

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 به صورت 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، گلی، 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 مهندسين برق و مخابرات بوده است، اما در سال‌های گذشته به دلیل توجه خاص به تحلیل مباحث تئوری در ساخت و کدگشایی کدهای تصحیح‌کننده 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 این رو 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 به صورت 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 متأسفانه 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 آن که 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 به عنوان سومین نسخه، هنوز به اندازه کافی محبوب است، لذت بخش است. من از این فرصت به منظور 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 به جای 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 تعریف شده با استفاده از کدهای ساخته شده 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.

علاوه بر این، برخی مطالب مربوط به کدهای رید-سولومن گسترش یافته و کدهای رید-مولر گسترش یافته، اضافه شده‌اند که در سخنرانی‌های من در اشپرینگر<sup>۱</sup> ۲۰۱۱ 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 تصحیح کننده 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<sup>۲</sup>، دورسما<sup>۳</sup>، هالمن<sup>۴</sup> و ن تیلبرگ<sup>۵</sup>، و ویلسن<sup>۶</sup> تشکر می‌کنم. هم‌چنین از لطف پلیکان<sup>۷</sup> و کمک او در تهیه فصل ۷ تشکر مخصوص دارم.

ون لینت<sup>۸</sup>

شهر آیندهوون<sup>۹</sup>، نوامبر ۱۹۹۸.

<sup>۱</sup> Springer

<sup>۲</sup> C.P.J.M. Baggen

<sup>۳</sup> I.M. Duursma

<sup>۴</sup> H.D.L. Hollmann

<sup>۵</sup> H.C.A. van Tilborg

<sup>۶</sup> R. M. Wilson

<sup>۷</sup> R.A. Pellikaan

<sup>۸</sup> J. H. van Lint

<sup>۹</sup> Eindhoven



# فهرست مطالب

۱	پیش‌زمینهٔ ریاضی	فصل اول
۲	جبر	۱.۱
۱۹	چندجمله‌ای‌های کراچوک	۱.۲
۲۲	نظریه ترکیبیات	۱.۳
۲۵	نظریه احتمالات	۱.۴
۲۹	قضیه شانون	فصل دوم
۲۹	مقدمه	۲.۱
۳۵	قضیه شانون	۲.۲
۳۸	بهره کدگذاری	۲.۳
۴۰	پیشنهادها	۲.۴
۴۲	مسائل	۲.۵
۴۴	کدهای خطی	فصل سوم
۴۴	کدهای بلوکی	۳.۱
۴۶	کدهای خطی	۳.۲
۵۱	کدهای همینگ	۳.۳
۵۳	کدگشایی با منطق اکثریت	۳.۴
۵۴	شمارنده‌های وزن	۳.۵
۵۶	متریک لی	۳.۶
۵۹	پیشنهادها	۳.۷
۵۹	مسائل	۳.۸

۶۲	فصل چهارم برخی کدهای خوب	
۶۲	کدهای هادامارد و تعمیم‌ها	۴.۱
۶۳	کد دوتایی گُلی	۴.۲
۶۸	کد گلی سه‌تایی	۴.۳
۶۸	ساختن کدها از کدهای دیگر	۴.۴
۷۲	کدهای رید-مولر	۴.۵
۷۹	کدهای کرداک	۴.۶
۸۲	پیشنهادها	۴.۷
۸۲	مسائل	۴.۸
۸۵	فصل پنجم کران‌هایی روی کدها	
۸۵	مقدمه؛ کران گیلبرت	۵.۱
۸۹	کران‌های بالای	۵.۲
۹۸	کران برنامه‌ریزی خطی	۵.۳
۱۰۳	پیشنهادها	۵.۴
۱۰۴	مسائل	۵.۵
۱۰۷	فصل ششم کدهای دوری	
۱۰۷	تعاریف	۶.۱
۱۱۰	ماتریس مولد و چندجمله‌ای بررسی	۶.۲
۱۱۱	صفرهای یک کد دوری	۶.۳
۱۱۳	خودتوان یک کد دوری	۶.۴
۱۱۷	نمایش‌های دیگر کدهای دوری	۶.۵
۱۲۰	کدهای BCH	۶.۶
۱۲۹	کدگشایی کدهای BCH	۶.۷
۱۳۱	کدهای رید-سولومن	۶.۸
۱۳۵	کدهای باقی‌مانده مربعی	۶.۹
۱۳۹	کدهای دوری دودویی با طول $2^n$ ( $n$ فرد)	۶.۱۰
۱۴۲	کدهای رید-مولر گسترش‌یافته	۶.۱۱

۱۴۵	پیشنهادها	۶.۱۲
۱۴۵	مسائل	۶.۱۳
۱۴۸	کدهای کامل و کدهای به‌طور یکنواخت بسته‌بندی شده	فصل هفتم
۱۴۸	قضیه لوید	۷.۱
۱۵۲	چند جمله‌ای مشخصه یک کد	۷.۲
۱۵۶	کدهای به‌طور یکنواخت بسته‌بندی شده	۷.۳
۱۵۹	مثال‌هایی از کدهای به‌طور یکنواخت بسته‌بندی شده	۷.۴
۱۶۳	قضایای عدم وجود	۷.۵
۱۶۷	پیشنهادها	۷.۶
۱۶۸	مسائل	۷.۷
۱۶۹	کدهای روی $\mathbb{Z}_4$	فصل هشتم
۱۶۹	کدهای چهارتایی	۸.۱
۱۷۰	کدهای دودویی به‌دست آمده از کدهای روی $\mathbb{Z}_4$	۸.۲
۱۷۵	حلقه‌های گالوا روی $\mathbb{Z}_4$	۸.۳
۱۸۰	کدهای دوری روی $\mathbb{Z}_4$	۸.۴
۱۸۳	مسائل	۸.۵
۱۸۴	کدهای گاپا	فصل نهم
۱۸۴	انگیزه	۹.۱
۱۸۵	کدهای گاپا	۹.۲
۱۸۸	کمترین-فاصله کدهای گاپا	۹.۳
۱۸۹	رفتار مجانبی کدهای گاپا	۹.۴
۱۹۰	کدگشایی کدهای گاپا	۹.۵
۱۹۱	کدهای BCH گسترش‌یافته	۹.۶
۱۹۴	پیشنهادها	۹.۷
۱۹۴	مسائل	۹.۸

۱۹۶	فصل دهم	کدهای هندسه جبری
۱۹۷	۱۰.۱	خم‌های جبری
۲۰۵	۱۰.۲	مقسوم‌علیه‌ها
۲۰۸	۱۰.۳	مشتق‌های روی یک منحنی
۲۱۱	۱۰.۴	قضیه ریمن-روچ
۲۱۳	۱۰.۵	کدها از خم‌های جبری
۲۱۶	۱۰.۶	برخی کدهای هندسی
۲۲۰	۱۰.۷	بهبود کران گیلبرت-ورشامو
۲۲۱	۱۰.۸	پیشنهادها
۲۲۲	۱۰.۹	مسائل

۲۲۳	فصل	کدهای جبری به‌طور مجانبی خوب
۲۲۳	۱۱.۱	یک مثال ساده غیرساختنی
۲۲۴	۱۱.۲	کدهای جاستسن
۲۲۹	۱۱.۳	پیشنهادها
۲۲۹	۱۱.۴	مسائل

۲۳۰	فصل	کدهای حسابی
۲۳۰	۱۲.۱	کدهای AN
۲۳۴	۱۲.۲	وزن پیمان‌های و حسابی
۲۳۸	۱۲.۳	کدهای مندلبوم-باروس
۲۳۹	۱۲.۴	پیشنهادها
۲۴۰	۱۲.۵	مسائل

۲۴۱	فصل	کدهای کانولوشن
۲۴۱	۱۳.۱	مقدمه
۲۴۶	۱۳.۲	کدگشایی کدهای کانولوشن
۲۴۸	۱۳.۳	مقایسه کران گیلبرت برای برخی کدهای کانولوشن
۲۴۹	۱۳.۴	ساختن کدهای کانولوشن از کدهای بلوکی دوری
۲۵۳	۱۳.۵	خودریختی‌های کدهای کانولوشن

۲۵۶ ..... پیشنهادها ۱۳.۶

۲۵۷ ..... مسائل ۱۳.۷

۲۵۸ فصل راهنمایی‌ها و حل مسائل

۲۵۸ راهنمایی‌ها و حل مسائل

۲۸۷ مراجع

۲۹۵ واژه‌نامه

# فصل ۱

## پیش‌زمینه ریاضی

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

<sup>۱</sup> designs

<sup>۲</sup> geometries

<sup>۳</sup> orthogonal polynomials

<sup>۴</sup> Krawtchouk

## ۱.۱ جبر

ما تنها به مقدمات بسیار کمی از نظریه اعداد نیاز داریم. از قبل می دانیم که هر عضو  $\mathbb{N}$  را می توان تنها به یک روش، به صورت حاصل ضرب اعداد اول نوشت (اگر از ترتیب عوامل صرف نظر کنیم). اگر  $b$  بر  $a$  بخش پذیر باشد، می نویسیم  $a|b$ . اگر  $p$  یک عدد اول باشد و  $a|p$ ، اما  $a \nmid p^{r+1}$  می نویسیم  $a|p^r$ . اگر  $k \in \mathbb{N}$ ،  $k > 1$ ، آن گاه برای  $0 \leq i \leq l$ ، یک نمایش از  $n$  در پایه  $k$  به صورت:

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

می باشد. بزرگ ترین عدد صحیح  $n$  به طوری که  $n|a$  و  $n|b$  بزرگ ترین مقسوم علیه مشترک  $a$  و  $b$  نامیده می شود و با نماد  $(a, b)$  ب.م.م یا به اختصار  $(a, b)$  نمایش داده می شود. اگر  $m|(a-b)$  آن گاه می نویسیم  $a \equiv b \pmod{m}$ .

### قضیه ۱.۱.۱.۱. اگر:

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

آن گاه:

$$\varphi(n) = n \prod_{p|n} (1 - 1/p) \quad (۱)$$

$$\sum_{d|n} \varphi(d) = n \quad (۲)$$

تابع  $\varphi$  شاخص اویلر<sup>۵</sup> نامیده می شود.

قضیه ۲.۱.۱. اگر  $(a, m) = 1$  آن گاه  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

قضیه ۲.۱.۱، قضیه اویلر-فرما نامیده می شود.

تعریف ۳.۱.۱. تابع موبیوس<sup>۶</sup>  $\mu$ ، به صورت زیر تعریف می شود:

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

<sup>۵</sup> Euler indicator

<sup>۶</sup> Möbius

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

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

آن‌گاه:

$$f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right).$$

قضیه ۴.۱.۱ به فرمول معکوس موبیوس<sup>۷</sup> 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  $(G, \cdot)$  یک مجموعه  $G$  می‌باشد؛ به طوری که یک عمل‌گر حاصل ضرب روی آن تعریف شده و این عمل‌گر در خواص زیر صدق می‌کند:

$$\forall a \in G \forall b \in G [ab \in G], \quad (1)$$

$$\forall a \in G \forall b \in G \forall c \in G [(ab)c = a(bc)], \quad (2)$$

$$\exists e \in G \forall a \in G [ae = ea = a], \quad (3)$$

(عضو  $e$  یکتاست)

$$\forall a \in G \exists b \in G [ab = ba = e], \quad (4)$$

( $b$  وارون  $a$  نامیده می‌شود و با  $a^{-1}$  نمایش داده می‌شود.)

علاوه بر این اگر:

$$\forall a \in G \forall b \in G [ab = ba], \quad (5)$$

آن‌گاه گروه یادشده، آبلی یا جابه‌جایی نامیده می‌شود.

<sup>۷</sup> Möbius inversion formula



اگر  $(G, )$  یک گروه باشد و  $H \subset G$  به طوری که  $(H, )$  نیز یک گروه باشد، آن گاه  $(H, )$  یک زیرگروه  $(G, )$  نامیده می شود. تعداد عناصر یک گروه متناهی، مرتبه آن گروه نامیده می شود. اگر  $(G, )$  یک گروه باشد و  $a \in G$  آن گاه کوچک ترین عدد صحیح مثبت  $n$  به طوری که  $a^n = e$  (اگر چنین  $n$ ی موجود باشد)، مرتبه  $a$  نامیده می شود. در این حالت عناصر  $e, a, a^2, \dots, a^{n-1}$  تشکیل یک زیرگروه، معروف به زیرگروه دوری، می دهند که  $a$  به عنوان مولد آن شناخته می شود. اگر  $(G, )$  آبلی باشد و  $(H, )$  یک زیرگروه آن باشد، آن گاه مجموعه های  $aH := \{ah \mid h \in H\}$  هم مجموعه های  $H$  نامیده می شوند. از آنجا که دو هم مجموعه به وضوح برابر یا مجزا می باشند، هم مجموعه ها تشکیل یک افراز برای  $G$  می دهند. یک عضو انتخابی از یک هم مجموعه یک نماینده از آن هم مجموعه نامیده می شود. اگر حاصل ضرب هم مجموعه ها را با  $(aH)(bH) := abH$  تعریف کنیم، نشان دادن این که هم مجموعه ها مجدداً یک گروه تشکیل می دهند، مشکل نیست. این گروه، گروه خارج قسمتی<sup>۱</sup> نامیده می شود و با  $G/H$  نمایش داده می شود. به عنوان یک نتیجه، دقت دارید که اگر  $a \in G$  آن گاه مرتبه  $a$  مرتبه  $G$  را عاد می کند (هم چنین اگر  $G$  آبلی نباشد). یک قضیه اساسی از نظریه گروه ها بیان می کند که یک گروه آبلی متناهی، مجموع مستقیم گروه های دوری است.

**تعریف ۶.۱.۱.** یک مجموعه  $R$  با دو عملگر، که معمولاً جمع و ضرب نامیده می شوند، و نمایش داده شده به وسیله  $(R, +, )$ ، یک حلقه است اگر:

$$(1) \quad (R, +) \text{ یک گروه آبلی باشد.}$$

$$(2) \quad \forall a \in R \forall b \in R \forall c \in R [(ab)c = a(bc)],$$

$$(3) \quad \forall a \in R \forall b \in R \forall c \in R [a(b+c) = ab+ac \wedge (a+b)c = ac+bc].$$

عضو همانی  $(R, +)$  معمولاً با  $0$  نمایش داده می شود.

اگر خاصیت اضافی

$$(4) \quad \forall a \in R \forall b \in R [ab = ba],$$

برقرار باشد، آن گاه این حلقه را جابه جایی می نامیم.

اعداد صحیح  $\mathbb{Z}$  بهترین مثال شناخته شده از یک حلقه می باشد.

اگر  $(R, +, )$  یک حلقه جابه جایی باشد، آن گاه یک عضو ناصفر  $a \in R$  یک مقسوم علیه صفر نامیده می شود اگر یک عضو ناصفر  $b \in R$  موجود باشد، به قسمی که  $ab = 0$ . حلقه ای که شامل هیچ مقسوم علیه صفری نباشد، یک قلمرو صحیح نامیده می شود. مشابه روشی که  $\mathbb{Z}$  به اعداد  $\mathbb{Q}$  گسترش داده می شود،

<sup>۱</sup> factor group

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

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

$$(1) \quad \forall a \in S \forall b \in S [a - b \in S]$$

$$(2) \quad \forall a \in S \forall b \in R [ab \in S \wedge ba \in S]$$

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

تعریف ۸.۱.۱. یک میدان، یک حلقه  $(R, +, \cdot)$  است به طوری که  $(R - \{0\}, \cdot)$  یک گروه آبلی است.

قضیه ۹.۱.۱. هر حلقه متناهی  $R$  با حداقل دو عضو به طوری:

$$\forall a \in R \forall b \in R [ab = 0 \Rightarrow (a = 0 \vee b = 0)],$$

یک میدان است.

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

$$(1) \quad \forall a \in V [1a = a]$$

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

$$(2) \quad \forall \alpha \in \mathbb{F} \forall a \in V \forall b \in V [\alpha(a + b) = \alpha a + \alpha b]$$

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

در این صورت سه‌تایی  $(V, +, \mathbb{F})$  یک فضای برداری روی میدان  $\mathbb{F}$  نامیده می‌شود. هم‌چنین عضو همانی  $(V, +)$  با  $0$  نمایش داده می‌شود.

