار می‌افتد. اگرچه می‌توان درباره این سوال که کدام یک از این مقایسه‌ها مفید است، بحث نمود، این مثال (به‌کار رفته توسط مولف) از جمله مطالبی بود که چندین مهندس را که به‌شدت اعتقاد داشتند که تنها کدهای مفید برای آنها کدهای RS بوده، متقاعد نمود تا به کدهای مطرح از هندسه جبری نظر بیشتری بیندازند. این مطلب به نتایج زیبایی درباره کدگشایی، مساله‌ای که ما در این کتاب از آن صرف‌نظر کردیم، اما به‌وضوح کاربردهایی اساسی دارد، منجرشده است.

مثال ۴.۱۰.۶. فرض کنید χ چهارتایی کلاین روی $\mathbb{F}_۸$ از مثال ۱۲.۱۰.۱ باشد. با استفاده از قضیه ۶.۱۰.۳، گونا برابر با ۳ است. با استفاده از قضیه ۱.۱۰.۶، χ می‌تواند شامل حداکثر ۲۵ نقطه گویا باشد و هم‌چنان که در مثال ۱۲.۱۰.۱ دیدیم، شامل ۲۴ نقطه گویاست؛ (درواقع، با استفاده از اصلاح قضیه ۱.۱۰.۶ توسط سِره[۴۶] [۹۸] این بهینه است). فرض کنید $Q := (۰ : ۰ : ۱)$ و فرض کنید D مجموع ۲۳ نقطه گویای دیگر باشد و $G = ۱۰Q$. از قضیه ۲.۱۰.۵، داریم که $C(D,G)$ دارای بعد $۸ = ۱ + g - ۱۰$ و کمترین—فاصله $d \geq ۲۳ - ۱۰ = ۱۳$ است. حال این کد را با کد بررسی‌توازن واحد $[۴, ۳, ۲]$ به‌صورت زیر متصل کنید. سمبل‌های موجود در کدکلمات $C(D,G)$، عناصر $\mathbb{F}_۸$ هستند

[۴۵] bursty channel

[۴۶] J.-P.Serre

که ما آنها را به‌عنوان بردارهای ستونی با طول ۳ روی $\mathbb{F}_۲$ تفسیر می‌کنیم و سپس بررسی‌توازن را اضافه می‌کنیم. کد حاصل C یک کد $[۹۲, ۲۴, ۲۶]$ دودویی است. کد پنچرشده حاصل، یک کد $[۹۱, ۲۴, ۲۵]$ (ساخته‌شده توسط بارگ[۴۷] [۸۲] در سال ۱۹۸۷) است که رکورد جهانی جدیدی برای کدهای با $n = ۹۱$، $d = ۲۵$ ایجاد نمود. چندین کد دیگر از این نوع در همان مقاله داده شده است.

مثال ۵.۱۰.۶ ما چگونگی ساخت یک ماتریس مولد برای کد موجود در مثال قبل را نشان می‌دهیم. توابع y/z، z/x و x/y را درنظر می‌گیریم. نقاطی که این توابع می‌توانند دارای ریشه یا قطب باشند $P_۱ := (۱ : ۰ : ۰)$، $P_۲ := (۰ : ۱ : ۰)$ و $Q = (۰ : ۰ : ۱)$ هستند. چون خط با معادله $y = ۰$ (در مختصات آفین) در Q بر خم با معادله $x^۳y + y^۳ + x = ۰$ مماس نمی‌باشد، می‌بینیم که y/z یک پارامتر موضعی در Q (ایده‌ای که در مثال‌های اخیر به‌کار رفته است) است. به‌طور مشابه، z/x یک پارامتر موضعی در $P_۱$ است و x/y یک پارامتر موضعی در $P_۲$ می‌باشد. ما رفتار y/z در $P_۱$ و $P_۲$ را بررسی می‌کنیم. در $P_۱$ داریم:

$$\frac{y}{z} = (\frac{z}{x})^۲ \frac{x^۳}{x^۳ + y^۲z},$$

بنابراین، y/z شامل یک ریشه با تکرار ۲ در $P_۱$ است. به‌طور مشابه، در $P_۲$ داریم:

$$\frac{y}{z} = (\frac{y}{x})^۲ \frac{y^۳ + z^۲x}{y^۳},$$

بنابراین، $P_۲$ یک قطب مرتبه ۳ برای تابع y/z است. از این‌رو $(\frac{y}{z}) = ۲P_۱ - ۳P_۲ + Q$. به روش مشابه $(\frac{z}{x}) = P_۱ + ۲P_۲ - ۳Q$ و $(\frac{x}{y}) = -۳P_۱ + P_۲ + ۲Q$ را محاسبه می‌کنیم. از این مقسوم‌علیه‌ها، می‌توانیم نتیجه بگیریم که توابع $(z/x)^i(y/x)^i$ برای $۰ \le ۳i + ۲j \le ۱۰$ و $۰ \le j \le ۲i$، متعلق به $\mathcal{L}(۱۰Q)$ هستند؛ بنابراین، توابع وزنی در $\mathcal{L}(۱۰Q)$ با قطب‌هایی در Q از مرتبه به‌ترتیب ۰، ۳، ۵، ۶، ۷، ۸، ۹ و ۱۰ داریم. از این‌رو آنها مستقل هستند و چون $l(۱۰Q) = ۸$، آنها پایه‌ای از $\mathcal{L}(۱۰Q)$ هستند. با جای‌گزین نمودن مختص‌های نقاط گویای χ در این توابع، ماتریس مولد ۸ در ۲۳ این کد را می‌یابیم.

مثال ۶.۱۰.۶. فرض کنید $\mathbb{F}_۴ = \{۰, ۱, \alpha, \bar{\alpha}\}$، که در آن $\alpha^۲ = \alpha + ۱ = \bar{\alpha}$. خم χ روی $\mathbb{F}_۴$ داده‌شده توسط معادله $x^۲y + \alpha y^۲z + \bar{\alpha}z^۲x = ۰$ را درنظر بگیرید. این خم، یک خم نامنفرد با گونای ۱ است. ۹

[۴۷] A.M.Barg

نقطه گویای آن به‌صورت زیر داده شده است:

	P_1	P_2	P_3	P_4	P_5	P_6	Q_1	Q_2	Q_3
x	۱	۰	۰	۱	۱	۱	α	۱	۱
y	۰	۱	۰	α	$\bar{\alpha}$	۱	۱	α	۱
z	۰	۰	۱	$\bar{\alpha}$	α	۱	۱	۱	α

.

فرض کنید $D := P_1 + P_2 + \cdots + P_6$ و $G := 2Q_1 + Q_2$. ادعا می‌کنیم توابع $x/(x+y+\bar{\alpha}z)$، $y/(x+y+\bar{\alpha}z)$ و $\bar{\alpha}z/(x+y+\bar{\alpha}z)$ پایه‌ای از $\mathcal{L}(G)$ هستند. برای دیدن این مطلب، توجه کنید که صورت این کسرها در Q_1 و Q_2 برابر با صفر نیست و این‌که خط با معادله $x+y+\bar{\alpha}z = 0$ با χ در Q_2 تلاقی دارد و بر χ در Q_1 مماس است. با به‌کار گیری قضیه ۱.۱۰.۵، کد $C(D,G)$ از طول ۶ دارای کمترین—فاصله حداقل ۳ است. اما، این کد درواقع یک کد MDS است، یعنی کد شش‌تایی موجود در بخش ۴.۲.

۱۰.۷ بهبود کران گیلبرت—ورشامو

الفبای $\mathbb{F}_q$ را ثابت نگه می‌داریم. کدهای $C(D,G)$ آن‌چنان که در بخش ۱۰.۵ تعریف شد، با یک خم χ را که شامل $n+1$ نقطه گویای P_1، P_2، $\cdots$، P_n، Q است، درنظر می‌گیریم. گیریم $G = mQ$، به‌طوری که $2g-2 < m < n$. تعریف می‌کنیم $\gamma(\chi) := g/n$. این مطلب توسط فسمن[۴۸]، ولادوت[۴۹] و زینک[۵۰] [۹۸] نشان داده شده است که دنباله‌ای از خم‌های χ وجود دارد، به‌طوری که کدهای هندسی متناظر، دنباله‌ای از کدهایی هستند که بهبودی از قضیه ۸.۵.۱ را نتیجه می‌دهند. آنها قضیه زیر را اثبات نمودند.

قضیه ۱.۱۰.۷. فرض کنید q توانی از یک عدد اول و یک مربع باشد. دنباله‌ای از خم‌های χ_i روی $\mathbb{F}_q$ $(i \in \mathbb{N})$ وجود دارند؛ به‌طوری که χ_i شامل n_i+1 نقطه گویا و گونای g_i است، که در آن $n_i \to \infty$ وقتی $i \to \infty$ و $\gamma(\chi_i) \to (q^{\frac{1}{2}}-1)^{-1} =: \bar{\gamma}$ برای $i \to \infty$.

هم‌چنان که در قضیه ۲.۱۰.۵ دیدیم، کدهای متناظر $C_i := C(D,G)$ روی χ_i دارای نرخ $R_i = (m_i - g_i + 1)/n_i$ و فاصله $d_i \geq n_i - m_i$ هستند؛ بنابراین، با نمادگذاری موجود در بخش ۵.۱ داریم $R_i + \delta_i \geq 1 - \gamma(\chi_i)$. از این‌رو با توجه به قضیه ۱.۱۰.۷ داریم:

---

[۴۸] Tsfasman

[۴۹] Vlăduţ

[۵۰] Zink

قضیه ۲.۱۰.۷. $\delta + \alpha(\delta) \geq 1 - \bar{\gamma}$.

این یک تمرین مقدماتی در حسابان است که آیا خط مستقیم در صفحه (δ, α)، تعریف شده توسط معادله $\delta + \alpha = 1 - \bar{\gamma}$، با خم موجود در قضیه ۸.۵.۱ اشتراک دارد یا خیر. در حالت اشتراک، داریم $q \geq ۴۳$ و چون q باید یک مربع باشد، بهبودی از کران گیلبرت—ورشامو را برای $q \geq ۴۹$ داریم.

۱۰.۸ پیشنهادها

اولین روش‌های کدگشایی جالب در مقاله‌ای توسط جاستسن[۵۱] [۹۱] داده شد. این ایده‌ها توسط اسکروبوگاتو[۵۲] و ولادوت[۵۳] [۹۶] تعمیم داده شدند. از آن پس، این روش‌ها به‌طور قابل ملاحظه‌ای بهبود یافته (ر.ک. مرجع [۸۴]) و توسط فنگ[۵۴] و چندین فرد دیگر ساده شدند. برای مشاهده این نتایج خواننده را به یک مقاله گردآوری و جمع‌بندی در این زمینه، مرجع [۸۹]، ارجاع می‌دهیم.

هم‌چنان که در مقدمه ذکر شد، بسیاری از نتایج این فصل می‌توانند با دوری جستنِ کم و بیش از قضایای عمیق در هندسه جبری، تشریح شوند. این ایده‌ها توسط فنگ[۵۵] و سایرین در مراجع [۸۵] و [۸۶] از نو طراحی شدند و می‌توان آنها را در مرجع [۹۰] یافت.

تعدادی دست‌نوشته درباره محتویات این فصل وجود دارد. ما مرجع [۹۷] را پیشنهاد می‌کنیم که صرفاً یک دیدگاه جبری توسط میدان‌های توابع را به‌کار می‌برد.

بهبودهایی از کران گیلبرت—ورشامو (ر.ک. مرجع [۸۱])، نظریه خم‌های پیمانه‌ای را به‌کار می‌برد. این مطلب یک مطلب اصلی است، ولی با ریاضیات بیشتری، خیلی بیشتر از قضیه ریمن—روچ، درگیر است. نظریه طرح‌ها، یعنی خم‌های روی حلقه‌ها به‌جای میدان‌ها و خواص جبری و تحلیلی خم‌ها، لازم به نظر می‌آید.

کار اخیر گارسیا[۵۶] و استیچتنوث[۵۷] [۸۷]، توصیفی روشن از دنباله خم‌ها با اثبات قضیه ۱.۱۰.۷ به‌وسیله ابزارهایی معتدل‌تر از هندسه جبری ارائه نمود.

---

[۵۱] J. Justesen
[۵۲] A. N. Skorobogatov
[۵۳] S. G. Vlăduţ
[۵۴] G.-L.Feng
[۵۵] G.-L.Feng
[۵۶] Garcia
[۵۷] Stichtenoth

۱۰.۹ مسائل

۱.۱۰.۹. خم موجود در مثال ۷.۱۰.۱ را درنظر بگیرید. رفتار تابع x/z در نقطه $(۰ : ۰ : ۱)$ چگونه است؟

۲.۱۰.۹. نشان دهید که اگر چهارتایی کلاین روی $\mathbb{F}_p$ منفرد باشد، آن‌گاه $p = ۷$. اگر $p = ۷$، آن‌گاه یک نقطه منفرد بیابید.

۳.۱۰.۹. سهمی χ از مثال ۷.۱۰.۱ روی $\mathbb{F}_۴$ را درنظر بگیرید. فرض کنید $g = (z^۳ + xyz)/x^۳$. مقسوم‌علیه g را تعیین کنید.

۴.۱۰.۹. فرض کنید χ یک خم تصویری روی بستار جبری $\mathbb{F}_۲$ تعریف‌شده به‌وسیله معادله $x^۴y + y^۴z + z^۴x = ۰$ باشد. مقسوم‌علیه $f := x/z$ را تعیین کنید.

۵.۱۰.۹. نشان دهید که کد موجود در مثال ۶.۱۰.۶ درواقع هم‌ارز با کد شش‌تایی است.

۶.۱۰.۹. خم موجود در مثال ۴.۱۰.۶ را درنظر بگیرید. قضیه ریمن—روچ درباره $l(۳Q)$ چه می‌گوید؟ نشان دهید $l(۳Q) = ۲$.

فصل ۱۱

کدهای جبری به‌طور مجانبی خوب

۱۱.۱ یک مثال ساده غیرساختنی

در فصل‌های قبل، چندین ساختار از کدها را توصیف کردیم. اگر این کدها را از دیدگاه فصل ۵ درنظر بگیریم، آن‌گاه در مورد این کدها ناامید خواهیم شد. کدهای هادامارد موجود در بخش ۴.۱ دارای $\delta = \frac{1}{2}$ بوده و اگر $n \to \infty$، آن‌گاه نرخ آنان، R، به‌سمت صفر میل می‌کند. برای کدهای همینگ R به ۱ میل می‌کند، اما δ به صفر میل می‌کند. در مورد کدهای BCH نیز داریم $\delta \to 0$، اگر نرخ را ثابت نگه داریم. در تمامی مثال‌ها از کدهایی که مورد بحث قرار دادیم، یک دنباله تعریف شده صریح از این کدها داریم که $\delta \to 0$ یا $R \to 0$.

به عنوان مقدمه‌ای برای بخش بعدی، اینک نشان می‌دهیم که فرد می‌تواند یک تعریف جبری ساده که کدهای خوبی را نتیجه می‌دهد، ارائه نماید. اما این تعریف، ساختاری نیست و در همان نقطه‌ای که در قضیه ۱.۲.۲ به آن رسیدیم، باقی مانده‌ایم. ما کدهای دودویی با نرخ $R = \frac{1}{2}$ را توصیف خواهیم نمود. m را ثابت نگه دارید و یک عضو $\alpha_m \in \mathbb{F}_{2^m}$ را انتخاب کنید. روشی که این عضو انتخاب می‌شود، در زیر تشریح خواهد شد. ما بردارهای $a \in \mathbb{F}_2^m$ را به‌صورت عناصری از $\mathbb{F}_{2^m}$ تعبیر نموده و تعریف می‌کنیم:

$$C_\alpha := \{(a, \alpha a) \mid a \in \mathbb{F}_2^m\}.$$

فرض کنید $\lambda = \lambda_m$ داده شده است. اگر C_α شامل کلمه ناصفر $(a, \alpha a)$ با وزن کمتر از $2m\lambda$ باشد، آن‌گاه این کلمه به‌طور یکتا α را به‌عنوان خارج‌قسمت (در $\mathbb{F}_{2^m}$) تقسیم αa بر a تعیین می‌کند. نتیجه

می‌شود حداکثر $\sum_{i<۲m\lambda} \binom{۲m}{i}$ انتخاب برای α منجر به یک کد C_α خواهد شد که دارای کمترین–فاصله کمتر از $۲m\lambda$ است. حال درنظر می‌گیریم $\lambda := H^{\leftarrow}(\frac{۱}{۲} - (۱/\log m))$. با استفاده از قضیه ۵.۱.۴، تعداد انتخاب‌های "بد" برای α برابر است با $o(۲^m)$، $m \to \infty$؛ بنابراین، برای حداکثر تمامی انتخاب‌های α داریم:

$$d \geq ۲mH^{\leftarrow}(\frac{۱}{۲} - \frac{۱}{\log m}).$$

که در آن d معرف کمترین–فاصله C_α می‌باشد. با قرار دادن $m \to \infty$ و درنظر گرفتن انتخاب‌های مناسب برای α_m، دنباله‌ای از کدهای با نرخ $\frac{۱}{۲}$ را داریم؛ به‌طوری که δ متناظر در رابطه زیر صدق می‌کند:

$$\delta = H^{\leftarrow}(\frac{۱}{۲}) + o(۱), \qquad (m \to \infty).$$

بنابراین، این دنباله به کران گیلبرت ۸.۵.۱ دست می‌یابد. اگر بتوانیم روش صریحی از انتخاب α_m ارائه دهیم، آن‌گاه نتیجه‌ای مهیج حاصل خواهد شد. برای مدت زمانی طولانی، تردیدی جدی وجود داشت که آیا اصلاً ارایه یک ساختار جبری روشن از دنباله‌ای از کدها که در آن هم نرخ و هم d/n از صفر دور شوند، امکان‌پذیر است. در سال ۱۹۷۲، جاستسن[۱] در انجام این کار موفق گردید. ایده اصلی، تغییر ساختاری است که در بالا بیان شد. به‌جای آن (که در انتخاب مشکل است) مقدار α، تمامی مضارب α در یک کدکلمه رخ می‌دهد. تاثیر متوسط، تقریباً به اندازه انتخاب زیرکانه α خوب می‌باشد.

۱۱.۲ کدهای جاستسن

کدهایی که تشریح خواهیم کرد، تعمیمی از کدهای الحاقی[۲] هستند که توسط فُرنی[۳] در مرجع [۲۲] معرفی شدند. ایده آن، ساختن کد در دو مرحله با شروع از یک کد $C_۱$ و تعبیر کلمات $C_۱$ به عنوان سمبل‌های یک الفبای جدید که با آن $C_۲$ ساخته می‌شود، می‌باشد. ما این مطلب را با جزییات بیشتر تشریح می‌کنیم. فرض کنید $C_۲$ کدی روی $\mathbb{F}_{۲^m}$ باشد. سمبل‌های c_i از یک کدکلمه $(c_۰, c_۱, \cdots, c_{n-۱})$ می‌تواند به‌صورت m–تایی‌هایی روی $\mathbb{F}_۲$ نوشته شود؛ یعنی $c_i = (c_{i۱}, c_{i۲}, \cdots, c_{im})$ $(i = ۰, ۱, \cdots, n-۱)$، که در آن $c_{ij} \in \mathbb{F}_۲$. چنین m–تایی، دنباله‌ای از سمبل‌های اطلاعاتی برای یک کلمه متعلق به $C_۱$ معروف به کد داخلی[۴] است. بیایید ساده‌ترین حالت را درنظر بگیریم، که در آن نرخ برابر $\frac{۱}{۲}$ است. متناظر با $c_i = (c_{i۱}, c_{i۲}, \cdots, c_{im})$، کلمه‌ای با طول $۲m$ در کد داخلی داریم.

---

[۱] J. Justesen

[۲] concatenated codes

[۳] G. D. Forney

[۴] inner code

نرخ کد الحاقی، نصف نرخ $C_۲$ است. ایده جاستسن، تغییر کد داخلی $C_۱$ بود؛ یعنی اجازه داشتن برای انتخاب $C_۱$ وابسته به i. مانند بخش قبل، کدهای داخلی طوری انتخاب شده‌اند که کلمه با طول $۲m$ با سمبل‌های c_i آغاز گردد. برای کد خارجی[۵] $C_۲$ ما یک کد رید–سولومن را درنظر می‌گیریم.

جزییات ساختن در ادامه می‌آیند. چون مایلیم که m را به بی‌نهایت میل دهیم، باید یک ساختار ساده برای $\mathbb{F}_{۲^m}$ داشته باشیم. قضیه ۲۴.۱.۱ را به‌کار می‌بریم؛ بنابراین، قرار دهید $m = ۲.۳^{l-۱}$ و $\mathbb{F}_{۲^m}$ را در نمایشی به‌صورت $\mathbb{F}_۲[x]$ (در پیمانه $g(x)$) درنظر بگیرید، که در آن $g(x) = x^m + x^{m/۲} + ۱$. کد رید–سولومن $C_۲$ که کد خارجی است، به‌صورت زیر تعبیر می‌شود (مراجعه به بخش ٦.٨). یک m–تایی از سمبل‌های اطلاعات $(i_۰, i_۱, \cdots, i_{m-۱})$ به‌صورت عضو $i_۰ + i_۱x + \cdots + i_{m-۱}x^{m-۱} \in \mathbb{F}_{۲^m}$ تفسیر می‌شود. K مقدار متوالی m–تایی $a_۰$، $a_۱$، ...، $a_{K-۱}$ را درنظر بگیرید و چندجمله‌ای $a(Z) = a_۰ + a_۱Z + \cdots + a_{K-۱}Z^{K-۱} \in \mathbb{F}_{۲^m}[Z]$ را تشکیل دهید. برای $N := ۲^m - ۱ = ۱, ۲, \cdots, ۲^m - ۱$، $j(x)$ را با $j(x) = \sum_{i=۰}^{m-۱} \varepsilon_i x^i$ نشان دهید، اگر $\sum_{i=۰}^{m-۱} \varepsilon_i ۲^i$ نمایش دودویی j باشد؛ در این‌صورت $j(x)$ در میان عناصر ناصفر $\mathbb{F}_{۲^m}$ تغییر می‌کند. ما اینها را با $a(Z)$ جانشین می‌کنیم؛ بنابراین، دنباله‌ای از N عضو $\mathbb{F}_{۲^m}$ را به‌دست می‌آوریم. این یک کدکلمه در کد خطی $C_۲$ است که دارای نرخ K/N است. چون $a(Z)$ دارای درجه کمتر یا مساوی $K-۱$ است، آن دارای حداکثر $K-۱$ ریشه است؛ یعنی دارای کمترین–فاصله $D \geq N - K + ۱$ (ارجاع به بخش ٦.٨). این یک روش کاملاً ساختاری در تولید دنباله‌ای از کدهای رید–سولومن است. به روشی مشابه آن را تا تشکیل کدهای داخلی ادامه می‌دهیم. اگر c_j نمایش jامین سمبل در یک کدکلمه در کد خارجی باشد (هنوز در نمایش به‌صورت چندجمله‌ای روی $\mathbb{F}_۲$)، آن‌گاه ما آن را با $(c_j, j(x)c_j)$ جای‌گزین می‌کنیم، که در آن، ضرب مجدداً در پیمانه $g(x)$ درنظر گرفته می‌شود. سرانجام ما آن‌را به‌صورت یک $۲m$–تایی از عناصر $\mathbb{F}_۲$ تفسیر می‌کنیم.

تعریف ۱.۱۱.۲. فرض کنید $m = ۲.۳^{l-۱}$، $N = ۲^m - ۱$. K به‌روش مناسب زیر انتخاب خواهد شد؛ $D = N + ۱ - K$. کد دودویی با طول کلمه $n := n_m := ۲mN$ تعریف شده به‌صورت بالا، با φ_m نشان داده می‌شود. این کد، کد جاستسن[٦] گفته می‌شود. بعد φ_m برابر با $k := mK$ و نرخ آن برابر با $\frac{۱}{۲}K/N$ است.

در تحلیل ما از φ_m، ایده مشابهی مانند بخش ۱۱.۱ را به‌کار می‌بریم؛ یعنی این واقعیت که یک $۲m$–تایی ناصفر $(c_j, j(x)c_j)$ واقع در یک کدکلمه φ_m، مقدار j را مشخص می‌کند.

لم ۲.۱۱.۲. فرض کنید $\gamma \in (۰, ۱)$ و $\delta \in (۰, ۱)$. فرض کنید $(M_L)_{L \in \mathbb{N}}$ دنباله‌ای از اعداد طبیعی با

[۵] outer code

[٦] Justesen code

خاصیت $M_L.۲^{-L\delta} = \gamma + o(۱)$ $(L \to \infty)$ باشد. فرض کنید W مجموع وزن‌های M_L کلمه متمایز در $\mathbb{F}_۲^L$ باشد؛ در این صورت:

$$W \geq \gamma L ۲^{L\delta}\{H^{\leftarrow}(\delta) + o(۱)\}, \qquad (L \to \infty).$$

اثبات. برای L به قدر کافی بزرگ، تعریف می کنیم:

$$\lambda := H^{\leftarrow}(\delta - \frac{۱}{\log L}).$$

با استفاده از قضیه ۵.۱.۴ داریم:

$$\sum_{۰ \leq i \leq \lambda L} \binom{L}{i} \leq ۲^{L(\delta - (۱/\log L))}.$$

بنابراین:

$$\begin{aligned} W \geq & \quad \{M_L - \textstyle\sum_{۰ \leq i \leq \lambda L} \binom{L}{i}\}\lambda L \geq \lambda L\{M_L - ۲^{L(\delta-(۱/\log L))}\} \\ = & \quad \lambda L ۲^{L\delta}\{\gamma + o(۱)\} = \gamma L ۲^{L\delta}\{H^{\leftarrow}(\delta) + o(۱)\}, \qquad (L \to \infty). \end{aligned}$$

□

یک نرخ R، $۰ < R < \frac{۱}{۲}$، را انتخاب می‌کنیم. عدد K در تعریف ۱.۱۱.۲، کمترین مقداری درنظر گرفته شده است به‌طوری که $R_m := \frac{۱}{۲}K/N \geq R$. این ما را مطمئن می‌سازد که دنباله کدهای φ_m حاصل از درنظر گرفتن $l = ۱, ۲, \cdots$ در تعریف ۱.۱۱.۲ دارای نرخ $R_m \to \infty$ $(l \to \infty)$ باشد. کمترین–فاصله φ_m چه‌طور است؟ یک کلمه ناصفر در کد خارجی دارای وزن حداقل $D = N - K + ۱$ است.

علاوه‌براین:

$$\begin{aligned} N - K + ۱ > N - K = & \quad N(۱ - ۲R_m) \\ = & \quad (۲^m - ۱)\{۱ - ۲R + o(۱)\}, \qquad (m \to \infty). \end{aligned} \tag{۱}$$

هر سمبل ناصفر در یک کدکلمه از کد خارجی یک $۲m$–تایی $(c_j, j(x)c_j)$ در کدکلمه متناظر c از φ_m است و اینها همگی متفاوت خواهند بود (با استفاده از ملاحظه زیر ۱.۱۱.۲). لم ۲.۱۱.۲ را به‌کار گرفته تا وزن c را تخمین بزنیم. گیریم $L = ۲m$، $\delta = \frac{۱}{۲}$، $\gamma = ۱ - ۲R$ و $M_L = D$. با استفاده از رابطه ۱، شرایط لم، برقرار است؛ بنابراین:

$$w(c) \geq (۱ - ۲R).۲m.۲^m\{H^{\leftarrow}(\frac{۱}{۲}) + o(۱)\}, \qquad (m \to \infty).$$

از این‌رو:

$$d_m/n \geq (1 - 2R)\{H^{\leftarrow}(\frac{1}{2}) + o(1)\}, \quad (m \to \infty).$$

بنابراین، قضیه زیر را ثابت کرده‌ایم.

قضیه ۳.۱۱.۲. فرض کنید $0 < R < \frac{1}{2}$. کدهای جاستسن φ_m تعریف شده در بالا دارای طول کلمه $n = 2m(2^m - 1)$، نرخ R_m و کمترین —فاصله d_m هستند، که در آن:

۱) $R_m \to R$، $(m \to \infty)$؛

۲) $\liminf_{m\to\infty} d_m/n \geq (1 - 2R)H^{\leftarrow}(\frac{1}{2})$.

حال با به‌کارگیری نماد موجود در فصل ۵، برای مقادیر R کمتر از $\frac{1}{2}$ داریم $\delta \geq (1 - 2R)H^{\leftarrow}(\frac{1}{2})$. برای اولین بار، برای $n \to \infty$، δ به صفر میل نمی‌کند.

یک تغییر کوچک در ساختار قبل برای رسیدن به نرخ‌های بزرگ‌تر از $\frac{1}{2}$ لازم است. فرض کنید $0 \leq s < m$ (s را بعداً انتخاب خواهیم کرد). φ_m را درنظر بگیرید. برای هر $2m$—تایی $(c_j, j(x)c_j)$ در کدکلمه c، s سمبل آخر را حذف می‌کنیم. کد حاصل با $\varphi_{m,s}$ نشان داده می‌شود. فرض کنید R ثابت باشد، $0 < R < 1$. برای m و s داده شده، K را کوچک‌ترین عدد صحیحی انتخاب می‌کنیم، که در آن $R_{m,s} := [m/(2m - s)](K/N) \geq R$ (اگر $m(2m - s) \geq R$)، آن‌گاه این کار امکان‌پذیر است). در اثبات قضیه ۳.۱۱.۲، این واقعیت را که کدکلمه c شامل حداقل D تا $2m$—تایی متمایز ناصفر $(c_j, j(x)c_j)$ است، به‌کار بردیم. با استفاده از برش[۷]، $(2m - s)$—تایی‌هایی را به‌دست آورده‌ایم که لزوماً دیگر متمایز نمی‌باشند، اما هر مقدار ممکن، حداکثر 2^s بار رخ خواهد داد؛ بنابراین، حداقل $M_s := 2^{-s}(N - K) = 2^{-s}N(1 - \frac{2m-s}{m}R_{m,s})$ $(2m - s)$—تایی‌های متمایز در یک کدکلمه c از $\varphi_{m,s}$ وجود خواهند داشت.

مجدداً لم ۲.۱۱.۲ را به‌کار می‌بریم؛ این بار با پارامترهای زیر:

$$L = 2m - s, \quad \delta = \frac{m-s}{L}, \quad \gamma = 1 - \frac{2m-s}{m}R, \quad M_L = M_s.$$

فرض کنید $d_{m,s}$ کمترین—فاصله $\varphi_{m,s}$ باشد؛ داریم:

$$d_{m,s} \geq (1 - \frac{2m - s}{m}R)(2m - s)2^{m-s}\{H^{\leftarrow}(\frac{m - s}{2m - s}) + o(1)\}2^s, \quad (m \to \infty)$$

$$\frac{d_{m,s}}{n} \geq (1 - \frac{2m - s}{m}R)\{H^{\leftarrow}(\frac{m - s}{2m - s}) + o(1)\}, \quad (m \to \infty) \qquad (2)$$

[۷] truncating

حال باید انتخابی از s را بیابیم که بهترین نتیجه را تولید نماید. فرض کنید r ثابت باشد، $r \in (\frac{1}{2}, 1)$ و $s := \lfloor m(2r-1)/r \rfloor + 1$. اگر $r \geq R$، آن‌گاه هم‌چنین داریم $m/(2m-s) \geq R$. با توجه به رابطه ۲ داریم:

$$\frac{d_{m,s}}{n} \geq (1 - \frac{R}{r})H^{\leftarrow}(1-r) + o(1)\}, \qquad (m \to \infty) \tag{۳}$$

طرف راست رابطه ۳ بیشترین است، اگر r در رابطه زیر صدق کند.