فرض می‌کنیم خواننده با فضای برداری  $\mathbb{R}^n$  شامل تمامی  $n$ -تایی‌های  $(a_1, a_2, \dots, a_n)$  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  $(a_{11}, a_{12}, \dots, a_{1n}) := (a_1,$

هر  $a \in C$  را بتوان به طور یکتا به صورت  $\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k$  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، به طور معمول بردارها را به‌عنوان بردارهای سطری می‌نویسیم. ضرب داخلی  $\langle a, b \rangle$  از دو بردار  $a$  و  $b$  به صورت:

$$\langle a, b \rangle := a_1 b_1 + a_2 b_2 + \dots + a_n b_n,$$

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

$$C^\perp := \{y \in \mathbb{R}^n \mid \forall x \in C [\langle x, y \rangle = 0]\}.$$

در ادامه، وقتی که  $\mathbb{R}$  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 ۱۱.۱.۱.** فرض کنید  $(V, +)$  یک فضای برداری روی میدان  $\mathbb{F}$  باشد و ضرب  $V \times V \rightarrow V$  با خواص زیر تعریف شده باشد:

$$(1) \quad (V, +, \cdot) \text{ یک حلقه باشد،}$$

$$(2) \quad \forall \alpha \in \mathbb{F} \forall a \in V \forall b \in V [(\alpha a)b = a(\alpha b)]$$

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

فرض کنید یک گروه متناهی  $(G, \cdot)$  داریم و عناصر  $G$  را به‌عنوان پایه‌ی یک فضای برداری  $(V, +)$  روی میدان  $\mathbb{F}$  در نظر گرفته‌ایم. در این صورت عناصر  $V$  توسط ترکیبات خطی  $\alpha_1 g_1 + \alpha_2 g_2 + \dots + \alpha_n g_n$  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:

$$\left(\sum_i \alpha_i g_i\right) * \left(\sum_j \beta_j g_j\right) := \sum_i \sum_j (\alpha_i \beta_j) (g_i \cdot g_j),$$

که می‌تواند به صورت  $\sum_k \gamma_k g_k$  نوشته شود، جایی که  $\gamma_k$  مجموع عناصر  $\alpha_i b_j$  روی تمامی زوج‌های  $(i, j)$  می‌باشد به طوری که  $g_i \cdot g_j = g_k$ . 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 ارائه شده در بالا را می‌آوریم.

اگر  $A := \{a_1, a_2, \dots, a_n\}$  یک مجموعه متناهی باشد، آن‌گاه تمامی توابع یک‌به‌یک از  $A$  به  $A$  را در نظر بگیرید. اینها جای‌گشت‌ها نامیده می‌شوند. اگر  $\sigma_1$  و  $\sigma_2$  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. به آسانی 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  $\sigma$  از اعداد صحیح  $1, 2, \dots, n$  را در نظر بگیرید که برای هر  $(c_1, c_2, \dots, c_n) \in C$ ، بردار  $(c_{\sigma(1)}, c_{\sigma(2)}, \dots, c_{\sigma(n)})$  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 نگاشت‌ها، 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  $1$  در هر سطر و ستون می‌باشد. گوئیم  $P$  متناظر با جای‌گشت  $\sigma$  از  $\{1, 2, \dots, n\}$  می‌باشد وقتی که  $p_{ij} = 1$  اگر و تنها اگر  $i = \sigma(j)$ . با این قرارداد، حاصل ضرب جای‌گشت‌ها متناظر با حاصل ضرب ماتریس‌های آنها می‌باشد. با این روش، نمایش ماتریسی معروفی از یک گروه جای‌گشت‌ها به‌دست می‌آید.

یک گروه  $G$  متشکل از جای‌گشت‌های روی مجموعه  $\Omega$ ، یک  $k$ -تراگذر روی  $\Omega$  نامیده می‌شود اگر برای هر  $k$ -تایی مرتب  $(a_1, a_2, \dots, a_k)$  از عناصر متمایز  $\Omega$  و برای هر  $k$ -تایی  $(b_1, b_2, \dots, b_k)$  از عناصر متمایز  $\Omega$  یک عضو  $\sigma \in G$  موجود باشد به طوری 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  $(R, +, \cdot)$  باشد. چون  $(S, +)$  یک زیرگروه از گروه آبدلی  $(R, +)$  است می‌توانیم گروه عامل را تشکیل دهیم. این هم مجموعه‌ها در اینجا کلاس‌های باقی‌مانده به پیمانه  $S$

نامیده می‌شوند. برای این کلاس‌ها، ما ضرب بدیهی  $ab + S := (a + S)(b + S)$  را تعریف می‌کنیم. خواننده‌ای که با این مفهوم آشنا نیست، باید خوش‌تعریف بودن آن را 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  $\mathbb{Z} := \mathbb{Z}$  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 این صورت  $R/S$  حلقه اعداد صحیح به پیمانه  $p$  است. عناصر  $R/S$  با  $0, 1, \dots, p-1$  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  $p = 7$ ، در این صورت  $2 + 5 = 7$  زیرا در  $\mathbb{Z}$  داریم  $2 + 5 \equiv 7 \pmod{7}$ . به روش مشابه  $6 = 4.5$  در  $\mathbb{Z}/7\mathbb{Z} = \mathbb{Z}/(7)$ . اگر  $S$  یک ایده‌آل در  $\mathbb{Z}$  باشد و  $S \neq \{0\}$ ، آن‌گاه کوچک‌ترین عدد صحیح  $k$  در  $S$  وجود دارد. فرض کنید  $s \in S$ . می‌توانیم  $s$  را به صورت  $ak + b$  بنویسیم که در آن  $0 \leq b < k$ . با تعریف ایده‌آل، داریم  $ak \in S$ ؛ بنابراین،  $b = s - ak \in S$  و بنابر تعریف  $k$  نتیجه می‌شود  $b = 0$ . از این رو  $S = (k)$ . 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 سراسر است 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. در ابتدا مطالب بیشتری درباره حلقه‌ها و ایده‌آل‌ها را بیان می‌کنیم. فرض کنید  $\mathbb{F}$  یک میدان متناهی باشد. مجموعه  $\mathbb{F}[x]$  شامل تمامی چندجمله‌ای‌ها به صورت  $a_0 + a_1x + \dots + a_nx^n$  می‌باشد که در آن می‌تواند هر عدد صحیح در  $\mathbb{N}$  باشد و برای  $0 \leq i \leq n$  داریم  $a_i \in \mathbb{F}$ . با تعریف متداول جمع و ضرب چندجمله‌ای‌ها،  $(\mathbb{F}[x], +, \cdot)$  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 این صورت می‌باشند.

**قضیه ۱۳.۱.۱.**  $\mathbb{F}[x]$  یک حلقه ایده‌آل اصلی می‌باشد.

حلقه کلاس‌های باقی‌مانده  $\mathbb{F}/(g(x))$  را می‌توان به صورت 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 به طریق 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  $g(x) = x^2 + x + 1$ . آن‌گاه  $x^3 + x^2 + x + 1 = (x+1)(x^2+1) + 1$ . این مثال برای مطالعه دقیق کسی که با میدان‌های متناهی ناآشناست، یک نمونه مفید است. در ابتدا 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  $\mathbb{F}_2[x]/(g(x))$ ، حاصل ضرب هر دو عضو  $a(x)$  و  $b(x)$  برابر با صفر است اگر و تنها 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 ۱۴.۱.۱.** فرض کنید  $p$  یک عدد اول و  $g(x)$  یک چندجمله‌ای تحویل‌ناپذیر با درجه  $r$  در حلقه  $\mathbb{F}_p[x]$  باشد؛ در این صورت 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  $g(x) = x^2 + x + 1$ .

**قضیه ۱۵.۱.۱.** فرض کنید  $\mathbb{F}$  یک میدان با  $n$  عضو باشد؛ در این صورت  $n$  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  $3 = 2 + 1$  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 مجموعه  $k$  تا  $1$  برابر با مجموع  $l$  تا  $1$  باشد ( $k > l$ ). بنابراین، مجموعه  $(k - l)$  تا  $1$  برابر با صفر است؛ یعنی اولین باری که با یک عضو تکراری مواجه شدیم، آن عضو صفر است. گوییم  $0$  مجموعه  $k$  تا  $1$  است. اگر  $k$  یک عدد مرکب باشد،  $k = ab$ ، آن گاه حاصل ضرب عناصری که آنها را به ترتیب  $a$  و  $b$  نامیده ایم، برابر با صفر می باشد که یک تناقض است؛ بنابراین،  $k$  یک عدد اول مانند  $p$  می باشد و ما نشان داده ایم که  $\mathbb{F}_p$  زیرمیدانی از  $\mathbb{F}$  است. استقلال خطی یک مجموعه از عناصر  $\mathbb{F}$  را نسبت به (ضرایبی از)  $\mathbb{F}_p$  به طور طبیعی تعریف می کنیم. در میان تمام زیرمجموعه های مستقل خطی  $\mathbb{F}$ ، فرض کنید  $\{x_1, x_2, \dots, x_r\}$  دارای بیشترین عضو باشد. اگر  $x$  متعلق به  $\mathbb{F}$  باشد، آن گاه عناصر  $x, x_1, x_2, \dots, x_r$  مستقل خطی نیستند؛ یعنی ضرایب  $\alpha_1, \alpha_2, \dots, \alpha_r \neq 0$  موجودند به طوری که  $\alpha x + \alpha_1 x_1 + \dots + \alpha_r x_r = 0$  و از این رو  $x$  یک ترکیب خطی از  $x_1$  تا  $x_r$  است. چون به طور آشکار  $p^r$  ترکیب خطی مجزا از عناصر  $x_1$  تا  $x_r$  وجود دارد، اثبات کامل است.  $\square$

از قضایای قبل می دانیم که یک میدان با  $n$  عضو وجود دارد اگر و تنها اگر  $n$  توانی از یک عدد اول باشد. به این صورت که ما می توانیم نشان دهیم برای هر  $r \geq 1$  یک چندجمله ای تحویل ناپذیر با درجه  $r$  در  $\mathbb{F}_p[x]$  وجود دارد. ما این مطلب را با محاسبه تعداد چنین چندجمله ای هایی اثبات خواهیم نمود.  $p$  را ثابت فرض کنید و  $I_r$  را تعداد چندجمله ای های تحویل ناپذیر با درجه  $r$  تعریف کنید که تکین هستند؛ یعنی ضریب  $x^r$  در آنها برابر با  $1$  است. ادعا می کنیم:

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

برای اثبات آن در ابتدا می بینیم که ضرایب  $z^n$  در طرف چپ معادله فوق برابر با  $p^n$  می باشد که برابر با تعداد چندجمله ای های تکین با درجه  $n$  و ضرایب در  $\mathbb{F}_p$  است. می دانیم هر چنین چندجمله ای را می توان به طور یکتا به صورت حاصل ضرب عوامل تحویل ناپذیر تجزیه نمود؛ بنابراین، باید خود را قانع کنیم که این عوامل در طرف راست معادله  $1$  شمارش شده اند. برای نشان دادن این مطلب، دو چندجمله ای تحویل ناپذیر  $a_1(x)$  با درجه  $r$  و  $a_2(x)$  با درجه  $s$  را در نظر می گیریم. 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  $(1 + z_1^r + z_1^{2r} + \dots)$  و  $(1 + z_2^s + z_2^{2s} + \dots)$  وجود دارد. اگر ما  $z_1$  و  $z_2$  را برابر با  $z$  قرار دهیم، آن گاه توان  $z$  برابر با درجه  $(a_1(x))^k (a_2(x))^l$  می باشد. حال به جای دو چندجمله ای  $a_1(x)$  و  $a_2(x)$ ، تمامی چندجمله ای های تحویل ناپذیر را در نظر می گیریم و رابطه  $1$  نتیجه می شود.

در رابطه  $1$ ، از دو طرف لگاریتم گرفته و سپس مشتق می گیریم. سرانجام دو طرف را در  $z$  ضرب

می‌کنیم؛ داریم:

$$\frac{pz}{1-pz} = \sum_{r=1}^{\infty} I_r \frac{rz^r}{1-z^r} \quad (2)$$

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

$$p^n = \sum_{r|n} r I_r. \quad (3)$$

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

$$\begin{aligned} I_r &= \frac{1}{r} \sum_{d|r} \mu(d) p^{r/d} > \frac{1}{r} \{p^r - p^{r/2} - p^{r/3} - \dots\} \\ &> \frac{1}{r} (p^r - \sum_{i=0}^{r/2} p^i) > \frac{1}{r} p^r (1 - p^{-r/2+1}) > 0. \end{aligned} \quad (4)$$

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  $f(a) = 0$ ، در نظر بگیرید. سپس با تقسیم کردن، متوجه می‌شویم که یک  $g(x) \in \mathbb{F}[x]$  وجود دارد به طوری 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  $\alpha$  یک عضو با مرتبه  $e$  در گروه حاصل ضربی  $(\mathbb{F}_{p^r} - \{0\})$  باشد، آن‌گاه  $\alpha$  یک ریشه از چندجمله‌ای  $x^e - 1$  است. در واقع داریم:

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

در نتیجه تنها عناصر با مرتبه  $e$  در این گروه، توان‌های  $\alpha^i$  هستند، که در آن  $1 \leq i < e$  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 حاصل ضربی  $(\mathbb{F}_q - \{0\})$  یک گروه دوری است.

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

تعریف ۱۷.۱.۱. یک مولد از گروه حاصل ضربی 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  $q$  ریشه متمایز از چندجمله‌ای  $x^q - x$  هستند. یک عضو  $\beta$  که  $\beta^k = 1$  و برای  $0 < l < k$  داشته باشیم  $k, \beta^l \neq 1$  امین ریشه اولیه واحد نامیده می‌شود. به‌وضوح یک عضو اولیه  $\alpha$  از  $\mathbb{F}_q$ ،  $(q-1)$  امین ریشه اولیه واحد نامیده می‌شود. اگر  $q-1$  بر  $e$  بخش‌پذیر باشد آن‌گاه  $\alpha^e$  یک  $(q-1)/e$  امین ریشه اولیه واحد نامیده می‌شود. علاوه بر آن به عنوان یک نتیجه از قضیه ۱۶.۱.۱ داریم  $\mathbb{F}_{p^r}$  زیرمیدانی از  $\mathbb{F}_{p^s}$  است اگر و تنها اگر  $s$  بر  $r$  بخش‌پذیر باشد. در واقع این مطلب ممکن است برای خواننده کمی گیج‌کننده به نظر آید. در نمادگذاری هایمان این‌طور به نظر 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 به طوری که  $r | n$ . از رابطه ۳ نتیجه می‌شود که ما تمامی چندجمله‌ای‌های تحویل‌ناپذیر با درجه  $r$  را که در آن  $r | n$ ، به کار برده‌ایم. به عبارت دیگر، حاصل ضرب 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  $\varphi: \mathbb{F} \rightarrow \mathbb{F}'$  وجود دارد که یک به یک است و جمع و ضرب را حفظ می‌کند.

قضیه زیر بیشتر اوقات در این کتاب به کار برده می‌شود.

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

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

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

**اثبات.**

(۱) با به کارگیری 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 به اندازه کافی گسترش یافته از  $\mathbb{F}_q$ ، چندجمله‌ای  $g(x)$ ، حاصل ضرب عوامل  $x - \alpha_i$ ، یعنی عوامل مرتبه ۱، می‌باشد و اگر  $x - \alpha_i$  یکی از آن عوامل باشد، آن‌گاه  $\alpha_i^q - \alpha_i = 0$ .

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  $\alpha_i$  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  $\alpha$  روی  $\mathbb{F}_q$ ، چندجمله‌ای تحویل‌ناپذیر  $f(x) \in \mathbb{F}_p[x]$  است به طوری که  $f(\alpha) = 0$ . اگر  $\alpha$  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 به طوری که  $p^m \equiv 1 \pmod{e}$ .

برخی اوقات، یک میدان  $\mathbb{F}_q$  را با یک عضو اولیه ثابت  $\alpha$  مشخص می‌کنیم. در آن حالت  $m_i(x)$  را به عنوان چندجمله‌ای مینیمال  $\alpha^i$  به کار 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 جزئیات آن می‌آوریم.

مثال ۱۹.۱.۱. چندجمله‌ای  $x^4 + x + 1$  روی  $\mathbb{F}_2$  یک چندجمله‌ای اولیه است. میدان  $\mathbb{F}_{2^4}$  به وسیله چندجمله‌ای‌های با درجه کمتر از ۴ نمایش داده می‌شود. چندجمله‌ای  $x$  یک عضو اولیه است. از آنجایی که ما به کارگیری نماد  $x$  را برای اهداف دیگری ترجیح می‌دهیم، این عضو اولیه را  $\alpha$  می‌نامیم. توجه دارید که  $\alpha^4 + \alpha + 1 = 0$ . هر عضو  $\mathbb{F}_{2^4}$  یک ترکیب خطی از عناصر  $1, \alpha, \alpha^2, \alpha^3$  است. جدول ۱.۱ را برای  $\mathbb{F}_{2^4}$  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  $\mathbb{F}_{2^4}$  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 حاصل ضرب (جمع توان‌ها در پیمانه ۱۵) است و ستون سمت راست برای حاصل جمع (جمع بردارها). حال به آسانی می‌توان بررسی نمود که:

$$m_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) = x^4 + x + 1,$$

$$m_3(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) = x^4 + x^3 + x^2 + x + 1,$$

$$m_5(x) = (x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1,$$

$$m_7(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) = x^4 + x^3 + 1.$$

جدول ۱.۱: جدول عناصر  $\mathbb{F}_{2^4}$ 

$0$	$=$		$= (0000)$
$1$	$=$	$1$	$= (1000)$
$\alpha$	$=$	$\alpha$	$= (0100)$
$\alpha^2$	$=$	$\alpha^2$	$= (0010)$
$\alpha^3$	$=$	$\alpha^3$	$= (0001)$
$\alpha^4$	$=$	$1 + \alpha$	$= (1100)$
$\alpha^5$	$=$	$\alpha + \alpha^2$	$= (0110)$
$\alpha^6$	$=$	$\alpha^2 + \alpha^3$	$= (0011)$
$\alpha^7$	$=$	$1 + \alpha + \alpha^2$	$= (1101)$
$\alpha^8$	$=$	$1 + \alpha^2$	$= (1010)$
$\alpha^9$	$=$	$\alpha + \alpha^2 + \alpha^3$	$= (0101)$
$\alpha^{10}$	$=$	$1 + \alpha + \alpha^2$	$= (1110)$
$\alpha^{11}$	$=$	$\alpha + \alpha^2 + \alpha^3$	$= (0111)$
$\alpha^{12}$	$=$	$1 + \alpha + \alpha^2 + \alpha^3$	$= (1111)$
$\alpha^{13}$	$=$	$1 + \alpha^2 + \alpha^3$	$= (1011)$
$\alpha^{14}$	$=$	$1 + \alpha^2$	$= (1001)$

و تجزیه  $x - x^{16}$  به عوامل تحویل ناپذیر برابر است با:

$$x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)$$

$$x(x^4+x^3+1)(x^4+x^2+x+1).$$

دقت دارید که  $x^4 - x = x(x-1)(x^2+x+1)$  متناظر با اعضای  $0, 1, \alpha^5$  و  $\alpha^{10}$  می‌باشد که تشکیل زیرمیدان  $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$  را می‌دهند. چند جمله‌ای  $m_3(x)$  تحویل ناپذیر 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  $\mathbb{F}_9, \mathbb{F}_{27}$  و  $\mathbb{F}_{64}$  را با چند جمله‌ای‌های مینیمال و زیر میدان‌های متناظر آن بسازد. در مورد 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 به صورت نمادی، به شکل:

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

تعریف نماییم. قواعد عمومی مشتق مجموع و حاصل ضرب 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  $\alpha$  یک ریشه تکراری در یک میدان گسترش‌یافته از  $\mathbb{F}_q$  باشد، آن‌گاه  $\alpha$  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. به منظور دسترسی به شباهت کامل با نظریه چندجمله‌ای‌ها بر روی  $\mathbb{R}$ ، مشتق هسه<sup>۹</sup> از یک چندجمله‌ای  $f(x) \in \mathbb{F}_q[x]$  را به صورت 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  $\alpha$  یک ریشه از  $f(x)$  با تکرار  $k$  است اگر و تنها اگر برای  $0 \leq i < k$ ،  $\alpha$  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؛ به طوری که:

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

<sup>۹</sup> 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 این صورت، روش قبل را می‌توان ادامه داد تا چندجمله‌ای‌های تحویل‌ناپذیر با درجه ۳ را تولید نمود و به همین ترتیب ادامه داد. در بخش ۹.۲، چندجمله‌ای‌های تحویل‌ناپذیر روی  $\mathbb{F}_2$  با درجات به دلخواه بزرگ را نیاز خواهیم داشت. فرایند ترسیم‌شده در فوق برای این منظور رضایت‌بخش نمی‌باشد. در واقع به جای این فرایند، کار را به روش زیر ادامه می‌دهیم:

لم ۲۲.۱.۱.

$$3^{\beta+1} \mid (2^{3^\beta} + 1).$$

اثبات.

(۱) برای  $\beta = 0$  و  $\beta = 1$  این ادعا درست می‌باشد.

(۲) فرض کنید  $3^t \mid (2^{3^\beta} + 1)$ ؛ در این صورت از:

$$(2^{3^{\beta+1}} + 1) = (2^{3^\beta} + 1)\{(2^{3^\beta} + 1)(2^{3^\beta} - 2) + 3\},$$

نتیجه می‌شود که اگر  $t \geq 2$  آن‌گاه  $3^{t+1} \mid (2^{3^{\beta+1}} + 1)$ .

□

لم ۲۳.۱.۱. اگر  $m$  دارای مرتبه ۲ (به پیمانه  $3^l$ ) باشد، آن‌گاه:

$$m = \varphi(3^l) = 2 \cdot 3^{l-1}.$$

اثبات. اگر  $2^\alpha \equiv 1 \pmod{3}$  آن‌گاه  $\alpha$  زوج می‌باشد؛ بنابراین،  $m = 2s$ . از این رو  $2^s + 1 \equiv 0 \pmod{3^l}$ . اکنون، حکم از قضیه ۲.۱.۱ و لم ۲۲.۱.۱ به دست می‌آید. □

قضیه ۲۴.۱.۱. قرار دهید  $m = 2 \cdot 3^{l-1}$ ؛ در این صورت:

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

روی  $\mathbb{F}_3$  تحویل‌ناپذیر است.

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

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

یک چندجمله‌ای از درجه  $m$  می‌باشد. دقت دارید که:

$$x^{3^l} + 1 = (1 + x)(1 + x + x^2)(1 + x^3 + x^6) \dots (1 + x^{3^{l-1}} + x^{2 \cdot 3^{l-1}}),$$

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  $0$ ،  $\frac{q-1}{2}$  مربع ناصفر و  $\frac{q-1}{2}$  نامربع است. اعداد صحیح  $k$ ،  $1 \leq k \leq p-1$ ، که مربع‌هایی در  $\mathbb{F}_p$  هستند معمولاً باقی‌مانده‌های مربعی (به پیمانانه  $p$ ) نامیده می‌شوند. با در نظر گرفتن  $k \in \mathbb{F}_p$  به‌عنوان توانی از یک عضو اولیه در این میدان، می‌بینیم که  $k$  یک باقی‌مانده مربعی (به پیمانانه  $p$ ) است اگر و تنها اگر  $k^{(p-1)/2} \equiv 1 \pmod{p}$ . برای عضو  $-1 = p-1$  داریم  $-1$  یک مربع در  $\mathbb{F}_p$  است اگر و تنها اگر  $4 \equiv 1 \pmod{p}$ . در بخش ۶.۹ نیاز داریم بدانیم که آیا  $2$  در  $\mathbb{F}_p$  یک مربع است یا نه. برای تصمیم‌گیری درباره این سوال، عناصر  $1, 2, \dots, (p-1)/2$  را در نظر می‌گیریم و  $a$  را برابر با حاصل ضرب آنها قرار می‌دهیم. با ضرب هر یک از این عناصر در  $2$ ، مقادیر  $2, 4, \dots, p-1$  را به دست می‌آوریم.

این دنباله شامل  $\lfloor (p-1)/4 \rfloor$  عامل است که عوامل  $a$  می‌باشند و برای هر عامل دیگر  $k$  از  $a$  می‌بینیم که  $-k$  یکی از اعداد صحیح زوج بزرگ‌تر از  $(p-1)/2$  می‌باشد. این نتیجه می‌دهد که در  $\mathbb{F}_p$  داریم

$a^{(p-1)/2} = (-1)^{\lfloor (p-1)/4 \rfloor - (p-1)/2}$  و چون  $a \neq 0$  می‌بینیم که  $2$  یک مربع است اگر و تنها اگر:

$$\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor,$$

زوج باشد و این؛ یعنی  $p \equiv \pm 1 \pmod{8}$ .

## اثر

فرض کنید  $q = p^r$ . نگاشت  $Tr : \mathbb{F}_q \rightarrow \mathbb{F}_p$  که اثر  $1^\circ$  نامیده می‌شود، به صورت زیر تعریف می‌شود:

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

$$Tr(\xi) := \xi + \xi^p + \xi^{p^2} + \dots + \xi^{p^{r-1}}.$$

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؛ به طوری که  $Tr(\xi) \neq 0$ .

(۳)  $Tr$  یک نگاشت خطی است.

اثبات.

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

(۲) معادله  $x + x^p + \dots + x^{p^{r-1}} = 0$  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  $p^{-1}q$  بار اختیار می‌کند و می‌بینیم که تابع چندجمله‌ای  $x + x^p + \dots + x^{p^{r-1}}$  حاصل ضرب چندجمله‌ای‌های مینیمال است (برای بررسی آن به مثال ۱۹.۱.۱ رجوع نمایید).

## سرشت‌ها

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

$$\forall g_1 \in G \forall g_2 \in G [\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)]. \quad (5)$$

از این تعریف نتیجه می‌شود که برای هر سرشت  $\chi$  داریم  $\chi(0) = 1$ . اگر برای هر  $g \in G$  داشته باشیم  $\chi(g) = 1$ ، آن‌گاه  $\chi$  یک سرشت اصلی نامیده می‌شود.

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

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{اگر } \chi \text{ سرشت اصلی باشد} \\ 0, & \text{در غیر این صورت} \end{cases}$$

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

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

اگر  $\chi$  سرشت اصلی نباشد، آن‌گاه می‌توان  $h$  را به گونه‌ای یافت که در آن  $\chi(h) \neq 1$ . □

## 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<sup>۱۲</sup>. 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<sup>۱۳</sup> [۶۷]؛ جکسون<sup>۱۴</sup> [۳۶] و تریکومی<sup>۱۵</sup> [۷۰]). در واقع، خواننده

<sup>۱۱</sup>character

<sup>۱۲</sup>Krawtchouk polynomial

<sup>۱۳</sup>G. Szegő

<sup>۱۴</sup>D. Jackson

<sup>۱۵</sup>F. G. Tricomi



را در مورد برخی از اثبات قضایایی که در زیر بیان می‌کنیم، به متون مربوط با آن ارجاع می‌دهیم. به جهت 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  $k = 0, 1, 2, \dots$  چندجمله‌ای کراچوک  $K_n(x)$  به صورت زیر تعریف می‌شود:

$$K_k(x; n, q) := K_k(x) := \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j},$$

که در آن:

$$\binom{x}{j} := \frac{x(x-1)\cdots(x-j+1)}{j!}, \quad (x \in \mathbb{R}).$$

توجه کنید که در حالت  $q = 2$  داریم:

$$K_k(x) = \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{n-x}{k-j} = (-1)^k K_k(n-x). \quad (6)$$

با ضرب سری‌های تیلور  $(1+z(q-1))^n$  و  $(1-z)^x$  داریم:

$$\sum_{k=0}^{\infty} K_k(x) z^k = (1+(q-1)z)^{n-x} (1-z)^x. \quad (7)$$

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:

$$\sum_{i=0}^n \binom{n}{i} (q-1)^i K_k(i) K_l(i) = \delta_{kl} \binom{n}{k} (q-1)^k q^n. \quad (8)$$

خواننده به آسانی 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  $\infty$ ) جمع بسته و از رابطه ۷ کمک بگیرد. از آنجا که دو مجموع برابر می‌باشند، ادعا صحیح است. از تعریف ۱.۱.۲ داریم:

$$(q-1) \binom{n}{i} K_k(i) = (q-1)^k \binom{n}{k} K_i(k), \quad (9)$$

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

$$\sum_{i=0}^n K_l(i) K_i(k) = \delta_{lk} q^n. \quad (10)$$

تعدادی از چندجمله‌ای‌های کراچوک را ( $k \leq 2$ ) لیست می‌کنیم:

$$K_0(n, x) = 1,$$

$$K_1(n, x) = n(q-1) - qx, \quad (= n - 2x; q = 2 \text{ اگر})$$

$$K_2(n, x) = \frac{1}{q} \{q^2 x^2 - q(2qn - q - 2n + 2)x + (q-1)^2 n(n-1)\}, \quad (11)$$

$$(= 2x^2 - 2nx + \binom{n}{2}; q = 2 \text{ اگر})$$

در فصل ۷ به ضرایب  $x^k, x^{k-1}, x^{k-2}$  و  $x^0$  در عبارت  $K_k(x)$  نیاز داریم. اگر  $K_k(x) = \sum_{i=0}^k c_i x^i$ ، آن‌گاه در حالت  $q = 2$  داریم:

$$\begin{aligned} c_k &= (-2)^k / k!, \\ c_{k-1} &= (-2)^{k-1} n / (k-1)!, \\ c_{k-2} &= \frac{1}{q} (-2)^{k-2} \{3n^2 - 3n + 2k - 4\} / (k-2)!. \end{aligned} \quad (12)$$

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

$$(k+1)K_{k+1}(x) = \{k + (q-1)(n-k) - qx\}K_k(x) - (q-1)(n-k+1)K_{k-1}(x). \quad (13)$$

این رابطه با مشتق‌گیری از طرفین رابطه ۷ نسبت به  $z$ ، ضرب نتیجه در  $(1 + (q-1)z)(1-z)$  و مقایسه ضرایب، به آسانی ثابت می‌شود. یا حتی یک تمرین آسان‌تر، جای‌گذاری  $x$  با  $x-1$  در رابطه ۷ است که نتیجه می‌دهد:

$$K_k(z) := K_k(z-1) - (q-1)K_{k-1}(z) - K_{k-1}(z-1), \quad (14)$$

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

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

$$P(x) = \sum_{k=0}^l \alpha_k K(x), \quad (15)$$

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-داربوک<sup>۱۶</sup>

<sup>۱۶</sup>Christoffel-Darboux

می باشد.

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

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

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

خاصیت زیر یک بار دیگر از رابطه ۷ و با ضرب دوسری توانی نتیجه می شود ( $q = 2$ ). اگر  $x = 0, 1, 2, \dots, n$  آن گاه:

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

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:

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

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

### ۱.۳ نظریه ترکیبیات

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

تعریف ۱.۱.۳. فرض کنید  $S$  یک مجموعه با  $v$  عضو باشد و  $B$  یک مجموعه از زیرمجموعه‌های  $S$  (که آنها را بلوک می نامیم) باشد به طوری که:

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

(۲) برای هر  $T \subset S$  با  $|T| = t$ ، دقیقاً  $\lambda$  بلوک  $B$  موجود باشد؛ به طوری که  $T \subset B$ .

در این صورت زوج  $(S, \mathcal{B})$  یک  $t$ -طرح نامیده می‌شود (نماد  $(t - (v, k, \lambda))$ ). عناصر  $S$ ، نقاط<sup>۱۷</sup> طرح نامیده می‌شوند. اگر  $\lambda = 1$ ، آن‌گاه این طرح یک دستگاه اشتاینر<sup>۱۸</sup> نامیده می‌شود.

یک  $t$ -طرح اغلب با ماتریس وقوع<sup>۱۹</sup> خود، یعنی  $A$ ، نمایش داده می‌شود که دارای  $|B|$  سطر و  $|S|$  ستون است به طوری که سطرها توابع مشخصه‌ای از بلوک‌ها باشند.

تعریف ۲.۱.۳. هر طرح بلوکی با پارامترهای  $(v, k; b, r, \lambda)$  یک  $(v, k, \lambda) - 2$  است با  $|B| = b$ . 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  $(n^2 + n + 1, n + 1, 1) - 2$  طرح است. در این حالت، بلوک‌ها، خطوط صفحه نامیده می‌شوند. یک صفحه تصویری از مرتبه  $n$ ، با  $PG(2, n)$  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 به کار می‌بریم). یک زیرفضای آفین  $k$ -بعدی از یک  $k$ -سطح، یک هم‌مجموعه از زیرفضای خطی  $k$ -بعدی (به عنوان زیرگروه) است. اگر  $k = m - 1$ ، 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 در حالت  $m = 1$  است. هندسه تصویری با بعد  $m$  روی  $\mathbb{F}_q$  (نماد  $PG(m, q)$ )، شامل زیرفضاهای خطی  $AG(m + 1, q)$  است. زیرفضاهای با بعد ۱، نقاط نامیده می‌شوند. زیرفضاهای با بعد ۲، خطوط نامیده می‌شوند و به همین ترتیب.