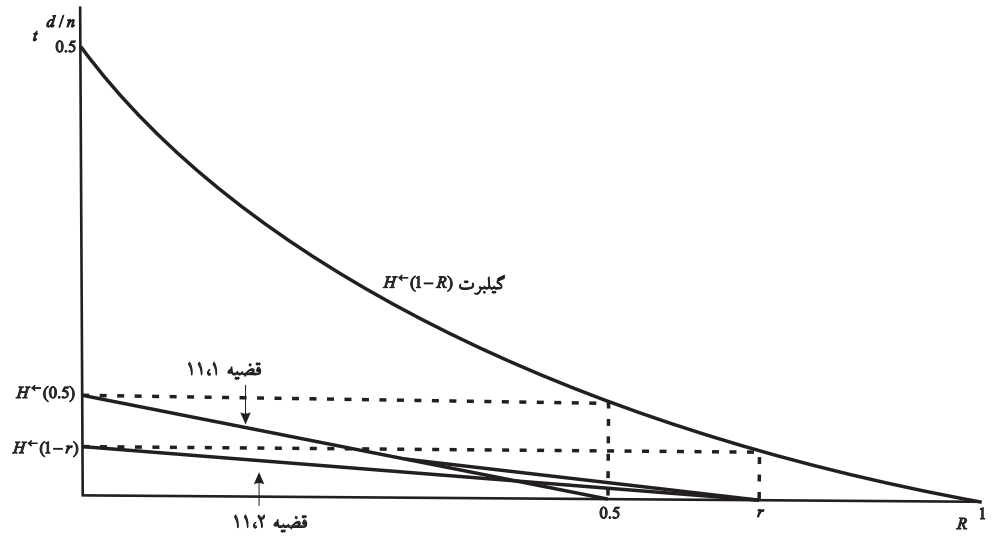
$$R = \frac{r^2}{1 + \log\{1 - H^{\leftarrow}(1-r)\}}. \tag{۴}$$

اگر جواب معادله ۴ کمتر از $\frac{1}{2}$ باشد، آن‌گاه درنظر می‌گیریم $r = \frac{1}{2}$. قضیه زیر، این ساختار را خلاصه می‌کند.

قضیه ۴.۱۱.۲. فرض کنید $0 < R < 1$ و فرض کنید r ماکسیمم $\frac{1}{2}$ و جواب معادله ۴ باشد. فرض کنید $s = \lfloor m(2r-1)/r \rfloor + 1$. کدهای جاستسن $\varphi_{m,s}$ دارای طول کلمه n، نرخ $R_{m,s}$ و کمترین—فاصله $d_{m,s}$ هستند، که در آن:

$$\liminf \frac{d_{m,s}}{n} \geq (1 - \frac{R}{r})H6 \leftarrow (1-r).$$

در شکل ۱۱.۱ کدهای جاستسن را با کران گیلبرت مقایسه می‌کنیم. برای $r > \frac{1}{2}$، این خم، محیط بر خطوطی است که توسط رابطه ۳ داده شده‌اند.



شکل ۱۱.۱:

۱۱.۳ پیشنهادها

ایده واقعاً ساده موجود در بخش ۱۱.۱ تاکنون توجه بسیار کمی را به خود اختصاص داده است. تلاشی جدی‌تر ممکن است به کشف انتخاب‌های صریحی از α که کدهای نسبتاً خوبی را نتیجه می‌دهد، منجر گردد (با این حال، مساله ۱.۱۱.۴ را ببینید). کشف کدهای جاستسن یکی از پیشرفت‌های اساسی در نظریه کدگذاری در سال ۱۹۷۰ بود.

۱۱.۴ مسائل

۱.۱۱.۴. فرض کنید $\mathbb{F}_{۲^۶}$ همان باشد که در بخش ۱۱.۲ نمایش داده شد. نشان دهید هیچ مقداری از α برای ساختار بخش ۱۱.۱ وجود ندارد، به‌طوری که C_α دارای فاصله بیشتر از ۳ باشد. آن‌را با سایر کدهای $[۱۲, k]$ معروف با نرخ بزرگ‌تر یا مساوی $\frac{۱}{۲}$ مقایسه کنید.

۲.۱۱.۴. فرض کنید $\alpha(x)$ چندجمله‌ای با درجه کمتر از k باشد. یک کد $[۲k, k]$ گردشی دوگانه[۸] دودویی شامل تمامی کلمات به شکل $(a(x), \alpha(x)a(x))$ است، که در آن حاصل‌ضرب در پیمانه $(x^k - ۱)$ محاسبه شده است. در این حالت، کد، تحت یک شیفت دوری هم‌زمان از هردو نیمه کلمات، پایا می‌باشد. یک کد $[۱۲, ۶]$ از این نوع بسازید که دارای $d = ۴$ باشد.

۳.۱۱.۴. روش برش‌دادن[۹] موجود در بخش ۱۱.۲ را به‌کار برید تا نشان دهید که ایده موجود در بخش ۱۱.۱ منجر به کدهایی می‌شود که به کران گیلبرت برای هر نرخ R دست می‌یابند.

[۸] double circulant

[۹] truncation

فصل ۱۲

کدهای حسابی

۱۲.۱ کدهای AN

در این فصل، مقدمه‌ای خلاصه‌وار درباره کدهایی که برای بررسی و تصحیح عمل‌گرهای حسابی استفاده‌شده توسط یک کامپیوتر به‌کار رفته‌اند، ارائه خواهیم داد. عمل‌گرها اینک قوانین حساب عادی هستند و به‌عنوان یک نتیجه، این نظریه، کاملاً متفاوت از فصل‌های قبل می‌باشد. اما در چندین موقعیت، شباهتی با نظریه کدهای دوری وجود دارد. در برخی از حالات، ما جزییات اثبات را به خواننده واگذار می‌کنیم. برای اطلاعات بیشتر درباره این موضوع، مراجع مذکور در بخش ۱۲.۴ را ببینید.

عمل‌گرهای حسابی در این فصل با اعدادی که در دستگاه اعداد بر پایه r ($r \in \mathbb{N}$، $r \geq ۲$) نمایش داده شده‌اند، محاسبه شده‌اند. برای اهداف عملی، حالت دودویی ($r = ۲$) و حالت ده‌تایی ($r = ۱۰$) مهم‌ترین می‌باشند. اولین چیزی که ما باید انجام دهیم یافتن یک تابع فاصله مناسب می‌باشد. در فصل‌های قبل، فاصله همینگ را به‌کار بردیم، اما آن یک تابع فاصله مناسب برای اهداف فعلی نمی‌باشد. یک خطا در یک جمع می‌تواند باعث ارقام نادرست بسیاری در پاسخ گردد، به‌دلیل حمل خطا. به یک تابع فاصله نیاز داریم به خطاهای محاسباتی نظیر شود، مشابه با روشی که فاصله همینگ به اشتباهات چاپی موجود در کلمات نظیر می‌شود.

تعریف ۱.۱۲.۱. وزن حسابی[۱] $w(x)$ از یک عدد صحیح x کوچک‌ترین $t \geq ۰$ است، به‌طوری که یک

[۱] arithmetic weight

نمایش:

$$x = \sum_{i=1}^{t} a_i r^{n(i)},$$

با مقادیر صحیح a_i و $n(i)$ وجود داشته باشد که $|a_i| < r$، $n(i) \geq 0$ $(i = 1, 2, \cdots, t)$. فاصله حسابی[۲] دو عدد صحیح به‌صورت زیر تعریف می‌شود:

$$d(x, y) := w(x - y).$$

به‌آسانی چک می‌شود که این درواقع یک متریک روی $\mathbb{Z}$ است. فاصله حسابی تحت انتقال پایاست؛ یعنی $d(x, y) = d(x + z, y + z)$. این مطلب برای فاصله همینگ دو عدد صحیح (با نمایش r–تایی) درست نمی‌باشد. فاصله حسابی حداکثر برابر با فاصله همینگ است.

کدهای C به‌شکل زیر را درنظر خواهیم گرفت:

$$C := \{AN \mid N \in \mathbb{Z}, 0 \leq N < B\},$$

که در آن A و B اعداد صحیح مثبت ثابتی هستند. چنین کدهایی، کدهای AN نامیده می‌شوند. این کدها به‌روش زیر به‌کار رفته‌اند. فرض کنید می‌خواهیم دو عدد صحیح N_1 و N_2 (هردو مثبت و کوچک در مقایسه با B) را اضافه کنیم. این کدها به‌صورت AN_1 و AN_2 کد می‌شوند و سپس این دو عدد صحیح اضافه می‌شوند. فرض کنید S این مجموع باشد. اگر هیچ خطایی ایجاد نگردد، آن‌گاه $N_1 + N_2$ را با تقسیم بر A داریم. اگر S بر A بخش‌پذیر نباشد؛ یعنی خطاهایی ایجاد شده‌اند، به دنبال کدکلمه AN_3 می‌گردیم به‌طوری که $d(S, AN_3)$ کمترین است. مقدار با بیشترین احتمال $N_1 + N_2$ برابر با N_3 است. به منظور قادر بودن برای تصحیح تمامی الگوهای ممکن از حداکثر e خطا، مجدداً کافی و لازم است که کد C دارای کمترین–فاصله بزرگ‌تر یا مساوی $2e + 1$ است. مانند قبل، این مطلب هم‌ارز با این شرط است که C دارای کمترین–وزن حداقل $2e + 1$ باشد. این خصوصیات از کد C برپایه شباهت C با زیرگروه $H := \{AN \mid N \in \mathbb{Z}\}$ از $\mathbb{Z}$ است. گرفتن H به‌عنوان کد، خود ایده خوبی نمی‌باشد، زیرا H دارای کمترین–وزن کمتر یا مساوی ۲ است (مساله ۱.۱۲.۵ را ببینید).

به‌منظور اجتناب از این مشکل، کدهای معروف به کدهای پیمانه‌ای[۳] AN را درنظر خواهیم گرفت. تعریف کنید $m := AB$. حال می‌توانیم C را به‌عنوان زیرگروهی از $\mathbb{Z}/m\mathbb{Z}$ درنظر بگیریم. این مطلب، تغییر تابع فاصله ما را لازم می‌سازد. عناصر $\mathbb{Z}/m\mathbb{Z}$ را به‌صورت بردارهایی از یک گراف Γ_m درنظر بگیرید

[۲] arithmetic distance

[۳] modular codes

و فرض کنید x (در پیمانه m) و x' (در پیمانه m) با استفاده از یک یال به‌هم وصل شوند، اگر و تنها اگر:

$$x - x' \equiv \pm c.r^j \bmod m,$$

برای برخی مقادیر صحیح c, j با شرط $0 < c < r$، $j \geq 0$.

تعریف ۲.۱۲.۱. فاصله پیمانه‌ای[۴] دو عدد صحیح x و y (درنظر گرفته‌شده به‌صورت $\mathbb{Z}/m\mathbb{Z}$) فاصله x و y در گراف Γ_m است. وزن پیمانه‌ای[۵] $w_m(x)$ از x برابر با $d_m(x, 0)$ است. توجه دارید که:

$$w_m(x) = \min\{w(y) \mid y \in \mathbb{Z}, y \equiv x \bmod m\}.$$

اگرچه دراینجا به شباهتی قوی با کدهای خطی دست یافته‌ایم، مشکل دیگری وجود دارد. توجه دارید که هر انتخابی برای m خوب است؛ برای مثال، اگر درنظر بگیریم $r = 3$، $A = 5$، $B = 7$؛ یعنی $m = 35$، آن‌گاه با استفاده از تعریف ۲.۱۲.۱ داریم $d_m(0, 4) = 1$؛ زیرا $3^{10} \equiv 4 \bmod 35$. اما خیلی منطقی نیست که زمانی‌که مجموع اعداد صحیح، کمتر از ۳۵ باشد، خطاها را در مکان متناظر با 3^{10} درنظر بگیریم. محدود کردن j در تعریف یال‌های Γ_m نیز زیان‌بار است. ثابت می‌شود که اگر درنظر بگیریم $m = r^n - 1$ ($n \in \mathbb{Z}$، $n \geq 2$)، آن‌گاه می‌توانیم به نظریه‌ای قابل‌قبول دست یابیم. در عمل نیز، این انتخاب خوبی است؛ زیرا بسیاری از کامپیوترها محاسبات را در پیمانه $2^n - 1$ انجام می‌دهند.

هر عدد صحیح x دارای نمایش یکتایی به‌صورت زیر است:

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \bmod r^n - 1,$$

که در آن $c_i \in \{0, 1, \cdots, r-1\}$ ($0 \leq i < n$) و تمامی c_iها به‌طور هم‌زمان صفر نمی‌باشند؛ بنابراین، $\mathbb{Z}/(r^n - 1)$ می‌تواند به‌صورت مجموعه‌ای از کلمات ناصفر به طول n روی الفبای $\{0, 1, \cdots, r-1\}$ تفسیر شود. البته لازم نیست که صفر را خارج کنیم، اگر درنظر گرفته باشیم $m = r^n$؛ که مجدداً انتخابی عملی است، زیرا بسیاری از کامپیوترها در پیمانه 2^n کار می‌کنند. اما زمانی که $r = 2$ و $m = 2^n$، نمی‌توانیم انتظار کدهای خوبی را داشته باشیم. مجبوریم فرض کنیم $A = 2^k$، برای یک k و پس از آن کد C شامل مقادیر صحیح $\sum_{i=0}^{n-1} c_i 2^i$، $c_i \in \{0, 1\}$ است، که در آن $c_0 = c_1 = \cdots = c_{k-1} = 0$. یک مقدار صحیح x (در پیمانه B) با اضافه‌کردن k تا صفر به نمایش آن، کد می‌گردد. این روش هیچ هدفی را دنبال نخواهد کرد. برای مقدار دلخواه r، ایرادهای مشابه وجود دارد. خواننده باید خود را قانع کند که

[۴] modular distance

[۵] modular weight

در حالت $AB = m = r^n - ۱$، فاصله‌پیمانه‌ای، یک تابع طبیعی برای محاسبه در $\mathbb{Z}/m\mathbb{Z}$ است و این که C به‌صورت یک کد خطی عمل می‌کند. در واقع، حتی یک شباهت قوی‌تر با فصل‌های اخیر داریم.

تعریف ۳.۱۲.۱. یک کد AN دوری[۶] به طول n و پایه r، یک زیرگروه C از $\mathbb{Z}/(r^n - ۱)$ است. چنین کدی یک ایده‌آل اصلی در این حلقه است؛ یعنی مقادیر صحیح A و B وجود دارند؛ به‌طوری که $AB = r^n - ۱$ و

$$C = \{AN \mid N \in \mathbb{Z}, ۰ \leq N < B\}.$$

مانند بخش ۶.۱، A را مولد[۷] کد C می‌نامیم. تا به‌حال، این مطلب برای خواننده تعجب‌انگیز نبوده که ما درابتدا به کدهای C با یک نرخ بزرگ $((۱/n)\log_r B =)$ و یک کمترین—فاصله بزرگ علاقه‌مند شدیم. اصطلاح موجود در تعریف ۳.۱۲.۱ مطابق با تعریف ۱.۶.۱ می‌باشد. اگر $x \in C$، آن‌گاه $rx \bmod r^n - ۱$ نیز یک کدکلمه است، زیرا C یک گروه است و $rx \bmod r^n - ۱$ در واقع یک شیفت دوری از x است (هردو در پایه r نمایش داده شده‌اند). عدد صحیح B می‌تواند با چندجمله‌ای بررسی یک کد دوری مقایسه شود.

ایده کدهای نادوری می‌تواند به روش یکسانی با درنظر گرفتن $m = r^n + ۱$ و سپس درنظر گرفتن زیرگروه‌های $\mathbb{Z}/m\mathbb{Z}$ گسترش یابد.

مثال ۴.۱۲.۱. فرض کنید $r = ۲$، $n = ۱۱$؛ در این‌صورت $m = r^n - ۱ = ۲۰۴۷$. فرض می‌کنیم $A = ۲۳$، $B = ۸۹$. کد AN دوری شامل ۸۹ مضرب از ۲۳ تا ۲۰۴۷ را به‌دست می‌آوریم. ۲۲ روش برای ساختن یک خطا، متناظر با اعداد صحیح $\pm ۲^j$ $(۰ \leq j < ۱۱)$ وجود دارد. اینها دقیقاً اعداد صحیح در پیمانه ۲۳ به‌جز صفر هستند؛ بنابراین، هر مقدار صحیح در بازه $[۱, ۲۰۴۷]$ دارای فاصله‌پیمانه‌ای ۰ یا ۱ تا دقیقاً یک کدکلمه است؛ بنابراین، این کد AN دوری، کامل[۸] است. این تعمیمی از کدهای همینگ است.

---

[۶] cyclic

[۷] generator

[۸] perfect

۱۲.۲ وزن پیمانه‌ای و حسابی

به منظور قادر بودن برای ساخت کدهای AN دوری که بیشتر از یک خطا را تصحیح می‌کنند نیاز به روشی آسان برای محاسبه وزن پیمانه‌ای یا حسابی یک عدد صحیح داریم.

با استفاده از تعریف ۱.۱۲.۱، هر عدد صحیح x می‌تواند به‌صورت زیر نوشته شود:

$$x = \sum_{i=1}^{w(x)} a_i r^{n(i)},$$

با مقادیر صحیح a_i، $n(i)$، $|a_i| < r$، $n(i) \geq 0$ $(i = 1, \cdots, w(x))$. یافتن مثال‌هایی که نشان می‌دهد این نمایش یکتا نیست، آسان می‌باشد. ما محدودیت‌های بیشتری روی ضرایبی که نمایش را یکتا می‌سازد، قرار خواهیم داد.

تعریف ۱.۱۲.۲. فرض کنید $b \in \mathbb{Z}$، $c \in \mathbb{Z}$، $|b| < r$ و $|c| < r$. زوج (b, c) قابل‌قبول[۹] نامیده می‌شود، اگر یکی از شرایط زیر برقرار باشد:

۱) $bc = 0$؛

۲) $bc > 0$ و $|b + c| < r$؛

۳) $bc < 0$ و $|b| > |c|$.

توجه دارید که اگر $r = 2$، آن‌گاه ما باید احتمال (۱) را داشته باشیم؛ بنابراین، یک نمایش $x = \sum_{i=0}^{\infty} c_i 2^i$ به‌طوری که تمامی زوج‌های (c_{i+1}, c_i) قابل‌قبول باشند، دارای هیچ دو رقم ناصفر مجاوری نمی‌باشند. این منجر به نام فرم غیرمجاور[۱۰] (NAF) می‌گردد که ما اینک آن‌را تعمیم می‌دهیم.

تعریف ۲.۱۲.۲. نمایش:

$$x = \sum_{i=0}^{\infty} c_i r^r,$$

با $c_i \in \mathbb{Z}$، $|c_i| < r$ برای تمامی iها و $c_i = 0$ برای تمام iهای بزرگ، یک NAF برای x نامیده می‌شود، اگر برای هر $i \geq 0$، زوج (c_{i+1}, c_i) قابل قبول باشد.

---

[۹] admissible

[۱۰] nonadjacent form

قضیه ۳.۱۲.۲. هر عدد صحیح x شامل دقیقاً یک NAF است. اگر این نمایش به صورت:

$$x = \sum_{i=0}^{\infty} c_i r^i,$$

باشد، آن‌گاه:

$$w(x) = |\{i \,|\, i \geq 0, c_i \neq 0\}|.$$

اثبات.

۱) فرض کنید x به‌صورت $\sum_{i=0}^{\infty} b_i r^i$، $|b_i| < r$ نمایش داده شود. فرض کنید i کمترین مقداری باشد که زوج (b_{i+1}, b_i) قابل‌قبول نباشد. بدون کاستن از کلیت $b_i > 0$ (درغیر این‌صورت $x-$ را درنظر بگیرید). b_i را با $b'_i := b_i - r$ جای‌گزین کنید و b_{i+1} را با $b'_{i+1} := b_{i+1} + 1$ (اگر $b_{i+1} + 1 = r$، آن‌گاه این‌کار را ادامه می‌دهیم). اگر $b_{i+1} > 0$ آن‌گاه داریم $b'_{i+1} = 0$ یا $b'_i b'_{i+1} < 0$ و $|b'_i| = r - b_i > b_{i+1} + 1 = b'_{i+1}$ چون (b_i, b_{i+1}) قابل‌قبول نبوده است. بنابراین، (b'_{i+1}, b'_i) قابل‌قبول نیست و به روشی مشابه می‌توان بررسی کرد که (b'_{i+1}, b'_i) قابل‌قبول است. در این روش می‌توانیم یک NAF بسازیم و در این فرایند، وزن این نمایش افزایش نمی‌یابد.

۲) تنها مطلبی که باقی می‌ماند این است که NAF یکتاست. فرض کنید برخی x ها دارای دو نمایش به‌صورت $x = \sum_{i=0}^{\infty} c_r^i = \sum_{i=0}^{\infty} c'^i_r$ باشند. بدون کاستن از کلیت ممکن است فرض کنیم $c_0 \neq c'_0$، $c_0 > 0$. بنابراین، $c'_0 = c_0 - r$. نتیجه می‌شود که $c'_1 \in \{c_1 + 1 - r, c_1 + 1, c_1 + 1 + r\}$. اگر $c'_1 = c_1 + 1 - r$، آن‌گاه $c_1 \geq 0$؛ بنابراین، $c_0 + c_1 \leq r - 1$. چون $c'_0 c'_1 > 0$ باید داشته باشیم $r < -c'_0 - c'_1$، یعنی $r < r - c_0 + r - c_1 - 1$، بنابراین، $c_0 + c_1 > r - 1$ که تناقض است. به روشی مشابه فرض‌های $c'_1 = c_1 + 1$، به‌ترتیب $c'_1 = c_1 + 1 + r$ به تناقض منجر می‌گردد؛ بنابراین، NAF یکتاست. □

یک روش مستقیم برای یافتن NAF یک عدد صحیح x در قضیه بعد آمده است.

قضیه ۴.۱۲.۲. فرض کنید $x \in \mathbb{Z}$، $x \geq 0$. فرض کنید نمایش‌های $r-$تایی $(r+1)x$ و x به‌صورت زیر باشد:

$$(r+1)x = \sum_{j=0}^{\infty} a_j r^j, \quad x = \sum_{j=0}^{\infty} b_j r^j.$$

با $a_j, b_j \in \{۰, ۱, ..., r-۱\}$ برای تمامی jها و $a_j = b_j = ۰$ برای jهای به‌اندازه کافی بزرگ؛ بنابراین، NAF برای x به‌صورت زیر است:

$$x = \sum_{j=۰}^{\infty} (a_{j+۱} - b_{j+۱}) r^j.$$

اثبات. ما اعداد a_j را با اضافه‌نمودن $\sum_{j=۰}^{\infty} b_j r^j$ و $\sum_{j=۰}^{\infty} b_j r^{j+۱}$ محاسبه می‌کنیم. فرض کنید دنباله انتقالی به‌صورت $\varepsilon_۰, \varepsilon_۱, \cdots$ باشد؛ بنابراین، $\varepsilon_۰ = ۰$ و $\varepsilon_{i+۱} := \lfloor (\varepsilon_{i-۱} + b_{i-۱} + b_i)/r \rfloor$. داریم $a_i = \varepsilon_{i-۱} + b_{i-۱} + b_i - \varepsilon_i r$. اگر $a_i - b_i$ را با c_i نشان دهیم، آن‌گاه $c_i = \varepsilon_{i-۱} + b_{i-۱} - \varepsilon_i r$. حال باید بررسی کنیم که آیا $(c_i, c_{i+۱})$ یک زوج قابل قبول است یا نه. این مطلب که $|c_{i+۱} + c_i| < r$، نتیجه‌ای بدیهی از تعریف ε_i است. فرض کنید $c_i > ۰$، $c_{i+۱} < ۰$؛ بنابراین، $\varepsilon_i = ۰$. پس داریم $c_i = \varepsilon_{i-۱} + b_{i-۱}$، $c_{i+۱} = b_i - r$ و شرط $|c_{i+۱}| > |c_i|$ هم‌ارز با $b_i + \varepsilon_{i-۱} + b_{i-۱} < r$ است؛ یعنی $\varepsilon_i = ۰$. حالت آخر مشابه است. □

NAF متناظر با x به ما یک تخمین ساده از x آن‌چنان که در قضیه بعد نشان داده شده است، ارائه می‌دهد.

قضیه ۵.۱۲.۲. اگر بیشترین مقدار i را به‌طوری که $c_i \neq ۰$ در یک NAF برای x با $i(x)$ نشان دهیم و تعریف کنیم $i(۰) =: -۱$، آن‌گاه:

$$i(x) \leq k \Leftrightarrow |x| < \frac{r^{k+۲}}{r+۱}.$$

اثبات کاملاً مقدماتی این قضیه را به خواننده واگذار می‌کنیم.

حال، از بخش ۱۲.۱ واضح خواهد بود که این ایده‌ها را باید به روش مشابهی برای نمایش‌های پیمانه‌ای گسترش دهیم؛ داریم $m = r^n - ۱$، $n \geq ۲$.

تعریف ۶.۱۲.۲. نمایش:

$$x \equiv \sum_{i=۰}^{n-۱} c_i r^i \bmod m,$$

با $c_i \in \mathbb{Z}$، $|c_i| < r$ یک CNAF (= NAF دوری) برای x نامیده می‌شود، اگر $(c_{i+۱}, c_i)$ برای $i = ۰, ۱, \cdots, n-۱$ قابل‌قبول باشد؛ بنابراین، $c_n := c_۰$.

دو قضیه بعدی از CNAFها توسیع‌های سرراست از قضیه ۳.۱۲.۲ می‌باشند و می‌توانند از این قضیه یا به‌کارگیری قضیه ۴.۱۲.۲ به‌دست آیند. اندکی دقت به دلیل وجود استثنا لازم است، اما خواننده نباید با اثبات این قضایا مشکلی داشته باشد.

قضیه ۷.۱۲.۲. هر عدد صحیح x دارای یک CNAF در پیمانه m است؛ این CNAF یکتاست، مگر این‌که:

$$(r+۱)x \equiv ۰ \not\equiv x \bmod m,$$

که در این حالت، دو CNAF برای x (در پیمانه m) وجود دارد. اگر $x \equiv \sum_{i=۰}^{n-۱} c_i r^i \bmod m$ یک CNAF برای x باشد، آن‌گاه:

$$w_m(x) = |\{i \mid ۰ \le i < n, c_i \neq ۰\}|.$$

قضیه ۸.۱۲.۲. اگر $(r+۱)x \equiv ۰ \not\equiv x \bmod m$، آن‌گاه $w_m(x) = n$؛ مگر این‌که $n \equiv ۰ \bmod ۲$ و $x \equiv \pm[m/(r+۱)] \bmod m$ که در این حالت $w_m(x) = \frac{۱}{۲}n$.

قضیه ۹.۱۲.۲. اگر یک NAF برای x داشته باشیم، به‌طوری که $c_{n-۱} = ۰$، آن‌گاه شرط اضافی برای این‌که این NAF یک CNAF باشد، برقرار است؛ بنابراین، قضیه ۵.۱۲.۲ قضیه زیر را ایجاب می‌کند. یک عدد صحیح x شامل یک CNAF با $c_{n-۱} = ۰$ است، اگر و تنها اگر یک $y \in \mathbb{Z}$ با $x \equiv y \bmod m$، $|y| \le m/(r+۱)$ وجود داشته باشد.

این قضیه به روش دیگری برای یافتن وزن پیمانه‌ای یک عدد صحیح منجر می‌شود.

قضیه ۱۰.۱۲.۲. برای $x \in \mathbb{Z}$ داریم:

$$w_m(x) = |\{j \mid ۰ \le j < n, \exists y \in \mathbb{Z},\ m/(r+۱) < y \le m/(r+۱), y \equiv r^j x \bmod m\}|.$$

اثبات. به‌وضوح یک CNAF برای rx یک شیفت دوری از یک CNAF برای x است؛ یعنی $w_m(rx) = w_m(x)$. فرض کنید $x \equiv \sum_{i=۰}^{n-۱} c_i r^i \bmod m$ یک CNAF باشد و $c_{n-۱-j} = ۰$؛ در این‌صورت $r^j x$ دارای یک CNAF با صفر به‌عنوان ضریب $r^{n-۱}$ است. با استفاده از قضیه ۹.۱۲.۲ این حالت مطلوب است، اگر وجود داشته باشد یک y با شرط $y \equiv r^j x \bmod m$ و $|y| \le m/(r+۱)$. چون وزن پیمانه‌ای برابر با تعداد ضرایب ناصفر است، ادعا حاصل می‌گردد؛ مگر این‌که ما در یکی از حالات استثنایی قضیه ۷.۱۲.۲ باشیم، اما در این‌صورت نتیجه با توجه به قضیه ۸.۱۲.۲ نتیجه می‌شود. □

۱۲.۳ کدهای مندلبوم–باروس

حال کلاسی از کدهای AN دوری تصحیح‌کننده چند خطا را معرفی می‌کنیم که تعمیمی از کدهای معرفی‌شده توسط باروس[۱۱] و مندلبوم[۱۲] هستند. در ابتدا نیاز به قضیه‌ای درباره وزن پیمانه‌ای در کدهای AN دوری داریم.

قضیه ۱.۱۲.۳. فرض کنید $C \subset \mathbb{Z}/(r^n - ۱)$ یک کد AN دوری با مولد A باشد و فرض کنید:

$$B := (r^n - ۱)/A = |c|.$$

در این‌صورت:

$$\sum_{x \in C} w_m(x) = n(\lfloor \frac{rB}{r+۱} \rfloor - \lfloor \frac{B}{r+۱} \rfloor).$$

اثبات. فرض کنیم که هر $x \in C$ شامل یک CNAF یکتای زیر باشد:

$$x \equiv \sum_{i=۰}^{\infty} c_{i,x} r^i \bmod r^n - ۱.$$

حالتی که C شامل یک عضو با دو CNAF است کمی مشکل‌تر است. ما آن‌را به خواننده واگذار می‌کنیم. باید تعداد ضرایب ناصفر $c_{i,x}$، که آنها را به‌عنوان عناصر یک ماتریس درنظر می‌گیریم، تعیین کنیم؛ جایی که در آن $۰ \leq i \leq n - ۱$ و $x \in C$. چون C دوری است هر ستون این ماتریس شامل تعداد یکسانی صفر است؛ بنابراین، تعداد تعیین‌شده، مساوی با $n \mid \{x \in C | c_{n-۱,x} \neq ۰\} \mid$ است. با استفاده از قضیه ۹.۱۲.۲ داریم $c_{n-۱,x} \neq ۰$، اگر و تنها اگر وجود داشته باشد یک $y \in \mathbb{Z}$ به‌طوری که $y \equiv x \bmod r^n - ۱$ و $m/(r+۱) < y \leq mr/(r+۱)$. چون x دارای شکل AN (در پیمانه $r^n - ۱$) $(۰ \leq N < B)$ است، باید داشته باشیم $B/(r+۱) < N \leq Br/(r+۱)$. □

عبارت موجود در قضیه ۱.۱۲.۳ تقریباً برابر با $n|c|[(r-۱)/(r+۱)]$ است؛ بنابراین، این قضیه با نتیجه اخیرمان:

$$\sum_{x \in C} w(x) = n|c|.\frac{q-۱}{q},$$

برای یک کد خطی C، شباهت دارد.

قضیه بعدی کدهای مندلبوم–باروس تعمیم یافته را معرفی می‌کند و نشان می‌دهد که این کدها هم‌ارز می‌باشند.