در اینجا مثالی می‌آوریم.  $AG(3, 3)$  را در نظر بگیرید. ۲۷ نقطه و  $(27 - 1) / 4 = 13$  خط وجود دارند که از  $(0, 0, 0)$  می‌گذرند و ۱۳ صفحه که از  $(0, 0, 0)$  می‌گذرند. این ۱۳ خط، نقاط  $PG(2, 3)$  هستند و ۱۳ صفحه در  $AG(3, 3)$ ، خطوط هندسه تصویری هستند. روشن است که این یک طرح

<sup>۱۷</sup>points

<sup>۱۸</sup>Steiner

<sup>۱۹</sup>incidence matrix

(۱، ۴، ۱۳) - ۲ است. هنگام صحبت درباره مختصات یک نقطه در  $PG(m, q)$ ، منظور ما، مختصات هر یک از نقاط متناظر است که در  $AG(m+1, q)$  متفاوت از  $(0, 0, \dots, 0)$  می‌باشند؛ بنابراین، در مثال  $PG(2, 3)$ ، سه‌تایی‌های  $(1, 2, 1)$  و  $(2, 1, 2)$ ، مختصات نقطه یکسانی در  $PG(2, 3)$  هستند.

در فصل ۱۰، صفحه تصویری  $n$ -بعدی  $\mathbb{P}^n$  را روی میدان  $k$  در نظر می‌گیریم. یک نقطه با  $(a_0 : a_1 : \dots : a_n)$  نمایش داده خواهد شد که تمامی  $a_i$ ها هم‌زمان صفر نیستند و اگر برای یک  $c \in k$  که  $c \neq 0$  داشته باشیم  $b_i = ca_i$  برای هر  $0 \leq i \leq n$ .

تعریف ۵.۱.۳. یک ماتریس مربعی  $H$  از مرتبه  $n$  با عناصر  $+1$  و  $-1$  به طوری که  $HH^T = nI$ ، یک ماتریس هادامارد<sup>۲۰</sup> نامیده می‌شود.

تعریف ۶.۱.۳. ماتریس مربعی  $C$  از مرتبه  $n$  با اعضای  $0$  در قطر اصلی و  $+1$  و  $-1$  خارج از قطر اصلی به طوری که  $CC^T = (n-1)I$ ، یک ماتریس کنفرانس<sup>۲۱</sup> نامیده می‌شود.

چندین روش معروف برای ساخت ماتریس‌های هادامارد وجود دارد. یکی از آنها برپایه حاصل ضرب معروف کرونگر<sup>۲۲</sup> برای ماتریس‌ها می‌باشد که به صورت 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 حاصل ضرب کرونگر  $A \otimes B$  یک ماتریس  $mn \times mn$  است که به صورت زیر تعریف می‌شود:

$$A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mm}B \end{pmatrix}.$$

نشان دادن این‌که حاصل ضرب کرونگر ماتریس‌های هادامارد، مجدداً یک ماتریس هادامارد است، مشکل نمی‌باشد. با شروع از  $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  می‌توانیم دنباله  $H_{2^n}$  را بیابیم که در آن  $H_{2^n}^{\otimes 2} = H_2 \otimes H_2$  و به همین ترتیب. این ماتریس‌ها در موقعیت‌های متفاوتی از این کتاب مشاهده می‌گردند (برخی اوقات به شکل پنهان).

یکی از بهترین روش‌های ساختاری مربوط به پالی<sup>۲۳</sup> است (ر.ک. مرجع [۹۳]). فرض کنید  $q$  یک عدد فرد اول باشد. تابع  $\chi$  را بر روی  $\mathbb{F}_q$  تعریف می‌کنیم به طوری که  $\chi(0) = 0$  و  $\chi(x) = 1$  اگر  $x$  یک

<sup>۲۰</sup> Hadamard matrix

<sup>۲۱</sup> conference matrix

<sup>۲۲</sup> Kronecker product

<sup>۲۳</sup> R. E. A. C. Paley

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

قضیه ۱.۱.۳. ماتریس پالی  $S$  از مرتبه  $q$  تعریف شده به صورت  $S_{ij} := \chi(a_i - a_j)$  دارای خواص زیر است:

$$;SJ = JS = 0 \quad (۱)$$

$$;SS^T = qI - J \quad (۲)$$

$$.S^T = (-1)^{(q-1)/2} S \quad (۳)$$

ماتریس  $S$  به این صورت را در نظر گرفته و ماتریس  $C$  از مرتبه  $q+1$  را به صورت زیر تشکیل می‌دهیم:

$$C := \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ -1 & & & & \\ -1 & & S & & \\ \vdots & & & & \\ -1 & & & & \end{pmatrix}, \quad (۲۰)$$

در این صورت  $C$  یک ماتریس کنفرانس از مرتبه  $q+1$  است. اگر  $q \equiv 3 \pmod{4}$ ، 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 به طوری که تعداد متناهی از مقادیر  $x_1, x_2, \dots$  را اختیار می‌کند. به طور معمول، احتمال این که  $x$  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 به کار خواهیم بست. انحراف معیار  $\sigma$  و واریانس  $\sigma^2$  به صورت زیر تعریف می شوند:

$$\sigma^2 := \sum_i p_i x_i^2 - \mu^2 = \mathcal{E}(x - \mu)^2, \quad (\sigma > 0),$$

که در آن  $\mu = \mathcal{E}(x)$ . هم چنین به بعضی از روابط درباره توزیع های دو بعدی نیاز داریم. نمادگذاری  $p_i := P(x = x_i) = \sum_j p_{ij}$ ,  $p_{ij} := P(x = x_i \wedge y = y_j)$  و برای احتمال شرطی، نمادگذاری  $P(x = x_i | y = y_j) = p_{ij}/p_j$  را به کار می بریم. گوئیم  $x$  و  $y$  مستقل هستند اگر برای تمامی  $i$  و  $j$  داشته باشیم  $p_{ij} = p_i \cdot p_j$ . 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 می توان در کتاب های درسی استاندارد از نظریه احتمالات (برای نمونه فلر<sup>۲۴</sup> [۲۱]) یافت نمود. روابط مشابهی برای نتایج زیر برقرار خواهد بود که آنها را در فصل ۲ به کار خواهیم برد.

قضیه ۱.۱.۴. (نامساوی چیشف). فرض کنید  $x$  یک متغیر تصادفی با میانگین  $\mu$  و واریانس  $\sigma^2$  باشد؛ در این صورت برای هر  $k > 0$  داریم:

$$P(|x - \mu| \geq k\sigma) < k^{-2}.$$

توزیع احتمالی که دارای بیشترین نقش در فصل بعد خواهد بود، توزیع دوجمله ای است. در اینجا  $x$  مقادیر  $0, 1, \dots, n$  را می گیرد و  $P(x = i) = \binom{n}{i} p^i q^{n-i}$  که در آن  $0 \leq p \leq 1$  و  $q := 1 - p$ . برای این توزیع داریم  $\mu = np$  و  $\sigma^2 = np(1 - p)$ . هنگام تخمین ضرایب دوجمله ای، ابزار مهمی به کار می رود که در قضیه زیر آمده است:

قضیه ۲.۱.۴. (فرمول استرلینگ).

$$\log n! = (n - \frac{1}{2}) \log n - n + \frac{1}{2} \log(2\pi) + o(1), \quad (n \rightarrow \infty),$$

$$= n \log n - n + O(\log n), \quad (n \rightarrow \infty),$$

لم مفید دیگری که درباره ضرایب دوجمله ای است، لم زیر است.

لم ۳.۱.۴. داریم:

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

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  $q$  بزرگ‌تر از ۲ گسترش می‌دهیم. در ادامه بحث، تمامی لگاریتم‌ها در پایه ۲ هستند.

تعریف ۴.۱.۴. تابع آنتروپی دوتایی  $H$  به صورت زیر تعریف می‌شود:

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

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

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

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

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

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 این صورت  $m = \lambda n + O(1)$  برای  $n \rightarrow \infty$ ؛ بنابراین، از قضیه ۲.۱.۴ داریم:

$$\begin{aligned} n^{-1} \log \sum_{0 \leq i \leq \lambda n} \binom{n}{i} &\geq n^{-1} \log \binom{n}{m} \\ &= n^{-1} \{n \log n - m \log m - (n - m) \log(n - m) + o(n)\} \\ &= \log n - \lambda \log(\lambda n) - (1 - \lambda) \log((1 - \lambda)n) + o(1) \\ &= H(\lambda) + o(1), \quad n \rightarrow \infty \text{ که زمانی} \end{aligned}$$

□ در این صورت، حکم از قسمت (۱) به دست می آید.

توزیع احتمالی که نقش مهمی در نظریه اطلاعات ایفا می نماید، توزیع نرمال یا گوسی است. این توزیع برای توصیف انواع مشترکی از نویز بر روی کانال های مخابراتی به کار می رود. گوییم یک توزیع تصادفی پیوسته دارای توزیع گوسی با میانگین  $\mu$  و واریانس  $\sigma^2$  است؛ اگر تابع توزیع آن به صورت زیر باشد:

$$p(x) := \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right).$$

## 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 می‌آید، 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، می‌آوریم. بسیاری از خوانندگان، عکس‌های باکیفیت عالی از مریخ، زحل و سایر سیاره‌هایی که با ماهواره‌هایی همچون مارینر<sup>۱</sup>، وُیاگر<sup>۲</sup> 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 دستگاه‌های 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<sup>۳</sup> در موسسه صنعتی کالیفرنیا در شهر پاسادنا<sup>۴</sup>) منتقل می‌شوند. سیگنال رسیده

<sup>۱</sup> Mariners

<sup>۲</sup> Voyagers

<sup>۳</sup> The Jet Propulsion Laboratory

<sup>۴</sup> Pasadena

بسیار ضعیف می‌باشد و باید تقویت شود. به واسطه تاثیر نويز حرارتی، گاه‌وبی‌گاه به نظر می‌آید که سیگنالی که به‌عنوان  $\circ$  ارسال شده توسط گیرنده به ۱ تعبیر می‌شود و به‌عکس. اگر دنباله ۶ تایی از  $\circ$  و ۱ هایی که در بالا بیان کردیم، به این صورت منتقل شوند، آن‌گاه خطاهایی که توسط گیرنده رخ می‌دهد، تاثیر زیادی بر روی عکس‌ها می‌گذارد. برای جلوگیری از این خطا، چیزی به‌اسم افزونگی<sup>۵</sup> روی سیگنال اعمال می‌شود، به این معنی که دنباله منتقل شده 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. در نتیجه 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  $\circ$  و ۱ ها، یعنی اعداد صحیح از  $\circ$  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 شش تایی‌ها از  $\circ$  و ۱ در انتقال عکس (مارینر ۱۹۶۹) با رشته‌های طولانی‌تر (که آنها را همیشه کدکلمات می‌نامیم) جای‌گزین شدند. در واقع، در مارینر ۱۹۶۹، کدکلمات شامل ۳۲ سمبل بودند (ر.ک. مرجع [۵۶]). در اینجا، خواننده باید این را بپذیرد که دستگاهی باید طراحی شود تا ۶۴ رشته اطلاعاتی ممکن (۶ تایی‌ها از  $\circ$  و ۱) را به ۶۴ کدکلمه ممکن (۳۲ تایی‌ها از  $\circ$  و ۱) تغییر دهد. این دستگاه، کدکننده نامیده می‌شود. چیزهایی که انتقال می‌یابند، کدکلمات هستند. نويزها را هم تصادفی در نظر می‌گیریم؛ یعنی خطاها به پیام اضافه شده‌اند (جمع به پیمانہ ۲).

در پایان، اگر کلمه دریافتی یکی از ۶۴ کدکلمه قابل قبول نباشد، دستگاهی که کدگشا نامیده می‌شود، ۳۲ تایی دریافتی را به کدکلمه با بیشترین احتمال<sup>۶</sup> تغییر می‌دهد و پس از آن، ۶ 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

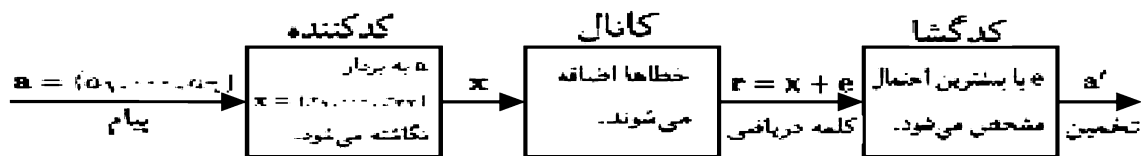
<sup>۵</sup> redundancy

<sup>۶</sup> 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،  $1/5$  برابر زمانی است که بدون کدگذاری و با احتمال خطای بالا در دسترس بود! این مثال را با جزئیات بیشتر در بخش ۲.۳ خواهیم آورد.

در عمل، این وضعیت دارای پیچیدگی بیشتری است؛ چرا که مشکل اصلی به خاطر زمان انتقال نیست که تغییر می‌کند، بلکه به خاطر میزان انرژی قابل دسترس در هر بیت انتقال یافته است.

بیشترین کاربرد عملی نظریه کدهای تصحیح‌کننده خطا، سیستم صوتی دیجیتال یک دیسک فشرده است که توسط فیلیپس<sup>۷</sup> (هلندی‌ها) اختراع شد. موفقیت این سیستم (در میان سایر سیستم‌ها) به خاطر استفاده از کدهای رید-سولومن<sup>۸</sup> بود. این کدها در بخش ۶.۸ مورد بررسی قرار می‌گیرند. شکل ۴.۶ 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 در نظر 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 در صورت ممکن از فرستنده برای ارسال مجدد درخواست می‌کند. تفاوت دیگری که ایجاد می‌شود، فرق بین کدگشایی‌های معروف به تصمیم سخت<sup>۹</sup> و تصمیم نرم<sup>۱۰</sup> می‌باشد. این تصمیم به سمبل‌های ورودی وابسته است. بیشتر آنها به سیگنالی از  $0$  و  $1$  تشبیه می‌گردند که دریافت کننده هیچ شکی نداشته باشد. اما در سایر حالات، این مطلب درست نخواهد بود و می‌توانیم قرار دادن یک  $?$  را به جای تصمیم‌گیری درباره این که آیا سمبل ورودی  $0$  بوده یا  $1$ ، ترجیح دهیم. این

<sup>۷</sup> Philips

<sup>۸</sup> Reed Solomon

<sup>۹</sup> hard decision

<sup>۱۰</sup> soft decision

مطلب اغلب به عنوان یک پاک‌شدگی<sup>۱۱</sup> تعبیر می‌شود. سیستم‌های پیچیده‌تر، یک احتمال را به این سمبل الحاق می‌کنند.

## مقدمه‌ای بر قضیه شانون

به منظور حصول ایده بهتری درباره اصل نظریه کدگذاری، آزمایش خیالی زیر را در نظر 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  $0$  و  $1$  می‌نامیم. این کانال، نویزدار است و تاثیر آن به این صورت است که  $0$  (یا  $1$ ) فرستاده شده با احتمال  $p$  توسط گیرنده به عنوان  $1$  (یا  $0$ ) تفسیر می‌شود. چنین کانالی یک کانال دوتایی متقارن (B.S.C.) نامیده می‌شود. علاوه بر آن 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  $0$  را انتقال می‌دهیم و اگر خط بیاید،  $1$  را انتقال می‌دهیم. در پایان انتقال، گیرنده به اندازه 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. به جای  $0$  (یا  $1$ )،  $N$  تا  $0$  (یا  $1$ ) را انتقال می‌دهیم. گیرنده  $N$  تایی دریافتی را در نظر 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  $0 = (0, 0, \dots, 0)$  و  $1 = (1, 1, \dots, 1)$  است. به عنوان نمونه فرض کنیم  $p = 0.001$ ؛ در این صورت احتمال این که کدگشا دچار اشتباه شود، به صورت زیر است:

$$\sum_{0 \leq k \leq N/2} \binom{N}{k} q^k p^{N-k} < (0.007)^N, \quad (q := 1 - p) \quad (1)$$

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

به خاطر وجود محدودیت زمانی، یک مشکل جدی داریم! برای هر پرتاب سکه، تنها دو سمبل را می‌توانیم انتقال دهیم. در ارسال دوبار هر سمبل به جای یک بار هم هیچ نکته خاصی وجود ندارد. برجسته‌ترین قضیه در این مورد توسط شانون<sup>۱۲</sup> (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

<sup>۱۱</sup>erasure

<sup>۱۲</sup>C.E.Shannon

درباره روش اثبات می‌تواند به صورت زیر به دست آید. نتیجه دوبار پرتاب یک سکه را به صورت زیر انتقال می‌دهیم:

$$\begin{aligned} & \rightarrow 0000, \text{ شیر، شیر} \\ & \rightarrow 0111, \text{ خط، شیر} \\ & \rightarrow 1001, \text{ شیر، خط} \\ & \rightarrow 1110, \text{ خط، خط} \end{aligned}$$