---

[۱۱] J. T. Barrows

[۱۲] D. Mandelbaum

قضیه ۲.۱۲.۳. فرض کنید B یک عدد اول باشد که بر r بخش‌پذیر نیست با این خاصیت که $(\mathbb{Z}/B\mathbb{Z})$ توسط عناصر r و -۱ تولید شده است. فرض کنید n یک عدد صحیح مثبت با خاصیت $r^n \equiv ۱ \bmod B$ باشد و $A := (r^n - ۱)/B$؛ در این‌صورت کد $C \subset \mathbb{Z}/(r^n - ۱)$ تولید شده توسط A یک کد هم‌ارز با فاصله زیر است:

$$\frac{n}{(B-۱)}(\lfloor \frac{rB}{r+۱} \rfloor - \lfloor \frac{B}{r+۱} \rfloor).$$

اثبات. فرض کنید $x \in C$، $x \neq ۰$؛ در این‌صورت $x = AN \bmod r^n - ۱$، به‌طوری که $N \not\equiv ۰ \bmod B$. فرض‌های ما ایجاب می‌کنند که یک j به‌طوری که $N \not\equiv \pm r^j \bmod B$، وجود دارد؛ بنابراین، $w_m(x) = w_m(\pm r^j A) = w_m(A)$. این مطلب نشان می‌دهد که C هم‌فاصله[۱۳] است؛ بنابراین، وزن ثابت، از قضیه ۱.۱۲.۳ نتیجه می‌شود. □

کدهای مندلبوم–باروس متناظر با کدهای دوری مینیمال M_i^- از بخش ٦.۲ هستند. توجه دارید که این کدها دارای طول کلمه حداقل $\frac{۱}{۲}(B-۱)$ هستند که این مقدار نسبت به تعداد کدکلمات که همان B است، بزرگ است؛ بنابراین، برای اهداف عملی، این کدها به‌نظر مهم نمی‌رسند.

۱۲.۴ پیشنهادها

خواننده علاقه‌مند به جزییات بیشتر درباره کدهای حسابی به مرجع [۵۳] توسط پترسون[۱۴] و ولدون[۱۵] و مرجع [۴۸] توسط مسی[۱٦] و گارسیا[۱۷] و مرجع [۵۸] توسط رائو[۱۸] ارجاع داده می‌شود. کدهای AN دوری کامل تصحیح‌کننده یک خطا به‌طور وسیعی مورد مطالعه قرار گرفته‌اند. در این زمینه مرجع [۲۸] توسط گوتو[۱۹]، مرجع [۲۹] توسط گوتو و فاکومارا[۲۰] و مرجع [۳۱] توسط گریتسنکو[۲۱] را معرفی می‌کنیم. یک کد AN دوری کامل تصحیح‌کننده یک خطا با $r = ۱۰$ یا $r = ۲^k$ $(k > ۱)$ وجود ندارد.

---

[۱۳] equidistance
[۱۴] W. W. Peterson
[۱۵] E. J. Weldon
[۱٦] J. L. Massey
[۱۷] O. N. Garcia
[۱۸] T. R. N. Rao
[۱۹] M. Goto
[۲۰] T. Fukumara
[۲۱] V. M. Gritsenko

برای دیدن جزییات بیشتر درباره NAF و CNAF، خواننده را به مراجع [۱۴] و [۱۵] توسط کلارک[۲۲] و لیانگ[۲۳] ارجاع می‌دهیم. منابعی برای کدهای مندلبوم–باروس دودویی می‌توانند در مرجع [۴۸] یافت شوند. کلاسی از کدهای AN دوری وجود دارد که شامل برخی شباهت‌ها با کدهای BCH است. این کدها می‌تواند در مرجع [۱۲] توسط چِن[۲۴]، چِین[۲۵] و لیو[۲۶]، یافت شوند.

برای یافتن اطلاعات بیشتر درباره کدهای حسابی کامل، خواننده را به کار مشترکی که عنوان آن توسط لنسترا[۲۷] در سمینار دلنگی–پیزت–پویتو[۲۸] (نظریه اعداد[۲۹]، ۱۹۷۷/۷۸) مطرح شده، ارجاع می‌دهیم.

۱۲.۵ مسائل

۱.۱۲.۵. ثابت کنید $\min\{w(AN) \mid N \in \mathbb{Z}, N \neq 0\} \leq 2$ برای هر $A \in \mathbb{Z}$، اگر w همانند تعریف ۱.۱۲.۱ تعریف شده باشد.

۲.۱۲.۵. مثال ۴.۱۲.۱ را توسعه دهید. یک مثال با $r = 3$ بیابید.

۳.۱۲.۵. نمایش‌های سه‌تایی در پیمانه $3^6 - 1$ را درنظر بگیرید. یک CNAF برای ۴۵۵ با به‌کارگیری روش موجود در اثبات قضیه ۳.۱۲.۲ بیابید.

۴.۱۲.۵. کلمات کد مندلبوم–باروس با $B = 11$، $r = 3$، $n = 5$ تعیین کنید.

---

[۲۲] W. E. Clark
[۲۳] J. J. Liang
[۲۴] C. L. Chen
[۲۵] R. T. Chien
[۲۶] C. K. Liu
[۲۷] H. W. Lenstra
[۲۸] Séminaire Delange-Pisot-Poitou
[۲۹] Théorie des Nombres

فصل ۱۳

کدهای کانولوشن

۱۳.۱ مقدمه

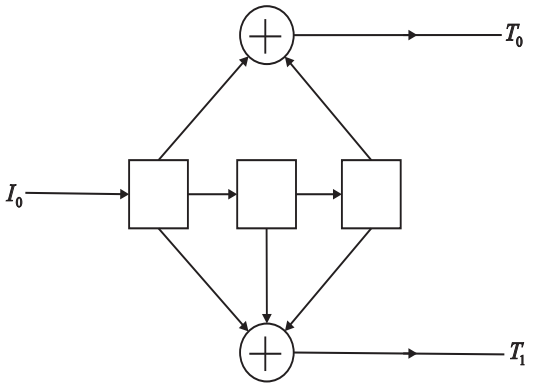
کدهایی که دراین فصل درنظر می‌گیریم کاملاً با کدهایی که در فصل‌های قبل مطالعه کردیم، متفاوت هستند. آنها کدهای بلوکی نیستند، به‌این معنی که کلمات، طول ثابتی ندارند. اگرچه این کدها شباهت‌ها و ارتباط‌هایی با کدهای بلوکی دارند، اما یک تفاوت بزرگ بین آنها وجود دارد، به این معنا که تئوری ریاضی کدهای کانولوشن به‌خوبی توسعه نیافته است. این یکی از دلایلی است که ریاضی‌دانان به سختی به این کدها علاقه‌مند می‌شوند.

به هر حال، ما در مقدمه خود، مخابره اطلاعات توسط ماهواره‌ها را به‌عنوان یکی از مثال‌های بسیار موثر از کاربرد نظریه کدگذاری معرفی کردیم که در حال حاضر یکی از مهم‌ترین ابزاری که در این زمینه استفاده می‌شود، کدگذاری کانولوشن است. بنابراین، یک مقدمه کوتاه در مورد این موضوع، مناسب به‌نظر می‌رسد. برای مقایسه کدهای گلی و کانولوشن، خواننده را به مرجع [۵۱] بخش ۱۱.۴ ارجاع می‌دهیم. پس از بخش‌های مقدمه، کمی بیشتر به جنبه‌های ریاضی این موضوع می‌پردازیم. زمینه اصلی تحقیق محققان درباره این کدها، کاهش پیچیدگی کدگشایی می‌باشد. ما به این جنبه‌ها کاری نداریم و خواننده علاقه‌مند را به دست نوشته‌های مربوط در این زمینه ارجاع می‌دهیم.

در این بخش، فرض می‌کنیم که حروف الفبا دودویی هستند. توسیع آن به میدان $\mathbb{F}_q$ سرراست می‌باشد. به‌نظر می‌رسد هر مقدمه درباره کدگذاری کانولوشن، مثال یکسانی را به‌کار می‌برد. اضافه نمودن

نمونه بیشتر به این لیست، ممکن است عقیده برخی از دانشجویان که معتقدند هیچ مثال دیگری وجود ندارد را تقویت نماید، اما با وجود این، ما این مثال متعارف را به‌کار خواهیم برد.

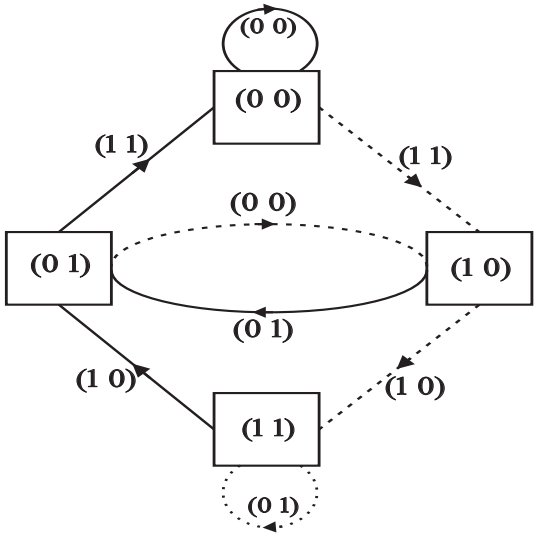
در شکل ۱۳.۱، ابزار کدگذاری برای کدهای خود را تشریح می‌کنیم. سه مربع موجود در شکل، سلول‌های ذخیره‌ای[۱] (مدار دوضربه‌ای[۲]) هستند که می‌توانند در یکی از دو وضعیت احتمالی که ما آنها را با ۰ و ۱ نمایش می‌دهیم، باشند. این دستگاه توسط یک ساعت بیرونی هر t_0 ثانیه یک سیگنال تولید می‌کند (برای سادگی، واحد زمان را $t_0 = 1$ انتخاب می‌کنیم).



شکل ۱۳.۱:

اثر این سیگنال این است که محتویات مدارهای دوضربه‌ای در جهت پیکان‌ها به‌سوی عناصر بعدی حرکت می‌کند که آن در اصطلاح رجیستر تغییر مکان[۳] نامیده می‌شود. عناصر $\oplus$ جمع‌گرهای به پیمانه ۲ را نشان می‌دهند. برای هر ضربه ساعت، می‌بینیم که محتویات اولین و سومین مدارهای دوضربه‌ای جمع شده و سپس کدگذار را از طریق جریان T_0 ترک می‌کند. اطلاعات پردازش شده در سمت چپ به‌صورت جریان I_0 وارد می‌شود. دقت کنید که اولین مدار دوضربه‌ای در واقع زاید می‌باشد چراکه آن تنها برای جدا کردن جریان ورودی به سه جهت به‌کار می‌رود. عناصر دوم و سوم رجیستر تغییرمکان، تفاوت ضروری با کدگذاری بلوکی را نشان می‌دهند. این عناصر، عناصر—حافظه‌ای هستند که با نگاهی به نمودار مذکور در زمان t، می‌توان دید که اینها سیگنال‌های ورودی در زمان‌های $t-1$ و $t-2$ هستند که هنوز دردسترس می‌باشند. خروجی، به این سه سمبل ورودی بستگی دارد. در عمل، جریان های خروجی T_0 و T_1، برای تولید یک جریان خروجی، درهم آمیخته می‌شوند؛ بنابراین، اگر ما با حالت (۰, ۰, ۰) در رجیستر شروع کنیم و یک جریان پیام شامل ۱ همراه با صفرها داشته باشیم، خواهیم دید که رجیستر درابتدا به حالت (۱, ۰, ۰) تغییر می‌یابد و خروجی (۱, ۱) را به‌وجود می‌آورد؛ سپس با خروجی (۰, ۱) به حالت

[۱] storage elements
[۲] flip-flops
[۳] shift register



شکل ۱۳.۲:

(۰, ۱, ۰) تغییر حالت می‌دهد؛ درادامه به حالت (۱, ۰, ۰) با خروجی (۱, ۱) و سپس به حالت اولیه و رشته‌ای از صفرها باز می‌گردد.

یک روش موثر برای توصیف طرز کار این کدگذار از طریق نمودار حالت [۴] ، شکل ۱۳.۲، داده شده است. دراینجا محتویات دومین و سومین مدارهای دوضربه‌ای، حالت رجیستر نامیده می‌شود. ما دو حالت را توسط یک یال توپر به‌هم وصل می‌کنیم، اگر رجیستر از یکی به سمت دیگری با یک ورودی صفر حرکت کند. به‌طور مشابه، یک یال نقطه‌چین متناظر با یک ورودی ۱ می‌باشد. روی این یال‌ها داخل براکت‌ها، دو خروجی در T_0 و T_1 را نشان می‌دهیم. یک جریان ورودی I_0 متناظر با یک گشت در گراف شکل ۱۳.۲ می‌باشد.

یک توصیف ریاضی در این روند کدگذاری، می‌تواند به‌صورت زیر باشد:

جریان ورودی i_0، i_1، i_2، $\cdots$ توسط سری توانی $I_0(x) := i_0 + i_1 x + i_2 x^2 + \cdots$ با ضرایبی در $\mathbb{F}_2$ توصیف می‌شود. به‌همین شکل خروجی‌ها را در T_0 و T_1 توسط سری‌های توانی $T_0(x)$، به‌ترتیب $T_1(x)$، توصیف می‌کنیم. زمان را طوری هماهنگ می‌کنیم که اولین ورودی متناظر با اولین خروجی باشد.

پس واضح است که:

$$T_0(x) = (1 + x^2) I_0(x),$$

$$T_1(x) = (1 + x + x^2) I_0(x).$$

[۴] State diagram

پس از آن ارتباط داده‌های T_0 و T_1 به‌صورت زیر توصیف می‌شود:

$$T(x) = T_0(x^2) + xT_1(x^2).$$

در این مثال، $I_0 = 1$ را وارد نموده و دنباله خروجی

$$11 \quad 01 \quad 11 \quad 00 \quad 00 \quad \cdots,$$

را به دست می‌آوریم که درنتیجه:

$$G(x) := 1 + x + x^3 + x^4 + x^5 = (1 + (x^2)^2) + x(1 + (x^2) + (x^2)^2).$$

بنابراین، اگر تعریف کنیم $I(x) := I_0(x^2)$، آن‌گاه:

$$T(x) = G(x)I(X). \qquad (1)$$

بنابر دلایلی که واضح هستند، می‌گوییم نرخ این کد کانولوشن برابر با $\frac{1}{2}$ است. مطابق معمول، کد مذکور مجموعه دنباله‌های خروجی ممکن $T(x)$ است. چندجمله‌ای $G(x)$ گاهی اوقات چندجمله‌ای مولد این کد نامیده می‌شود.

در توصیف داده شده در بالا، سمبل اطلاعاتی i_v با ورود به رجیستر تغییرمکان، شش تا از سمبل‌های دنباله منتقل شده را تحت تاثیر قرار می‌دهد. این عدد، طول محدود[5] کد نامیده می‌شود. این طول محدود برابر با درجه $G(x)$ به‌علاوه ۱ می‌باشد. خواننده باید توجه کند که حداقل دو تعریف دیگر برای طول محدود وجود دارد که توسط نویسندگان دیگر به کار برده شده است (یکی از اینها به این‌صورت است: طول رجیستر تغییرمکان که برای مثال در شکل ۱۳.۱ برابر با ۳ است). در این مثال گوییم که حافظه تخصیص یافته به کد کانولوشن برابر با ۲ است، زیرا کدگذار باید دو ورودی قبلی را برای تولید خروجی، زمانی‌که i_v ارایه شده است، به یاد داشته باشد.

می‌دانیم که یکی از مهم‌ترین اعداد مربوط به کد بلوکی C، کمترین—فاصله آن است. برای کدهای کانولوشن، یک مفهوم مشابه وجود دارد که مجدداً یک نقش اساسی در بررسی کدگشایی دارد. این عدد، فاصله آزاد[6] کد نامیده می‌شود و برابر با کمترین وزن تمامی دنباله‌های خروجی ناصفر تعریف شده است. در مثالی که در بالا بیان شد، این فاصله آزاد برابر با وزن $G(x)$، یعنی ۵، می‌باشد.

هم‌اکنون، در روشی کاملاً مشابه، کدهای کانولوشن با نرخ $\frac{1}{n}$ را معرفی می‌کنیم. یک دنباله از سمبل‌های اطلاعاتی داده‌شده توسط سری‌های I_0 را داریم. n دنباله $T_0(x)$، $T_1(x)$، $\cdots$، $T_{n-1}(x)$ وجود

[5] constraint length

[6] free distance

دارند که رجیستر تغییرمکان را ترک می‌کنند، درحالی که هر دنباله کدشده $T_i(x)$ با ضرب I_0 در یک چندجمله‌ای مانند $G_i(x)$ به‌دست می‌آید. دنباله منتقل‌شده $T(x)$ برابر با $\sum_{i=0}^{n-1} x^i T_i(x^n)$ است. مانند قبل، تعریف می‌کنیم $I(x) := I_0(x^n)$ و $G(x) := \sum_{i=0}^{n-1} x^i G_i(x^n)$؛ در این‌صورت $T(x) = G(x)I(x)$.

واضح است که انتخاب چندجمله‌ای‌های $G_i(x)$، $i = 0, 1, \cdots, n-1$، خوب یا بد بودن کد را تعیین می‌کند، هر چند در هر صورت آن را بامعنا می‌دانیم. حال اجازه دهید موقعیتی را که به‌وضوح بد است، تشریح نماییم. فرض کنید جریان ورودی $I_0(x)$ شامل تعداد نامتناهی ۱ باشد؛ درحالی که دنباله خروجی متناظر $T(x)$ شامل تنها تعداد متناهی ۱ باشد. اگر به‌طور ناگهانی در موقعیت‌هایی از کانال که این ۱ها قرار دارند، خطا رخ دهد، جریان خروجی حاصل از ورودی $I_0 = 0$ توسط گیرنده، بردار تماماً صفر خواهد بود؛ بنابراین، یک تعداد محدود از خطاهای کانال، یک تعداد نامحدود از خطاهای کدگشایی را نتیجه می‌دهد! چنین کدی یک کد فاجعه‌آمیز[۷] نامیده می‌شود. روشی آسان برای اجتناب از فاجعه‌آمیز شدن یک کد کانولوشن با نرخ $\frac{1}{n}$، وجود دارد؛ یعنی با برقراری شرط زیر:

$$\gcd(G_0(x), G_1(x), ..., G_{n-1}(x)) = 1.$$

قبلاً دیده شده است که این تساوی وجود چندجمله‌ای‌های $a_i(x)$، $i = 0, \cdots, n-1$، را ایجاب می‌کند که در شرط $\sum_{i=0}^{n-1} a_i(x)G_i(x) = 1$ صدق می‌کنند. با توجه به این مطلب، داریم:

$$G(x) := \sum_{i=0}^{n-1} a_i(x^n)T_i(x^n) = \sum_{i=0}^{n-1} a_i(x^n)G_i(x^n)I_0(x^n) = I(x),$$

این بدان معناست که ورودی می‌تواند از خروجی مشخص شود و علاوه‌برآن تعداد متناهی خطا در $T(x)$ نمی‌تواند باعث ایجاد تعداد نامتناهی خطا در کدگشایی گردد.

دو روش برای توصیف تعمیم این مطلب به کدهای با نرخ $\frac{k}{n}$ وجود دارد. در اینجا ما k تا رجیستر تغییرمکان با جریان‌های ورودی $I_0(x)$، $I_1(x)$، $\cdots$، $I_{k-1}(x)$ داریم. متناظر با این ورودی‌ها n جریان خروجی $T_i(x)$، $i = 0, ..., n-1$، وجود دارد، که در آن هر $T_i(x)$ با به‌کارگیری تمامی رجیسترهای تغییرمکان شکل گرفته است. در ابتدا روشی که در بالا استفاده کردیم را به‌کار می‌بریم. بنابراین، در اینجا نیاز به kn چندجمله‌ای G_{ij}، $i = 0, ..., k-1$، $j = 0, ..., n-1$، برای تبیین این موقعیت داریم. اما داریم:

$$T_j(x) := \sum_{i=0}^{k-1} G_{ij}(x)I_i(x).$$

در این حالت، دیگر امکان توصیف فرایند کدگذاری با استفاده از یک چندجمله‌ای مولد وجود ندارد. لذا روش دیگری برای توصیف کدهای کانولوشن با نرخ k/n را ترجیح می‌دهیم که این کدها را به کدهای

[۷] catastrophic code

بلوکی روی یک میدان به طور مناسب انتخاب‌شده تبدیل می‌کند.

فرض کنید $\mathfrak{F}$ میدان خارج‌قسمتی $\mathbb{F}_۲[x]$ باشد؛ یعنی میدان تمامی سری‌های لوران[۸] به‌صورت:

$$\sum_{i=r}^{n-۱} a_i x^i, \qquad (r \in \mathbb{Z}, a_i \in \mathbb{F}_۲).$$

k بیت ورودی به رجیسترهای تغییرمکان متفاوت در زمان t به‌عنوان برداری در $\mathbb{F}_۲^k$ درنظر گرفته می‌شوند. این بدان معناست که دنباله‌های ورودی به‌عنوان برداری در $\mathfrak{F}^k$ تفسیر می‌شوند (مانند بخش ۳، بردارها، بردارهای سطری هستند). حال kn چندجمله‌ای $G_{ij}(x)$ را به‌عنوان درایه‌های یک ماتریس مولد G درنظر می‌گیریم. البته، n دنباله خروجی می‌توانند به‌عنوان عناصر $\mathfrak{F}^n$ دیده شوند. این مطلب به تعریف زیر منتهی می‌شود.

تعریف ۱.۱۳.۱. یک کد کانولوشن دودویی C با نرخ $\frac{۱}{n}$ زیرفضای k–بعدی از فضای $\mathfrak{F}^n$ است که شامل پایه‌ای متشکل از k بردار متعلق به $\mathbb{F}[x]^n$ می‌باشد. این بردارهای پایه، سطرهای G هستند.

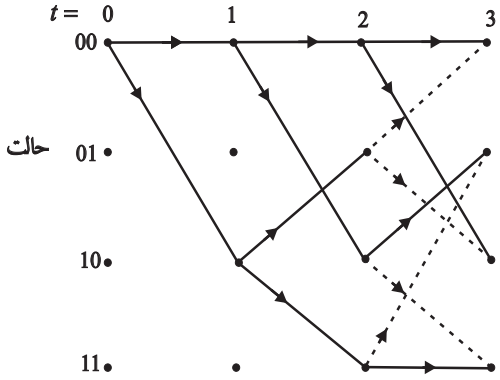
اگرچه این تعریف، برخی شباهت‌ها را با کدهای بلوکی نشان می‌دهد، دشواری آن را با به‌کارگیری $\mathfrak{F}$ مخفی می‌کنیم و علاوه‌براین، محدودشدن روی عناصر G کاری کاملاً سخت‌گیرانه است. عملاً تمامی پیام‌ها متناهی هستند و می‌توانیم فرض کنیم که در حالت $t < ۰$ در کار توقف وجود دارد. این بدان معناست که ما واقعاً به $\mathfrak{F}$ نیازی نداریم و هر کاری را می‌توانیم با $\mathbb{F}[x]$ انجام دهیم. چون این یک میدان نیست، مشکلات دیگری در این روی‌کرد وجود خواهد داشت.

هنگام صحبت درباره کدهای بلوکی، اشاره کردیم که برای هر کد داده شده، انتخاب‌های متعددی از G وجود دارد که برخی از آنها ممکن است تحلیل C را آسان‌تر نماید. وضعیت یکسانی در مورد کدهای کانولوشن اتفاق می‌افتد. برای چنین عمل‌کردی از ماتریس مولد، خواننده را به مرجع [۲۳] ارجاع می‌دهیم. این یکی از اندک مثال‌های مربوط به تحلیل ریاضی کدهای کانولوشن است.

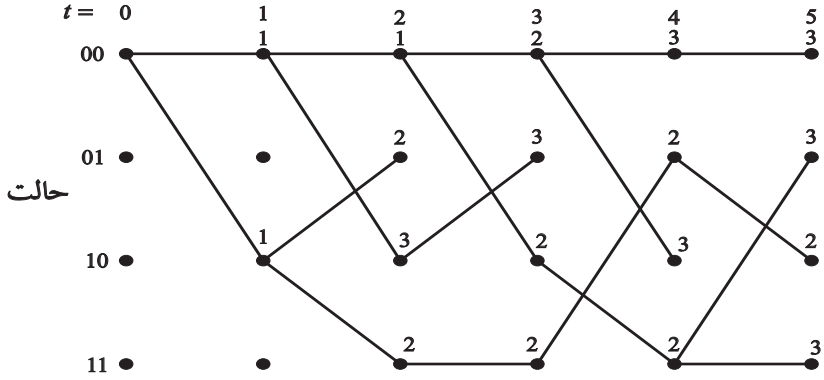
۱۳.۲ کدگشایی کدهای کانولوشن

چندین الگوریتم در عمل برای کدگشایی کدهای کانوشن به‌کار رفته است. آنها کم و بیش شبیه به‌هم هستند و ازنظر ریاضی زیاد عمیق نیستند. درواقع، آنها به کدگشایی کدهای بلوکی از نظر مقایسه کلمه دریافت شده با تمامی کدکلمات، شباهت دارند. چون کدکلمات یک کد کانولوشن دارای طول نامتناهی هستند، این مقایسه ناقص است، به این معنی که فرد باید اولین l سمبل پیام دریافتی را مورد مطالعه

[۸] Laurent series



شکل ۱۳.۳:



شکل ۱۳.۴:

قرار دهد. بعد از مقایسه، فرد باید اولین سمبل اطلاعاتی پیام را تعیین نموده و سپس این روش را برای سمبل‌های بعدی تکرار نماید. ما الگوریتم معروف‌به الگوریتم ویتربی[۹] را با جزییات بیشتر با به‌کارگیری مثال موجود در شکل‌های ۱۳.۱ و ۱۳.۲ مطرح می‌کنیم.

فرض کنید که پیام دریافتی به‌صورت ... ۰۰ ۱۰ ۰۱ ۰۰ ۱۰ باشد. نمودار شکل ۱۳.۳، حالت‌های ممکن در لحظه $t = ۰, ۱, ۲, ۳$ نشان می‌دهد، پیکان‌ها مسیر موجود در شکل ۱۳.۲ را نشان می‌دهند.

چهار تا از این خط‌ها در شکل ۱۳.۳ نقطه‌چین هستند و این خط‌ها در شکل بعدی حذف شده‌اند. برای دانستن علت آن، فرض می‌کنیم که در $t = ۳$، رجیستر در حالت ۰۰ است. یک راه رسیدن به این حالت، مسیر افقی است که متناظر با خروجی ... ۰۰ ۰۰ ۰۰ است؛ بنابراین، این فرض به‌معنی آن است که در لحظه $t = ۳$ دو خطا رخ داده است. اگر از طرف دیگر، حالت ۰۰ از طریق ۱۰ و ۰۱ رخ دهد، خروجی ۱۱ ۰۱ ۱۱ به‌وجود می‌آید؛ بنابراین، دراین لحظه سه خطا وجود دارد. نمی‌دانیم که

[۹] Viterbi-algorithm

آیا رجیستر در حالت ۰۰ است یا نه و اگر این طور باشد، در این‌صورت مسیر افقی، مسیر محتمل‌تری برای رسیدن به آنجا است. به‌علاوه، این مسیر شامل دو خطاست. بیایید شکل ۱۳.۳ را به شکل ۱۳.۴ توسعه دهیم، که در آن $t = ۴$ و $t = ۵$ را شامل می‌شود و نیز تعداد خطاهایی را که در راه رسیدن به مراحل مختلف وجود دارد، نشان می‌دهیم.

البته می‌تواند موقعیتی اتفاق بیفتد که در آن دو روش بااحتمال یکسان برای رسیدن به یک حالت مشخص وجود داشته باشد، که در این‌صورت فرد باید یکی را انتخاب کند و دیگری را دور بیندازد. مطابق با هر زمان و هر حالت، فرد می‌تواند محتمل‌ترین خروجی‌ها را مطابق باآن فرض، گردآوری نماید؛ بنابراین، شکل ۱۳.۴ به لیست خروجی‌های زیر منتهی می‌شود:

	$t=۱$	$t=۲$	$t=۳$	$t=۴$	$t=۵$											
حالت	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰	۰۰
	۰۱	–	۱۱	۰۱	۰۰	۱۱	۰۱	۱۱	۱۰	۰۱	۱۰	۰۰	۰۰	۱۱	۱۰	۱۰
	۱۰	۱۱	۰۰	۱۱	۰۰	۰۰	۱۱	۰۰	۰۰	۰۰	۱۱	۱۱	۱۰	۰۱	۱۰	۰۰
	۱۱	–	۱۱	۱۰	۱۱	۱۰	۰۱	۰۰	۰۰	۱۱	۱۰	۰۰	۰۰	۱۱	۱۰	۰۱

به‌وضوح در لحظه $t = ۵$، قاعده تصمیم با بیشترین درست‌نمایی نتیجه می‌دهد که رجیستر در حالت ۱۰ بوده، دو خطا رخ داده و خروجی برابر با ۰۰ ۱۰ ۰۱ ۱۰ ۱۱ شده است. ورودی متناظر می‌تواند با توجه به شکل ۱۳.۴ به‌دست آید. ساده‌ترین روش، علامت‌گذاری هر یال با سمبل ورودی متناظر با آن یال است. این مطلب را به خواننده واگذار می‌کنیم تا چندین روش برای ادامه دادن قبل از مرحله بریدن کد، ابداع نماید. این مطلب واضح است که ما با مسائلی از زمان محاسبه و ذخیره‌سازی مواجه خواهیم شد. یک سوال ریاضی جالب‌تر، محاسبه تاثیر یک تصمیم نادرست برروی تصمیمات کدگشایی بعدی و هم‌چنین فهمیدن عوامل موثر بر روی فاصله آزاد کد در تعیین صحت کدگشایی می‌باشد. برای تعیین جزییات بیشتر درباره این سوال، خواننده را به مرجع [۵۱] ارجاع می‌دهیم.

۱۳.۳ مقایسه کران گیلبرت برای برخی کدهای کانولوشن

کلاس خاصی از کدهای کانولوشن با نرخ k/n را درنظر بگیرید؛ یعنی آنهایی که به‌صورت زیر تعریف شده‌اند. k دنباله ورودی $I_۰(x)$، $\cdots$، $I_{k-۱}(x)$ را درنظر گرفته و

$$I(x) := \sum_{i=۰}^{k-۱} I_i(x^n),$$

را تشکیل دهید. معنای آن این است که هر n–تایی از بیت‌های اطلاعات به $n-k$ تا صفر ختم می‌شود. ماتریس مولد $G(x)$ را درنظر گرفته و خروجی را توسط $T(x) = G(x)I(x)$ تعریف نمایید.

این مطلب متناظر با یک انتخاب ویژه از چندجمله‌ای‌های $G_{ij}(x)$ در توصیف اخیرمان از کدهای با نرخ k/n است. مانند قبل، طول محدود کد را برابر با $l+۱ = ۱ + deg(G(x))$ تعریف نموده و تنها کدهایی را درنظر می‌گیریم که $l+۱ \leq mn$ و در آن m ثابت فرض شده است. ما علاقه‌مند به فاصله آزاد d_f، برای چنین کدهایی هستیم. به‌وضوح $d_f \leq l+۱$. با شیفت دادن مقیاس زمان، می‌بینیم که در مطالعه روش کدگذاری، ممکن است محدودیت $i_۰ = t_۰ = G(۰) = ۱$ را قرار دهیم. برای هر mn–تایی اولیه $۱ = t_۰, t_۱, \cdots, t_{mn-۱}$ از دنباله خروجی و هر mk–تایی $۱ = i_۰, i_۱, \cdots, i_{mk-۱}$، دقیقاً یک چندجمله‌ای $G(x)$ از درجه کمتر یا مساوی mn وجود دارد، به‌طوری که این دنباله‌های اولیه با $T(x) = G(x)I(x)$ در تناظر باشند. می‌خواهیم تا تمامی بخش‌های اولیه $T(x)$ را که دارای وزن کمتر از d هستند را خارج نماییم. این بدان معناست که ما حداکثر $۲^{mk-۱}\sum_{i=۰}^{d-۲}\binom{mn-۱}{i}$ چندجمله‌ای با $G(۰) = ۱$ را به‌عنوان مولد خارج می‌کنیم. بنابراین، یک انتخاب از $G(x)$ وجود دارد که حداقل فاصله آزاد لازم را القا می‌کند، اگر:

$$۲^{mk}\sum_{i=۰}^{d}\binom{mn}{i} < ۲^{mn}.$$

با درنظر گرفتن $d = \lambda mn$ و نوشتن $R := k/n$، از قضیه ۵.۱.۴ قسمت (۱)، با گرفتن لگاریتم داریم:

$$\frac{۱}{mn}\log\sum_{i=۰}^{d}\binom{mn}{i} < H(\lambda) < ۱ - R,$$

اگر:

$$\lambda < H^{\leftarrow}(۱ - R).$$

در اینجا λ خارج‌قسمت فاصله آزاد و طول محدود می‌باشد. این کران باید با قضیه ۸.۵.۱ مقایسه شود.