مشاهده کنید که اولین دو سمبل ارسالی، اطلاعات واقعی را حمل می‌کنند؛ دو سمبل آخر اضافی هستند. کدگشا، الگوریتم کدگشایی کامل زیر را به کار می‌برد. اگر ۴ تایی دریافتی یکی از کدکلمه‌های بالا نباشد، آن‌گاه فرض کنید چهارمین سمبل درست است و این که یکی از سه سمبل اولیه نادرست است. اگر فرض بالا درست باشد، آن‌گاه هر ۴ تایی دریافتی می‌تواند به طور یکتا و صحیح کدگشایی گردد. بدون کدگذاری، احتمال این که دو سمبل به طور صحیح دریافت شده باشند، برابر با  $q^2 = 0.998$  است. توسط کدی که در بالا توصیف شد، این احتمال برابر با  $q^4 + 3q^2p = 0.999$  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 به وسیله انتقال نتایج پرتاب سکه به کار رفت، به سه پرتاب در یک لحظه گسترش می‌دهیم. در این صورت اطلاعاتی که قصد انتقال آن را داریم به صورت سه تایی از ۰ و ۱، که آن را  $(a_1, a_2, a_3)$  می‌نامیم، می‌باشد. به جای این ۳ تایی، ما ۶ تایی  $a = (a_1, \dots, a_6)$  را انتقال می‌دهیم که در آن  $a_4 := a_2 + a_3$ ,  $a_5 := a_1 + a_3$ ,  $a_6 := a_1 + a_2$  (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 به عنوان چیزی که به پیام اضافه می‌شود در نظر می‌گیریم؛ یعنی کلمه دریافتی  $b$  به صورت  $a + e$  است که در آن  $e = (e_1, e_2, \dots, e_6)$  الگوی خطا (بردار خطا) نامیده می‌شود؛ داریم:

$$e_2 + e_3 + e_4 = b_2 + b_3 + b_4 := s_1,$$

$$e_1 + e_3 + e_5 = b_1 + b_3 + b_5 := s_2,$$

$$e_1 + e_2 + e_6 = b_1 + b_2 + b_6 := s_3,$$

از آنجا که گیرنده  $b$  را می‌شناسد، او  $s_1, s_2, s_3$  را می‌شناسد. با فرض  $s_1, s_2, s_3$ ، کدگشا باید الگوی خطای  $e$  با بیشترین درست‌نمایی را به گونه‌ای انتخاب نماید که در این سه معادله صدق کند. بیشترین درست‌نمایی را آنی دارد که دارای کمترین سمبل ۱ باشد. می‌توان به آسانی مشاهده نمود که اگر  $(s_1, s_2, s_3) \neq (1, 1, 1)$ ، آن‌گاه انتخاب یکتایی برای  $e$  وجود دارد. اگر  $(s_1, s_2, s_3) = (1, 1, 1)$ ، آن‌گاه کدگشا باید یکی از سه احتمال  $(1, 0, 0, 1, 0, 0)$ ،  $(0, 1, 0, 0, 1, 0)$  و  $(0, 0, 1, 0, 0, 1)$  را برای  $e$

داشته باشد. می بینیم که اگر الگوی خطا دارای یک خطا باشد، به طور صحیح کدگشایی می شود و در میان سایر الگوهای خطا هم، الگویی با دو خطا وجود دارد که به طور صحیح کدگشایی می گردد؛ بنابراین، پس از فرایند کدگشایی، احتمال این که تمامی سه سمبل  $a_1, a_2, a_3$  به طور صحیح تفسیر شوند، برابر است با:

$$q^1 + 6q^5p + q^4p^2 = 0.999986.$$

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، آن گاه:

$$R := n^{-1} \log |c|$$

نرخ اطلاعاتی (یا فقط نرخ) کد نامیده می شود.

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  $\frac{7}{8}$  می باشد. مارینر ۱۳۶۹ از کدی با نرخ  $\frac{7}{33}$  استفاده نموده است. مثالی که قبل از تعریف نرخ آمد، دارای نرخ  $R = \frac{1}{3}$  است.

یادآوری می کنیم که کدی که توسط مارینر ۱۹۶۹ به کار رفت دارای این خاصیت بود که گیرنده قادر به تصحیح تا هفت خطا در کلمه دریافتی است. دلیل این که 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 می شود:

تعریف ۲.۲.۱. اگر  $x$  و  $y$  دو  $n$  تایی از  $0$  و  $1$  باشند، آن گاه گوئیم فاصله همینگ آنها (معمولاً فقط فاصله) برابر است با:

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

(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 می باشند. به همین خاطر است که هر الگوی خطا با یک خطا، می تواند تصحیح شود. این کد، یک کد تصحیح کننده خطای واحد است.

توصیف ما از قوانین کدگشایی، بر پایه دو فرض می باشد. اولین آنها این است که در زمان مخابره، تمامی کدکلمات دارای احتمال یکسان باشند. علاوه بر آن از این واقعیت استفاده نموده ایم که اگر  $n_1 > n_2$ ، آن گاه یک الگوی خطا با  $n_1$  خطا دارای احتمال کمتری از یک الگو با  $n_2$  خطا است.

معنای آن این است که اگر  $y$  دریافت شده باشد، آن گاه سعی می‌کنیم تا کدکلمه  $x$  را بیابیم به طوری که  $d(x, y)$  کمترین باشد. این اصل، قاعده کدگشایی با بیشترین درست‌نمایی<sup>۱۳</sup> 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  $q = 1 - p$ ). فرض کنید کد  $C$  شامل  $M$  کدکلمه به طول  $n$  را به کار می‌بریم؛ به طوری که هر کلمه با احتمال یکسان رخ داده است. اگر  $x_1, x_2, \dots, x_M$  کدکلمات باشند و از قاعده کدگشایی با بیشترین درست‌نمایی استفاده کنیم، آن گاه فرض کنید  $P_i$  احتمال تصمیم نادرست به شرط انتقال  $x_i$  باشد. در این حالت احتمال کدگشایی نادرست کلمه دریافتی برابر است با:

$$P_C := M^{-1} \sum_{i=1}^M P_i. \quad (2)$$

حال تمامی کدهای ممکن  $C$  با پارامترهای داده شده را در نظر بگیرید و تعریف کنید:

$$P^*(M, n, p) := P_C \text{ مقدار کمترین مقدار.} \quad (3)$$

قضیه ۱.۲.۲. (شانون ۱۹۴۸). اگر  $0 < R < 1 + p \log p + q \log q$  و  $M_n := 2^{\lfloor Rn \rfloor}$ ، آن گاه  $P^*(M_n, n, p) \rightarrow 0$  زمانی که  $n \rightarrow \infty$ .

(در اینجا تمامی لگاریتم‌ها در پایه ۲ است). توجه می‌کنیم که در مثال بخش قبل داشتیم  $p = 0.001$  که در این حالت  $1 + p \log p + q \log q$  نزدیک به ۱ است. در عمل، شرط ما این بود که نرخ باید حداقل  $\frac{1}{4}$  باشد. اما می‌بینیم که برای  $\varepsilon > 0$  و  $n$  به قدر کافی بزرگ، کد  $C$  با طول  $n$  و نرخ نزدیک به ۱ وجود دارد به طوری که  $P_C < \varepsilon$ . (البته اگر  $T$  به اندازه کافی کوچک باشد، آن گاه کدهای طولانی نمی‌توانند به کار روند).

قبل از آوردن اثبات قضیه ۱.۲.۲ درباره برخی از جزئیات 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.

<sup>۱۳</sup> maximum-likelihood-decoding



تعداد خطاها در یک کلمه دریافتی، یک متغیر تصادفی با مقدار میانگین  $np$  و واریانس  $np(1-p)$  می‌باشد. اگر  $b := (np(1-p)/(\varepsilon/2))^{1/2}$ ، آن‌گاه از نامساوی چیشف (قضیه ۱.۱.۴) داریم:

$$P(w > np + b) \leq \frac{1}{4}\varepsilon. \quad (۴)$$

از آنجا که  $p < \frac{1}{4}$ ، برای  $n$  به قدر کافی بزرگ، عدد  $\rho := \lfloor np + b \rfloor$  کمتر از  $\frac{1}{4}n$  می‌شود. فرض کنید  $B_\rho(x)$  مجموعه کلمات  $y$  با شرط  $d(x, y) \leq \rho$  باشد؛ در این صورت:

$$B_\rho(x) = \sum_{i \leq \rho} \binom{n}{i} < \frac{1}{4}n \binom{n}{\rho} \leq n \cdot \frac{n^n}{\rho^\rho (n-\rho)^{n-\rho}} e \quad (۵)$$

(ارجاع به لم ۳.۱.۴). مجموعه  $B_\rho(x)$  معمولاً گوی به شعاع  $\rho$  و مرکز  $x$  (اگرچه اصطلاح توپ<sup>۱۴</sup> مناسب‌تر به نظر می‌آید) نامیده می‌شود.

تخمین‌های زیر را به کار خواهیم برد:

$$\frac{\rho}{n} \log \frac{\rho}{n} = \frac{1}{n} \lfloor np + b \rfloor \log \frac{\lfloor np + b \rfloor}{n} = p \log p + O(n^{-1/2}), \quad (۶)$$

$$\left(1 - \frac{\rho}{n}\right) \log \left(1 - \frac{\rho}{n}\right) = q \log q + O(n^{-1/2}), \quad (n \rightarrow \infty),$$

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

$$u \in \{0, 1\}^n, v \in \{0, 1\}^n.$$

در این صورت:

$$f(u, v) := \begin{cases} 0, & \text{اگر } d(u, v) > \rho \\ 1, & \text{اگر } d(u, v) \leq \rho \end{cases} \quad (۷)$$

اگر  $x_i \in C$  و  $y \in \{0, 1\}^n$ ، آن‌گاه:

$$g_i(y) := 1 - f(y, x_i) + \sum_{j \neq i} f(y, x_j). \quad (۸)$$

دقت می‌کنید اگر  $x_i$  تنها کدکلمه‌ای باشد که  $d(x_i, y) \leq \rho$ ، آن‌گاه  $g_i(y) = 0$  و در غیر این صورت  $g_i(y) \geq 1$ .

<sup>۱۴</sup>ball

اثبات قضیه ۱.۲.۲. در اثبات قضیه شانون، کدکلمات  $x_1, x_2, \dots, x_M$  را به طور تصادفی (مستقل) برمی‌گزینیم. به صورت زیر کدگشایی می‌کنیم. اگر  $y$  دریافت شود و اگر دقیقاً یک کدکلمه  $x_i$  موجود باشد به طوری که  $d(x_i, y) \leq \rho$  آن‌گاه  $y$  را به  $x_i$  کدگشایی می‌کنیم. در غیر این صورت وقوع یک خطا را اعلام می‌کنیم (یا اگر مجبور به کدگشایی گردیم، آن‌گاه همیشه به  $x_1$  کدگشایی می‌کنیم). فرض کنید  $P_i$  به صورت بالا تعریف شده باشد؛ داریم:

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

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  $\frac{1}{q}\varepsilon$  می‌باشد. بنابراین، داریم:

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

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 به طور تصادفی انتخاب شده‌اند؛ بنابراین، داریم:

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

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

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

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

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

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

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<sup>۱۵</sup> بیان می‌شود که در اینجا آن را تعریف می‌کنیم (جزئیات 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  $1$  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  $\sigma^2$  پیروی می‌کند. یک گیرنده، با تصمیم‌های سخت، هر سیگنال ارسالی با دامنه  $r$  را با آستانه  $0$  مقایسه می‌کند و اگر  $r > 0$ ، تصمیم به  $1$  می‌گیرد و در غیر این صورت تصمیم به  $0$  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:

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

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  $E_b/\sigma^2$ ، نسبت سیگنال به نویز (SNR) نامیده می‌شود.

اگر کد  $C$  را به‌کار ببریم که  $k$  بیت را بر روی  $n$  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 بفروستیم تا به سرعت موردنیاز، ارسال  $B$  بیت در هر ثانیه، برسیم. به‌خاطر این که توان دارای محدودیت  $W$  وات است، تنها به‌اندازه  $E' := W/(B/R) = R \cdot E_b$  ژول

<sup>۱۵</sup>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) به صورت:

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

به دست می‌آید.

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

بیابید مجدداً به مارینر ۶۹/نگاهی دقیق‌تر بیندازیم. به جای نامیدن سمبل‌های ارسالی با ۰ و ۱، آنها را با ۱ و -۱ نشان دهیم. ۶۴ دنباله به طول ۳۲ که مارینر به کار برد سطرهای ماتریس‌های  $H_4^{\otimes 5}$  و  $H_4^{\otimes 5} - H_4^{\otimes 5}$  از بخش ۱.۳ بودند. برای یک سیگنال دریافتی (با تصمیم‌های سخت)، سطر دریافتی شامل ۳۲ سمبل  $\pm 1$  برداشته شد و ضرب داخلی این سطر و سطر ۳۲  $H_4^{\otimes 5}$  محاسبه گردید. اگر خطایی رخ نمی‌داد، ۳۱ تا از این حاصل ضرب‌ها ۰ بودند و یکی برابر با  $\pm 32$  که نشان‌دهنده این است که سیگنال دریافتی درست بوده است. در حالت یک خطا، حاصل ضرب‌های داخلی  $\pm 2$  بودند، با یک استثنای  $\pm 30$ ، 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 بیابید به تاثیر کدگذاری نگاهی کنیم.

مثال ۱.۲.۳. مثال کد مارینر را در نظر 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  $10^{-4}/6 \approx 10^{-4} \approx Q(\sqrt{17.22})$  و  $P_E = 1 - (1 - p_e)^6 \approx 10^{-4}$ .

سپس، فرض کنید که از کد [۳۲، ۶] 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 خطا 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  $H_0^{\otimes 5}$  مرتبط می‌شود. در این حالت، احتمال این که سیگنالی که ما به عنوان شبیه‌ترین سیگنال انتخاب نموده‌ایم، در واقع همان سیگنال ارسالی باشد، بیشتر است.

خاطر نشان می‌کنیم که اگر تصمیم نرم را در مثال ۱.۲.۳ به کار برده بودیم، آنگاه احتمال خطا به  $10^{-11} \times 2$  کاهش یافته بود.

روش دیگری برای نگاه به مساله در این حالت وجود دارد. می‌توانیم کدگذاری را برای نیاز به انرژی کمتر<sup>۱۶</sup> به کار ببریم. ممکن است  $C$  را نه برای کاهش نرخ خطا، بلکه برای کاهش SNR لازم، انتخاب نماییم.

در مثال مارینر، احتمال  $10^{-4}$  را برای دریافت یک ۶ تایی غلط داشتیم. برای رسیدن به  $P'_E = 10^{-4}$ ، 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 به اندازه ۱۵ درصد را می‌دهد. به وسیله 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. وقتی که احتمال خطا را ثابت فرض کرده‌ایم، نسبت بین SNR (کد نشده) و SNR' (کد شده) 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 به عنوان یک بهره کدگذاری با اندازه ۰.۶۵dB 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 پردازیم.

## ۲.۴ پیشنهادها

مقاله شانون با عنوان تئوری ریاضی مخابرات (۱۹۴۸) [۶۲] نشان از آغاز نظریه کدگذاری دارد. از آنجا که این قضیه نشان می‌دهد کدهای خوب وجود دارند، طبیعی بود که هر کسی تلاشی را بر ساختن این

<sup>۱۶</sup>need less energy

کدها آغاز نماید. چون این کدها اغلب برای پشتیبانی دستگاه‌های الکتریکی خیلی کوچک به کار می‌رود، محققان به خصوص به کدهایی با ساختارهای زیاد علاقه‌مند بودند که الگوریتم‌های کدگشایی نسبتاً ساده‌ای داشته باشند. در فصل‌های بعد، خواهیم دید که به دست 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<sup>۱۷</sup> هستند. علاوه بر شانون، افرادی مانند برلیکمپ<sup>۱۸</sup>، گیلبرت<sup>۱۹</sup>، همینگ<sup>۲۰</sup>، لوید<sup>۲۱</sup>، مک‌ویلیامز<sup>۲۲</sup>، اسلیپان<sup>۲۳</sup> و اسلون<sup>۲۴</sup> را ذکر می‌کنیم. این مطلب تعجب برانگیز نیست که بسیاری از متون درباره نظریه کدگذاری در ژورنال علمی آزمایشگاه بل<sup>۲۵</sup> می‌تواند یافت شود. نویسنده به طور عمیق اعتراف می‌کند که بسیاری از دانش او در زمینه کدگذاری در خلال ملاقات وسیع او با آزمایشگاه‌های بل بوده است. خواننده‌ای که به جزئیات بیشتر درباره کد به کار 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.