۱۳.۴ ساختن کدهای کانولوشن از کدهای بلوکی دوری

از آنجا که در مورد کدهای بلوکی مطالب کاملاً زیادی به‌دست آمده است، این موضوع که چندین مولف، کدهای بلوکی خوب را برای ساخت کدهای کانولوشن با خواص مطلوب به‌کار برده‌اند، تعجب بر انگیز نمی‌باشد. در این بخش، ما به یکی از این روش‌ها خواهیم پرداخت که قبلاً توسعه داده شده است.

در اینجا نمادگذاری‌های بخش ۴.۵ را به‌کار می‌بریم.

لم ۱.۱۳.۴. فرض کنید $q = ۲^r$، $p(x) \in \mathbb{F}_q[x]$، $c \in \mathbb{F}_q - \{۰\}$، $n \geq ۰$ و $N \geq ۰$؛ در این‌صورت:

$$w(P(x)(x^n - c)^N) \geq w((x-c)^N).w(P(x) \bmod (x^n - c)).$$

اثبات. $P(x)$ را به‌صورت $\sum_{i=0}^{n-1} x^i Q_i(x^n)$ درنظر بگیرید؛ در این‌صورت با توجه به قضیه ۲.۴.۵ داریم:

$$\begin{aligned} w(P(x)(x^n-c)^N) &= \sum_{i=0}^{n-1} w(Q_i(x)(x-c)^N) \\ &\geq \sum_{i=0}^{n-1} w(Q_i(x))w((x-c)^N) \\ &= w((x-c)^N).w(\sum_{i=0}^{n-1} Q_i(c)x^i) \\ &= w((x-c)^N).w(P(x) \bmod (x^n-c)). \end{aligned}$$

□

تذکر ۱.۱۳.۴ اثبات لم ۱.۱۳.۴ برای هر میدان دلخواه $\mathbb{F}_q$ مشکل نیست.

قضیه ۲.۱۳.۴. فرض کنید $g(x)$ چندجمله‌ای مولد یک کد دوری با طول n (فرد) روی میدان $\mathbb{F}_q$ ($q = 2^r$) با کمترین —فاصله d_q باشد و $h(x)$ چندجمله‌ای بررسی‌توازن و d_h کمترین —فاصله کد با چندجمله‌ای مولد $h(x)$ باشد؛ در این‌صورت کد کانولوشن با نرخ $1/(2m)$ روی میدان مشابه و با چندجمله‌ای مولد $G(x) = g(x)$ فاجعه‌آمیز نبوده و در شرط $d_f \geq \min\{d_g, 2d_h\}$ صدق می‌کند.

اثبات.

۱) بنویسید $G(x) = \sum_{j=0}^{2m-1} x^j (\hat{G}_j(x^m))^2$. اگر نمایش کد کانولوشن با چندجمله‌ای‌های $G_0(x)$، ...، $G_{2m-1}(x)$ از بخش ۱۳.۱ را درنظر بگیریم، در این‌صورت برای هر عامل مشترک تحویل‌ناپذیر $A(x)$ از این چندجمله‌ای‌ها، $G(x)$ بر $A(x)$ بخش‌پذیر است و از آنجا که n عددی فرد است، این کار امکان‌پذیر نیست و $g(x)$ عاد می‌کند $x^n - 1$ را؛ بنابراین، این کد فاجعه‌آمیز نمی‌باشد.

۲) دنباله اطلاعاتی $I_0(x)$ را درنظر بگیرید. داریم $T(x) = G(x)I_0(x^{2m}) = G(x)(\hat{I}_0(x^m))^2$؛ بنابراین، $T(x)$ به شکل زیر می‌باشد:

$$T(x) = P(x)(g(x))^{2i+1}(h(x))^{2j},$$

به‌طوری که $i \geq 0$، $j \geq 0$، $P(x) \neq 0$، $P(x)$ بر $g(x)$ یا $h(x)$ بخش‌پذیر نمی‌باشد. دو حالت را درنظر می‌گیریم:

الف) فرض کنید $i \geq j$؛ در این‌صورت داریم:

$$T(x) = P(x)(g(x))^{۲(i-j)+۱}(x^n - ۱)^{۲j}.$$

و بنابر لم ۱.۱۳.۴ داریم:

$$w(T(x)) \geq w((x-۱)^{۲j}).w(P(x)(g(x))^{۲(i-j)+۱} \bmod (x^n - ۱)) \geq d_g.$$

زیرا عامل دوم بستگی به کدکلمه‌ای در کد دوری تولید شده توسط $g(x)$ دارد.

ب) فرض کنید $i < j$؛ در این‌صورت داریم:

$$T(x) = P(x)(h(x))^{۲(j-i)-۱}(x^n - ۱)^{۲i+۱}.$$

و بنابر لم ۱.۱۳.۴ داریم $w(T(x)) \geq ۲d_h$؛ زیرا:

$$w((x-۱)^{۲i+۱}) \geq ۲.$$

□

قبل از پرداختن به مثال‌های بیشتر درباره این بحث، کران بالایی را برای فاصله آزاد بیان می‌کنیم. یک کد کانولوشن با نرخ $۱/n$ روی $\mathbb{F}_q$ با چندجمله‌ای مولد $G(x) = \sum_{i=۰}^{n-۱} G_i(x^n)$ را درنظر بگیرید. فرض کنید:

$$L := n(۱ + \max\{deg(G_i(x) \mid ۰ \leq i \leq n-۱)\}).$$

(برخی از مولفین، L را طول محدود می‌نامند). واضح است که:

$$d_f \leq L.$$

این کران بدیهی دارای یک تشابه معین با کران سینگلتون $d \leq n - k + ۱$ برای کدهای بلوکی است. در اینجا ما ساختاری را بیان می‌کنیم که توسط جاستسن[۱۰] مرجع[۳۸] از کدهای کانولوشنی که به این کران دست می‌یابند، مطرح گردید. درابتدا نشان می‌دهیم که این شرط، کرانی را روی L القا می‌کند.

لم ۳.۱۳.۴. اگر برای یک کد کانولوشن روی $\mathbb{F}_q$ داشته باشیم $d_f = L$، آن‌گاه $L \leq nq$.

[۱۰] J. Justesen

اثبات. اگر $d_f = L$، آن‌گاه هر یک از چندجمله‌ای‌های $G_i(x)$ دارای وزن L/n می‌باشد. دنباله ورودی $I_0(x) = 1 + \alpha x$ را درنظر می‌گیریم، که در آن α متعلق به $\mathbb{F}_q - \{0\}$ بوده و وزن متوسط $\bar{\omega}$ از دنباله کدگذاری شده متناظر را تعیین می‌کند. داریم:

$$\begin{aligned}\bar{\omega} &= (q-1)^{-1} \sum_{\alpha \in \mathbb{F}_q - \{0\}} \sum_{i=0}^{n-1} w(G_i(x)(1+\alpha x)) \\ &= (q-1)^{-1} n\{2(q-1) + (\tfrac{L}{n} - 1)(q-2)\}.\end{aligned}$$

چون $L \geq \bar{\omega}$، باید داشته باشیم $L \leq nq$. □

با به‌کارگیری روشی مشابه با روش موجود در قضیه ۲.۱۳.۴، می‌توانیم مثال آسانی از یک کد کانولوشن با $d_f = L$ ارائه دهیم.

مثال ۴.۱۳.۴. فرض کنید α یک عضو اولیه از $\mathbb{F}_4$ باشد. فرض کنید $g_1(x) = x^2 + \alpha x + 1$، $g_2(x) = x^2 + \alpha^2 x + 1$؛ در این صورت $(x^5 - 1) = (x-1)g_1(x)g_2(x)$ و $g_1(x)$ و $g_2(x)$ نسبت به‌هم اول می‌باشند. کد کانولوشن C با نرخ $\frac{1}{2}$ روی $\mathbb{F}_4$ با چندجمله‌ای مولد:

$$G(x) := g_1(x^2) + x g_2(x^2),$$

را درنظر بگیرید. این کد فاجعه‌آمیز نمی‌باشد. یک دنباله اطلاعاتی را به‌صورت $I_0(x) = I'_0(x)(x^5 - 1)^N$ درنظر بگیرید، که در آن N ماکسیمال می‌باشد. با استفاده از لم ۱.۱۳.۴ داریم:

$$\begin{aligned}w(T(x)) &= w(g_1(x)I_0)(x)) + w(g_2(x)I_0)(x)) \\ &\geq w((x-1)^N).w(g_1(x)I'_0(x) \bmod (x^5 - 1)) \\ &\quad + w(g_2(x)I'_0)(x) \bmod (x^5 - 1))\}.\end{aligned}$$

حال، اگر $I'_0(x)$ مضربی از $(x-1)g_1(x)$ یا $(x-1)g_2(x)$ نباشد، آن‌گاه کران BCH نشان می‌دهد که هر دو جمله در عامل دوم در طرف راست بزرگ‌تر یا مساوی ۳ هستند. اگر از طرف دیگر $I'_0(x)$ مضربی از $(x-1)g_1(x)$ باشد، آن‌گاه هر دو جمله در طرف راست در خط بالا زوج می‌باشند (به‌خاطر عامل $x-1$) و هردو مثبت هستند. اگر دومی برابر با ۲ باشد، آن‌گاه اولی حداقل برابر با ۴ است، مجدداً توسط کران BCH؛ بنابراین، C دارای فاصله آزاد حداقل ۶ است. چون $L = 6$، داریم $d_f = L$.

برای تعمیم ایده پنهان در قضیه ۲.۱۳.۴ به‌منظور ساخت کدهای با نرخ $\frac{1}{2}$ بر روی $\mathbb{F}_q$، چندجمله‌ای‌های به‌شکل:

$$g_i(x) := (x - \alpha^m)(x - \alpha^{m+1}) \cdots (x - \alpha^{m+d-2}),$$

را درنظر می‌گیریم، که در آن α یک عضو اولیه از $\mathbb{F}_q$ است. $g_1(x)$ و $g_2(x)$ را انتخاب می‌کنیم، به‌طوری که هر دو دارای درجه $\lfloor \frac{1}{3}q \rfloor$ باشند و این‌که آنها دارای هیچ صفر مشترکی نمی‌باشند؛ در این‌صورت $G(x) := g_1(x^2) + xg_2(x^2)$ یک کد کانولوشن C روی $\mathbb{F}_q$ تولید می‌کند که فاجعه‌آمیز نمی‌باشد. دو کد دوری با چندجمله‌ای‌های مولد $g_1(x)$ و $g_2(x)$ هر دو دارای کمترین—فاصله بزرگ‌تر یا مساوی $d := \lfloor \frac{1}{3} \rfloor + 1$ هستند. فرض کنید این کدها دارای چندجمله‌ای‌های بررسی توازن $h_1(x)$ و $h_2(x)$ هستند. یک دنباله اطلاعاتی $I_0(x)$ برای C به‌صورت:

$$I_0(x) = (x^{q-1} - 1)^r (h_1(x))^s (h_2(x))^t p(x),$$

می‌باشد، که در آن $p(x)$ مضربی از $h_1(x)$ یا $h_2(x)$ نبوده و s یا t برابر با صفر است. در ابتدا فرض کنید $s = t = 0$. با استفاده از لم ۱.۱۳.۴ داریم:

$$\begin{aligned} w(T(x)) &= w(g_1(x)I_0(x)) + w(g_2(x)I_0(x)) \\ &\geq \textstyle\sum_{i=1}^{2} w((x-1)^r) w(p(x)g_i(x) \bmod (x^{q-1} - 1)) \\ &\geq 2d. \end{aligned}$$

اگر $s > 0$، آن‌گاه با روشی مشابه داریم:

$$\begin{aligned} w(T(x)) = {} & w((x^{q-1} - 1)^r (h_1(x))^s g_1(x) p(x)) + w((x^{q-1} - 1)^r (h_1(x))^s g_2(x) p(x)) \\ \geq {} & w((x-1)^{r+1} w(p(x)(h_1(x))^{s-1} \bmod (x^{q-1} - 1)) \\ & + w((x-1)^r . w(p(x)(h_1(x))^s g_2(x) \bmod (x^{q-1} - 1)) \\ \geq {} & 2 + (q - \lfloor \tfrac{1}{3}q \rfloor) \geq 2 + 2\lfloor \tfrac{1}{3}q \rfloor = 2d. \end{aligned}$$

با توجه به این ساختار داریم $L = 2(1 + \lfloor \frac{1}{3} \rfloor)$، بنابراین، $d_f = L$.

این مثال‌ها بیان می‌کنند که این یک روش خوب برای ساخت کدهای کانولوشن است. این روش به نرخ $1/n$ تعمیم می‌یابد. برای جزییات بیشتر به مرجع [۳۸] رجوع می‌کنیم.

۱۳.۵ خودریختی‌های کدهای کانولوشن

از قبل مانند فصل مربوط به کدهای دوری دیده‌ایم که این شرط که کدی تحت گروه معینی از جای‌گشت‌ها پایا باشد، به پیشرفت‌های جالبی منجر می‌گردد. روش‌های با دید جبری قوی، می‌توانست

معرفی گردد و چندین کد خوب به این روش یافت شدند؛ بنابراین، این مطلب تعجب‌آور نخواهد بود که در مورد کدهای کانولوشن نیز مطلب مشابهی پیگیری شود. ما برخی از این ایده‌ها را طرح نموده و کدهای کانولوشن دوری را تعریف می‌کنیم. ما بسیاری از جزییات را بیان ننموده، اما امیدواریم که این طرز عمل برای خواننده کافی باشد تا تصمیم بگیرد که آیا او به این موضوع علاقه‌مند می‌گردد، که در این‌صورت او به کار پیرت[۱۱] (مراجع [۵۴] و [۵۵] را ببینید) ارجاع داده می‌شود. این کار توسط روس[۱۲] (ر.ک. مرجع [۵۹]) از نو طراحی شد. این ایده‌ها بر روی برخی کدهای نسبتاً خوب به‌کار گرفته شد و آنها به‌طور قطع در تحقیقات بعدی مفید خواهند بود.

یک کد کانولوشن را همانند آنچه در تعریف ۱.۱۳.۱ آمده درنظر می‌گیریم. چنین کدی را دوری می‌نامیم، اگر یک شیفت دوری هم‌زمان از ضرایب a_i از x^i $(a_i \in \mathbb{F}_2^n)$، کد مذکور را حفظ کند. در این حالت ما چیز جالبی به‌دست نمی‌آوریم. درواقع، به‌آسانی دیده می‌شود این کد، یک کد بلوکی است. این مطلب نشان می‌دهد که تعریف خودریختی‌ها به یک روش محسوس، کاری مشکل می‌باشد. ما این کار را به‌صورت زیر انجام می‌دهیم. فرض کنید K گروه جای‌گشت‌های روی $\mathbb{F}_2^n$ باشد. $K^{\mathbb{Z}}$، یعنی مجموعه تمامی توابع $\varphi : \mathbb{Z} \to K$، را درنظر بگیرید که با تعریف $\varphi_1\varphi_2(n) := \varphi_1(n)\varphi_2(n)$ به یک گروه تبدیل کرده‌ایم. φ_n را به‌جای $\varphi(n)$ خواهیم نوشت. دقت کنید که $\varphi_n \in K$؛ در این‌صورت عملی از φ را روی عناصر $\mathfrak{F}^n$ به‌صورت:

$$\varphi(\sum_{i=r}^{\infty} a_i x^i) := \sum_{i=r}^{\infty} \varphi_i(a_i) x^i, \qquad (۲)$$

تعریف می‌کنیم.

تعریف ۱.۱۳.۵. اگر C یک کد کانولوشن باشد، آن‌گاه مجموعه تمام عناصر $\varphi \in K^{\mathbb{Z}}$، که در آن $\varphi(C) = C$، گروه خودریختی C نامیده می‌شود.

از تعریف کدهای کانولوشن، این مطلب بدیهی است که کد C تحت حاصل‌ضرب در x پایاست؛ بنابراین، اگر φ یک خودریختی باشد، آن‌گاه $\varphi^x := x^{-1}\varphi x$ نیز یک خودریختی است. علاوه‌براین، این مطلب واضح است که اگر ما تنها عملی را درنظر بگیریم که روی یک مکان، ثابت باشد و آن‌را φ_i بنامیم، یک گروه جای‌گشتی روی $\mathbb{F}_2^n$ به‌دست می‌آوریم که تصویر گروه خودریختی روی iامین مختصات است. با توجه به تذکر فوق و این واقعیت که $\varphi_i^x(a_i) = \varphi_{i+1}(a_i)$، می‌بینیم که تمامی تصویرها، گروه یکسانی هستند؛ بنابراین، تلاش برای یافتن کدهایی که این تصویر یک گروه دوری است، طبیعی به‌نظر می‌آید. ما این مطلب را با به‌کارگیری تقریب جبری یکسان همانند آنچه در مورد کدهای بلوکی انجام دادیم،

[۱۱] Ph. Piret
[۱۲] C. Roos

انجام می‌دهیم. متغیر z را معرفی نموده و $\mathbb{F}_۲^n$ را با $\mathbb{F}_۲[z]$ در پیمانه $(z^n - ۱)$ یکی می‌کنیم. فرض کنید π عدد صحیحی باشد، به‌طوری که $(\pi, n) = ۱$ و فرض کنید σ خودریختی $\mathbb{F}_۲^n$ تعریف شده به‌صورت $\sigma : f(Z) \to f(z^\pi)$ باشد. حال عناصر $\mathfrak{F}^n$ می‌توانند به‌صورت $\sum_{i=r}^{\infty} a_i x^i$ نوشته شوند، که در آن $a_i = a_i(z)$ $(i \in \mathbb{Z})$ یک چندجمله‌ای با درجه کمتر از n است. در $\mathfrak{F}^n$، جمع را به‌طور طبیعی و ضرب (نشان داده شده با $*$) را به‌صورت زیر تعریف می‌کنیم:

$$\sum_i a_i x^i * \sum_j b_j x^j := \sum_i \sum_j \sigma^j(a_i) b_j x^{i+j}. \qquad (۳)$$

فرض کنید عامل سمت چپ برابر با z باشد؛ یعنی $a_۰ = z$، $a_i = ۰$ برای $i \neq ۰$؛ در این‌صورت از رابطه ۳ داریم:

$$z * \sum_j b_j x^j := \sum_j (z^{\pi^j} b_j) x^j. \qquad (۴)$$

این بدان معناست که ضرایب b_j از x^j به‌طور دوری روی مکان‌های π^j در پیمانه n شیفت داده شده‌اند. نکته اصلی تعریف بالا این است که $(\mathfrak{F}^n, +, *)$ یک جبر است که آن را با $\mathcal{A}(n, \pi)$ نشان می‌دهیم.

تعریف ۲.۱۳.۵. یک کد کانولوشن دوری (نماد CCC) یک ایده‌آل چپ در جبر $\mathcal{A}(n, \pi)$ است که پایه‌ای شامل چندجمله‌ای‌ها دارد.

در اینجا مشاهده می‌کنید که با استفاده از رابطه ۴، در واقع گروهی از خودریختی‌های کد داریم. این گروه شامل گروه دوری به عنوان تصویر روی یک مختصات است. تفاوت آن با مکان بدیهی در این واقعیت است که شیفت‌های دوری برای هر مکان یکسان نمی‌باشد. در اینجا مثالی می‌آوریم تا نشان دهیم که ما دارای کلاسی از اشیاء غیربدیهی که مطالعه آنها ارزشمند می‌باشد، هستیم. یک کد کانولوشن دودویی با نرخ $\frac{۴}{۷}$ با حافظه یک توسط ماتریس G به‌صورت زیر داده شده است:

$$G = \begin{pmatrix} ۱ & ۱ & ۱ & ۱ & ۱ & ۱ & ۱ \\ ۱+x & ۱ & ۱ & x & ۱ & x & x \\ ۰ & ۱ & ۱+x & ۱ & x & ۱+x & x \\ ۰ & x & ۱ & ۱+x & ۱+x & x & ۱ \end{pmatrix}. \qquad (۵)$$

حال می‌خواهیم عناصر $\mathbb{F}_۲^۷$ با چندجمله‌ای‌هایی در $\mathbb{F}_۲[z]$ به پیمانه $(z^۷ - ۱)$ را مشخص نماییم. با نوشتن $z^۷ - ۱ = (۱+z)(۱+z+z^۳)(۱+z^۲+z^۳) = m_۰(z)m_۱(z)m_۲(z)$ می‌توانیم G را به‌صورت زیر خلاصه نماییم:

$$G = \begin{pmatrix} m_۱ m_۳ \\ m_۰ m_۳ \\ z m_۰ m_۳ \\ z^۲ m_۰ m_۳ \end{pmatrix} + \begin{pmatrix} ۰ \\ m_۰^۳ m_۱ \\ z^{-۱} m_۰^۳ m_۱ \\ z^{-۲} m_۰^۳ m_۱ \end{pmatrix} x. \qquad (۶)$$

ادعا می‌کنیم که G ماتریس مولد برای یک CCC در $A(۷,-۱)$ است. چون $\pi = -۱$، باتوجه به رابطه ۴ داریم:

$$z * \sum_i c_i x^i = \sum_i (z^{(-۱)^i} c_i) x^i. \qquad (۷)$$

برای نشان دادن این‌که این کد یک CCC است، کافی است کلمات $G(۱۰۰۰)$، $G(۰۱۰۰)$، $G(۰۰۱۰)$، $G(۰۰۰۱)$ را درنظر بگیریم. سپس آنها را از طرف چپ در z ضرب نموده و نشان دهیم که این حاصل‌ضرب، متعلق به کد می‌باشد. برای سه‌تای اول این مطلب با توجه به روابط ٦ و ۷ واضح است؛ برای مثال:

$$\begin{aligned} z * (۰۱۰۰)G = &\quad z * (m_۰ m_۳ + m_۰^۳ m_۱ x) \\ = &\quad z m_۰ m_۳ + z^{-۱} m_۰^۳ m_۱ x = (۰۰۱۰)G. \end{aligned}$$

علاوه‌براین:

$$\begin{aligned} z * (۰۰۰۱)G = &\quad z * (z^۲ m_۰ m_۳ + z^{-۲} m_۰^۳ m_۱ x) \\ = &\quad z^۳ m_۰ m_۳ + z^{-۳} m_۰^۳ m_۱ x \\ = &\quad (۱+z) m_۰ m_۳ + (۱+z^٦) m_۰^۳ m_۱ x \\ = &\quad (۰۱۱۰)G. \end{aligned}$$

نکته اصلی از قضیه پیرت آن است که یک CCC همیشه دارای یک ماتریس مولد با یک شکل "ساده" مشابه با رابطه ٦ است. این مطلب، امکان ساخت مثال‌هایی به‌نسبت آسان و مطالعه خواص آنها نظیر فاصله آزاد را ممکن می‌سازد.

۱۳.٦ پیشنهادها

کدهای کانولوشن توسط الیاس[۱۳] در سال ۱۹۹۵ (ر.ک. مرجع [۲۰]) معرفی شدند. بحث‌های نسبتاً زیادی درمورد این سوال که آیا کدهای کانولوشن " بهتر" از کدهای بلوکی هستند یا خیر، مطرح شد. به‌رقم کمبود یک دید ریاضی عمیق، کدهای کانولوشن در عمل به‌طور موفق به‌کار برده شدند. بسیاری از این کدها به‌آسانی به‌طور تصادفی انتخاب شده‌اند. برای ماموریت یکی از ماهواره‌ها در عمق فضا (ر.ک. مرجع [۱])، یک پروژه طراحی شد که در آن ترکیبی از کدهای بلوکی و کدهای کانولوشن مطرح گردید. ایده آن به این صورت بود که یک رشته از اطلاعات را گرفته، آن را به بلوک‌هایی به طول ۱۲ بیت تقسیم

[۱۳] P. Elias

نموده و این بلوک‌ها را توسط کد گلی گسترش‌یافته [۲۴, ۱۲] کد نمایید. رشته به‌دست آمده به یک کدکننده کانولوشن وارد می‌شود. این مطلب مشابه ایده‌ای است که در مورد کدهای الحاقی از بخش ۹.۲ به‌کار برده شد.

برای مشاهده ارتباطی میان کدهای شبه‌دوری و کدهای کانولوشن، خواننده را به مقاله‌ای از سولومن[۱۴] و تیلبرگ[۱۵] ، مرجع [٦٦]، ارجاع می‌دهیم. آنها نشان دادند که به‌طور مثال کد گلی می‌تواند با استفاده از کانولوشن کدگذاری و کدگشایی شود.

در بخش ۳.۲ دیدیم که در کدگشایی کدهای بلوکی، فرایند تخمین الگوی خطا، به کلمه ارسالی بستگی ندارد. این ایده برای معرفی هم‌رفت[۱٦] (ارجاع به تعریف ۵.۳.۲) بود. ایده مشابهی به‌طور خیلی موفق برای کدهای کانولوشن به‌کار رفت. برای مشاهده جزییات بیشتر درباره این ایده، خواننده را به مقاله‌ای از شالکویج[۱۷] و پاست[۱۸] ، مرجع [٦٠]، ارجاع می‌دهیم. برخی از نتایج مربوط به احتمال خطا پس از کدگشایی کدهای کانولوشن در مرجع [۵۱] بخش ۹.۳ آمده است.

کامل‌ترین بحث درباره کدهای کانولوشن در کتاب اخیر پیرت[۱۹] ، مرجع [۷۹]، یافت می‌شود.

۱۳.۷ مسائل

۱.۱۳.۷. فرض کنید در شکل ۱۳.۱، ما ارتباط بین سومین مدار دوضربه‌ای را با جمع‌وند متناظر با T_1 قطع نموده‌ایم. نشان دهید که کد حاصل فاجعه‌آمیز می‌باشد.

۲.۱۳.۷. فرض کنید $g(x)$ چندجمله‌ای مولد یک کد دوری با کمترین —فاصله d باشد. مانند بخش ۱۳.۱، دو چندجمله‌ای $G_0(x)$ و $G_1(x)$ را برای تولید یک کد کانولوشن با نرخ $\frac{1}{2}$ استفاده می‌کنیم. اگر ما این چندجمله‌ای‌ها را طوری درنظر بگیریم که $g(x) = G_0(x^2) + xG_1(x^2)$، آن‌گاه به واسطه رابطه ۱، تمامی دنباله‌های کدشده، مضربی از $g(x)$ هستند. مثالی ارائه دهید، که در آن فاصله آزاد کمتر از d باشد. نتیجه را با ساختن کدکننده موجود در شکل ۱۳.۱ چک کنید.

۳.۱۳.۷. فاصله آزاد CCC داده‌شده توسط رابطه ٦ را تعیین کنید.

---

[۱۴] G. Solomon
[۱۵] H. C. A. Van Tilborg
[۱٦] syndrome
[۱۷] J. P. M. Schalkwijk
[۱۸] K. A. Post
[۱۹] Ph. Piret

فصل ۱۴

راهنمایی‌ها و حل مسائل

فصل ۲

۱.۲.۵.

$$\sum_{0\le k<N/2}\binom{N}{k}q^k p^{n-k} < (pq)^{N/2}\sum_{0\le k<N/2}\binom{N}{k}$$

$$= 2^{N-1}(pq)^{N/2} < (0.07)^N.$$

۲.۲.۵. ۶۴ الگوی خطای ممکن وجود دارد. می‌دانیم که ۸ تا از اینها منجر به ۳ سمبل اطلاعاتی درست پس از کدگشایی می‌گردد. برای بررسی مابقی، باید تشخیص داد که تنها ۴ تا ۳—تایی لزوماً متمایز (s_1, s_2, s_3) وجود دارد. یک احتمال، به‌طور مثال $(s_1, s_2, s_3) = (1, 1, 0)$ را درنظر بگیرید. این احتمال می‌تواند توسط الگوهای خطای (۱۰۱۰۱۱)، (۰۱۱۱۰۱)، (۱۱۰۰۰۰)، (۰۱۰۰۱۱)، (۱۰۰۱۰۱)، (۰۰۰۱۱۰)، (۱۱۱۱۱۰) و البته (۰۰۱۰۰۰) که محتمل‌ترین آنها می‌باشد، ایجاد شود. تصمیم ما این است که فرض کنیم $e_3 = 1$؛ بنابراین، دراینجا دو سمبل اطلاعاتی درست با احتمال $2p^2q^4 + p^4q^2$ و یک سمبل اطلاعاتی درست با احتمال $2p^3q^3 + p^5q$ را به‌دست می‌آوریم.

با بررسی سایر حالات به‌روش مشابه، احتمال خطای سمبل را به صورت زیر داریم:

$$\tfrac{1}{3}(22p^2q^4 + 36p^3q^3 + 24p^4q^2 + 12p^5q + 2p^6)$$

$$= \tfrac{1}{3}(22p^2 - 52p^3 + 48p^4 - 16p^5).$$

در مثال ما، این مقدار برابر با ۰.۰۰۰۰۰۷ است که می‌توان آن را با مقدار ۰.۰۰۱ بدون کدگشایی مقایسه نمود.

۳.۲.۵. به‌عنوان کدکلمه، تمامی ۸–تایی‌ها به‌صورت زیر را درنظر بگیرید:

$$(a_1, a_2, a_3 \quad a_2 + a_3, \quad a_1 + a_3, \quad a_1 + a_2, \quad a_1 + a_2 + a_3).$$

این کد با گرفتن هشت کلمه از مساله قبل و اضافه‌نمودن یک سمبل اضافی که مجموع شش سمبل اول است، ایجاد شده است. تاثیر آن، این است که هر دو کدکلمه متمایز در تعدادی زوج مکان با یکدیگر تفاوت دارند؛ یعنی $d(x, y) \geq 4$ برای هر دو کدکلمه متمایز x, y.

بررسی الگوهای خطا مشابه با موردی است که در بخش ۲.۲ به آن پرداخته شد. برای $(e_1, e_2, \cdots, e_7)$ داریم:

$$e_2 + e_3 + e_4 = s_1,$$

$$e_1 + e_3 + e_5 = s_2,$$

$$e_1 + e_2 + e_6 = s_3,$$

$$e_1 + e_2 + e_3 + e_7 = s_4,$$

۱۶ خروجی (s_1, s_2, s_3, s_4) ممکن وجود دارد. هشت تا از اینها می‌توانند توسط الگوی خطا با هیچ خطا یا یک خطا تشریح شوند. از میان مابقی، هفت تا وجود دارند، به‌طوری که هر یک از آنان می‌توانند توسط ۳ الگوی متفاوت خطا با دو خطا تشریح شوند؛ به‌طور مثال $(s_1, s_2, s_3, s_4) = (1, 1, 0, 0)$ متناظر با $(e_1, e_2, \cdots, e_7)$ که به‌صورت $(0\,0\,0\,1\,0\,0\,0)$، $(1\,1\,0\,0\,0\,0\,0)$ یا $(0\,0\,0\,1\,1\,0\,0)$ است، می‌باشد. بیشترین توصیف محتمل برای $(1, 1, 1, 0)$، وقوع سه خطا می‌باشد. بنابراین احتمال کدگشایی درست به‌صورت زیر است.

$$q^7 + 7q^6p + 7q^5p^2 + q^4p^3.$$

آن حدوداً برابر با $14p^2 - 1$ است؛ یعنی این کد خیلی بهتر از قبلی نیست، اگرچه دارای نرخ کمتر است.

۴.۲.۵. برای این کد با استفاده از تکرار سمبل‌ها، احتمال دریافت درست یک سمبل تکراری برابر با $1 - p^2$ است؛ بنابراین، کد با طول ۶ با کدکلمات $(a_1, a_2, a_3, a_1, a_2, a_3)$ دارای احتمال $(1 - p^2)^3 = 0.97$ دریافت درست است. کد موجود در مساله ۲.۲.۵ دارای این خاصیت است که هر دو کدکلمه در سه مکان فرق دارند؛ بنابراین، دو مکان پاک‌شده، نمی‌توانند ضرری برسانند. درواقع، بررسی تمام الگوهای خطای ممکن با سه مکان پاک‌شده نشان می‌دهد که ۱۶ تا از اینها نیز ضرری نمی‌رسانند. این مطلب، به احتمال دریافت صحیح $(1 - p)^3(1 + 3p + 6p^2 + 6p^3) = 0.996$ منجر می‌شود. این مقدار بهبود قابل ملاحظه‌ای با درنظر گرفتن این واقعیت است که دو کد بسیار مشابه هستند.

۵.۲.۵. با پاک‌شده، مانند صفرها برخورد کنید. حاصل‌ضرب‌های داخلی با حداکثر $2e_1 + e_2$ تغییر می‌کنند.

۶.۲.۵. یک ۱ را با ۱− و یک ۰ را با ۱+ جای‌گزین کنید. شرایط (۱) و (۲) ایجاب می‌کند که تصاویر کدکلمات، بردارهای متعامدی در $\mathbb{R}^{16}$ باشند؛ بنابراین، $|c| \leq 16$. برای ساخت چنین کدی، به یک ماتریس هادامارد مرتبه ۱۶ با شش تا ۱− در هر سطری نیاز داریم. یک ساختار معروف وجود دارد. آن یک کد دودویی را القا می‌کند که آسان‌ترین روش توصیف آن، نوشتن کدکلمات به‌صورت ماتریس‌های ۴ در ۴ است. یک سطر و ستون را ثابت نگه دارید؛ ۱ ها را در این سطر و ستون، مگر جایی که با یکدیگر تلاقی کنند، مستقر کنید. در این روش، ما ۱۶ کلمه با وزن ۶ یافته‌ایم که درواقع هر دوتای آنها دارای فاصله ۸ هستند.

۷.۲.۵. برای هر x، حداکثر $n/2$ کدکلمه وجود دارند، به‌طوری که با x در دو مکان متفاوت هستند. اگر کدکلمه‌ای وجود داشته باشد که با x دقیقاً در یک مکان تفاوت داشته باشد، آن‌گاه حداکثر $(n-2)/2$ کدکلمه دیگر وجود دارند، به‌طوری که با x در دو مکان متفاوت هستند (زیرا n زوج است). برای هر کدکلمه c، دقیقاً n کلمه وجود دارند، به‌طوری که با x در یک مکان متفاوت است و $\binom{n}{2}$ کلمه وجود دارند، به‌طوری که در دو مکان متفاوت هستند.

زوج‌های (x, c) را به دو روش بشمارید، داریم:

$$|c|.\binom{n}{2} \leq |c|.n.\frac{n-2}{2} + (2^n - |c|.(n+1)).\frac{n}{2},$$

که در آن نتیجه حاصل می‌شود. کد موجود در بخش ۲.۱ مثالی است که در مورد آن تساوی برقرار است.

فصل ۳

۱.۳.۸. با استفاده از شرط ۶.۳.۱ داریم $\sum_{i=0}^{3}\binom{n}{i} = 2^l$ برای برخی مقادیر صحیح l. این معادله به $(n+1)(n^2-n+6) = 3.2^{l+1}$، یعنی $(n+1)\{(n+1)^2 - 3(n+1) + 8\} = 3.2^{l+1}$، کاهش می‌یابد. اگر $n+1$ بر ۱۶ بخش‌پذیر باشد، آن‌گاه دومین عامل طرف چپ بر ۸ بخش‌پذیر است، اما بر ۱۶ بخش‌پذیر نیست؛ یعنی آن ۸ یا ۲۴ است که یک تناقض است؛ بنابراین، $n+1$ یک مقسوم‌علیه ۲۴ است. چون $n \geq 7$ می‌بینیم که $n = 7, 11$ یا ۲۳، اما $n = 11$ در این معادله صدق نمی‌کند. برای $n = 7$، کد $M = \{0, 1\}$ یک نمونه است. برای $n = 23$، بخش ۴.۲ را ببینید.

۲.۳.۸. فرض کنید $c \in C$، $w(c) \leq n-k$. مجموعه‌ای از k مکان وجود دارد که c دارای مختصاتی برابر با صفر است. چون C روی این k مکان متقارن است، داریم $c = 0$؛ بنابراین، $d > n-k$. برای k مکان داده شده، کدکلماتی وجود دارند که شامل $d-1$ صفر در این مکان‌ها هستند؛ یعنی $d \leq n-k+1$.

مطابق با تعریف تفکیک‌پذیر داده شده در بخش ۳.۱، یک کد $[n, k, n-k+1]$ یک کد تفکیک‌پذیر با بیشترین فاصله[1] (کد MDS) نامیده می‌شود.

۳.۳.۸. چون $C \subset C^\perp$، هر $c \in C$ دارای این خاصیت است که $< c, c >= 0$، یعنی $w(c)$ زوج است؛ بنابراین، $< c, 1 >= 0$. اما $< 1, 1 >= 1$، چون طول کلمه فرد است؛ بنابراین، $C^\perp \backslash C$ با اضافه نمودن ۱ به تمامی کلمات C به‌دست آمده است.

۴.۳.۸. $|B_1(x)| = 1 + 6 = 7$. چون $|c| = 63 < 2^6$، ممکن است کسی فکر کند چنین کد Cیی وجود دارد. اما، اگر چنین Cیی وجود داشته باشد، آن‌گاه با استفاده از اصل لانه کبوتری، برخی از کلمات ۳—تایی C شامل سمبل‌های یکسانی در دو مکان آخر هستند. با حذف این سمبل‌ها یک کد دودویی C' با سه کلمه به‌طول ۴ و کمترین—فاصله ۳ ایجاد می‌شود. بدون کاستن از کلیت، یکی از این کلمات برابر با صفر است؛ بنابراین، دوتای دیگر دارای وزن بیشتر یا مساوی ۳ است و از این‌رو فاصله کمتر یا مساوی ۲ است که یک تناقض می‌باشد.

۵.۳.۸. با استفاده از جبرخطی مقدماتی، برای هر i ممکن است یک پایه برای C بیابیم، به‌طوری که $k-1$ بردار پایه شامل یک صفر در مکان i باشد و مابقی شامل یک ۱ در آن مکان باشد؛ بنابراین، دقیقاً q^{k-1} کدکلمه شامل یک ۰ در مکان i است.

۶.۳.۸. زیرکد C شامل کلمات با وزن زوج با اضافه‌نمودن سطر ۱ به ماتریس بررسی‌توازن C به‌دست می‌آید. این باعث کاهش بعد کد به اندازه ۱ عدد می‌شود.

۷.۳.۸. از ماتریس مولد برای هر $c \in C$ داریم:

$$c_1 + c_2 + c_5 = c_3 + c_4 + c_6 = c_1 + c_2 + c_3 + c_4 + c_7 = 0.$$

بنابراین، سیندروم‌های:

$$(s_1, s_2, s_3) = (e_1 + e_2 + e_5, e_3 + e_4 + e_6, e_1 + e_2 + e_3 + e_4 + e_7),$$

برای سه کلمه دریافتی به ترتیب برابر با $(0,0,0)$، $(0,0,1)$، $(0,1,0)$، $(1,0,0)$ هستند؛ بنابراین، (۱) یک کدکلمه است؛ با استفاده از کدگشایی با بیشترین درست‌نمایی (۲) شامل یک خطا در مکان ۷ است؛ (۳) شامل یک خطا در مکان ۱ یا یک خطا در مکان ۲ است، بنابراین، ما یک انتخاب داریم.

۸.۳.۸.

۱) اگر $p \equiv 1 \bmod 4$، آن‌گاه یک $\alpha \in \mathbb{F}_p$ وجود دارد، به‌طوری که $\alpha^2 = -1$؛ در این‌صورت $G = (I_4, \alpha I_4)$ یک ماتریس مولد از کد موردنظر است.

[1] maximum distance separable code

۲) اگر $p \equiv ۳ \bmod ۴$، آن‌گاه از این واقعیت استفاده می‌کنیم که تمامی عناصر $\mathbb{F}_p$ مربعی نیستند؛ بنابراین، یک α وجود دارد که مربعی است، گوییم $\alpha = \beta^۲$، که در آن $\alpha + ۱$ مربعی نیست؛ یعنی $\alpha + ۱ = -\gamma^۲$، لذا $\beta^۲ + \gamma^۲ = -۱$؛ پس:

$$G = \begin{pmatrix} ۱ & ۰ & ۰ & ۰ & \beta & \gamma & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & -\gamma & \beta & ۰ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۰ & \beta & \gamma \\ ۰ & ۰ & ۰ & ۱ & ۰ & ۰ & -\gamma & \beta \end{pmatrix},$$

این کار را انجام می‌دهد.

۳) اگر $p = ۲$، آن‌گاه مثال ۳.۳.۳ را ببینید.

۹.۳.۸.

۱) فرض کنید $(\bar{A}_۰, \bar{A}_۱, \cdots, \bar{A}_n, \bar{A}_{n+۱})$ توزیع وزنی $\bar{C}$ باشد؛ در این‌صورت $\bar{A}_{۲k-۱} = ۰$ و $\bar{A}_{۲k} = A_{۲k-۱} + A_{۲k}$. چون $\sum A_{۲k} z^{۲k} = \frac{۱}{۲}\{A(z)+A(-z)\}$ و $\sum A_{۲k-۱} z^{۲k-۱} = \frac{۱}{۲}\{A(z)-A(-z)\}$، داریم $\bar{A}(z) = \frac{۱}{۲}\{(۱+z)A(z) + (۱-z)A(-z)\}$.

۲) از (۱) و رابطه (۲)، شمارنده وزنی کد گسترش‌یافته با طول $n + ۱ = ۲^k$ به‌صورت زیر می‌باشد:

$$\frac{۱}{۲}\left\{\frac{(۱+z)^{n+۱} + (۱-z)^{n+۱}}{n+۱}\right\} + \frac{n}{n+۱}(۱-z^۲)^{(n+۱)/۲}.$$

حال قضیه ۲.۳.۵ را به‌کار می‌گیریم. شمارنده وزنی کد دوگان برابر با $۱ + ۲nz^{(n+۱)/۲} + z^{n+۱}$ است؛ یعنی تمامی کلمات این کد به‌جز ۰ و ۱ دارای وزن $۲^{k-۱}$ هستند.

۱۱.۳.۸. این الگوی خطا، یک کدکلمه ناصفر c است. اگر $w(c) = i$، آن‌گاه احتمال این الگوی خطا برابر با $p^i(۱-p)^{n-i}$ است؛ بنابراین، احتمال یک خطای تشخیص داده نشده برابر با $(۱-p)^n\{-۱ + A(p/(۱-p))\}$ است.

۱۲.۳.۸. فرض کنید G_i $(i = ۱, ۲)$ یک ماتریس مولد برای C_i در فرم استاندارد باشد. تعریف کنید $A_{ij} \in \mathcal{R}$ $(۱ \le i \le k_۱,\ ۱ \le j \le k_۲)$ آن‌چنان که در ادامه می‌آید. $k_۱$ سطر اول A_{ij}، جز سطر i که برابر با iامین سطر $G_۱$ است، برابر با صفر هستند و به‌طور مشابه $k_۲$ ستون اول، جز ستون j که ترانهاده jامین ستون $G_۲$ است، برابر با صفر هستند. به‌آسانی دیده می‌شود که این مطلب به‌طور یکتا یک عضو A_{ij} در $\mathcal{R}$ را تعیین می‌کند. A_{ij}ها $k_۱k_۲$ عنصر مستقل خطی $\mathcal{R}$ هستند که کد C را تولید می‌کنند. اگر $A \in \mathcal{R}$ شامل یک سطر ناصفر باشد، آن‌گاه این سطر دارای وزن بزرگتر یا مساوی $d_۱$ است؛ یعنی شامل حداقل $d_۱$ ستون با وزن بزرگتر یا مساوی $d_۲$؛ بنابراین، C دارای کمترین—فاصله بزرگتر یا مساوی $d_۱d_۲$ است. درواقع تساوی برقرار است.

۱۳.۳.۸. این زیرکد روی مکان‌های ۱، ۹ و ۱۰ کد تکرار است که کامل بوده و تصحیح‌کننده یک خطاست. این زیرکد روی هفت مکان باقی‌مانده، کد همینگ $[7,4]$ است که هم‌چنین کامل است؛ بنابراین، روش یکتایی در تصحیح حداکثر یک خطا روی هر یک از این دو زیرمجموعه از مکان‌ها داریم. C دارای کمترین—فاصله ۳ و شعاع پوششی ۲ است.

۱۴.۳.۸.

۱) ادعای A_k :=" پس از 2^k انتخاب، یک کد خطی داریم و برای $i < k$ طول کلمه پس از 2^i مرحله افزایش می‌یابد" را درنظر بگیرید. برای $k = 1$، این ادعا درست است. فرض کنید A_k برای برخی مقادیر k درست باشد. کدکلمه c_{2^k} را درنظر بگیرید. لیست کلمات انتخاب‌شده شبیه زیر است:

$$
\begin{array}{ll}
A & \left\{\begin{array}{ll} c_0 & = 0\ 0\ \cdots\ 0\ 0\ \cdots\ 0 \\ \vdots & \\ c_{2^{k-1}-1} & = *\ *\ \cdots\ 1\ 0\ \cdots\ 0 \end{array}\right. \\
B & \left\{\begin{array}{ll} c_{2^{k-1}} & = *\ *\ \cdots\ *\ 11\ \cdots\ 1 \\ \vdots & \\ c_{2^k-1} & = *\ *\ \cdots\ *\ 11\ \cdots\ 1 \end{array}\right.
\end{array}
$$

که در آن کلمات موجود در B با اضافه‌نمودن $c_{2^{k-1}}$ به کلمات A به‌دست آمده‌اند. اگر c_{2^k} دارای طولی یکسان با کلمات B باشد، چون آن از نظر الفبایی بزرگتر است، آن‌گاه c_{2^k} باید به‌شکل $c_{2^{k-1}} + x$ باشد، که در آن x شامل بردار صفر در آخرین مکان است. اما $d \le d(c_{2^{k-1}} + x, c_{2^{k-1}} + c_i) = d(x, c_i)$، که در آن $0 \le i < 2^{k-1}$، نشان می‌دهد که ما باید x را به‌جای $c_{2^{k-1}}$ انتخاب کرده باشیم که یک تناقض است؛ بنابراین، طول این کد، هنگامی که c_{2^k} را انتخاب می‌کنیم، افزایش می‌یابد. حال فرض کنید نشان داده‌ایم $c_{2^k+i} = c_{2^k} + c_i$ برای $0 \le i < j$ (این مطلب برای $i = 0$ درست است). داریم $d(c_{2^k} + c_j, c_{2^k} + c_i) = d(c_i, c_j) \ge d$، $d(c_{2^k} + c_j, c_i) = d(c_{2^k}, c_i + c_j) \ge d$ چون با استفاده از فرض خطی بودن داریم $c_i + c_j = c_v$ برای مقداری v. این مطلب اثبات می‌کند که $c_{2^k} + c_j$ یک انتخاب ممکن برای کدکلمه c_{2^k+j} است. قسمت مشکل، نشان دادن این مطلب است که آن کمترین انتخاب است. برعکس، فرض کنید ایت انتخاب برابر با $c_{2^k} + x$ باشد، که در آن $c_{2^k} + x \prec c_{2^k} + c_j$ (نماد $\prec$ را برای ترتیب الفبایی به‌کار می‌بریم). با استفاده از فرض استقرا داریم $x \succ c_j$. این نامساوی ایجاب می‌کند c_j، x و c_{2^k} شبیه زیر باشند.

$$
\begin{array}{lllllllllllll}
c_j & = & * & \cdots & * & 0 & a_1 a_2 & \cdots & a_t & 0 & 0 & \cdots & 0 & 0 \\
x & = & * & \cdots & * & 1 & a_1 a_2 & \cdots & a_t & 0 & 0 & \cdots & 0 & 0 \\
c_{2^k} & = & * & \cdots & * & 1 & ** & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & *1
\end{array}
$$

فرض این‌که $c_{۲^k}+x$ یک انتخاب قابل‌قبول است، ایجاب می‌کند (مجدداً با به‌کارگیری خطی‌بودن) که:

$$d(c_{۲^k}+x, c_j+c_i)\geq d, \quad ۰\leq i<۲^k \text{ برای},$$

یعنی:

$$d(c_{۲^k}+x+c_j, c_i)\geq d, \quad ۰\leq i<۲^k \text{ برای}.$$

اما $c_{۲^k}+x+c_j \prec c_{۲^k}$؛ یعنی این انتخاب $c_{۲^k}$ کمترین نبوده است که یک تناقض است. این مطلب، اثبات ادعای A_k را با توجه به استقرا کامل می‌کند.

۲) حال، حالت $d=۳$ را درنظر بگیرید. فرض کنید n_k طول کد پس از انتخاب ۲^k بردار باشد. اگر C_k کامل نباشد، آن‌گاه یک بردار x به‌طول n_k وجود دارد که دارای فاصله بزرگتر یا مساوی ۲ با هر کلمه از C_k است؛ بنابراین، $(x,۱)$ یک انتخاب ممکن برای $c_{۲^k}$ است. این به ما $n_{k+۱}=n_k+۱$ را می‌دهد. اگر، از طرف دیگر، C_k کامل باشد، آن‌گاه واضح است که $n_{k+۱}=n_k+۲$ و $c_{۲^k}=(۱,۰,۰,\cdots,۰,۱,۱)$. حال ادعای B_α: "طول n_k برای $k=۲^a-a-۱+i$ و $۱\leq i<۲^a$ برابر با ۲^a+i است." با استفاده از استقرا در مشاهده فوق نتیجه می‌شود. در هر یک از دنباله‌های مذکور در B_α، کد نهایی یک کد همینگ است.

۱۵.۳.۸. اگر C یک کد $[۱۵,۸,۵]$ باشد، آن‌گاه C باید شامل یک کلمه به وزن ۵ باشد، زیرا درغیر این‌صورت می‌توانیم یک کد $[۱۴,۸,۵]$ را پنچر کنیم که نمی‌تواند وجود داشته باشد، زیرا $۲^۸$ گوی با شعاع ۲ شامل نقاط بسیار زیادی است (قضیه ۹.۵.۲ را ببینید). چنین کلمه‌ای را به‌عنوان سطر اول ماتریس مولد درنظر بگیرید. روی مکان‌هایی که این سطر شامل صفر است، هفت سطر دیگر یک کد $[۱۰,۷]$ تولید می‌کنند که باید شامل کمترین—فاصله ۳ باشد. مجدداً، این شرط گوی—پوششی را نقض می‌کند. (قسمت کدهای باقی‌مانده در بخش ۴.۴ را ببینید).

فصل ۴

۱.۴.۸. با استفاده از تعریف ۶.۴.۵، $\mathcal{R}(۱,m)$ دارای بعد $m+۱$ است؛ یعنی آن شامل $۲^{m+۱}$ کلمه به‌طول $n=۲^m$ است. با استفاده از قضیه ۹.۴.۵، هر یک از $۲(۲^m-۱)$ ابرصفحه $AG(m,۲)$ یک کدکلمه $\mathcal{R}(۱,m)$ را ایجاب می‌کند؛ یعنی جز برای ۰ و ۱، هر کدکلمه تابع مشخصه‌ای از یک ابرصفحه است. کدکلمه صفر و کدکلمات متناظر با ابرصفحه مار بر مبدا را درنظر بگیرید. در هر یک از این مختصات، سمبل صفر را با ۱— جای‌گزین کنید. چون دو ابرصفحه در $۲^{m-۱}$ نقطه تلاقی دارند، این n بردار دوبه‌دو متعامد هستند.

۲.۴.۸. چون این کد کامل است، هر کلمه با وزن ۳ در $\mathbb{F}_3^{11}$ دارای فاصله ۲ با یک کدکلمه به وزن ۵ است؛ بنابراین، $A_5 = 2^3\binom{11}{3}/\binom{5}{2} = 132$. مجموعه ۵تایی متناظر با x را با $B(x)$ نشان دهید. فرض کنید x و y، $y \notin \{x, 2x\}$، کدکلمه‌ای به وزن ۵ باشند، به‌طوری که $|B(x) \cap B(y)| > 3$؛ بنابراین، $w(x+y) + w(2x+y) \leq 8$ که غیرممکن است، زیرا $x+y$ و $2x+y$ کدکلمه هستند. از این‌رو ۶۶ مجموعه $B(x)$، به تعداد $\binom{11}{4} = \binom{5}{4}.66$ مجموعه ۴تایی، یعنی تمام مجموعه‌های ۴تایی را می‌پوشانند.

۳.۴.۸. با به‌کارگیری قضیه ۸.۱.۳، هر دو سطر A دارای فاصله ۶ است و پس از یک جای‌گشت سمبل‌ها، آنها برابر با (۱۱۱,۱۱۱,۰۰۰,۰۰) و (۱۱۱,۰۰۰,۱۱۱,۰۰) می‌باشند. در این‌صورت هر سطر دیگر A باید از سنخ (۱۰۰,۱۱۰,۱۱۰,۱۰) یا (۱۱۰,۱۰۰,۱۰۰,۱۱) باشد. ۶۶ کلمه x_i، به‌ترتیب $x_j + x_k$، را درنظر بگیرید. با استفاده از دو کاربرد شکل استاندارد فوق (برای هر سه‌تایی (x_i, x_j, x_k) داریم $d(x_i, x_i + x_k) = w(x_k) = 6$، ۸ یا ۴ $= d(x_i, x_j + x_k) = w(x_i + x_j + x_k)$. چون $d(x, 1+y) = 11 - d(x, y)$ اضافه‌نمودن مولفه‌های ۶۶ کلمه به مجموعه، کمترین—فاصله را به ۳ تقلیل می‌دهد.

۴.۴.۸. ساختار موجود در بخش ۴.۱ را برای ماتریس پالی مرتبه ۱۷ به‌کار گیرید.

۵.۴.۸.

۱) نشان دهید این زیرکد متناظر با زیرکد کد ۶تایی تولیدشده توسط $(1, \omega, 1, \omega, 1, \omega)$ است.

۲) مانند اثبات برای $\mathcal{G}_{24}$، نشان دهید که این زیرکد دارای بعد ۴ است.

۳) نشان دهید $d = 4$.

۶.۴.۸. فرض کنید C یک کد (n, M, d) و d زوج باشد. C را پنچر کنید. کد جدید C' یک کد $(n-1, M, d-1)$ است (اگر ما آن را به یک روش مناسب پنچر کنیم). کد $\bar{C}'$ یک کد (n, M, d) است، زیرا تمامی کلمات $\bar{C}'$ دارای وزن زوج هستند.

۷.۴.۸. اگر R و S ماتریس‌های ۳ در ۳ باشند، آن‌گاه بنویسید:

$$\begin{pmatrix} R & S & S & S \\ S & R & S & S \\ S & S & R & S \\ S & S & S & R \end{pmatrix} := M(R, S).$$

سطرهای A، B، C و D به‌ترتیب دارای وزن‌های ۵، ۶، ۸ و ۹ هستند. برای دو کلمه a، b داریم $d(a, b) = w(a) + w(b) - 2 < a, b >$، که در آن $< a, b >$ در $\mathbb{Z}$ محاسبه شده است. با استفاده از ضرب

بلوکی داریم:

$$AA^T = M(۴I + J, ۲J), \qquad BB^T = M(۳I + ۳J, ۳J - I),$$

$$AB^T = M(۵J, ۳J) - ۲B^T, \quad \text{یک ماتریس با درایه‌های ۳ یا ۱}.$$

نتیجه می‌شود که دو سطر A، به‌ترتیب B، دارای فاصله ۶ یا ۸ هستند و این‌که یک سطر از A و یک سطر از B دارای فاصله ۵ یا ۹ می‌باشند. به‌روش مشابه، این واقعیت که فاصله‌های باقی‌مانده حداقل برابر با ۵ هستند از روابط زیر نتیجه می‌شود:

$$CA^T = (۴J - ۲I, ۴J - ۲I, ۴J - ۲I, ۴J - ۲I),$$

$$CB^T = (۴J, ۴J, ۴J, ۴J),$$

$$DA^T = ۳J + D, \quad DB^T = ۳J + ۲D,$$

$$CC^T = ۴J + ۴I, \quad DD^T = ۳I + ۶J, DC^T = ۶J.$$

(این ساختار توسط ون‌لینت[۲] مرجع [۴۳] ارائه شد).

۸.۴.۸. از قضیه ۸.۱.۳ داریم $A^T = -A$ و $AA^T = ۱۱I$. چنین بر می‌آید که روی $\mathbb{F}_۳$ هر دو سطر G دارای ضرب داخلی صفر هستند؛ یعنی G یک کد خوددوگان $[۲۴, ۱۲]$ تولید می‌کند؛ بنابراین، $(A \quad I)$ نیز یک ماتریس مولد برای C است. بنابراین، زمانی که به دنبال کلمات با کمترین—وزن می‌گردیم، ممکن است فرض کنیم که ۲۱ موقعیت اول، حداکثر در نیمی از کل وزن شرکت می‌کنند. چون C خوددوگان است، تمام وزن‌ها بر ۳ بخش‌پذیر هستند. هر سطر G دارای وزن $۱۲ = ۱۱ + ۱$ است و یک ترکیب خطی از دو سطر دارای وزن $۹ = ۷ + ۲$ است (این مطلب از $AA^T = ۱۱I$ نتیجه می‌شود)؛ بنابراین، یک ترکیب خطی از این سه سطر دارای وزن حداقل $(۷ - ۱۱) + ۳$ است و از این‌رو دست کم برابر با ۹ می‌باشد. این مطلب نشان می‌دهد که C دارای کمترین—وزن ۹ است.

تذکر ۱.۱۴.۰. این کد و کد سه‌تایی گلی نمونه‌هایی از کدهای متقارن[۳] هستند. این کدها توسط پلس[۴] (۱۹۷۲) معرفی شدند. کلمات با وزن ثابت در چنین کدهایی اغلب، t–طرح‌ها (حتی با $t = ۵$) موجود در مساله ۲.۴.۸ را القا می‌کنند. خواننده علاقه‌مند در این زمینه را به مرجع [۱۱] ارجاع می‌دهیم.

۹.۴.۸ فرض کنید $v_۰$، ...، $v_{m-۱}$ بردارهای پایه از $\mathcal{R}(۱, m)$ باشند. پس از ۳.۴.۵ قسمت (۱) و (۲) می‌بینیم که $w_۰ = (v_۰, v_۰)$، ...، $w_{m-۱} = (v_{m-۱}, v_{m-۱})$، $w_m = (۰, ۱)$ بردارهای $۱ = (۱, ۱)$،

[۲] J. H. van Lint

[۳] symmetry codes

[۴] V. Pless

پایه (با طول $۲^{m+۱}$) از $\mathcal{R}(۱, m+۱)$ هستند؛ بنابراین، یک بردار پایه $\mathcal{R}(\nabla+\infty, \Updownarrow+\infty)$ به شکل $w_{i_۱}\cdots w_{i_s}$ از نوع (u,u) با u به‌عنوان یک بردار پایه از $\mathcal{R}(r+۱,m)$ است ، اگر w_m در این حاصل‌ضرب رخ ندهد و آن از نوع $(۰,v)$ است، که در آن v یک بردار پایه از $\mathcal{R}(r,m)$ باشد، اگر w_m در حاصل‌ضرب رخ دهد. اگر $d(r,m)$ کمترین—فاصله $\mathcal{R}(r,m)$ باشد آن‌گاه از $(u,u+v)$—ساختار می‌دانیم که $d(r+۱,m+۱)=\min\{۲d(r+۱,m), d(r,m)\}$ و سپس قضیه ۷.۴.۵ با استقرا نتیجه می‌شود.

۱۰.۴.۸.

۱) بردارهای x^* و $c^*=\pm a_i$ را به‌عنوان بردارهایی در $\mathbb{R}^n$ درنظر می‌گیریم. واضح است که $< x^*, c^* >= n-۲d(x,c)$. ممکن است فرض کنیم که a_iها طوری انتخاب شده‌اند که $< x^*, a_i >$ مثبت است $(۱\le i\le n)$. بردارهای x^* و تمامی a_iها دارای طول $\sqrt{n}$ هستند؛ بنابراین، $\sum_{i=۱}^{n} < x^*, a_i >^۲ = n^۲$، زیرا a_iها دوبه‌دو متعامد هستند. نتیجه می‌شود که یک i وجود دارد، به‌طوری که $< x^*, a_i >$ حداقل برابر با $\sqrt{n}$ است.

۲) حال فرض کنید $m=۲k$ و $c\in\mathcal{R}(۱,m)$. با استفاده از تعریف c لیست مقادیر یک تابع خطی روی $\mathbb{F}_۲^m$ است و بنابراین، $d(x,c)$ تعداد نقاط متعلق به $\mathbb{F}_۲^m$ است، که در آن مجموع $x_۱x_۲+x_۳x_۴+\cdots+x_{۲k-۱}x_{۲k}$ و این تابع خطی مقدار ۱ را می‌گیرند. توجه داشته باشید که:

$$x_۱x_۲+x_۳x_۴+\cdots+x_{۲k-۱}x_{۲k}+x_۱$$

$$x_۱\bar{x}_۲+x_۳x_۴+\cdots+x_{۲k-۱}x_{۲k},$$

که در آن $\bar{x}_۲ := x_۲+۱$؛ بنابراین، دنباله‌ای از تبدیلات مختصات $\bar{x}_i := x_i+۱$ (برای $\mathbb{F}_۲^m$) این مجموع را به عبارتی هم‌ارز با $x_۱x_۲+\cdots+x_{۲k-۱}x_{۲k}$ یا مکمل آن (رگر جمله ۱ در این تابع خطی رخ دهد) تغییر می‌دهد. نقاط xیی را می‌شماریم، که در آن $x_۱x_۲+\cdots+x_{۲k-۱}x_{۲k}=۱$. این تعداد را با n_k نشان دهید. به‌وضوح $n_k=۳n_{k-۱}+(۲^{۲k-۲}-n_k)$، که از آن داریم $n_k=۲^{۲k-۱}-۲^{k-۱}$. این‌مقدار هم‌چنین می‌تواند با درنظرگرفتن بردار $(x_۱,x_۲,\cdots,x_{۲k-۱})$ محاسبه گردد. اگر این صفر نباشد، آن‌گاه $۲^{k-۱}$ انتخاب برای $(x_۲,x_۴,\cdots,x_{۲k})$ امکان‌پذیر است. از این رو $n_k=(۲^k-۱)۲^{k-۱}$.

۱۱.۴.۸. از آنجا که کد همینگ سه‌تایی خوددوگان می‌باشد نتیجه می‌شود که C خوددوگان است؛ $(J+I$ دارای رتبه ۴ است و ازاین‌رو C دارای بعد ۶ است)؛ بنابراین، کمترین—فاصله C یا ۳ یا ۶ می‌باشد. بدیهی است یک ترکیب خطی از اولین چهار سطر G دارای وزن بیشتر از ۴ است. از سوی دیگر یک ترکیب خطی از دو سطر آخر G دارای وزن ۶ است. باز هم چون $J+I$ دارای رتبه ۴ است، ترکیبی

شامل سطرهای هر دو نوع نمی‌تواند دارای وزن ۳ باشد.