<sup>۱۷</sup>Bell Telephone Laboratories

<sup>۱۸</sup>Berlekamp

<sup>۱۹</sup>Gilbert

<sup>۲۰</sup>Hamming

<sup>۲۱</sup>Lloyd

<sup>۲۲</sup>MacWilliams

<sup>۲۳</sup>Slepian

<sup>۲۴</sup>Sloan

<sup>۲۵</sup>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، در نظر بگیرید. نشان دادیم که احتمال آن که کلمه دریافتی به طور صحیح کدگشایی شده باشد برابر با  $q^6 + 6q^5p + q^4p^2$  است. حال فرض کنید که پس از کدگشایی، تنها سه سمبل اول از هر کلمه کدگشایی شده را حفظ کرده ایم؛ 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<sup>۲۶</sup> می نامیم 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 به طور صحیح کدگشایی شده باشد، تعیین کنید.

۴.۲.۵. در یک کانال دوتایی با احتمال  $q = 0.9$  سمبل انتقال یافته به طور صحیح دریافت شده و با احتمال  $p = 0.1$  پاک شده است (یعنی ما؟ دریافت می کنیم). در این کانال می خواهیم کدی با نرخ  $\frac{1}{4}$  را به کار ببریم. آیا اگر ما هر سمبل انتقال را تکرار نماییم، احتمال تفسیر صحیح افزایش می یابد؟ آیا ممکن است کدی با هشت کلمه به طول ۶ را بسازیم به طوری که دو سمبل پاک شده قابل بازیابی باشند؟ احتمال های تفسیر صحیح این دو کد را بیابید (فرض کنید که دریافت کننده سمبل های پاک شده را با حدس یک سمبل تغییر ندهد).

۵.۲.۵. مثال ماریئر ۱۹۶۹ را در نظر بگیرید. فرض کنید یک سطر از ۳۲ سمبل با  $e_1$  خطا و  $e_2$  سمبل پاک شده دریافت شده است. نشان دهید که اگر  $2e_1 + e_2 < 16$ ، آن گاه سطر درست قابل بازیابی است.

۶.۲.۵. فرض کنید  $C$  یک کد دوتایی با طول ۱۶ باشد به طوری که:

الف. هر کدکلمه دارای وزن ۶ است.

ب. هر دو کدکلمه متمایز دارای فاصله ۸ هستند.

نشان دهید  $|c| \leq 16$ . آیا چنین کدی با  $|c| = 16$  موجود است؟

<sup>۲۶</sup>symbol error probability

۷.۲.۵. فرض کنید  $C$  یک کد باینری تصحیح‌کننده خطای واحد با طول زوج  $n$  باشد. نشان دهید

$$|c| \leq 2^n / (n + 2).$$

راهنمایی: تعداد زوج‌های  $(x, c)$  را بشمارید که  $x$  یک کلمه با طول  $n$  است،  $c \in C$  و  $x$  و  $c$  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 به طور خلاصه درباره یک مجموعه کاملاً متفاوت، به نام کدهای کانولوشن، بحث می‌کنیم که در آنجا یک دنباله نامتناهی از سمبل‌های اطلاعاتی  $i_0, i_1, i_2, \dots$  به دنباله نامتناهی از سمبل‌های پیام، کد شده است؛ برای مثال، برای نرخ  $\frac{1}{2}$  ممکن است داشته باشیم  $i_0, i'_0, i_1, i'_1, \dots \rightarrow i_0, i_1, i_2, \dots$  که در آن  $i'_n$  تابعی از  $i_0, i_1, \dots, i_n$  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:

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

وزن  $w(x)$ ،  $x$  به صورت:

$$w(x) := d(x, \circ)$$

تعریف می‌شود (همواره  $(0, 0, \dots, 0)$  را با  $0$  و  $(1, 1, \dots, 1)$  را با  $1$  نمایش می‌دهیم).

فاصله کد، تعریف شده توسط ۱.۳.۱، فاصله همینگ<sup>۱</sup> 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  $q - 1$  سمبل باقی‌مانده باشد، در این صورت 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  $|c| = 1$ ، کد را بدیهی می‌نامیم. اگر  $q = 2$ ، کد را یک کد دوتایی می‌نامیم، برای  $q = 3$ ، 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:

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

هم‌چنین مفهوم نرخ کد را به صورت زیر تعمیم می‌دهیم.

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

$$R := n^{-1} \log_q |C|$$

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:

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

<sup>۱</sup> Hamming distance

به خواننده یادآوری می‌کنیم که در فصل ۲، گوی  $B_\rho(x)$  با شعاع  $\rho$  و مرکز  $x$  به صورت مجموعه  $\{y \in Q^n \mid d(x, y) \leq \rho\}$  معرفی شد. اگر  $\rho$  بزرگ‌ترین عدد صحیح باشد به طوری که گوی‌های  $B_\rho(c)$  با  $c \in C$  مجزا باشند، آنگاه  $d = 2\rho + 1$  یا  $d = 2\rho + 2$ . شعاع پوششی برابر با کوچک‌ترین  $\rho$  ای است به طوری که گوی‌های  $B_\rho(c)$  که  $c \in C$ ، 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  $2e + 1$ ، کد کامل نامیده می‌شود، اگر هر  $x \in Q^n$  دارای فاصله کمتری مساوی  $e$  با دقیقاً یک کد کلمه باشد.

این واقعیت که کمترین-فاصله برابر با  $2e + 1$  است به این معناست که این کد تصحیح‌کننده  $e$ -خطاست. مطلب زیر واضح است:

### ۶.۳.۱. شرط گوی-پوششی<sup>۲</sup>

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

$$|c| \sum_{i=0}^e \binom{n}{i} (q-1)^i = q^n.$$

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  $Q^n$  به عنوان 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).

<sup>۲</sup> Sphere-packing

تعریف ۱.۳.۲. یک کد خطی  $q$ -تایی، یک زیرفضای  $\mathbb{F}_q^n$  است. اگر  $C$  دارای بعد  $k$  باشد، آن گاه  $C$  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، آن گاه  $C = \{aG \mid a \in \mathbb{F}_q^k\}$ .  $G$  را فرم استاندارد (اغلب فرم پلکانی کاهش‌یافته) خواهیم گفت، اگر  $G = (I_k \ P)$ ، که  $I_k$  ماتریس همانی  $k$  در  $k$  می‌باشد. کد  $(6, 4, 3)$  که در مثال بخش ۲.۱ به‌کار بردیم، یک کد خطی با ماتریس مولد  $G = (I \ J - I)$  است. اگر  $G$  به فرم استاندارد باشد، آن گاه  $k$  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 به‌کاررفته در رابط صفحه کلید  $PC$  که در مقدمه بیان شد، دارای یک بیت بررسی‌توازن (متناسب با این نام) و ماتریس مولد:

$$G = (I_7 \ 1^7)$$

است. تا آنجا که قدرت تصحیح خطا اهمیت دارد، دو کد  $C_1$  و  $C_2$  به‌طور یکسان خوب می‌باشند، اگر  $C_2$  با به‌کارگیری یک جای‌گشت ثابت از مکان‌های کد  $C_1$  به‌دست آمده باشد. چنین کدهایی را هم‌ارز می‌نامیم. برخی اوقات، تعریف هم‌ارزی 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، هم‌ارز 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<sup>۳</sup> نیز می‌نامند. از تعریف ۳.۳.۱، یک کد  $[n, k]$  دارای نرخ  $k/n$  است و این در تطابق با

<sup>۳</sup> separable

این واقعیت است که  $k$  تا از این  $n$  سمبل، اطلاعات را حمل می‌کنند. خواننده باید بررسی نماید که کد  $[6, 3, 3]$  به‌کاررفته 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  $d = 2e + 1$  باشد، آن‌گاه تا  $e$  خطا را در کلمه دریافتی تصحیح می‌کند. اگر  $d = 2e$ ، 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  $\binom{n}{2}$  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.  $d(x, y) = d(x - y, \circ) = w(x - y)$  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:

$$C^\perp := \{y \in \mathcal{R} \mid \forall x \in C [ \langle x, y \rangle = 0 ]\},$$

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  $C^\perp$  می‌تواند دارای اشتراکی بزرگ‌تر از  $\{0\}$  باشند و در واقع آنها حتی می‌توانند برابر باشند. اگر  $C = C^\perp$ ، آن‌گاه  $C$  یک کد خوددوگان نامیده می‌شود.

اگر  $G = (I_k \ P)$  ماتریس مولد در فرم استاندارد برای کد  $C$  باشد، آن‌گاه  $H = (-P^T \ I_{n-k})$  ماتریس مولد  $C^\perp$  می‌باشد. این مطلب از این واقعیت نتیجه می‌شود که  $H$  دارای طول و بعد  $C^\perp$  است و این‌که  $GH^T = 0$  ایجاب می‌کند که ضرب داخلی هر کدکلمه  $aG$  با هر سطر  $H$  برابر با صفر است؛ به بیان دیگر، داریم:

$$x \in C \Leftrightarrow xH^T = 0 \quad (1)$$

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

اگر  $y \in C^\perp$ ، آن‌گاه معادله  $\langle x, y \rangle = 0$  که برای هر  $x \in C$  برقرار است، یک (معادله) بررسی‌توازن و  $H$  ماتریس بررسی‌توازن  $C$  نامیده می‌شود. در مورد کد  $[6, 3]$  به‌کاررفته در بخش ۲.۱، معادله  $a_4 = a_2 + a_3$  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 بررسی توازن  $H$  باشد، آن گاه برای هر  $x \in Q^n$  مقدار  $xH^T$  را همرفت<sup>۴</sup>  $x$  می‌نامیم. مشاهده می‌نمایید که شعاع پوششی  $\rho(C)$  از کد  $[n, k]$  (ارجاع به تعریف (۴.۳.۱)، کوچک‌ترین عدد صحیح  $\rho$  است به طوری که هر بردار (ستونی) در  $Q^{n-k}$  را بتوان به صورت مجموع حداکثر  $\rho$  ستون از  $H$  نوشت.

در رابطه ۱ می‌بینیم که تنها کدکلمات هستند که دارای همرفت<sup>۵</sup> می‌باشند. همرفت در کدگشایی بردار دریافتی  $x$  یکی از مهم‌ترین ابزار کمکی است. قبلاً هم این ایده با به‌کارگیری کد  $[6, 3]$  معرفی شده بود. چون  $C$  زیرگروهی از  $Q^n$  است، می‌توانیم  $Q^n$  را به هم مجموعه‌های  $C$  افراز نماییم. دو بردار  $x$  و  $y$  در هم مجموعه 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 به طوری که  $e$  الگوی خطا باشد، آن گاه  $x$  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 هم مجموعه شامل  $x$  باید انتخاب نمود و سپس  $x$  را به صورت  $x - e$  کدگشایی کرد. بردار  $e$  را سردسته<sup>۵</sup> می‌نامیم. نحوه انجام این کار در عمل، در بخش ۲.۱ برای کد  $[6, 3]$  تشریح شد. برای هفت تا از هشت هم مجموعه، یک سردسته یکتا وجود داشت. تنها برای همرفت  $(s_1, s_2, s_3) = (1, 1, 1)$  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، آن گاه 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  $d = 2e + 1$  باشد، آن گاه هر الگوی خطا با وزن حداکثر  $e$ ، سردسته یکتایی از یک هم مجموعه است؛ چرا که دو بردار با وزن حداکثر  $e$  دارای فاصله حداکثر  $2e$  هستند؛ بنابراین، در هم مجموعه‌های متفاوتی هستند. اگر  $C$  کامل باشد، آن گاه سردسته دیگری وجود ندارد. اگر کد  $C$  دارای کمترین-فاصله  $2e + 1$  باشد و تمامی سردسته‌ها دارای وزن حداکثر  $e + 1$  باشند، آن گاه این کد شبه‌کامل نامیده می‌شود. کد  $[6, 3]$  از بخش ۲.۱ یک مثال از این دست است. شعاع پوششی برابر با وزن سردسته یک هم مجموعه با وزن ماکسیمم است.

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

<sup>۴</sup> syndrome

<sup>۵</sup> coset leader

یک کد  $[2k, k]$  خوددوگان دوتایی با ماتریس مولد  $G = (I_k \ P)$  باشد. اگر  $C$  بتواند ۳ خطا را تصحیح نماید و احتمال این که بیشتر از ۳ خطا در یک بردار دریافتی رخ دهد، خیلی کوچک باشد، آن گاه الگوریتم کدگشایی زیر، مفید خواهد بود.

ماتریس بررسی توازن را به صورت  $H = (P^T \ I_k)$  به دست می آوریم. اما  $G$  نیز یک ماتریس بررسی توازن است؛ چرا که  $C$  خوددوگان است. فرض کنید  $y = c + e$  بردار دریافتی باشد.  $e$  را به صورت  $(e_1; e_2)$  می نویسیم که در آن  $e_1$  متناظر با  $k$  مکان اول است و  $e_2$  متناظر با  $k$  مکان آخر. دو همرفت زیر را محاسبه می کنیم:

$$s^{(1)} := yH^T = e_1P + e_2,$$

$$s^{(2)} := yG^T = e_1 + e_2P^T.$$

اگر  $t \leq 3$  خطا همگی در نیمه ابتدایی یا انتهایی  $y$ ، یعنی  $e_1 = 0$  یا  $e_2 = 0$  رخ دهند، آن گاه یکی از همرفت‌ها دارای وزن  $3 \geq$  است و ما فوری  $e$  را به دست می آوریم. اگر این حالت اتفاق نیفتد، آن گاه فرض  $t \leq 3$  ایجاب می کند که  $e_1$  یا  $e_2$  دارای وزن ۱ باشد.  $2k$  بردار  $y^{(i)}$  حاصل از تغییر  $i$  امین مختصات  $y$  ( $1 \leq i \leq 2k$ ) را در نظر می گیریم. برای هر یک از این بردارها  $s_1$  (برای  $i \leq k$ ) و  $s_2$  (برای  $i > k$ ) را به ترتیب محاسبه می کنیم. اگر ما همرفت با وزن  $2 \geq$  را بیابیم، می توانیم خطاهای باقی مانده را تصحیح کنیم. اگر ما همرفتی با وزن ۳ را بیابیم، چهار خطا را تشخیص داده ایم، اگر  $C$  یک کد با فاصله ۸ باشد و اگر  $C$  دارای فاصله  $10 \leq$  باشد، آن گاه می توانیم این الگوی چهار خطا را هم تصحیح کنیم.

اغلب ثابت می شود که الحاق یک بیت اضافی، مطابق برخی قواعد طبیعی، به هر کد کلمه از کد  $C$ ، مفید خواهد بود. متعارف ترین اینها در تعریف زیر داده شده است.

تعریف ۶.۳.۲. اگر  $C$  یک کد با طول  $n$  روی الفبای  $\mathbb{F}_q$  باشد، آن گاه کد توسعه  $\bar{C}$  به صورت زیر تعریف می شود:

$$\bar{C} := \{(c_1, c_2, \dots, c_n, c_{n+1}) \mid (c_1, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}.$$

اگر  $C$  یک کد خطی با ماتریس مولد  $G$  و ماتریس بررسی توازن  $H$  باشد، آن گاه  $\bar{C}$  دارای ماتریس مولد  $\bar{G}$  و ماتریس بررسی توازن  $\bar{H}$  است که در آن  $\bar{G}$  با اضافه نمودن یک ستون به  $G$  به دست آمده است،

به طوری که مجموع ستون‌های  $\bar{G}$  برابر با  $\circ$  گردد و

$$\bar{H} := \begin{pmatrix} 1 & 1 & 1 & 1 \\ & & H & \circ \\ & & & \circ \\ & & & \vdots \\ & & & \circ \end{pmatrix}.$$

اگر  $C$  یک کد دوتایی با کمترین فاصله فرد  $d$  باشد، آن‌گاه  $\bar{C}$  دارای کمترین فاصله  $d + 1$  است؛ زیرا تمامی وزن‌ها و فاصله‌ها برای  $\bar{C}$  زوج هستند.

### ۳.۳ کدهای همینگ

فرض کنید  $G$  ماتریس مولد  $k$  در  $n$  از یک کد خطی  $[n, k]$  روی  $\mathbb{F}_q$  باشد. اگر هر دو ستون  $G$  مستقل خطی باشند؛ یعنی ستون‌ها متناظر با نقاط متمایز  $PG(k-1, q)$  باشند، آن‌گاه  $C$  یک کد تصویری<sup>۱</sup> نامیده می‌شود. کد دوگان  $C^\perp$  دارای ماتریس بررسی توازن  $G$  است. اگر  $c \in C^\perp$  و  $e$  بردار خطا با وزن ۱ باشد، آن‌گاه هم‌رفت  $G^T(c+e)$  مضربی از یک ستون  $G$  می‌باشد. چون این مقدار به طور 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  $n := (q^k - 1)/(q - 1)$ . کد همینگ  $[n, n - k]$  روی  $\mathbb{F}_q$  کدی است که ستون‌های ماتریس بررسی توازن آن دو به دو مستقل خطی (روی  $\mathbb{F}_q$ ) می‌باشند؛ یعنی ستون‌ها یک مجموعه ماکسیمال از بردارهای مستقل خطی هستند. در اینجا، به وضوح 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  $n = (q^k - 1)/(q - 1)$ . اگر  $x \in C$ ، آن‌گاه:

$$B_1(x) = 1 + n(q - 1) = q^k.$$

<sup>۱</sup> projective code



بنابراین، 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 ۶.۳.۱).

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

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

اگر ما دو ستون از  $H$  و مجموع این دو (برای مثال سه ستون اول  $H$ ) را در نظر بگیریم، آن گاه یک کلمه با وزن ۳ در  $C$  با ۱ هایی در مکان‌های متناظر با این ستون‌ها (برای مثال (۱۱۱۰۰۰)) موجود است؛ بنابراین،  $C$  دارای هفت کلمه به وزن ۳ است به طوری که وقتی به عنوان 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 گسترش یافته  $\bar{C}$  خوددوگان است.

مثال ۴.۳.۳. فرض کنید که ما یک کد همینگ گسترش یافته با طول  $2^m$  را روی کانال BSC با احتمال خطای بیت  $p$  ( $q := 1 - p$ ) به کار 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، آن گاه خطا تشخیص داده می‌شود، اما تصحیح خطا نداریم؛ بنابراین، دو خطا باقی می‌ماند. در غیر این صورت، 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:

$$\begin{aligned} & 2 \binom{n}{2} p^2 q^{n-2} + \sum_{i=3}^n (i+1) \binom{n}{i} p^i q^{n-i} \\ &= 2 \binom{n}{2} p^2 \left\{ q^{n-2} + \sum_{i=3}^n \frac{(i+1) \binom{n}{i}}{2 \binom{n}{2}} p^{i-2} q^{n-i} \right\} \\ &\leq 2 \binom{n}{2} p^2 \left\{ q^{n-2} + \sum_{i=3}^n \binom{n-2}{i-2} p^{i-2} q^{n-i} \right\} \\ &= n(n-1)p^2 < (np)^2. \end{aligned}$$

اگر  $p$  به اندازه کافی کوچک باشد، آن گاه این دست آورد یک پیشرفت قابل ملاحظه می‌باشد. این تخمین خطا را در بخش ۴.۴ به کار خواهیم برد.

## ۳.۴ کدگشایی با منطق اکثریت

در این بخش، به طور خلاصه طراحی یک روش کدگشایی را که در بسیاری از کدهای خطی به کار 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  $\circ = \langle x, y^{(v)} \rangle$ ،  $(1 \leq v \leq r)$ ، متعامد نسبت به مکان  $i$  (برای کد  $C \in C^\perp$ ) نامیده می‌شود، اگر:

$$(1) \quad y_i^{(v)} = 1 \quad (1 \leq v \leq r).$$

$$(2) \quad \text{اگر } j \neq i \text{، آن‌گاه برای حداکثر یک مقدار } v \text{ داشته باشیم } y_j^{(v)} \neq 0.$$

حال فرض کنید  $x$  یک کلمه دریافتی باشد که شامل  $t$  خطاست و  $t \leq \frac{1}{4}r$ ؛ بنابراین:

$$\left. \begin{array}{l} t \geq \text{مقدار } v, \\ r - (t - 1) \leq \text{مقدار } v, \end{array} \right\} \text{ برای } \langle x, y^{(v)} \rangle \neq 0 \text{ اگر } x_i \text{ درست باشد.}$$

چون  $t > r - (t - 1)$ ، اکثریت مقادیر  $\langle x, y^{(v)} \rangle$ ، یعنی صفر، به ترتیب 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.

به عنوان مثال، دوگان کد همینگ [۷، ۴] را در نظر می‌گیریم (ارجاع به مثال ۳.۳.۳). معادلات بررسی‌توازن:

$$x_1 + x_2 + x_3 = 0,$$

$$x_1 + x_4 + x_5 = 0,$$

$$x_1 + x_6 + x_7 = 0,$$

نسبت به مکان ۱ متعامد هستند. اگر  $x$  شامل یک خطا باشد، آن‌گاه اگر  $x_1$  نادرست باشد این سه معادله به ترتیب دارای مقادیر ۱، ۱، ۱ و اگر  $x_1$  درست باشد دو تا ۰ و یکی ۱ خواهند بود. اگر دو تا از نتایج برابر ۱ باشد، می‌بینیم که بیشتر از یک خطا ایجاد شده است (این کد تشخیص دهنده دو خطاست).

کد  $[6, 3, 3]$  با ماتریس مولد  $G := (I \ J - I)$  را در نظر بگیرید و دو سبیل را به صورت  $a_7 = a_8 = a_1$  الحاق نمایید. خواننده باید بررسی نماید که هنوز داریم  $d = 3$ ، اما ماتریس بررسی توازن جدید دارای چهار سطر است که نسبت به مکان ۱ متعامد می‌باشند. بنابراین، حتی اگر دو خط 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 جزئی بیشتر درباره فاصله کد لازم به‌نظر می‌رسد. برای این هدف، ما مفهومی معروف به شمارنده وزنی<sup>۷</sup> 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 این صورت:

$$A(z) := \sum_{i=0}^n A_i z^i$$

شمارنده وزنی  $C$  نامیده می‌شود. دنباله  $(A_i)_{i=0}^n$  توزیع وزنی  $C$  نامیده می‌شود.

اگر  $C$  خطی باشد و  $c \in C$ ، آن‌گاه تعداد کدکلمات با فاصله  $i$  از  $c$  برابر با  $A_i$  می‌باشد. برای یک کد غیرخطی، این مطلب در حالت کلی درست نیست. کدی که دارای این خاصیت باشد (برای تمام کدکلمات و برای تمامی  $i$ ها)، پایا فاصله<sup>۸</sup> نامیده می‌شود (تعریف ۲.۵.۳ را نیز ببینید).

به‌عنوان یک مثال شمارنده وزنی کد دوتایی همینگ با طول  $n$  را محاسبه می‌کنیم.  $1 - i$  ستون از ماتریس بررسی توازن این کد را در نظر 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  $1 - i$  ستون را به  $\binom{n}{i-1}$  طریق انتخاب کنیم. امکان (۱)  $A_{i-1}$  بار رخ می‌دهد، امکان (۲)  $A_{i-2}$  بار و امکان (۳)  $i A_i$  بار رخ می‌دهد؛ بنابراین:

$$i A_i = \binom{n}{i-1} - A_{i-1} - (n - i + 2) A_{i-2},$$

<sup>۷</sup> weight enumerator

<sup>۸</sup> distance invariant

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

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

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

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

می باشد. یکی از نتایج بسیار اساسی در نظریه کدگذاری که توسط مک ویلیامز<sup>۹</sup> (۱۹۶۳) ارائه شده است، قضیه ای است که رابطه بین شمارنده وزنی یک کد و دوگان آن را بیان می کند.

**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 این صورت:

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

**اثبات.** فرض کنید  $\chi$  سرشت نابديهی  $(\mathbb{F}_q, +)$  باشد. به طور معمول فرض کنید  $\mathcal{R} = \mathbb{F}_q^n$ . تعریف می کنیم:

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

در این صورت داریم:

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

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

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

<sup>۹</sup> F.J. MacWilliams

این تابع وزن را به  $\mathbb{F}_q$ ، با قرار دادن  $w(\mathbf{v}) = 0$  اگر  $v = 0$  و  $w(\mathbf{v}) = 1$  در غیر این صورت، گسترش دهید؛ در این صورت، با نوشتن  $\mathbf{u} = (u_1, u_2, \dots, u_n)$  و  $\mathbf{v} = (v_1, v_2, \dots, v_n)$ ، از تعریف  $g(\mathbf{u})$  داریم:

$$\begin{aligned} g(\mathbf{u}) &= \sum_{(v_1, v_2, \dots, v_n) \in \mathcal{R}} z^{w(v_1) + \dots + w(v_n)} \chi(u_1 v_1 + \dots + u_n v_n) \\ &= \sum_{(v_1, v_2, \dots, v_n) \in \mathcal{R}} z^{w(v_1)} \chi(u_1 v_1) z^{w(v_2)} \chi(u_2 v_2) \dots z^{w(v_n)} \chi(u_n v_n) \\ &= \prod_{i=1}^n \sum_{v \in \mathbb{F}_q} z^{w(v)} \chi(u_i v) \end{aligned}$$

در عبارت آخر، اگر  $u_i = 0$ ، آن گاه مجموع داخلی برابر با  $1 + (q-1)z$  است و اگر  $u_i \neq 0$ ، آنگاه این مجموع برابر با:

$$1 + z \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \chi(\alpha) = 1 - z,$$

است؛ بنابراین:

$$g(\mathbf{u}) = (1 - z)^{w(\mathbf{u})} (1 + (q-1)z)^{n-w(\mathbf{u})}. \quad (۴)$$

□ 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 به صورت زیر داده می‌شود:

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

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

$$\text{Ham}_{C^\perp}(x, y) = \frac{1}{|c|} \text{Ham}_C(x + y, x - y).$$

این رابطه مستقیماً از قضیه ۲.۳.۵ نتیجه می‌شود.

## ۳.۶ متریک لی

در بسیاری از موضوعات مخابرات که در عمل به کار رفته، می‌توان حروف را به عنوان مجموعه‌ای از نقاطی که به طور منظم بر روی یک دایره واقع شده‌اند، مدل نمود. به عنوان مثال، الفبایی از این نوع شامل هفت سمبل را در نظر بگیرید. ما این سمبل‌ها را (که هنوز بر دایره واقع هستند) با عناصر  $\mathbb{Z}_7$  نشان می‌دهیم. در

این کانال، تاثیر نویز گوسی سفید باعث نمی‌گردد تا تمامی خطاها دارای احتمال یکسان گردند. احتمال آن که سمبل انتقال یافته به صورت 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. در واقع، می‌توان از وزن و فاصله معروف به لی استفاده نمود.

تعریف ۱.۳.۶.  $\mathbb{Z}_m$  را به عنوان الفبا در نظر بگیرید. وزن لی عدد صحیح  $i$  ( $0 \leq i < m$ ) به صورت زیر تعریف شده است:

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

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

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

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 این که فاصله لی در واقع یک تابع فاصله است مشکل نیست.

در فصل بعد، به طور خاص علاقه‌مند به الفبای  $\mathbb{Z}_4$  خواهیم بود. حال این مطلب را با جزئیات بیشتر می‌آوریم. در  $\mathbb{Z}_4$ ، وزن‌های لی ۰، ۱ و ۲ به ترتیب 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<sup>۱۰</sup> و شمارنده وزن لی<sup>۱۱</sup>.

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

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

داده شده است که در آن  $n_i(c)$  نمایش دهنده تعداد مولفه‌هایی از  $c$  است که برابر با  $i$  هستند.

<sup>۱۰</sup>symmetrized weight enumerator

<sup>۱۱</sup>Lee weight enumerator

تعریف ۲.۳.۶. شمارنده وزن لی یک کد  $C \subseteq \mathbb{Z}_4^n$  توسط رابطه:

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

داده می شود.

دقت کنید که:

$$\text{Lee}_C(x, y) = \text{swe}_C(x^2, xy, y^2). \quad (5)$$

بباید ببینیم که آیا یک تغییر کوچک بر روی اثبات قضیه ۲.۳.۵ می تواند باعث یک تعمیم از رابطه مک ویلیامز به کدهای روی  $\mathbb{Z}_4$  گردد؟ تابع  $\chi$  را به صورت سرشتی روی  $(\mathbb{Z}_4, +)$  در نظر می گیریم؛ حال تعریف می کنیم  $\chi(a) := i^a$  که  $\chi(a) = -1 = i^2$  در  $\mathbb{C}$ .

تابع  $f$  تعریف شده روی  $\mathbb{Z}_4^r := \mathcal{R}$  را در نظر گرفته و تعریف می کنیم:

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

با روش مشابهی همانند ۳ داریم:

$$\sum_{\mathbf{u} \in \mathcal{C}} g(\mathbf{u}) = |c| \sum_{\mathbf{v} \in \mathcal{C}^\perp} f(\mathbf{v}). \quad (6)$$

در قسمت بعدی اثبات، فرض می کنیم:

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

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  $u_i = 0$  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:

$$g(u) = (w + 2x + y)^{n_0(u)} (w - y)^{n_1(u) + n_3(u)} (w - 2x + y)^{n_2(u)}. \quad (7)$$

با جانشینی ۷ در ۶ داریم:

$$\text{swe}_{\mathcal{C}^\perp}(w, x, y) = \frac{1}{|c|} \text{swe}_C(w + 2x + y, w - y, w - 2x + y). \quad (8)$$

تعمیم قضیه ۲.۳.۵ را به صورت زیر داریم:

قضیه ۴.۳.۶. اگر  $C$  یک کد چهارتایی با دوگان  $C^\perp$  باشد، آنگاه:

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

اثبات. روابط ۵ تا ۸ را به کار بگیرید.

### ۳.۷ پیشنهادها

موضوع کدهای خطی به طور زیاد توسط مقالاتی از اسلپیان<sup>۱۲</sup> و همینگ<sup>۱۳</sup> در سال ۱۹۵۰ تحت تاثیر قرار گرفت. خواننده علاقه مند به کدگشایی با منطق اکثریت، می تواند به کتاب مَسی<sup>۱۴</sup> [۴۷] مراجعه نماید. چندین توسیع از قضیه مک ویلیامز، حتی برای کدهای غیرخطی، وجود دارد. یک بحث فراگیر در این باره را می توان در فصل ۵ مرجع [۴۶] یافت. به عنوان کاربردی از رابطه ۲ می توان 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  $\gamma$  باشد. نشان دهید  $\gamma = n$  یا  $n = 23$ .

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  $d = n - k + 1$  است.

۳.۳.۸. فرض کنید  $C$  یک کد  $[2k + 1, k]$  دوتایی است به طوری که  $C \subset C^\perp$ .  $C \setminus C^\perp$  را توصیف کنید.

<sup>۱۲</sup>D. E. Slepian

<sup>۱۳</sup>R. W. Hamming

<sup>۱۴</sup>J. L. Massey



۴.۳.۸ فرض کنید  $\mathbb{R} = \mathbb{F}_7$  و  $x \in \mathbb{R}$ .  $|B_1(x)|$  را تعیین کنید. آیا ممکن است مجموعه  $C \subset \mathbb{R}$  با  $|c| = 9$  یافت نمود به طوری 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  $\circ$  نباشد، آن گاه مجموع وزن کدکلمات  $C$  برابر با  $n(q-1)q^{k-1}$  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، آن گاه کلمات به طول زوج در  $C$  تشکیل یک کد  $[n, k-1]$  می دهند. این مطلب را اثبات نمایید.

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

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

کلمات دریافتی زیر را کدگشایی نمایید:

الف.  $(1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1)$

ب.  $(0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1)$

ج.  $(0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0)$

۸.۳.۸ فرض کنید  $p$  یک عدد اول باشد. آیا کد  $[8, 4]$  خوددوگان روی  $\mathbb{F}_p$  وجود دارد؟

۹.۳.۸ برای  $q = 2$  فرض کنید  $R_k$  نرخ کد همینگ تعریف شده توسط ۱.۳.۳ باشد.  $\lim_{k \rightarrow \infty} R_k$  را بیابید.

۱۰.۳.۸ فرض کنید  $C$  یک کد دوتایی با شمارنده وزن  $A(z)$  باشد. شمارنده وزنی  $\bar{C}$  چیست؟ شمارنده وزنی دوگان کد همینگ دوتایی گسترش یافته با طول  $2^k$  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  $p$  به کار می بریم. هدف ما تنها تشخیص خطاست. احتمال این که 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  $n_1 n_2$  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  $[n_1 n_2, k_1 k_2]$  کد با کمترین-فاصله  $d_1 d_2$  است. این کد حاصل ضرب 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  $c$  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  $c_0 = 0$  و  $c_1 = (1, \dots, 1, 0, \dots, 0)$  با وزن  $d$ ، شروع نمایید. اگر  $c_0, c_1, \dots, c_{l-1}$  انتخاب شده باشند، آن‌گاه  $c_l$  را طوری انتخاب کنید که در ترتیب قاموسی در ابتدا آید و (با  $l$ ها در سمت چپ تا آنجا که ممکن است)  $d(c_i, c_l) \geq d$  ( $0 \leq i \leq l-1$ ). پس از  $l$  مرتبه، طول کد به‌صورت طول قسمتی که مختص‌های  $l$  رخ داده است، تعریف می‌شود.