فصل ۵

۱.۵.۵ یک ماتریس بررسی‌توازن مناسب برای کد دلخواه C با استفاده از چینش متوالی ستون‌ها می‌سازیم. هر ستون ناصفر می‌تواند اولین انتخاب ما باشد. اگر m ستون انتخاب شده باشند، آن‌گاه سعی می‌کنیم تا ستون بعدی را که ترکیب خطی از i ستون قبلی، برای هر $i \leq d-۲$، نیست، بیابیم. این روش تضمین می‌کند که هیچ $(d-۱)$–تایی از ستون‌های ماتریس بررسی‌توازن وابسته‌خطی نباشند؛ یعنی این کد دارای کمترین—فاصله حداقل d است. این روش کار می‌کند، اگر تعداد ترکیبات خطی حداکثر $d-۲$ ستون از m ستون انتخاب‌شده کمتر از q^{n-k} (برای هر $m \leq n-۱$) باشد. پس یک شرط کافی به‌صورت زیر است:

$$\sum_{i=۰}^{d-۲} \binom{n-۱}{i} (q-۱)^i < q^{n-k}.$$

سمت چپ نامساوی موجود در قضیه ۶.۵.۱، حداقل $n(q-۱)/(d-۱)$ برابر بزرگ است، سمت راست معدله فوق تنها q برابر بزرگ است، یعنی مساله ۱.۵.۵ در حالت کلی نتیجه قوی‌تری است.

۲.۵.۵. با استفاده از تعریف ۳.۵.۱ داریم $A(۱۰,۵) = A(۱۱,۶)$. بهترین کران با استفاده از قضیه ۴.۵.۲ به‌دست می‌آید (نیز مثال پس از قضیه ۶.۵.۳ را ببینید). داریم $A(۱۱,۶) \leq ۱۲$. از رابطه ۲۰ (هم‌چنین جواب مساله ۳.۴.۸ را ببینید) یک کد $(۱۱,۱۲,۶)$ داریم؛ بنابراین، $A(۱۰,۵) = ۱۲$.

۳.۵.۵. تساوی در قضیه ۴.۵.۲ تنها زمانی می‌تواند برقرار باشد که برای نامساوی‌های به‌کار رفته در این اثبات نیز برقرار باشد و این نیز تنها زمانی ممکن است که $\frac{۱}{۲}M^۲$ یک عدد صحیح باشد؛ بنابراین، $M = l$ غیرممکن است.

۴.۵.۵. با استفاده از مساله ۴.۴.۸ داریم $A(۱۷,۸) \geq ۳۶$. بهترین تخمین از بخش ۵.۲ با به‌کارگیری کران پلاتکین به‌دست می‌آید. داریم $A(۱۷,۸) \leq ۴A(۱۵,۸) \leq ۶۴$. یک نتیجه بهتر با به‌کارگیری قضیه ۴.۵.۳ به‌دست می‌آید. خواننده می‌تواند بررسی کند که این نتیجه به‌صورت $A(۱۷,۸) \leq ۵۰$ است. بهترین کران به‌دست آمده با تصحیح روش قضیه ۴.۵.۳ به‌صورت $A(۱۷,۸) \leq ۳۷$ (ر.ک. مرجع [۶]) است.

۵.۵.۵. ستون‌های ماتریس مولد، نقاط $(x_۱, x_۲, x_۳, x_۴, x_۵)$ از $PG(۴,۲)$ است. می‌دانیم (ارجاع به مساله ۱۰.۳.۸) که تمامی کدکلمات ناصفر کد $[۳۱,۵]$ دارای وزن ۱۶ هستند. با به‌کارگیری نتیجه‌ای مشابه، مکان‌های متناظر با $x_۱ = x_۲ = ۰$، زیرکدی با طول ۷ شامل تمامی وزن‌های ناصفر برابر با ۴ است و مکان‌هایی که $x_۳ = x_۴ = x_۵ = ۰$، زیرکدی با طول ۳ شامل تمامی وزن‌های ناصفر برابر با ۲ است.

اگر ما کد را در این ده مکان پنچر کنیم، آن‌گاه در کد $[۲۱, ۵]$ باقی‌مانده داریم $d = ۱۶ - ۴ - ۲ = ۱۰$. از قضیه ۷.۵.۲ داریم $n \geq ۱۰ + ۵ + ۳ + ۲ + ۱ = ۲۱$؛ یعنی کد پنچرشده به کران گریسمر دست می‌یابد.

۶.۵.۵. این نتیجه مستقیمی از اثبات لم ۱۸.۵.۲ است (مقدار میانگین وقوع یک زوج از آنها برابر با $|c|.\binom{w}{۲}/\binom{n}{۲} = A(n-۲, ۲k, w-۲)$ است و هیچ زوجی نمی‌تواند بیشتر از این تعداد رخ دهد).

۷.۵.۵. فرض کنید $n = ۲^k - ۲$. با استفاده از لم ۱۸.۵.۲ داریم $A(n, ۳, ۳) \leq \frac{۱}{۶}n(n-۲)$. از این‌رو قضیه ۱۹.۵.۲ ایجاب می‌کند:

$$A(n, ۳) \leq ۲^n \Big/ \left\{ ۱ + n + \left(\binom{n}{۲} - \frac{۳n(n-۲)}{۶} \right) \Big/ \binom{n}{۲} \right\} = ۲^{n-k}.$$

بنابراین، کد همینگ کوتاه‌شده $[n, n-k, ۳]$ بهینه است.

۸.۵.۵. اگر دو کلمه c و c' با وزن w دارای فاصله ۲ باشند، گوییم $c_j = c'_k = ۱$، $c'_j = c_k = ۰$، آن‌گاه $\sum_{i=۰}^{n-۱} ic_i - \sum_{i=۰}^{n-۱} ic'_i \equiv j - k \bmod n$. نتیجه می‌شود که هر یک از کدهای C_l $(۰ \leq l \leq n-۱)$ دارای کمترین—فاصله ۴ است؛ بنابراین، $A(n, ۴, w) \geq ۱/n\binom{n}{w}$، چون $\sum_{l=۰}^{n-۱} |c_l| = \binom{n}{w}$. با استفاده از لم ۱۸.۵.۲ داریم $A(n, ۴, w) \leq \binom{n}{w}/(n-w+۱)$. با ترکیب نمودن این نامساوی‌ها، نتیجه حاصل می‌گردد (برای مشاهده تعمیم این مطلب به مرجع [۳۰] رجوع نمایید).

۹.۵.۵. فرض کنید C یک کد $(n, M, ۲k)$ دودویی باشد؛ تعریف کنید:

$$S := \{(c, x) | c \in C, x \in \mathbb{F}_۲^n, d(x, c) = w\}.$$

به‌وضوح $|S| = \binom{n}{w}M$. برای یک x ثابت، حداکثر $A(n, ۲k, w)$ کلمه c در C وجود دارند، به‌طوری که $d(x, c) = w$؛ بنابراین، $\binom{n}{w}M \leq ۲^n A(n, ۲k, w)$.

۱۰.۵.۵.

۱) اثبات این نامساوی لزوماً مشابه با اثبات لم ۱۳.۵.۲ است. اگر یک کد با وزن ثابت شامل m_i کلمه با یک ۱ در مکان i باشد، آن‌گاه با نمادگذاری معمول خود داریم:

$$۲k\binom{M}{۲} \leq \sum_{i=۱}^{n} m_i(M - m_i) \leq M^۲ w - n\left(\frac{Mw}{n}\right)^۲.$$

۲) فرض کنید $۲k/n \to \delta$ وقتی $n \to \infty$. فرض کنید $w/n \to \omega$ وقتی $n \to \infty$. پس $A(n, ۲k, w)$، وقتی $n \to \infty$، کراندار است و مساله ۹.۵.۵ ایجاب می‌کند $\alpha(\delta) \leq ۱ - H_۲(\omega)$. شرط $۱ - (w/k)(۱ - (w/n)) > ۰$ هنوز باید برقرار باشد؛ بنابراین، بهترین نتیجه حاصل می‌شود، اگر $۱ - (۲\omega/\delta)(۱ - \omega) = ۰$، یعنی $\omega = \frac{۱}{۲} - \frac{۱}{۲}\sqrt{۱ - ۲\delta}$ که قضیه ۱۶.۵.۲ است.

۱۱.۵.۵. داریم $K_۲(i) = ۲i^۲ - ۲ni + \binom{n}{۲}$ و این مقدار برای $d \le i \le n-d$، کمتر از $۲d^۲ - ۲nd + \binom{n}{۲}$ است. چون $A_۰ = A_n = ۱$ (بدون کاستن از کلیت) و $A_i = ۰$ برای سایر مقادیر i خارج از $[d, n-d]$، با توجه به لم ۳.۵.۳ داریم:

$$۲\binom{n}{۲} + (۲d^۲ - ۲nd + \binom{n}{۲}) \sum_{i=d}^{n-d} A_i \ge ۰.$$

این مطلب، نامساوی موردنیاز را ایجاب می‌کند.

۱۲.۵.۵. مساله تعیین $A(۹, ۴)$ با قضیه ۴.۵.۳ را درنظر بگیرید. ما چهار نامساوی برای $A_۴$، $A_۶$ و $A_۸$ یافتیم. ممکن است نامساوی بدیهی $A_۸ \le ۱$ به این دستگاه اضافه کنیم. یک محاسبه نسبتاً کسل‌کننده، جواب بهینه $A_۴ + A_۶ + A_۸ \le ۲۰\frac{۱}{۳}$ را ایجاب می‌کند؛ بنابراین، ما باید احتمال یک کد $(۹, ۲۱, ۴)$ را محاسبه کنیم. درنظر گرفتن $\omega = -۱$ در اثبات لم ۳.۵.۳ نامساوی زیر را نتیجه می‌دهد:

$$۲۱ \sum_{i=۰}^{۹} A_i K_k(i) \ge \binom{۹}{k},$$

یعنی با استفاده از:

$$K_k(۰) = \binom{۹}{k},$$

داریم:

$$\frac{۲۰}{۲۱} K_k(۰) + \sum_{i=۱}^{۹} A_i K_k(i) \ge ۰.$$

چون این کد دارای ۲۱ کلمه است، حداکثر ۱۰ زوج کدکلمه با فاصله ۸ وجود دارند؛ یعنی $A_۸ \le \frac{۲۰}{۲۱}$؛ بنابراین، مقادیر $\frac{۲۱}{۲۰}A_i$ باید در نامساوی مشابهی که ما آن را برای شروع حل کردیم، صدق کند. این مطلب ایجاب می‌کند $A_۴ + A_۶ + A_۸ \le \frac{۲۰}{۲۱}.\frac{۶۱}{۳} < ۲۰$ که یک تناقض است.

فصل ۶

۱.۶.۱۳. ما بخش‌های ۶.۱ و ۶.۲ را گسترش می‌دهیم. روی $\mathbb{F}_۳$ داریم $x^۴ + ۱ = (x^۲ + x + ۲)(x^۲ + ۲x + ۲)$؛ بنابراین، $x^۲ + x + ۲$ مولد یک کد نادوری $[۴, ۲]$ با ماتریس مولد $\begin{pmatrix} ۱ & ۰ & ۲ & ۱ \\ ۰ & ۱ & ۱ & ۲ \end{pmatrix}$ است. با استفاده از تعریف ۱.۳.۳ این یک کد همینگ $[۴, ۲]$ است.

۲.۶.۱۳. چون $x^۴ + x + ۱$ اولیه است، می‌توانیم آن را به‌عنوان مولد کد همینگ $[۱۵, ۱۱]$ درنظر بگیریم. حال روند اثبات قضیه ۱.۶.۴ را برای یافتن $a(x)(x^۴ + x + ۱)$ پیروی کنید که ثابت می‌شود آن برابر با $۱ + (x + x^۲ + x^۴ + x^۸) + (x^۳ + x^۶ + x^۹ + x^{۱۲})$، مجموعی از سه خودتوان متناظر با

هم‌مجموعه‌های دوری، است. روش توصیف شده پس از قضیه ۴.۶.۴ پ مثال داده‌شده در آنجا، یک جواب دوم تهیه می‌کند.

۳.۶.۱۳. ماتریس E معرفی‌شده در بخش ۴.۵ را درنظر بگیرید و اولین ستون آن را حذف کنید. حال یک لیست از نقاط مخالف با $(۰, ۰, \cdots, ۰)$ در $AG(m, ۲)$ داریم که به‌صورت بردارهای ستونی نوشته شده‌اند. نیز می‌توانیم این را به‌صورت لیستی از عناصر $\mathbb{F}_{۲^m}^*$ درنظر بگیریم. این یک گروه دوری تولیدشده توسط یک عضو اولیه ξ از $\mathbb{F}_{۲^m}$ است. نگاشت $A : \mathbb{F}_{۲^m} \to \mathbb{F}_{۲^m}$ تعریف شده به‌صورت $A(x) := \xi x$ به‌وضوح یک تبدیل خطی نامنفرد از $AG(m, ۲)$ به خودش است و به‌عنوان جای‌گشتی از نقاط $AG(m, ۲)\backslash\{۰\}$ دارای مرتبه $۲^m - ۱$ است. نگاشت A، نواحی مسطح را به نواحی مسطح تصویر می‌کند. حال از لم ۵.۴.۵ قسمت (۱)، تعریف ۶.۴.۵ و قضیه ۹.۴.۵ نتیجه می‌شود که جای‌گشت مکان‌های مختصات متناظر با A یک نمایش دوری از کد کوتاه‌شده ایجاب می‌کند.

۴.۶.۱۳. $x^۳ + ۲x + ۱$ را برای تولید $\mathbb{F}_۳^۳$ به‌کار برید. اگر β یک عضو اولیه باشد، آن‌گاه $x^۳ + ۲x + ۱$ چندجمله‌ای مینیمال آن است. با استفاده از جدول میدان متناظر آن، چندجمله‌ای مینیمال $\beta^۲$ را می‌یابیم که به‌صورت $(x - \beta^۲)(x - \beta^۶)(x - \beta^{۱۸}) = x^۳ + x^۲ + x + ۲$ است و چندجمله‌ای مینیمال $\beta^۴$ به‌صورت $(x^۳ + x^۲ + ۲)$ است. حاصل‌ضرب این توابع شامل ریشه‌های β، $\beta^۲$، $\beta^۳$ و $\beta^۴$ است؛ بنابراین، این کد مطلوب را ایجاد می‌کند. چندجمله‌ای مولد به‌صورت زیر است:

$$۱ + x + ۲x^۲ + ۲x^۳ + ۲x^۴ + x^۵ + x^۶ + x^۷ + ۲x^۸ + x^۹.$$

بعد کد برابر با ۱۷ است.

۵.۶.۱۳. درابتدا، جدولی از $\mathbb{F}_{۲^۵}$ بسازید. با جای‌گذاری داریم $E(\alpha^i) = R(\alpha^i)$ برای $i = ۱, ۲, ۳, ۴$. اینها به‌ترتیب $\alpha^{۲۸}$، $\alpha^{۲۵}$، ۱ و $\alpha^{۱۹}$ هستند. ما باید $\sigma(z) = ۱ + \sigma_۱ z + \sigma_۲ z^۲$ را از معادلات $۰ = \alpha^{۲۸} + \sigma_۱\alpha^{۲۵} + \sigma_۲ + ۱$ و $۰ = \alpha^{۱۹} + \sigma_۱ + \sigma_۲\alpha^{۲۵}$ بیابیم. داریم $\sigma_۱ = \alpha^{۲۸}$ و $\sigma_۲ = \alpha^{۱۰}$؛ یعنی:

$$\sigma(z) = (۱ - \alpha^{۱۴}z)(۱ - \alpha^{۲۷}z).$$

بنابراین، این کدکلمه برابر است با:

$$(۱۰۰۱۰۱۱۰۱۱۱۱۰۰۱۰۱۱۰۱۰۱۰۱۰۱۱۰۱۱۱).$$

مولد این کد برابر با $(۱ + x^۲ + x^۵)(۱ + x^۲ + x^۳ + x^۴ + x^۵)$ است؛ یعنی:

$$g(x) = ۱ + x^۳ + x^۵ + x^۶ + x^۸ + x^۹ + x^{۱۰}.$$

کدکلمه مذکور به‌صورت زیر است:

$$g(x)(۱ + x^{۱۱} + x^{۲۰}).$$

۶.۶.۱۳. چون مجموعه تعریف C شامل $\{\beta^j \mid j = -۲, -۱, ۱, ۲\}$ است، از مثال ۱۲.۶.۶ (با $d_A = ۳$ و $|B| = ۲$) نتیجه می‌شود که $d \geq ۴$. زیرکد C' از C شامل کلمات زوج را درنظر بگیرید. کلمات این کد دارای ریشه‌های $\beta^{-۲}$، $\beta^{-۱}$، $\beta^{۰}$، $\beta^{۱}$، $\beta^{۲}$ هستند؛ بنابراین، با استفاده از کران BCH، C' دارای کمترین—فاصله حداقل ۶ است. نتیجه می‌شود $d \geq ۵$.

۷.۶.۱۳. کد C' را که یک کد $[q+۱, ۲, q]$ است، درنظر بگیرید. این کد روی هر دو مکانی متقارن است (ارجاع به مساله ۲.۳.۸). برای ضرایب شمارنده وزنی این مطلب ایجاب می‌کند که:

$$(q+۱)A_{q+۱} + aA_q = (q+۱)(q^۲ - q).$$

چون $A_{q+۱} + A_q = q^۲ - ۱$ داریم $A_{q+۱} = ۰$؛ یعنی هر کدکلمه ناصفر دارای وزن q است. کدکلمه یکتای $c = (c_۰, c_۱, \cdots, c_q)$ طوری که $c_۰ = c_{(q+۱)/۲} = ۱$ وجود دارد. چون دقیقاً یکی از مختص‌های c برابر صفر است، یک شیفت دوری از c روی $\frac{۱}{۲}(q+۱)$ مکان، کلمه مشابه c را القا نمی‌کند؛ بنابراین، C' دوری نمی‌باشد.

۸.۶.۱۳. روی $\mathbb{F}_۳$ داریم:

$$x^{۱۱} - ۱ = (x-۱)(x^۵ - x^۳ + x^۲ - x - ۱)(x^۵ + x^۴ - x^۳ + x^۲ - ۱),$$

که در آن این عوامل تحویل‌ناپذیر هستند؛ بنابراین، مشابه با تعریف ۱.۶.۹، $g_۰(x) = x^۵ - x^۳ + x^۲ - x - ۱$ را به‌عنوان مولد کد QR $[۱۱, ۶]$ سه‌تایی C درنظر می‌گیریم. هم کران BCH و هم قضیه ۲.۶.۹ نتیجه می‌دهند $d \geq ۴$؛ در حالت آخر، محدودیت $c(۱) \neq ۰$ وجود دارد. کد $C^{\perp}$ دارای مولد $(x-۱)g_۰(x)$ است (ارجاع به بخش ۶.۲). حال کد $\bar{C}$ حاصل از اضافه‌نمودن یک بررسی‌توازن سراسری به روش معمول را درنظر بگیرید. اگر G یک ماتریس مولد برای $C^{\perp}$ باشد، آن‌گاه یک ماتریس مولد برای C با اضافه‌نمودن سطر ۱ به‌دست می‌آید و یک ماتریس مولد برای $\bar{C}$ به‌صورت زیر داده می‌شود:

$$\left(\begin{array}{ccc|c} & & & ۰ \\ & G & & ۰ \\ & & & \vdots \\ & & & ۰ \\ \hline ۱ & ۱ & \cdots\ ۱ & ۱ \end{array}\right)$$

می‌بینیم که $\bar{C}$ خوددوگان است. حاصل‌ضرب داخلی یک کدکلمه با خودش (روی $\mathbb{R}$) برابر با تعداد مختصات ناصفر است. بنابراین، هر کدکلمه در C دارای وزنی بخش‌پذیر بر ۳ است. این مطلب ثابت می‌کند $d \geq ۵$. این‌که C کامل است از تعریف و به‌کارگیری رابطه $۳^۵ = ۲^۲.\binom{۱۱}{۲} + ۲.\binom{۱۱}{۱} + ۱$ نتیجه می‌شود.

۹.۶.۱۳. با استفاده از نتیجه ۵.۶.۹ داریم d فرد است. با استفاده از قضیه ۲.۶.۹ قسمت (۲) و (۳) داریم $d^۲ - d + ۱ \geq ۴۷$ (یعنی $d \geq ۸$) و $d \equiv ۳ \bmod ۴$؛ بنابراین، $d \geq ۱۱$. با استفاده از کران همینگ (قضیه ۹.۵.۲) برای $d = ۲e + ۱$ داریم:

$$\sum_{i=۰}^{e} \binom{۴۷}{i} \leq ۲^{۴۷}/|c|.$$

چون C دارای بعد ۲۴ است، داریم $e \leq ۵$. نتیجه می‌شود $d = ۱۱$.

۱۰.۶.۱۳. در مثال بیان‌شده در بخش ۶.۹ و در مساله ۸.۶.۱۳ از قبل دیدیم که کد همینگ $[۷, ۴]$ و دو کد گلی، نمونه‌هایی از کدهای QR کامل بودند. یک کد QR کامل دیگر نیز وجود دارد. این‌که برای $e > ۱$ کد دیگری وجود ندارد، نتیجه مستقیمی از نتیجه فصل ۷ است. فرض کنید C یک کد QR به‌طول n روی $\mathbb{F}_q$ بوده و C یک کد کامل با $d = ۳$ باشد؛ در این‌صورت با استفاده از ۶.۳.۱ داریم:

$$۱ + n(q-۱) = q^{(n-۱)/۲}, \quad (\text{یا } q^{(n+۱)/۲})$$

دو حالت مشابه هستند. در اولی، داریم:

$$n = ۱ + q + q^۲ + \cdots + q^{(n-۳)/۲}.$$

اگر $n > ۵$، آن‌گاه طرف راست حداقل برابر است با:

$$۱ + ۲ + \frac{n-۵}{۲}.۴ = ۲n - ۷,$$

یعنی $n = ۷$ و $q = ۲$ و C کد همینگ $[۷, ۴]$ است. آنچه باقی می‌ماند امتحان $n = ۳$ و $n = ۵$ است؛ داریم:

$$۱ + ۳(q-۱) = q, \quad ۱ + ۵(q-۱) = q^۲ \text{ . به‌ترتیب}$$

بنابراین، تنها جواب برابر با $n = ۵$، $q = ۴$ است.

۱۱.۶.۱۳. فرض کنید β یک ریشه اولیه از $\mathbb{F}_n$ باشد. تعریف کنید $R_v := \{\beta^i \in \mathbb{F}_n \mid i \equiv v \bmod e\}$، $۰ \leq v < e$. فرض کنید α یک ریشه nام اولیه واحد در یک توسیع میدان $\mathbb{F}_q$ باشد. تعریف می‌کنیم:

$$g_v(x) := \prod_{r \in R_v} (x - \alpha^r), \qquad ۰ \leq v < e.$$

چون $q \in R_0$، هر یک از g_vها دارای ضرایبی در $\mathbb{F}_q$ است. علاوه‌براین، این چندجمله‌ای‌ها دارای درجه $(n-1)/e$ است و

$$x^n - 1 = (x-1)g_0(x)g_1(x)\cdots g_{e-1}(x).$$

eامین توان کد باقی‌مانده C دارای م.لد $g_0(x)$ باشد. کدهای با مولد $g_v(x)$ همگی هم‌ارز هستند. اثبات قضیه ۲.۶.۹ قسمت (۱) می‌تواند تکرار شود تا نتیجه بگیریم $d^e > n$. اگر $n = 31$، $e = 3$، $q = 2$ ایجاب می‌کند $d^3 > 31$؛ بنابراین، $d \geq 4$. چون $5^3 \equiv -1$ در $\mathbb{F}_{31}$. علاوه‌براین توسط کران همینگ داریم $d < 7$. درواقع، حتی کران همینگ نشان می‌دهد که کد شامل 2^{20} کلمه از C با وزن فرد نمی‌تواند دارای $d = 7$ باشد. از این‌رو $d = 5$.

۱۲.۶.۱۳.

۱) چون α، α^2، α^4، α^5 ریشه‌های کدکلمات هستند، $d \geq 4$ نتیجه مستقیمی از مثال ۱۲.۶.۶ است.

۲) با استفاده از کران BCH داریم $d \geq 3$. اگر $d = 3$، آن‌گاه کدکلمه‌ای با مختص‌های ۱ در مکان‌های ۰، i، j وجود خواهد داشت. فرض کنید $\xi = \alpha^i$، $\eta = \alpha^j$؛ در این‌صورت $1 + \xi + \eta = 0$، $\xi^2 + \eta^5 + 1 = 0$. پس داریم $(\xi+\eta)^5 = (\xi^5 + \eta^5) + \xi\eta(\xi^3 + \eta^3) = 1$؛ یعنی $\xi^3 + \eta^3 = 0$. این یک تناقض است، زیرا $2^m - 1 \not\equiv 0 \bmod 3$، بنابراین، $x^3 = 1$ دارای جواب یکتای $x = 1$ است، درحالی‌که $\xi \neq \eta$.

۳) اگر کلمه‌ای با وزن ۴ موجود باشد، آن‌گاه با یک شیفت دوری، کلمه‌ای با وزن ۴ وجود دارد که مختص‌های ناصفر آن در مکان‌های ξ، $1+\xi$، η و $1+\eta$ است. مجموع توان‌های پنجم این عناصر برابر صفر است. این مطلب ایجاب می‌کند $(\xi+\eta)^3 = 1$، یعنی $\xi + \eta = 1$ که یک تناقض است.

۱۳.۶.۱۳. نمایش مساله ۸.۶.۱۳ را درنظر بگیرید. فرض کنید α یک عضو اولیه از $\mathbb{F}_{32}$ باشد؛ در این‌صورت α^{22} یک ریشه ۱۱ ام اولیه واحد است؛ یعنی یک ریشه از $g_0(x)$ یا $g_1(x)$؛ بنابراین، نمایش‌های ۱، α^{22}، α^{44}، ...، α^{220} به‌عنوان عناصر $(\mathbb{F}_2)^5$، ستون‌هایی از یک ماتریس بررسی‌توازن C هستند. ستون‌های متناظر با α^{22i} برای $i > 5$ را در $\alpha^{121} - 1 = 0$ ضرب کنید و آنها را نگه داشته تا مقادیر ۱، α^{11}، α^{22}، ...، α^{110} متناظر با یک ریشه $x^{11} + 1$ به‌دست آید. این کد هم‌ارز با C است که یکتایی آن شناخته‌شده است و این نمایش نادوری است.

۱۴.۶.۱۳. مجموعه تعریف این کد به‌صورت زیر است:

$$R = \{\alpha^i \mid i = 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}.$$

نشان دهید مجموعه R شامل AB است، که در آن $A = \{\alpha^i \mid i = ۸, ۹, ۱۰\}$ و $B = \{\beta^j \mid j = ۰, ۱, ۳\}$، $\beta = \alpha^{۱۰}$. این مطلب ایجاب می‌کند $d \geq ۶$. برای زیرکد شامل وزن‌های زوج، در نظر بگیرید $A = \{\alpha^i \mid i = ۴, ۷, ۸, ۹\}$، $B = \{\beta^j \mid j = ۰, ۳, ۴\}$، $\beta = \alpha^{۸}$. قضیه ۱۱.۶.۶ را برای $|I| = ۶$ به‌کار بگیرید.

فصل ۷

۱.۷.۷. فرض کنید C کد مذکور باشد. چون کد همینگ با طول $n + ۱ = ۲^m - ۱$ برای $e = ۱$ کامل است، C دارای شعاع پوششی ۲ است. $n = ۲^m - ۲$، $|c| = ۲^{n-m}$، $e = ۱$ را در رابطه ۳ جای‌گزین کنید. ما به تساوی دست می‌یابیم. نتیجه می‌شود که C تقریباً کامل است.

۲.۷.۷. فرض کنید $\rho(u, C) = ۲$، یعنی $u = c + e$، که در آن $c \in C$ و e دارای وزن ۲ است. چون $c(\alpha) = c(\alpha^۳) = ۰$ و $e(x) = x^i + x^j$ برای برخی مقادیر i و j. ما روش‌های مختلفی که بتوانیم سه مکان را تغییر داده، برچسب‌گذاری شده با $x_۱$، $x_۲$، $x_۳$، محاسبه نموده و بدین گونه یک کدکلمه می‌یابیم؛ بنابراین، ما تعداد جواب‌های دستگاه زیر را محاسبه می‌کنیم:

$$x_۱ + x_۲ + x_۳ + \alpha^i + \alpha^j = ۰,$$

$$x_۱^۳ + x_۲^۳ + x_۳^۳ + \alpha^{۳i} + \alpha^{۳j} = ۰.$$

$y_i := x_i + e(\alpha)$ را جای‌گزین می‌کنیم؛ داریم:

$$y_۱ + y_۲ + y_۳ = ۰,$$

$$y_۱^۳ + y_۲^۳ + y_۳^۳ = s := \alpha^{i+j}(\alpha^i + \alpha^j),$$

که در آن $s \neq ۰$ و $y_k \notin \{\alpha^i, \alpha^j\}$.

از معادله اول داریم $y_۳ = y_۱ + y_۲$ که ما آن را در معادله دوم جای‌گزین می‌کنیم. نتیجه برابر است با:

$$y_۱ y_۲ (y_۱ + y_۲) = s.$$

چون $s \neq ۰$ داریم $y_۲ \neq ۰$. تعریف کنید $y := y_۱/y_۲$. این معادله به‌صورت زیر ساده می‌شود.

$$y(۱ + y) = s/y_۲^۳.$$

چون $(۳, ۲^{۲m+۱} - ۱) = (۳, n) = ۱$ نتیجه می‌شود که برای هر مقدار y، به‌جز $y = ۰$، $y = ۱$، این معادله دارای جواب یکتای $y_۲$ (در $\mathbb{F}_{۲^{۲m+۱}}$) است؛ بنابراین، $n - ۱$ جواب $\{y_۱, y_۲\}$ را یافته و سپس $y_۳$ نتیجه می‌شود. به‌وضوح، هر سه‌تایی، شش‌بار یافت می‌شود. علاوه‌براین، ما باید جواب $y_۱ = \alpha^i$، $y_۲ = \alpha^j$

را رد کنیم، زیرا اینها متناظر با $x_۱ = \alpha^j$، $x_۲ = \alpha^i$، $x_۳ = ۰$ (یا هر جای‌گشت) می‌باشند؛ بنابراین، $\rho(u, C) = ۲$ نتیجه می‌دهد که $\frac{۱}{۴}(n-۱) - ۱$ کدکلمه دارای فاصله ۳ با u هستند. به روش مشابه، می‌توان حالت $\rho(u, C) > ۲$ را بررسی نمود.

۳.۷.۷. کد C، کد پرپاراتا به‌طول ۱۵ است. اما، ما نیاز نداریم از این واقعیت استفاده کنیم. با کد نرد–استروم $\bar{C}$ (۱۶, ۲۵۶, ۶) شروع کنید و آن را پنچر کنید تا کد C (۱۵, ۲۵۶, ۵) را به‌دست آورید. این پارامترها در رابطه ۳ صدق می‌کنند.

۴.۷.۷. این‌که C با یک کد خطی هم‌ارز نیست، به‌آسانی دیده می‌شود. اگر چنین بود، آن‌گاه C درواقع یک کد خطی می‌بود، زیرا $۰ \in C$. پس مجموع دو کلمه از C مجدداً در C می‌باشد. این مطلب آشکارا درست نمی‌باشد. برای دیدن این‌که C کامل است، باید دو کدکلمه $a = (x, x+c, \sum x_i + f(c))$ و $b = (y, y+c', \sum y_i + f(c'))$ را درنظر بگیریم. اگر $c = c'$ و $x \neq y$، آن‌گاه واضح است که $d(a,b) \geq ۳$. اگر $c \neq c'$، آن‌گاه $d(a,b) \geq w(x-y) + w(x+c-y-c') \geq w(c-c') \geq ۳$. چون $|c| = ۲^{۱۱}$ و $d = ۳$، تساوی را در شرط ۶.۳.۱ داریم؛ یعنی C کامل است.

۵.۷.۷. برای دو ریشه $\Psi_۲$، از روابط ۲۰ و ۲۴ داریم:

$$x_۱ + x_۲ = n+۱ \quad و \quad x_۱ x_۲ = ۲^{l-۱}.$$

بنابراین، $x_۱ = ۲^a$، $x_۲ = ۲^b$ $(a < b)$. با توجه به شرط ۶.۳.۱ داریم $n^۲ + n + ۲ = ۲^c$ (که در آن $c \geq ۳$ چون $n \geq ۲$).

$$(۲^a + ۲^b)(۲^a + ۲^b - ۱) + ۲ = ۲^c,$$

چون در طرف چپ معادله فوق، یک جمله ۲ داریم، جمله دیگر بر ۴ بخش‌پذیر نیست؛ بنابراین، $a = ۰$ یا $a = ۱$. اگر $a = ۰$، آن‌گاه داریم $۲^b(۲^b + ۱) + ۲ = ۲^c$؛ یعنی $b = ۱$ و $n = ۲$ متناظر با کد $C = \{(۰۰)\}$ است. اگر $a = ۱$، آن‌گاه داریم $۲^{۲b} + ۳.۲^b + ۴ = ۲^c$؛ یعنی $b = ۲$ و از این‌رو $n = ۵$ متناظر با کد تکرار $C = \{(۰۰۰۰۰), (۱۱۱۱۱)\}$ است.

۶.۷.۷. درابتدا قضیه ۴.۷.۳ و رابطه ۱۱ را به‌کار برید. معادله زیر را داریم:

$$۴x^۲ - ۴(n+۱)x + (n^۲ + n + ۱۲) = ۰,$$

با ریشه‌های $x_{۱,۲} = \frac{۱}{۴}(n+۱ \pm \sqrt{n-۱۱})$.

درنتیجه $n - ۱۱ = m^۲$ برای برخی مقادیر صحیح m. از رابطه ۱۹ داریم:

$$۱۲.۲^n = |c|.(n^۲ + n + ۱۲) = |c|(n+۱+m)(n+۱-m).$$

بنابراین، $n+۱+m=a.۲^{\alpha+۱}$، $n+۱-m=b.۲^{\beta+۱}$ با ۳ یا ۱ $ab=۱$. درابتدا قرار دهید $a=b=۱$. داریم $n+۱=۲^{\alpha}+۲^{\beta}$، $m=۲^{\alpha}-۲^{\beta}$ $(\alpha>\beta)$؛ از این‌رو:

$$۲^{\alpha}+۲^{\beta}-۱۲=۲^{۲\alpha}-۲^{\alpha+\beta+۱}+۲^{۲\beta},$$

یعنی:

$$-۱۲=۲^{\alpha}(۲^{\alpha}-۲^{\beta+۱}-۱)+۲^{\beta}(۲^{\beta}-۱),$$

یک تناقض آشکار است.

سپس قرار دهید $b=۳$. در نتیجه $n+۱=a.۲^{\alpha}+۳.۲^{\beta}$، $m=a.۲^{\alpha}-۳.۲^{\beta}$؛ از این‌رو:

$$۳.۲^{\beta}(۳.۲^{\beta}-۲^{\alpha+۱}-۱)+۲^{\alpha}(۲^{\alpha}-۱)+۱۲=۰.$$

اگر $\alpha>۲$، آن‌گاه باید داشته باشید $\beta=۲$ و درنتیجه $\alpha=۴$. چون $\alpha\leq ۲$ جواب نمی‌دهد و حالت آخر $a=۳$ نیز چیزی را ایجاب نمی‌کند، ثابت کرده‌ایم که $n+۱=۲^{۴}+۳.۲^{۲}$؛ یعنی $n=۲۷$.

ساختار چنین کدی مشابه با مطلب موجود درباره یک کد RM پنچرشده (۲.۷.۴) است. فرم به‌کار رفته در ۲.۷.۴ را با $x_۱x_۲+x_۳x_۴+x_۵x_۶+x_۵+x_۶=۰$ جای‌گزین کنید. مابقی اثبات مشابه است. ما یک کد دووزنی با طول ۲۷ با وزن‌های ۱۲ و ۱۶ یافته و سپس قضیه ۵.۷.۳ را به‌کار می‌گیریم.

۷.۷.۷.

۱) فرض کنید N تعداد زوج‌های (x,c) باشد، طوری که $x\in \mathbb{F}_۳^{۱۴}$، $c\in C$، $d(x,c)=۲$. با اولین انتخاب c داریم $N=|c|.\binom{۱۴}{۲}.۲^{۲}$. برای هر x با شرط $d(x,c)=۲$، حداکثر هفت کدکلمه ممکن وجود دارد که $d(x,c)=۲$؛ از این‌رو:

$$N\leq (۳^{۱۴}-|c|(۱+۲.۱۴)).$$

با مقایسه این نتایج، می‌بینیم که در دومی، باید تساوی برقرار باشد. هر $x\in \mathbb{F}_۳^{۱۴}$ دارای فاصله حداکثر ۱ تا C یا فاصله ۲ تا دقیقاً هفت کدکلمه است.

۲) $\binom{۱۴}{۲}.۲^{۲}$ کلمه با وزن ۲ در $\mathbb{F}_۳^{۱۴}$ وجود دارد. هریک دارای فاصله ۲ تا ۰ است و از این‌رو دارای فاصله ۲ تا شش کدکلمه با وزن ۴ می‌باشد. چون هر کدکلمه با وزن ۴ دارای فاصله ۲ تا شش کلمه با وزن ۲ است، داریم $A_۴=۳۶۴$.

۳) با توجه به (۲) می‌بینیم که $۴A_۴=۱۴۵۶$ کلمه با وزن ۳ دارای فاصله ۱ تا C هستند. زوج‌های (x,c) را، که در آن $w(x)=۳$، $c\in C$ و $d(x,c)=۲$، می‌شماریم. آشکارا $۱۴۵۶-۲^{۳}.\binom{۱۴}{۳}$

انتخاب برای x وجود دارند. با شروع از کدکلمه c با وزن ۴، ۱۲ انتخاب برای x وجود دارد. اگر $w(c) = ۵$، آن‌گاه ۱۰ انتخاب برای x وجود دارد؛ بنابراین، داریم:

$$۱۲A_۴ + ۱۰A_۵ = ۷.۱۴۵۶,$$

یعنی $A_۵ = ۵۸۲\frac{۲}{۵}$ که بی‌معنی است. C وجود ندارد!

۸.۷.۷. در متریک لی، حجم گوی با شعاع ۱ برابر است با $V_۱ = ۱ + ۲n = m^۲$. کلمات متعلق به مجموعه $\mathbb{Z}_m^۲ \backslash \{(۰,۰)\}$ را به زوج‌های $(x,-x)$ تفکیک نموده و یکی را به‌عنوان ستونی از یک ماتریس بررسی‌توازن H، ۲ در n، درنظر بگیرید. با تعمیم نظریه کدهای همینگ، کد خطی C را به‌صورت زیر تعریف کنید:

$$c \in C \Leftrightarrow cH^T = ۰.$$

به‌وضوح C یک کد تصحیح‌کننده ۱ خطاست و C کامل است، زیرا $|c|.V_۱ = m^n$.

فصل ۸

۱.۸.۵. در ابتدا توجه دارید که در یک کد چهارتایی خوددوگان به‌طول ۶، کلمات دارای مختصات فرد شامل چهار تا مختصات این‌چنینی هستند. چون این کد باید شامل $۴^۳$ کلمه باشد، ماتریس مولد در فرم ۱ دارای $۲k_۱ + k_۲ = ۶$ است. به‌وضوح، $k_۱ = ۳$ غیرممکن است.

برای $k_۱ = ۰$ مثال بدیهی $\mathbb{F}_۲^۶$ را داریم. شمارنده وزنی لی آن $(x^۲ + y^۲)^۶$ یکی از دو جواب مستقل برای معادله موجود در قضیه ۴.۳.۶ در حالت خوددوگانگی است. دیگری برابر با $x^۲y^۲(x^۴ - y^۴)^۲$ است (اینها به‌آسانی با استفاده از این واقعیت که تمامی وزن‌ها زوج هستند، یافت می‌شوند). تمامی ترکیبات خطی با جمله $x^{۱۲}$ نیز شامل جمله $y^{۱۲}$ هستند، بنابراین، این کد شامل $(۲,۲,۲,۲,۲,۲)$ است.

حال $k_۱ = k_۲ = ۲$ را امتحان می‌کنیم. سطرهای $(A \quad B)$ هریک باید سه درایه فرد داشته باشند. به‌آسانی می‌توان مثالی یافت، به‌طور نمونه:

$$A = \begin{pmatrix} ۱ & ۱ \\ ۱ & ۱ \end{pmatrix}, \quad B = \begin{pmatrix} ۱ & ۰ \\ ۲ & ۱ \end{pmatrix}, \quad C = \begin{pmatrix} ۱ & ۱ \\ ۱ & ۱ \end{pmatrix}.$$

شمارنده وزنی، جواب معادله موجود در قضیه ۴.۳.۶ است که شامل جمله $x^{۱۰}y^۲$ نباشد؛ یعنی $x^{۱۲} + ۱۵x^۸y^۴ + ۳۲x^۶y^۶ + ۱۵x^۴y^۸ + y^{۱۲}$. دو سطر A می‌توانند رابطه‌ای غیرخطی ایجاد کنند، زیرا $\sigma(۱) + \sigma(۱) \neq \sigma(۲)$. کدکلمه (۰۰۲۲۰۰) آن را جبران می‌کند. توجه دارید که تصاویر دودویی از دو بردار پایه اول، متعامد نمی‌باشند.

برای $k_1 = 1$، $k_2 = 4$، به‌آسانی می‌توان جوابی یافت. قرار دهید $A = (1100)$، $B = (1)$، $C = (1100)^T$. تصویر دودویی، خطی و خوددوگان است.

توجه. در بالا مشاهده کردید که $k = 3$ غیرممکن است. با توجه به روابط ۱ و ۲، فوراً واضح است که کدهای چهارتایی با مولد $(I_3 \quad 2J_3 - I_3)$ و دوگان آن دارای شمارنده وزنی یکسانی می‌باشند (مانند فوق با ۱۵ کلمه به وزن ۴). این کد البته خوددوگان نیست. جالب است که تصویر دودویی آن یک کد خوددوگان است. آن هم‌ارز با با کد با مولد $(I_6 \quad J_6 - I_6)$ است.

۲.۸.۵. فرض کنید بردارهای v_i $(0 \le i \le m-2)$ بردارهای پایه $\mathcal{R}(1, m-1)$ باشند. کدکلمات $\mathcal{R}(2,m)$ ترکیبات خطی کلمات از نوع $(\sum \alpha_i v_i, 0)$، $(0, \sum \beta_i v_i)$، $(\sum \gamma_{ij} v_i v_j, \sum \gamma_{ij} v_i v_j)$ و $(\varepsilon_1, \varepsilon_2)$ هستند، که در آن $\varepsilon_i = 0$ یا ۱.

با استفاده از قضیه ۶.۸.۲ (و این واقعیت که $\mathcal{R}(2,m)$ خطی است)، تنها باید بررسی کنیم که آیا حاصل‌ضرب مختصات‌وار کلمات از نوع $(\sum \delta_i v_i + \varepsilon, \sum \delta_i v_i + \varepsilon)$ متعلق به این کد است و به‌وضوح این مطلب برقرار است.

۳.۸.۵. $\xi^a + 2\xi^b$ را آزمایش کنید. به‌آسانی دیده می‌شود $a = n - i$، $b = n - 2i + j$.

۴.۸.۵. با به‌کارگیری لم ۲.۴.۶، کد نرداستروم–رابینسن دارای شمارنده وزنی زیر است:

$$1 + 112z^6 + 30z^8 + 112z^{10} + z^{12}.$$

قضیه ۲.۳.۵ را به‌کار بگیرید. دراینجا، محاسبه کردن با فرم همگن آسان‌تر است.

۵.۸.۵. تعداد زوج‌های (x,c)، که در آن $c \in \mathcal{P}$، $w(x) = 2$ و $d(x,c) = 3$، برابر با $10A_5$ است. با استفاده از ۱.۷.۳ آن هم‌چنین برابر با $\binom{n}{2}\frac{n-3}{3} = \binom{n}{2}(r-1)$ است؛ از این‌رو:

$$A_5 = \frac{n(n-1)(n-3)}{6}.$$

$\binom{n}{3}$ کلمه با وزن ۳ وجود دارد. البته، $10A_5$ دارای فاصله ۲ تا این کد و از این‌رو فاصله ۳ تا $\frac{n-6}{3}$ کلمه با وزن ۶ است. $10A_5 - \binom{n}{3}$ کلمه با وزن ۳ دارای فاصله ۳ تا $\frac{n-3}{3} = r - 1$ کلمه با وزن ۶ است. چون یک کلمه با وزن ۶ دارای فاصله ۳ تا ۲۰ کلمه با وزن ۳ است، شمارش مجدد ایجاب می‌کند:

$$A_6 = \frac{n(n-1)(n-3)(n-5)}{18}.$$

برای $n = 15$ داریم $A_5 = 40$، $A_6 = 70$. می‌دانیم که کد نرداستروم–رابینسن تحت فاصله پایاست؛ بنابراین، شمارنده وزنی مذکور دارای $A_i = A_{16-i}$ است. می‌دانیم $A_6 = A_{10} = 112$ و از این‌رو $A_8 = 30$.

۶.۸.۵. این از مثال ۱.۸.۴ نتیجه می‌شود.

۷.۸.۵. از قضیه ۷.۷.۴ نتیجه می‌شود که پوشش خطی کد پرپاراتای توسیع‌یافته مشمول در کد همینگ توسیع‌یافته است؛ بنابراین، دارای فاصله ۴ است.

$GR(۴^m)$ را درنظر بگیرید. می‌دانیم $\xi + ۱$ می‌تواند به‌صورت $\xi^i + ۲\xi^j$ نوشته شود؛ بنابراین، C_m شامل کدکلمه a با مختص‌های ۱، ۱، ۱، ۳، ۲ در مکان‌های متناظر با ۰، ۱، ξ، ξ^i، ξ^j است. با یک شیفت دوری، یک کدکلمه مشابه b می‌یابیم با یک ۱ در مکان ۰ و سایر مختص‌های فرد در مکان‌هایی متفاوت با آن مکان‌هایی که a دارای مختصات فرد است. پوشش خطی C'_m شامل کلمه $\phi(a) + \phi(b) + \phi(a + b)$ است که دارای وزن ۲ است.

توجه دارید که این استدلال برای $m = ۳$ کار نمی‌کند.

فصل ۹

۱.۹.۸. در قضیه ۱.۹.۳، نشان داده شد که اگر ما $g(z)$ را با $\hat{g}(z) := z + ۱$ جای‌گزین کنیم، آن‌گاه کد مشابهی به‌دست می‌آوریم؛ بنابراین، $\Gamma(L, g)$ دارای بعد حداقل ۴ و کمترین—فاصله $d \geq ۳$ است. آن‌چنان که در قسمت اول بخش ۹.۳ نشان داده شده است، d ممکن است بزرگتر باشد. ماتریس بررسی‌توازن $H = (\, h_۰ \quad h_۱ \quad \cdots \quad h_{۷})$ را که h_i متعلق به مجموعه مقادیر $(\alpha^j + ۱)^{-۱}$ با شرط $(j, ۱۵) = ۱$ است. می‌دانیم H شامل تمامی بردارهای ستونی با یک ۱ در مکان آخر است؛ یعنی $\Gamma(L, g)$ کد همینگ گسترش‌یافته $[۸, ۴, ۴]$ است.

۲.۹.۸. فرض کنید a یک کلمه با وزن زوج در C باشد. با استفاده از رابطه ۲، چندجمله‌ای ماتسون—سولومن $A(X)$ بر X بخش‌پذیر است. با استفاده از قضیه ۱.۹.۶، چندجمله‌ای $X^{n-۱} \circ A(X)$، یعنی $X^{-۱}A(X)$، بر $g(X)$ بخش‌پذیر است. چون C دوری است، از رابطه ۲ می‌فهمیم که $X^{-۱}A(X)$ بر $g(\alpha^i X)$، برای $۰ < i \leq n - ۱$، نیز بخش‌پذیر است. اگر $g(X)$ دارای یک ریشه متفاوت با صفر در یک میدان گسترش‌یافته از $\mathbb{F}_۲$ باشد، آن‌گاه $n - ۱$ ریشه متمایز از $X^{-۱}A(X)$ داریم که یک تناقض است، زیرا $X^{-۱}A(X)$ دارای درجه کمتر از $n - ۱$ است؛ بنابراین، $g(z) = z^t$ برای برخی مقادیر t و C یک کد BCH است (مثال ۲.۹.۲ را ببینید).

۳.۹.۸. این دقیقاً همان چیزی است که در قسمت اول بخش ۹.۳ نشان دادیم. برای هر کدکلمه $(b_۰, b_۱, \cdots, b_{n-۱})$ داریم $\sum_{i=۰}^{n-۱} b_i \gamma_i^r = ۰$ برای $۰ \leq r \leq d_۱ - ۲$، که در آن $\gamma_i = \alpha^i$ (α یک عضو اولیه است)؛ بنابراین، کمترین—فاصله بزرگتر یا مساوی $(d_۲ - ۱) + (d_۱ - ۲) + ۲ = d_۱ + d_۲ - ۱$ است.

۴.۹.۸. فرض کنید $G^{-۱}(X)$ معرف معکوس $G(X)$ در حلقه $(T, +, \circ)$ باشد. تعریف کد GBCH می‌تواند به‌صورت زیر خوانده شود:

$$P(X).(\Phi a)(X) = Q(X)G(X) + R(X)(X^n - ۱),$$

که در آن $Q(X)$ دارای درجه کمتر از $n-t$ است. این هم‌ارز با زیر است:

$$(G^{-1}(X) \circ P(X))(\Phi a)(X) = Q(X) + R^*(X)(X^n - 1),$$

برای یک مقدار مناسب $R^*(X)$. شرط مشابه، شامل این شرط که $\deg Q(X) < n-t$ به‌دست می آید، اگر زوج $(\hat{P}(X), X^t)$ را درنظر بگیریم، که در آن:

$$\hat{P}(X) = x^t \circ G^{-1}(X) \circ P(X).$$

جواب دوم: به‌منظور اطمینان از این‌که ما دارای کد مشابهی هستیم، برای آن می‌بینیم که ماتریس بررسی‌توازن یکسانی مشابه با بخش ۹.۶ به‌دست می‌آوریم. داریم $h_i = p_i g_i^{-1}$، که در آن $p(x) = \sum p_i x^i = (\Phi^{-1}P)(x)$ و $g(x) = \sum g_i x^i = (\Phi^{-1}G)(x)$. ما باید $\hat{p}_i$ را طوری بیابیم که $\hat{p}_i \hat{g}_i^{-1} = p_i g_i^{-1}$. چون $\sum \hat{g}_i x^i = (\Phi^{-1}X^t)(x)$ دانسته شده، $\hat{p}(x)$ را نیز می‌دانیم .پس $P(X) = \Phi\hat{p}$.

۵.۹.۸. در تعریف ۱.۶.۶ قرار دهید $l = 5$ و $\delta = 2$. می‌فهمیم که C یک کد BCH با کمترین—فاصله $d \geq 2$ است. چون $(x+1)(x^2+x+1) = x^3+1 \in C$، داریم $d = 2$. اگر در تعریف ۱.۹.۲، $g(x)$ را با درجه بیشتر از ۱ درنظر بگیریم، آن‌گاه با استفاده از قضیه ۳.۹.۲ کد گاپای $\Gamma(L,g)$ دارای فاصله حداقل ۳ می‌باشد. اگر $g(z)$ از درجه ۱ باشد، آن‌گاه قضیه ۱.۹.۳ نتیجه یکسانی را ایجاب می‌کند؛ بنابراین، C یک کد گاپا نیست.

فصل ۱۰

۱.۱۰.۹. برای بررسی X در $(0:0:1)$، (y,z) را به‌صورت مختص‌های آفین درنظر می‌گیریم. معادله به‌صورت $z = y^2$ می‌شود. بنابراین، می‌بینیم که y یک پارامتر موضعی است (و z نیست)؛ بنابراین، در $(0:0:1)$، y/x را به‌صورت پارامتر موضعی درنظر می‌گیریم. چون $x/z = (x/y)^2$، می‌بینیم که یک قطب مرتبه ۲ در $(0:0:1)$ وجود دارد.

۲.۱۰.۹. اگر f و سه مشتق جزیی در $(x:y:z)$ صفر باشند، آن‌گاه $xyz \neq 0$ و سه معادله $2x^3 = y^2z$ و غیره را می‌یابیم. این سه به ما $8(xyz)^3 = (xyz)^3$ را می‌دهند، پس $p = 7$. ممکن است فرض کنیم $x = 1$؛ در این‌صورت معلات $y^2z = 2$ و $y = 2z^3$ جواب $y = 2$ و $z = 4$ را می‌دهند. از این‌رو یک نقطه منفرد وجود دارد.

۳.۱۰.۹. X دارای پنج نقطه است: $P = (0:0:1)$، $Q = (1:0:0)$ و $R_i = (\alpha^i : \alpha^{2i} : 1)$ $(0 \leq i \leq 2)$. به‌وضوح، هر نقطه R_i یک ریشه با تکرر ۱ است. در Q، y/x را به‌صورت یک پارامتر موضعی داریم و

$$g = (\frac{y}{x})^3 \frac{x^3+y^3}{x^3},$$

از این‌رو Q یک ریشه با تکرر ۳ است. در P، یک پارامتر موضعی، y/x است و

$$g = (\frac{z}{y})^{۳}\frac{z^{۳}+y^{۳}}{z^{۳}},$$

بنابراین، P یک قطب مرتبه ٦ است. از این‌رو $(g) = -٦P + ۳Q + R_۱ + R_۲ + R_۳$.

۴.۱۰.۹. ما تنها مجبوریم نگاهی به این سه نقطه بیندازیم، که در آن دو مختصات صفر هستند، $P = (۰ : ۰ : ۱)$، $Q = (۱ : ۰ : ۰)$ و $R = (۰ : ۱ : ۰)$. آسان‌ترین همان Q است، که در آن z/x یک پارامتر موضعی است. از این‌رو Q یک قطب مرتبه ۱ است. در P، پارامتر موضعی y/z و

$$\frac{x}{z} = (\frac{y}{z})^{۴}\frac{z^{۴}}{x^{۳}y+z^{۴}},$$

را داریم، که در آن دومین عامل یک یکه است؛ بنابراین، P یک ریشه با تکرر ۴ است. در R، یک پارامتر موضعی، x/y است. از

$$\frac{x}{z} = (\frac{y}{x})^{۳}\frac{y^{۴}+z^{۳}x}{y^{۴}},$$

می‌بینیم که R یک قطب مرتبه ۳ است؛ داریم:

$$(f) = ۴P - Q - ۳R.$$

۵.۱۰.۹. تنها مختصات نقاط $P_۱$ تا $P_٦$ را در سه تابع پایه جای‌گزین کنید. نشان داده شده است که با ضرب سطرها و ستون‌های معین در مقادیرثابت مناسب و یک جای‌گشت، دو ماتریس مولد متعلق به کدهای هم‌ارز هستند.

٦.۱۰.۹. چون $g = ۳$، از قضیه ۱.۱۰.۴ داریم $l(۳Q) \geq ۱$. از نتیجه ۳.۱۰.۴ نتیجه می‌شود که $l(۵Q) = ۳$. از مثال ۵.۱۰.٦ می‌بینیم که توابع ۱ و z/x در $\mathcal{L}(۳Q)$ هستند و نیز آنها یک پایه می‌باشند.

فصل ۱۱

۱.۱۱.۴. کلمات C_α دارای شکل $(a(x), \alpha(x)a(x))$ هستند، که در آن $a(x)$ و $\alpha(x)$ چندجمله‌ای‌هایی در پیمانه $x^{٦} + x^{۳} + ۱$ می‌باشند. برای رسیدن به $d > ۳$، باید آن $\alpha(x)$ هایی را که در آن یک ترکیب $a(x) = x^i$، $\alpha(x)a(x) = x^j + x^k$ و هم‌چنین معکوس‌های این $\alpha(x)$ ها محتمل است، خارج کنیم. چون $(x^{-۱}(x+۱))^{۸} = ۱ + x^{۸} = x^{-۱}(x + x^{۹}) = x^{-۱}(x + ۱)$، به‌آسانی دیده می‌شود که هر عضو ناصفر $\mathbb{F}_{۲^٦}$ دارای یک نمایش یکتای $x^i(۱ + x)^j$ است؛ که در آن:

$$i \in \{۰, \pm۱, \pm۲, \pm۳, \pm۴\}, \quad j \in \{۰, \pm۱, \pm۲ \pm ۴\}.$$

بنابراین، شرط $d > ۲$، نه مقدار $\alpha(x)$ را خارج می‌کند و شرط $d > ۳$، ۵۴ مقدار باقی‌مانده از $a(x)$ را خارج می‌نماید. این مطلب نشان می‌دهد که برای n کوچک، این ساختار خیلی خوب نیست! با استفاده از مساله ۱۴.۳.۸، یک کد $[۱۲, ۷]$ گسترش‌یافته با کمترین ترتیب الفبایی با $d = ۴$ وجود دارد. در لم ۱.۴.۶ دیدیم که یک کد غیرخطی با $n = ۱۲$، $d = ۴$ حتی با تعداد کلمات بیشتر وجود دارد.

۲.۱۱.۴. فرض کنید $\alpha(x)$ یک چندجمله‌ای با وزن ۳ باشد؛ در این‌صورت در $(a(x), \alpha(x)a(x))$، وزن‌های دو نیمه دارای توازن یکسان می‌باشد. از این‌رو تنها $d < ۴$ ممکن است، اگر یک انتخاب $a(x) = x^i + x^j$ وجود داشته باشد طوری که $\alpha(x)a(x) \equiv ۰ \bmod x^۶ - ۱$. این برقرار است، اگر $\alpha(x)$ متناوب باشد؛ یعنی $x + x^۳ + x^۵$ یا $۱ + x^۲ + x^۴$. برای تمامی انتخاب‌های دیگر داریم $d = ۴$.

۳.۱۱.۴. فرض کنید نرخ R در رابطه $l/(l+۱) < R \leq ۱/l$ $(l \in \mathbb{N})$ صدق کند. فرض کنید s کمترین مقدار صحیح باشد که $m/[(l+۱)m - s] \geq R$. کد C را با انتخاب l–تایی $(\alpha_۱, \alpha_۲, \cdots, \alpha_l) \in (\mathbb{F}_{۲^m})^l$ و سپس تشکیل $(a, \alpha_۱ a, \cdots, \alpha_l a)$ برای تمامی $a \in \mathbb{F}_۲^m$ و سرانجام حذف s سمبل آخر می‌سازیم. طول کلمه کد برابر $n = (l+۱)m - s$ است.

یک کلمه ناصفر $c \in C$ متناظر با ۲^s مقدار ممکن l–تایی $(\alpha_۱, \cdots, \alpha_l)$ است. برای اطمینان از این‌که کمترین—فاصله بزرگتر یا مساوی λn است، باید حداکثر $۲^s \sum_{i<\lambda n} \binom{n}{i}$ مقدار $(\alpha_۱, \cdots, \alpha_l)$ را خارج کنیم. خوشحال خواهیم شد، اگر این رابطه به ما یک انتخاب برای $(\alpha_۱, \cdots, \alpha_l)$ بدهد؛ یعنی اگر:

$$۲^s \sum_{i<\lambda n} \binom{n}{i} < ۲^{ml}.$$

آنگاه از قضیه ۵.۱.۴ داریم:

$$s + nH(\lambda) < ml,$$

یعنی:

$$H(\lambda) < \frac{ml - s}{n} = ۱ - \frac{m}{n} = ۱ - R + o(۱), \quad (m \to \infty).$$

فصل ۱۲

۱.۱۲.۵. دنباله r، $r^۲$، $r^۳$، $\cdots$ را درنظر بگیرید. دو عضو در این دنباله وجود دارد که در پیمانه A هم‌نهشت می‌باشند، گوییم $r^n - r^m \equiv ۰ \bmod A$ $(n > m)$.

۲.۱۲.۵. فرض کنید $m = r^n - ۱ = AB$، که در آن A یک عدد اول بزرگتر از $r^۲$ می‌باشد. فرض کنید r زیرگروه H از $\mathbb{F}_A^*$ با $|H| = n$ را تولید می‌کند که شامل $\{\pm c | c = ۱, ۲, \cdots, r-۱\}$ به‌عنوان مجموعه کاملی از معرف‌های هم‌مجموعه‌ای است. کد AN دوری C با طول n و پایه r را درنظر بگیرید.

به‌وضوح، هر مقدار صحیح در بازه $[1, m]$ دارای فاصله پیمانه‌ای ۰ یا ۱ تا دقیقاً یک کدکلمه است؛ بنابراین، C یک کد کامل است (چون $w_m(A) \geq ۳$ باید داشته باشیم $A > r^۲$). یک مثال بدیهی برای $r = ۳$ کد دوری $\{۱۳, ۲۶\}$ است. در اینجا فرض کرده‌ایم $m = ۳^۳ - ۱$ و $A = ۱۳$.

زیرگروه تولیدشده توسط ۳ در $\mathbb{F}_{۱۳}^*$ دارای شاخص ۴ است و معرف‌های هم‌مجموعه‌ای برابر با ± ۱ و ± ۲ هستند.

۳.۱۲.۵. داریم $۴۵۵ = \sum_{i=۰}^{۵} b_i ۳^i$، که در آن $(b_۰, b_۱, \cdots, b_۵) = (۲, ۱, ۲, ۱, ۲, ۱)$. الگوریتم توصیف شده در تعریف ۳.۱۰.۱ مقادیر اولیه ۲، ۱ را با ۱−، ۲ جای‌گزین می‌کند. در این روش، دنباله زیر از معرف‌ها را داریم:

$$(۲, ۱, ۲, ۱, ۲, ۱) \to (-۱, ۲, ۲, ۱, ۲, ۱) \to (-۱, -۱, ۰, ۲, ۲, ۱)$$

$$\to (-۱, -۱, ۰, -۱, ۰, ۲) \to (۰, -۱, ۰, -۱, ۰, -۱).$$

بنابراین، این نمایش در CNAF به‌صورت زیر است:

$$۴۵۵ \equiv -۲۷۳ = -۳ - ۳^۳ - ۳^۵.$$

۴.۱۲.۵. شرایط موجود در قضیه ۲.۱۰.۲ را بررسی می‌کنیم. در $\mathbb{F}_{۱۱}^*$، عضو ۳، زیرگروه $\{۱, ۳, ۹, ۵, ۴\}$ را تولید می‌کند؛ ضرب در ۱−، پنج عضو دیگر را ایجاب می‌کند. $A = ۱ + ۱ \times ۳ + ۲ \times ۳^۲ + ۱ \times ۳^۳ + ۰ \times ۳^۴ + ۱ \times ۳^۵ + ۰ \times ۳^۶ + ۱ \times ۳^۷ + ۰ \times ۳^۸ + ۱ \times ۳^۹ = ۱ + ۱۱ \times ۲۲ = ۲۴۳ = ۳^۵ = r^n$. چون داریم $A = ۲۲$، در نمایش سه‌تایی CNAF برای ۲۲ برابر با $۱ \times ۳^۴ + ۰ \times ۳^۳ + ۱ \times ۳^۲ + ۰ \times ۳ + ۲ \times ۱ - ۱$ (در پیمانه ۲۴۲) است. این کد شامل ده کلمه است؛ یعنی شیفت‌های دوری $(۱, -۲, ۰, ۱, ۰)$، به‌ترتیب $(۱, ۰, -۱, ۲, ۰, -۱)$. تمام وزن‌ها ۳ هستند.

فصل ۱۳

۱.۱۳.۷. با به‌کارگیری نماد موجود در بخش ۱۱.۱ داریم:

$$G(x) = (۱ + (x^۲)^۲) + x(۱ + x^۲) = ۱ + x + x^۳ + x^۴.$$

رشته اطلاعاتی $\cdots$ ۱ ۱ ۱ ۱ ۱ ۱ می‌دهد $I_۰(x) = (۱ + x)^{-۱}$؛ از این‌رو:

$$T(x) = (۱ + x^۲)^{-۱} G(x) = ۱ + x + x^۲,$$

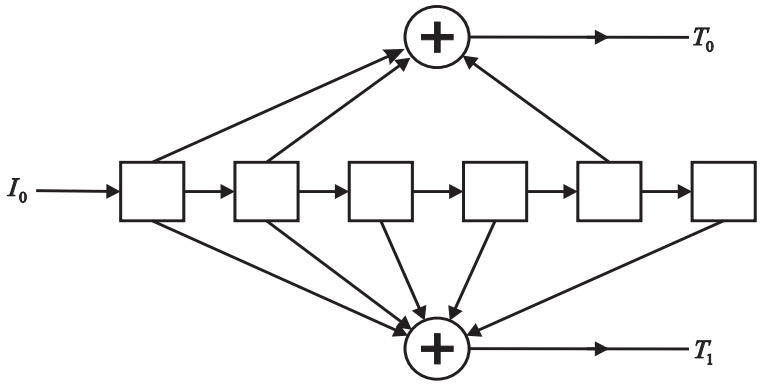
یعنی گیرنده $\cdots$ ۰ ۰ ۰ ۰ ۱ ۱ ۱ را دریافت می‌کند.

سه خطا در مکان‌های اولیه، سیگنال صفر را تولید می‌کند و منجر به تعداد بی‌نهایت خطا در کدگشایی می‌گردد.

۲.۱۳.۷. در قضیه ۲.۱۳.۴ نشان داده شد چگونه این موقعیت می‌تواند به‌وجود آید. فرض کنید $h(x) = x^4 + x + 1$ و $g(x)h(x) = x^{15} - 1$. می‌دانیم که $g(x)$ یک کد دوری تحویل‌ناپذیر با کمترین–فاصله ۸ ایجاد می‌کند. دنباله اطلاعاتی ۱ ۱ ۰ ۰ ۱ ۰ ۰ ۰ ۰ ۰ ... را درنظر بگیرید؛ یعنی $I_0(x) = h(x)$؛ در این‌صورت داریم:

$$T(x) = h(x^2)g(x) = (x^{15} - 1)h(x),$$

که دارای وزن ۶ است. با استفاده از قضیه ۲.۱۳.۴، این همان فاصله آزاد است. در این مثال، داریم $G_0(x) = 1 + x + x^4$؛ بنابراین، $g(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$، $G_1(x) = 1 + x + x^2 + x^3 + x^5$. کدگذار به‌شکل زیر است:



شکل ۱۴.۱:

و

$I_0 =$ ۱ ۱ ۰ ۰ ۱ ۰ ۰ ۰ ... یک خروجی ایجاد می‌کند

$T =$ ۱۱ ۰۰ ۱۰ ۰۰ ۰۰ ۰۰ ۰۰ ۰۱ ۱۰ ۰۱ ۰۰ ۰۰ ...

۳.۱۳.۷. یک دنباله خروجی متناهی درنظر بگیرید. این دنباله به شکل $(a_0 + a_1x + \cdots + a_lx^l)G$ می‌باشد، که در آن a_iها بردارهای سطری در $\mathbb{F}_2^4$ هستند. مانند رابطه ۶، G را به‌صورت $G_1 + xG_2$ می‌نویسیم. به‌وضوح هفت‌تایی ناصفر اولیه در خروجی، یک کدکلمه ناصفر در کد تولیدشده توسط m_3 است؛ بنابراین، آن دارای وزنی بزرگتر یا مساوی ۳ است. اگر این هم‌چنین هفت‌تایی ناصفر نهایی باشد، آن‌گاه آن برابر با (۱ ۰۰۰ ۱۱) است و وزن آن ۷ می‌باشد. اگر هفت‌تایی ناصفر نهایی، a_lG باشد، آن‌گاه آن کدکلمه ناصفری در کد تولیدشده توسط m_0m_1 است و از این‌رو دارای وزن حداقل ۴ می‌باشد. اما،

اگر $a_l = (۱۰۰۰)$، آن‌گاه $a_l G = ۰$ و هفت‌تایی ناصفر نهایی، کدکلمه ناصفری در کد تولیدشده توسط $m_۱$ است و آن دارای وزنی بزرگتر یا مساوی ۳ می‌باشد؛ بنابراین، فاصله آزاد برابر با ٦ است. این مطلب با توجه به ورودی $x(۱۰۰۰) * (۱۱۰۰)$ تشخیص داده می‌شود.

مراجع

[1] Baumert, L. D. and McEliece, R. J.: A golay-Viterbi Concatenated Coding Scheme for MJS '77. JPL Technichal Report 32-1526, pp. 76-83. Pasadena, Calif.: Jet Propulsion Laboratory, 1973.

[2] Berlekamp, E. R.: Algebraic Coding Theory. New York: McGraw-Hill, 1968.

[3] Berlekamp, E.R.: Decoding the Golay Code. JPL Technical Report 32-1256, Vol. IX, pp. 81-85. Pasadena, Calif.: Jet Propulsion Laboratory, 1972.

[4] Berlekamp, E. R.: Goppa codes. IEEE Trans. Info. Theory, 19, pp. 590-592 (1973).

[5] Berlekamp, E. R. and Moreno, O,: Extended double-error-correcting binary Goppa codes are cyclic. IEEE Trans. Info. Theroy, 19, pp. 817-818 (1973).

[6] Best, M. R., Brouwer, A. E., MacWilliams, F.J., Odlyzko, A. M. and Sloane, N. J. A.: Bounds for binary codes of length less than 25. IEEE Trans. Theroy, 23, pp. 81-93 (1977).

[7] Best, M. R.: On the Existense of Perfect Codes. Report ZN 82/78. Amsterdam: Mathematical Centre, 1978.

[8] Best, M. R.: Binary codes with a minimum distance of four. IEEE Trans. Info. Theory, 26, pp. 738-742 (1980).

[9] Bussey, W. H.: Galois field tables for $p^n \leq 169$. Bull. Amer. Math. Soc., 12, pp. 22-38(1905).

[10] Bussey, W. H.: Tables of Galois fields of order less than 1,000. Bull. Amer. Math. Soc., 16, pp. 188-206 (1910).

[11] Cameron, P. J. and van Lint, J.H.: Designs, Graphs, Codes and their Links. London Math. Soc. Student Texts, Vol. 22. Cambridge: Cambridge Univ. Press, (1991).

[12] Chen, C. L., Chien, R. T. and Liu, C. K.: On the binary representation form of Certain integers. SIAM J. Appl. Math., 26, pp. 285-293 (1974).

[13] Chien, R. T. and Choy, D.M.: Algebraic generalization of BCH-Goppa-Helgert Cods. IEEE Trans. Info. Theory, 21,pp. 70-79 (1975).

[14] Clark, W. E. and Liang, J. J.: On arithmetic weight for a general radix representation of integers. IEEE Trans. Info. Theory, 19, pp. 823-826(1973).

[15] Clark, W. E. and Liang, J. J.: On modular weight and cyclic nonadjacent forms for arithmetic codes. IEEE Trans. Info. Theory, 20, pp. 7'67-770 (1974).

[16] Curtis, C. W. and Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. New York-London: Interscience, 1962.

[17] . Cvetkovic, D. M. and van Lint, J. H.: An elementary proof of Lloyd's theorem. Proc. Kon. Ned. Akad. v. Wetensch. (A), 80, pp. 6-10 (1977).

[18] Delsarte, P.: An algebraic approach to coding theory. Philips Research Reports Supplements, 10(1973).

[19] Delsarte, P. and Goethals, J.-M.: Unrestricted codes with the Golay parameters are unique. Discrete Math., 12, pp. 211-224 (1975).

[20] Elias, P.: Coding for Noisy Channels. IRE Con v. Record, part 4, pp. 37-46.

[21] Feller, W.: An Introduction to Probability Theory and Its Applications, Vol. I. New York-London: Wiley, 1950.

[22] Forney, G. D.: Concatenated Codes. Cambridge, Mass.: MIT Press, 1966.

[23] Forney, G. D.: Convolutional codes I: algebraic structure. IEEE Trans. Info. Theory, 16, pp. 720-738 (1970); Ibid., 17, 360 (1971).

[24] Gallagher, R. G.: Information Theory and Reliable Communication. New York: Wiley, 1968.

[25] Goethals, J.-M. and van Tilborg, H. C. A.: Uniformly packed codes. Philips Research Reports, 30, pp. 9-36 (1975).

[26] Goethals, J.-M.: The extended Nadler code is unique. IEEE Trans. Info. Theory, 23, pp. 132-135(1977).

[27] Goppa, V. D.: A new class of linear error-correcting codes. Problems of Info. Transmission, 6, pp. 207-212 (1970).

[28] Goto, M.: A note on perfect decimal AN codes. Info, and Control, 29, pp. 385-387 (1975).

[29] Goto, M. and Fukumara, T.: Perfect nonbinary AN codes with distance three Info, and Control. 27, pp. 336-348 (1975).

[30] Graham, R. L. and Sloane, N. J. A.: Lower bounds for constant weight codes. IEEE Trans. Info. Theory, 26, pp. 37-40 (1980).

[31] Gritsenko, V. M.: Nonbinary arithmetic correcting codes, Problems of Info. Transmission. 5, pp 15-22(1969).

[32] Hall, M.: Combinatorial Theory. New York-London-Sydney-Toronto: Wiley (second printing), 1980.

[33] Hartmann, C. R. P. and Tzeng, K. K.: Generalizations of the BCH bound. Info, and Control, 20, pp. 489-498 (1972).

[34] Helgert, H. J. and Stinaff, R. D.: Minimum distance bounds for binary linear codes. IEEE Trans. Info. Theory, 19, pp. 344-356 (1973).

[35] Helgert, H. J.: Alternant codes. Info, and Control, 26, pp. 369-380 (1974).

[36] Jackson, D.: Fourier Series and Orthogonal Polynomials. Carus Math. Monographs, Vol. 6. Math. Assoc, of America, 1941.

[37] Justesen, J.: A class of constructive asymptotically good algebraic codes. IEEE Trans. Info. Theory, 18, pp. 652-656(1972).

[38] Justesen, J.: An algebraic construction of rate 1/v convolutional codes. IEEE Trans. Info. Theory, 21, 577-580(1975).

[39] Kasami, T.: An upper bound on k/n for affine invariant codes with fixed d/n. IEEE Trans. Info. Theory. 15, pp. 171-176(1969).

[40] Levenshtein, V. I.: Minimum redundancy of binary error-correcting codes. Info, and Control, 28, pp. 268-291 (1975).

[41] van Lint, J. H.: Nonexistence theorems for perfect error-correcting-codes. In: Computers in Algebra and Theory, Vol. IV (SIAM-AMS Proceedings) 1971.

[42] van Lint, J. H.: Coding Theory. Springer Lecture Notes, Vol. 201, Berlin-Heidelberg-New York: Springer, 1971.

[43] van Lint, J. H.: A new description of the Nadler code. IEEE Trans. Info Theory, 18, pp. 825-826(1972).

[44] van Lint, J. H.: A survey of perfect codes. Rocky Mountain J. Math., 5, pp. 199-224 (1975).

[45] van Lint, J. H. and Mac Williams, F. J.: Generalized quadratic residue codes. IEEE Trans. Info. Theory, 24, pp. 730-737 (1978).

[46] Mac Williams, F. J. and Sloane, N. J. A.: The Theory of Error-correcting Codes. Amsterdam-New York-Oxford: North Holland, 1977.

[47] Massey, J. L.: Threshold Decoding. Cambridge, Mass.: MIT Press, 1963.

[48] Massey, J. L. and Garcia, O. N.: Error-correcting codes in computer arithmetic. In: Advances in Information Systems Science, Vol. 4, Ch. 5. (Edited by J. T. Ton). New York: Plenum Press, 1972.

[49] Massey, J. L., Costello, D. J. and Justesen, J.: Polynomial weights and code construction. IEEE Trans. Info. Theory, 19, pp. 101-110(1973).

[50] McEliece, R. J., Rodemich, E. R., Rumsey, H. C. and Welch, L. R.: New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. IEEE Trans. Info. Theory, 23, pp. 157-166 (1977).

[51] McEliece, R. J.: The Theory of Information and Coding. Encyclopedia of Math, and its Applications, Vol. 3. Reading, Mass.: Addison-Wesley, 1977.

[52] McEliece, R. J.: The bounds of Delsarte and Lovasz and their applications to coding theory. In: Algebraic Coding Theory and Applications. (Edited by G. Longo, CISM Courses and Lectures, Vol. 258. Wien-New York: Springer, 1979.

[53] Peterson, W. W. and Weldon, E. J.: Error-correcting Codes. (2nd ed.). Cambridge, Mass.: MIT Press, 1972.

[54] Piret, Ph.: Structure and constructions of cyclic convolutional codes. IEEE Trans. Info. Theory, 22, pp. 147-155 (1976).

[55] Piret, Ph.: Algebraic properties of convolutional codes with automorphisms. Ph.D. Dissertation. Univ. Catholique de Lou vain, 1977.

[56] Posner, E. C: Combinatorial structures in planetary reconnaissance. In: Error Correcting Codes. (Edited by H. B. Mann), pp. 15-46. New York-London- Sydney-Toronto: Wiley, 1968.

[57] Preparata, F. P.: A class of optimum nonlinear double-error-correcting codes. Info, and Control, 13, pp. 378-400 (1968).

[58] Rao, T. R. N.: Error Coding for Arithmetic Processors. New York-London: Academic Press, 1974.

[59] Roos, G: On the structure of convolutional and cyclic convolutional codes. IEEE Trans. Info. Theory, 25, pp. 676-683 (1979).

[60] Schalkwijk, J. P. M., Vinck, A. J. and Post, K. A.: Syndrome decoding of binary rate k/n convolutional codes. IEEE Trans. Info. Theory, 24, pp. 553-562 (1978).

[61] Selmer, E. S.: Linear recurrence relations over finite fields. Univ. of Bergen, Norway: Dept. of Math., 1966.

[62] Shannon, G E.: A mathematical theory of communication. Bell Syst. Tech. J., 27, pp. 379-423, 623-656 (1948).

[63] Sidelnikov, V. M.: Upper bounds for the number of points of a binary code with a specified code distance. Info, and Control, 28, pp. 292-303 (1975).

[64] Sloane, N. J. A. and Whitehead, D. S.: A new family of single-error-correcting codes. IEEE Trans. Info. Theory, 16, pp. 717-719 (1970).

[65] Sloane, N. J. A., Reddy, S. M. and Chen, C. L.: New binary codes. IEEE Trans. Info. Theory, 18, pp. 503-510(1972).

[66] Solomon, G. and van Tilborg, H. C. A.: A connection between block and convolutional codes. SI AM J. Appl. Math., 37, pp. 358 - 369 (1979).

[67] Szego, G.: Orthogonal Polynomials. Colloquium Publications, Vol. 23. New York: Amer. Math. Soc. (revised edition), 1959.

[68] Tietavainen, A.: On the nonexistence of perfect codes over finite fields. SI AM J. Appl. Math., 24, pp. 88-96 (1973).

[69] van Tilborg, H. C. A.: Uniformly packed codes. Thesis, Eindhoven Univ. of Technology, 1976.

[70] Tricomi, F. G.: Vorlesungen uber Orthogonalreihen. Grundlehren d. math. Wiss. Band 76. Berlin-Heidelberg-New York: Springer, 1970.

[71] Tzeng, K. K. and Zimmerman, K. P.: On extending Goppa codes to cyclic codes. IEEE Trans. Info. Theory, 21, pp. 712-716 (1975).

[72] Baker, R. D., van Lint, J. H. and Wilson, R. M.: On the Preparata and Goethals codes. IEEE Trans. Info. Theory, 29, pp. 342-345 (1983).

[73] van der Geer, G. and van Lint, J. H.: Introduction to Coding Theory and Algebraic Geometry. Basel: Birkhauser, 1988.

[74] Hong, Y.: On the nonexistence of unknown perfect 6- and 8-codes in Hamming schemes H(n, q) with q arbitrary. Osaka J. Math., 21, pp. 687-700 (1984).

[75] Kerdock, A. M.: A class of low-rate nonlinear codes. Info and Control, 20, pp. 182-187(1972).

[76] van Lint, J. H. and Wilson, R. M.: On the Minimum Distance of Cyclic Codes. IEEE Trans. Info. Theory, 32, pp. 23-40 (1986).

[77] van Oorschot, P. C. and Vanstone, S. A.: An Introduction to Error Correcting Codes with Applications. Dordrecht: Kluwer, 1989.

[78] Peek, J. B. H.: Communications Aspects of the Compact Disc Digital Audio System. IEEE Communications Magazine, Vol. 23, No. 2 pp. 7-15 (1985).

[79] Piret, Ph.: Convolutional Codes, An Algebraic Approach. Cambridge, Mass.: The MIT Press, 1988.

[80] Roos, C: A new lower bound for the minimum distance of a cyclic code. IEEE Trans. Info. Theory, 29, pp. 330-332 (1983).

[81] Tsfasman, M. A., Vladut, S. G. and Zink, Th.: On Goppa codes which are better than the Varshamov-Gilbert bound. Math. Nachr., 109, pp. 21-28 (1982).

[82] Barg, A. M., Katsman, S. L., and Tsfasman, M. A.: Algebraic Geometric Codes from Curves of Small Genus. Probl. of Information Transmission, 23, pp. 34-38 (1987).

[83] Conway, J. H. and Sloane, N. J. A.: Quaternary constructions for the binary single-error-correcting codes of Julin, Best, and others. Designs, Codes and Cryptography, 41, pp. 31-42 (1994).

[84] Duursma, I. M.: Decoding codes from curves and cyclic codes. Ph. D. dissertation, Eindhoven University of Technology (1993).

[85] Feng, G.-L. and Rao, T. R. N.: A simple approach for construction of algebraic-geometric codes from affine plane curves. IEEE Trans. Info. Theory, 40, pp. 1003-1012 (1994).

[86] Feng, G.-L., Wei, V., Rao, T. R. N., and Tzeng, K. K.: Simplified understanding and efficient decoding of a class of algebraic-geometric codes. IEEE Trans. Info. Theory 40, pp. 981-1002 (1994).

[87] Garcia, A. and Stichtenoth, H.: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vludut bound. Invent. Math. 121, pp. 211-222 (1995).

[88] Hammons, A. R., Vijay Kumar, P., Calderbank, A. R., Sloane, N. J. A., and Sold, P.: The Z4-Linearity of Kerdock, Preparata, Goethals, and Related Codes. IEEE Trans. Info. Theory, 40, pp. 301-319 (1994).

[89] Hoholdt, T. and Pellikaan, R.: On the decoding of algebraic-geometric codes. IEEE Trans. Info. Theory 41, pp. 1589-1614 (1995).

[90] Heholdt, T., van Lint, J. H., and Pellikaan, R.: Algebraic Geometry Codes. In: Handbook of Coding Theory, (edited by V.S.Pless, W.C. Huffman, and R. A. Braaldi). Elsevier Science Publishers, Amsterdam 1998.

[91] Justesen, J., Larsen, K. J., Elbrend Jensen, H., Havemose, A., and Heholdt, T.: Construction and decoding of a class of algebraic geometry codes. IEEE Trans. Info. Theory 35, pp. 811-821(1989).

[92] van Lint, J. H.: Algebraic geometric codes. In: Coding Theory and Design Theory I, The IMA Volumes in Math, and Appl. 20, (edited by D. Ray-Chaudhuri). Springer Verlag 1990. 93. van Lint, J. H. and Wilson, R. M.: A Course in Combinatorics. Cambridge University Press 1992.

[93] Long, R. L.: Algebraic Number Theory. Marcel Dekker Inc., New York 1977

[94] Pellikaan, R.: On a decoding algorithm for codes on maximal curves, IEEE Trans. Info. Theory, 35, pp. 1228-1232 (1989).

[95] Serre, J.-R: Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini. C. R. Acad. Sc. Paris, 296, pp. 397-402 (1983).

[96] Skorobogatov, A. N. and VluduJ, S. G.: On the decoding of algebraic-geometric codes. IEEE Trans. Info. Theory. 36, pp. 1051-1060 (1990).

[97] Stichtenoth, H.: Algebraic Junction fields and codes. Universitext, Springer Verlag, Berlin 1993.

[98] Tsfasman, M. A., Vluduj, S. G. and Zink, T.: Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound. Math. Nachrichten, 109, pp. 21-28 (1982).

[99] Uspensky, J. V.: Theory of Equations. McGraw-Hill, New York 1948.

واژه‌نامه

admissible pair ..... زوج قابل‌قبول

affine

- curve ..... خم آفین
- geometry ..... هندسه آفین
- permutation group ..... گروه جای‌گشتی آفین
- plane ..... صفحه آفین
- subspace ..... زیرفضای آفین
- transformation ..... تبدیل آفین

algebra ..... جبر

alphabet ..... الفبا

arithmetic

- distance ..... فاصله حسابی
- weight ..... وزن حسابی

automorphism group ..... گروه خودریختی

basis ..... پایه

Bell Laboratories ..... آزمایشگاه‌های بل

Berlekamp decoder ..... کدگشای برلیکمپ

Bezout's theorem ..... قضیه بزوت

binary

- entropy ..... آنتروپی دودویی
- image ..... تصویر دودویی
- symmetric channel ..... کانال دودویی متقارن

binomial distribution ..... توزیع دوجمله‌ای

bit ..... بیت

block

کد بست ..... - Best

کد بلوکی ..... - block

کد فاجعه‌آمیز ..... - catastrophic

کد کاملا منظم ..... - completely regular

کد الحاقی ..... - concatenated

کد پایادوری ..... - constacyclic

کد کانولوشن ..... - convolutional

کد دوری ..... - cyclic

کد دوری AN ..... - - AN

کد دوری کانولوشن ..... - - convolutional,

کد دوری روی $\mathbb{Z}_4$ ..... - cyclic over $\mathbb{Z}_4$

حاصل‌ضرب مستقیم ..... - direct product

کد گردشی دوگانه ..... - double circulant

کد دوگان ..... - dual

کد الیاس ..... - Elias

کد هم‌فاصله ..... - equidistant

کد هم‌ارز ..... - equivalent

کد تصحیح‌کننده خطا ..... - error-correcting

کد تشخیص‌دهنده خطا ..... - error-detecting

کد گسترش‌یافته ..... - extended

کد BCH گسترش‌یافته ..... - generalized BCH

کد رید–مولر گسترش‌یافته ..... - generalized Reed-Muller

کد رید–سولومن گسترش‌یافته ..... - generalized Reed-Solomon

کد رید–سولومن گسترش‌یافته هندسی ..... - geometric generalized Reed-Solomon

کد گاپای هندسی ..... - geometric Goppa

کد گلی ..... - Golay

کد گلی دودویی ..... - - binary

کد گلی سه‌تایی ..... - - ternary

کد گاپا ..... - Goppa

کد گروهی ..... - group

کد هادامارد ..... - Hadamard

کد همینگ ..... - Hamming

کد داخلی ..... - inner

کد تحویل‌ناپذیر سطری ..... irreducible cyclic -
کد جاستسن ..... Justesen -
کد کرداک ..... Kerdock -
آخرین کد با ترتیب الفبایی ..... lexicographically least -
کد خطی ..... linear -
کد مندلبوم–باروس ..... Mandelbaum-Barrows -
کد ماکسیمال ..... maximal -
کد ماکسیمال دوری ..... - cyclic -
کدهای تفکیک‌پذیر با بیشترین فاصله ..... maximum distance separable -
کد MDS ..... MDS -
کد مینیمال دوری ..... minimal cyclic -
کد حسابی پیمانه‌ای ..... modular arithmetic -
کد نادلر ..... Nadler -
کد BCH کم‌عرض ..... narrow sense BCH -
کد تقریبا کامل ..... nearly perfect -
کد نادوری ..... negacyclic -
کد نرداستروم–رابینسن ..... Nordstrom-Robinson -
کد بهینه ..... optimal -
کد خارجی ..... outer -
کد کامل ..... perfect -
کد پرپاراتا ..... Preparata -
کد BCH اولیه ..... primitive BCH -
کد تصویری ..... projective -
کد پنچرشده ..... punctured -
کد QR ..... QR -
کد باقی‌مانده مربعی ..... quadratic residue -
کد شبه–کامل ..... quasi-perfect -
کد چهارتایی ..... quaternary -
کد رید–مولر ..... Reed-Muller -
کد رید–سولومن ..... Reed-Solomon -
کد منظم ..... regular -
کد تکراری ..... repetition -
کد باقی‌مانده ..... residual -

کدگشایی با منطق اکثریت ..... - majority logic

کدگشایی با بیشترین درست‌نمایی ..... - maximum likelihood

کدگشایی اکثریت چند مرحله‌ای ..... - multistep majority

کدگشایی ویتربی ..... - Viterbi

مجموعه تعریف ..... defining set

مشتق ..... derivative

طرح بلوکی ..... design block

دیفرانسیل ..... differential

حاصل‌ضرب مستقیم ..... direct product

distance

فاصله حسابی ..... - arithmetic

توزیع فاصله ..... - distribution

شمارنده فاصله ..... - enumerator

فاصله بیرونی ..... - external

فاصله آزاد ..... - free

فاصله همینگ ..... - Hamming

پایافاصله ..... - invariant

کمترین—فاصله ..... - minimum

divisor

مقسوم‌علیه کانونی ..... - canonical

درجه مقسوم‌علیه ..... - degree of

مقسوم‌علیه موثر ..... - effective

مقسوم‌علیه اصلی ..... - principal

کدگذار ..... encoder

آنتروپی ..... entropy

پاک‌کننده ..... erasure

چندجمله‌ای تشخیص خطا ..... error locator polynomial

شاخص اویلر ..... Euler indicator

مقدار متوسط ..... expected value

گروه خارج‌قسمتی ..... factor group

میدان متناهی ..... finite field

مسطح ..... flat

میدان تابعی ..... function field

Galois ring ..... حلقه گالوا

Gaussian distribution ..... توزیع گوسی

generator

- of a cyclic group ..... مولد یک گروه دوری

-of AN code ..... مولد یک کد AN

- matrix ..... ماتریس مولد

- polynomial چندجمله‌ای مولد

genus ..... گونا

Goppa polynomial ..... چندجمله‌ای گاپا

Graeffe's method ..... روش گرائف

Gray map ..... نگاشت گری

group

- abelian ..... گروه آبلی

- algebra ..... جبر گروهی

- commutative ..... گروه جابه‌جایی

- cyclic ..... گروه دوری

- Mathieu ..... گروه متیو

- transitive ..... گروه ترایا

Hadamard matrix ..... ماتریس هادامارد

Hasse derivative ..... مشتق هسه

Hasse-Weil bound ..... کران هسه—ویل

Hensel's lemma ..... لم هنسل

hexacode ..... کد شش‌تایی

hyperplane ..... ابرصفحه

ideal

- maximal ..... ایده‌آل ماکسیمال

- prime ..... ایده‌آل اول

- principal ..... ایده‌آل اصلی

idempotent ..... خودتوان

incidence matrix ..... ماتریس وقوع

independent

- variables ..... متغیرهای مستقل

- vectors ..... بردارهای مستقل

information

- rate ..... نرخ اطلاعات

- symbol ..... سمبل اطلاعاتی

inner

- distribution ..... توزیع داخلی

- product ..... حاصل‌ضرب داخلی

integral domain ..... دامنه صحیح

irreducible polynomial ..... چندجمله‌ای تحویل‌ناپذیر

Jet Propulsion Laboratory ..... آزمایشگاه پرتاب جت

Klein quartic ..... چهارتایی کلاین

Krawtchouk

- expansion ..... توسیع کراچوک

- polynomial ..... چندجمله‌ای کراچوک

Kronecker product ..... حاصل‌ضرب کرونکر

Lee

- distance ..... فاصله لی

- metric ..... متریک لی

- weight ..... وزن لی

- weight enumerator ..... شمارنده وزنی

linear

- programming bound ..... کران برنامه‌ریزی خطی

- recurring sequence ..... دنباله بازگشتی خطی

Lloyd theorem ..... قضیه لوید

local ring ..... حلقه موضعی

Mattson-Solomon polynomial ..... چندجمله‌ای ماتسون—سولومن

mean ..... میانگین

memory ..... حافظه

minimal polynomial ..... چندجمله‌ای مینیمال

modular

- distance ..... فاصله پیمانه‌ای

- weight ..... وزن پیمانه‌ای

Moebius

- function ..... تابع موبیوس

فرمول معکوس موبیوس ..... - inversion formula

چندجمله‌ای تکین ..... monic polynomial

گروه ضربی یک میدان ..... multiplicative group of a field

فرم غیرمجاور ..... nonadjacent form

توزیع نرمال ..... normal distribution

رتبه ..... order

بررسی‌توازن‌های متعامد ..... orthogonal parity checks

توزیع خارجی ..... outer distribution

ماتریس پالی ..... Paley matrix

parameter

پارامتر موضعی ..... - local

پارامتر یکنواخت‌کننده ..... - uniformizing

parity check

معادله بررسی‌توازن ..... - equation

ماتریس بررسی‌توازن ..... - matrix

سمبل بررسی‌توازن ..... - symbol

ماتریس جای‌گشتی ..... permutation matrix

فرمول پلاکر ..... Plücker formula

point

نقطه در بی‌نهایت ..... - at infinity

نقطه نامنفرد ..... - nonsingular

نقطه گویا ..... - rational

نقطه ساده ..... - simple

قطب ..... pole

primitive

عضو اولیه ..... - element

خودتوان اولیه ..... - idempotent

چندجمله‌ای اولیه ..... - polynomial

ریشه اولیه واحد ..... - root of unity

principal

سرشت اصلی ..... - character

ایده‌آل اصلی ..... - ideal

حلقه ایده‌آل اصلی ..... - ideal ring

projective

- geometry ..... هندسه تصویری

- plane ..... صفحه تصویری

quadratic residue ..... مانده مربعی

quotient field ..... میدان خارج‌قسمتی

redundancy ..... افزونگی

regular function ..... تابع منظم

representative ..... معرف

residue

- class ..... کلاس باقی‌مانده

- ring ..... حلقه باقی‌مانده

- theorem ..... قضیه باقی‌مانده

Riemann-Roch theorem ..... قضیه ریمن—روچ

ring ..... حلقه

Shannon theorem ..... قضیه شانون

shift register ..... رجیستر تغییرمکان

Signal to Noise Ratio ..... نسبت سیگنال به نویز

sphere packing condition ..... شعاع پوششی شر

standard

- deviation ..... مشتق استاندارد

- form ..... فرم استاندارد

state diagram ..... دیاگرام حالت

Steiner system ..... دستگاه اشتاینر

Stirling's formula ..... فرمول استرلینگ

subspace ..... زیرفضا

symbol error probability ..... احتمال خطای سمبل

symmetric group ..... گروه متقارن

symmetrized weight enumerator ..... شمارنده وزنی متقارن

symplectic form ..... فرم سیمپلکس

syndrome ..... سیندروم

trace ..... اثر

Vandermonde determinant ..... دترمینان واندرموند

variance ..... واریانس

variety

- affine ..... آفین چندگونا

- projective ..... تصویر چندگونا

vector space ..... فضای برداری

Viterbi algorithm ..... الگوریتم ویتربی

weight

- distribution ..... توزیع وزنی

- enumerator ..... شمارنده وزنی

word length ..... طول کلمه

Zariski topology ..... توپولوژی زاریسکی

zero divisor ..... مقسوم‌علیه صفر

zero of a cyclic code ..... ریشه یک کد دوری

Introduction to Coding Theory

by:

J. H. Van Lint

Translated by:

Mohammad Gholami

Assisatnt professor of Shahrekord university

and

Reza Sobhani

Assisatnt professor of Isfahan university