الف. نشان دهید پس از آن که  $2^k$  بردار انتخاب شدند، کوچک‌ترین کد با ترتیب قاموسی، خطی است!  
ب. برای  $d = 3$ ، کدهای همینگ در میان 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 در نظر 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  $-H_n$ ،  $-1$  را با  $0$  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، به کار رفت. به طور 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  $n \equiv 1 \pmod{4}$  و

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

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

که در آن  $I$  و  $J$ ،  $3$  در  $3$  هستند و

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

## ۴.۲ کد دوتایی گلی

مشهورترین کد در میان تمامی کدهای (دوتایی)، کد دوتایی معروف به کد گلی<sup>۱</sup>  $\mathcal{G}_{23}$  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، متعددی می‌باشد؛ بنابراین، کد  $\mathcal{G}_{23}$  نیز یکتاست.

ماتریس وقوع  $N$  از یک طرح  $(11, 6, 3)$  -  $2$  را در نظر می‌گیریم. به آسانی می‌توان نشان داد (دستی) که این طرح یکتاست. داریم  $NN^T = 3I + 3J$ .  $N$  را به عنوان ماتریسی با درایه‌هایی در  $\mathbb{F}_2$  در نظر بگیرید؛ در این صورت  $NN^T = I + J$ ؛ بنابراین،  $N$  دارای رتبه  $10$  می‌باشد و تنها بردار ناصفر  $x$  با  $xN = 0$  برابر با  $1$  می‌باشد. خواص این طرح به وضوح باعث می‌گردد تا تمامی سطرهای  $N$  دارای وزن  $6$  باشند و این که مجموع هر دو سطر متمایز  $N$  نیز دارای وزن  $6$  باشد. علاوه بر آن، می‌دانیم که مجموع سه یا چهار سطر  $N$  برابر با  $0$  نیست.

در ادامه، فرض کنید  $G$  ماتریس  $12$  در  $24$  (روی  $\mathbb{F}_2$ ) داده شده توسط  $G := (I_{12}P)$  باشد که در

<sup>۱</sup> Golay code

$$P := \begin{pmatrix} 0 & 1 & 1 \\ 1 & & \\ \vdots & & N \\ 1 & & \end{pmatrix}. \quad (2)$$

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 سطرهاى  $G$  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 سطرهاى  $G$  حداقل برابر با ۸ می‌باشد. کد دوتایی تولید شده توسط  $G$  را در نظر بگیرید و آن را  $\mathcal{G}_{24}$  بنامید. با حذف هر مولفه از آن می‌توان یک کد دوتایی  $[23, 12]$  با کمترین فاصله حداقل ۷ را یافت. این فاصله نمی‌تواند بیشتر باشد، چرا که شرط ۶.۳.۱ با  $e = 3$  برقرار است که در واقع نشان می‌دهد کد  $[23, 12, 7]$  یک کد کامل است! این کد را با  $\mathcal{G}_{23}$  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  $\mathcal{G}_{24}$  تشکیل یک  $(24, 8, 1)$  - طرح می‌دهند.

اثبات. با استفاده از یک بحث آسان مبتنی بر شمارش، می‌توان نشان داد که شمارنده وزنی یک کد کامل شامل ۵ به‌طور یکتا تعیین می‌شود. در واقع، داریم  $A_0 = A_{23} = 1$ ،  $A_7 = A_{16} = 253$ ،  $A_8 = A_{15} = 506$ ،  $A_{11} = A_{12} = 1288$ ؛ بنابراین،  $\mathcal{G}_{24}$  دارای ۷۵۹ کلمه با وزن ۸ است که هیچ دوتایی از آنها در بیشتر از چهار مکان، هم‌پوشانی<sup>۲</sup> ندارند؛ بنابراین، این کلمات با یکدیگر  $(\binom{24}{5}) = 759 \cdot (\binom{8}{5})$  پنج‌تایی را می‌پوشانند.  $\square$

قضیه ۲.۴.۲. اگر  $C$  یک کد دوتایی به طول ۲۴، با  $|C| = 2^{12}$  و کمترین فاصله ۸ باشد و  $0 \in C$ ، آن‌گاه  $C$  با  $\mathcal{G}_{24}$  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  $|C'| = 2^{12}$  را تولید می‌نماید؛ بنابراین، این کد کامل است و شمارنده وزنی آن همانند اثبات قضیه

<sup>۲</sup> 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. علاوه بر این، 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 پیمانۀ 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. به عبارت دیگر،  $C$  یک کد خطی خوددوگان است!

(۲) با در نظر گرفتن یک کلمه با وزن ۱۲ به عنوان سطر اول، ماتریس مولد  $G$  از کد  $C$  را تشکیل می‌دهیم. تحت جای گشت 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  $[۱۲, ۱۱, ۲]$  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. جای گشت دومی از ستون‌های  $G$ ، ماتریس مولد  $G'$  به شکل  $(I_{12} \ P)$  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!)  $(۱۱, ۶, ۳) - ۲$  باشد؛ بنابراین،  $C$  هم‌ارز  $G_{۲۴}$  است.

□

ساختار زیر از  $G_{۲۴}$  توسط تورین<sup>۳</sup> داده شده است.  $H$  کد همینگ  $[۷, ۴]$  با نمایش زیر را در نظر می‌گیریم. بردار ۰ و هفت شیفت دوری بردار  $(1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0)$  را در نظر بگیرید (دقت کنید که این هفت بردار، ماتریس وقوع  $PG(۲, ۲)$  را تشکیل می‌دهند). سپس هشت مکمل از این کلمات را در نظر بگیرید. اینها با یکدیگر تشکیل  $H$  را می‌دهند. فرض کنید  $H^*$  با معکوس نمودن ترتیب سببل‌ها در کلمات  $H$  به دست آمده باشد. با یک بررسی، می‌بینیم که  $\overline{H}$  و  $\overline{H^*}$  کدهای  $[۸, ۴]$  با خاصیت  $\overline{H} \cap \overline{H^*} = \{0, 1\}$  هستند. می‌دانیم که کدهای  $\overline{H}$  و  $\overline{H^*}$  خوددوگان با کمترین فاصله ۴ هستند.

<sup>۳</sup> R. J. Turyn

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

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

اجازه می‌دهیم  $a$  و  $b$  در میان عناصر یک پایه  $\overline{H}$  و  $x$  در میان عناصر یک پایه  $\overline{H}^*$  تغییر کنند. می‌بینیم که کلمات  $(a, 0, a)$ ،  $(0, b, b)$ ،  $(x, x, x)$  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  $c \in C$  می‌تواند دارای وزن کمتر از ۸ باشد؟ چون هر سه مولفه  $a + x$ ،  $b + x$ ،  $a + b + x$  آشکارا دارای وزن زوج می‌باشند، یکی از آنها باید برابر با ۰ باشد. مشاهده ما بر روی اشتراک  $\overline{H}$  و  $\overline{H}^*$  منجر به این نتیجه می‌گردد که  $x = 0$  یا  $x = 1$ . بدون کاستن از کلیت فرض کنیم  $x = 0$ . چون کلمات  $H$  دارای وزن ۰، ۴ یا ۸ می‌باشند، نتیجه می‌شود که  $c = 0$ .

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

ساختار بعدی توسط کانوی<sup>۴</sup> داده شده است. فرض کنید  $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$ . هم‌چنین فرض کنید  $C$ ، کد  $[۶, ۳]$  بر روی  $\mathbb{F}_4$  با کدکلمات  $(a, b, c, f(1), f(\omega), f(\overline{\omega}))$  باشد که در آن  $f(x) := ax^2 + bx + c$ . 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<sup>۵</sup> معروف است.

حال فرض کنید  $G$  یک کد دوتایی به طول ۲۴ باشد به طوری که کلمات آن با ماتریس‌های ۴ در ۶ دوتایی  $A$  نمایش داده شوند. چهار سطر چنین ماتریس  $A$  را با  $a_0, a_1, a_\omega, a_{\overline{\omega}}$  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  $a_0$  باشد.

$$(۲) \quad a_1 + \omega a_\omega + \overline{\omega} a_{\overline{\omega}} \in C$$

این شرایط به وضوح یک کد خطی تعریف می‌کنند.

اگر سطر اول  $A$  دارای توازن زوج باشد و کدکلمه موجود در رابطه (۲) برابر با صفر نباشد، آن‌گاه  $A$  دارای 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

<sup>۴</sup> J. H. Conway

<sup>۵</sup> 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، به صورت تمرین به خواننده واگذار می‌گردد؛ بنابراین، ماتریس‌های  $A$ ، کد  $G_{24}$  را تشکیل می‌دهند.

در بخش ۶.۹، ساختار دیگری از  $G_{24}$  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  $G_{24}$  متعددی است (درواقع ۵-متعددی؛ آن گروه متیوا<sup>۶</sup>  $M_{24}$  است)؛ بنابراین،  $G_{24}$  نیز یکتاست.

یادآوری می‌کنیم که ساختار تمرین ۱۴.۳.۸ با  $d = 8$  و  $k = 12$  نیز، کد گلی دوتایی گسترش‌یافته  $G_{24}$  را تولید می‌کند.

الگوریتم کدگشایی زیر برای  $G_{24}$  یک توسعه از بخش ۳.۴ مبتنی بر قضیه ۱.۴.۲ است. فرض کنید  $y_i, 1 \leq i \leq 253$ ، کدکلمه با وزن ۸ از  $G_{24}$  باشند با یک ۱ در یک مکان مفروض، گیریم مکان ۱. بررسی توازن‌های  $\langle x, y_i \rangle, 1 \leq i \leq 253$ ، را در نظر بگیرید؛ در اینجا ما این واقعیت را که  $G_{24}$  خوددوگان است به‌کار می‌بریم. فرض کنید  $x$  دریافت شده و شامل حداکثر ۴ خطاست. از قضیه ۲ نتیجه می‌شود که تعداد بررسی توازن‌هایی که رد می‌شوند، به صورت جدول زیر است:

	$x_1$ نادرست	$x_1$ درست
$t = 1$	۲۵۳	۷۷
۲	۱۷۶	۱۱۲
۳	۱۴۱	۱۲۵
۴	۱۲۸	۱۲۸

بنابراین، در حالت  $t \leq 3$  می‌توانیم سمبل  $x_1$  را تصحیح کنیم. خط متناظر با  $t = 4$  نشان می‌دهد که  $G_{24}$  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  $312 = 12 \times 26$  بررسی توازن است و تمامی مختص‌های بردار خطا را تولید می‌کند (اگر  $t \leq 3$ ).





عنوان مثالی دیگر کد  $(9, 20, 4)$  با ماتریس موجود در رابطه ۱ را در نظر بگیریم و آن را پنجر کنیم؛ یعنی سمبل آخر در هر کلمه را حذف کنیم، یک کد  $(8, 20, 3)$  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  $11010000, 11100100$  و  $10101010$  به همراه  $0$  و  $1$  به دست آید.

روش سوم، کوتاه نمودن<sup>۸</sup> کد  $C$  می‌باشد. در اینجا تمامی کدکلمات از  $C$  را در نظر 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).

بیاید به روشی کمی پیچیده‌تر نگاهی بیندازیم. از یکی از ساختارهای کد گلی دوتایی گسترش‌یافته  $G_{24}$  در بخش ۴.۲ فوراً می‌توان مشاهده نمود که  $G_{24}$  شامل زیرکدی با ۳۲ کلمه است که هشت مکان اول آنها برابر با صفر است. به‌طور مشابه، اگر قرار دهیم  $c_8 = 1$  و دقیقاً یکی از سمبل‌های  $c_1$  تا  $c_7$  برابر با ۱ باشد، آن‌گاه زیرکدی با ۳۲ کلمه  $(c_1, c_2, \dots, c_{24})$  یافت نموده‌ایم. با انجام این کار در تمامی حالات ممکن، زیرمجموعه‌ای از ۲۵۶ کلمه  $G_{24}$  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  $(6, 256, 16)$  است که غیرخطی است. این کد کد نورداستروم<sup>۹</sup>—رابینسن<sup>۱۰</sup> 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 پنجر کنیم، نتیجه یک کد  $(5, 64, 13)$  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<sup>۱۱</sup> ۱۹۷۷، مرجع [۲۶]). این دو کد عبارت‌اند از: کد معروف به کد نادلر<sup>۱۲</sup> و کد موجود در مساله ۷.۴.۸.

ساختاری مشابه با ساختار کد دوتایی گلی به صورت  $(u, u + v)$ —ساختار معروف است. فرض کنید  $C_i$  یک کد دوتایی  $(n, M_i, d_i)$  باشد  $(i = 1, 2)$ ؛ تعریف کنید:

$$C := \{(u, u + v) \mid u \in C_1, v \in C_2\}. \quad (3)$$

در این صورت  $C$  یک کد  $(2n, M_1 M_2, d)$  است که در آن  $d = \min\{2d_1, d_2\}$ . برای نشان دادن این مطلب، دو کدکلمه  $(u_1, u_1 + v_1)$  و  $(u_2, u_2 + v_2)$  را در نظر بگیرید. اگر  $v_1 = v_2$  و

<sup>۸</sup> shortening

<sup>۹</sup> Nordstrom

<sup>۱۰</sup> Robinson

<sup>۱۱</sup> J.-M. Goethals

<sup>۱۲</sup> Nadler

$u_1 \neq u_2$ ، آنگاه فاصله آنها حداقل برابر با  $2d_1$  است. اگر  $v_1 \neq v_2$ ، آنگاه این فاصله برابر با  $w(u_1 - u_2) + w(u_1 - u_2 + v_1 - v_2)$  است که به وضوح از  $w(v_1 - v_2)$  بیشتر است؛ یعنی حداقل برابر  $d_2$  است. به عنوان مثال برای  $C_2$ ، کد  $(8, 20, 3)$  ساخته شده در بالا را در نظر می‌گیریم و برای  $C_1$ ، کد با وزن زوج  $[8, 7]$  را در نظر می‌گیریم. این ساختار یک کد  $(16, 50, 29, 3)$  را نتیجه می‌دهد. تا به حال هیچ کد  $(16, M, 3)$  با  $M > 50, 29$  شناخته نشده است.

بسیاری از کدهای خوب با به کارگیری ایده زیر توسط هلگرت<sup>۱۳</sup> و استیناف<sup>۱۴</sup> (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  $d$  به عنوان سطر اول آن باشد؛ مثلاً:

$$G = \left( \begin{array}{c|ccc} 1 & & & \\ & G_1 & & \\ \hline & & 0 & 0 \\ & & & G_2 \\ & & & & 0 \end{array} \right).$$

فرض کنید  $d'$  کمترین-فاصله کد  $[n - d, k - 1]$ ، تولید شده توسط  $G_2$  باشد که ما آن را کد باقی‌مانده<sup>۱۵</sup> می‌نامیم (نسبت به اولین سطر  $G$ ). از  $G$  می‌بینیم که متناظر با هر کد کلمه از کد باقی‌مانده، دو کد کلمه از  $C$  وجود دارند که حداقل یکی از آنها در  $d$  مکان اول دارای وزن کمتر یا مساوی  $d$  است؛ بنابراین،  $d' \geq \frac{1}{2}d$ . 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  $G$  به صورت بالا خواهد بود که در آن  $G_2$  یک کد  $[7, 4]$  با فاصله  $d' \geq 3$  را تولید می‌کند؛ بنابراین، کد باقی‌مانده یک کد همینگ است. می‌توانیم  $G_2$  را چهار سطر با وزن ۳ در نظر بگیریم؛ بنابراین،  $G_1$  چهار سطر با وزن ۲ خواهد بود. چند امکان دیگر برای بررسی باقی می‌ماند که آنها هم منجر به  $d = 5$  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  $(10, M, 4)$  با  $M = 38$  تولید نموده است و در مدت زمان طولانی، عقیده بر این بود که این کد نمی‌تواند بهتر شود. بست<sup>۱۶</sup> (۱۹۷۸؛ مرجع [۸]) یک کد  $(10, 40, 4)$  را پیدا نمود که در زیر به شرح آن می‌پردازیم. در فصل بعد، خواهیم دید که در حالت  $d = 4$ ،  $n = 10$ ، این کد در واقع بهترین کد است! کد  $C_1$  را که یک کد  $[5, 3]$  با ماتریس مولد

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

است، در نظر بگیرید. با دو برابر کردن تمامی کدکلمات، یک کد  $[10, 3]$  با  $C_2$  با کمترین-فاصله  $d = 4$  را داریم. حال  $(10000 \ 00100)$  را به تمامی کلمات  $C_2$  اضافه نمایید. کد جدید، دیگر خطی نیست و شامل بردار 0 هم نمی‌باشد. با شماره‌گذاری مکان‌ها از ۱ تا ۱۰، مکان‌های

<sup>۱۳</sup>H. J. Helgert

<sup>۱۴</sup>R. D. Stinaff

<sup>۱۵</sup>residual code

<sup>۱۶</sup>M. R. Best

کدکلمات را با عناصری از زیرگروه  $S_1$  تولیدشده توسط  $(1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$  جای گشت می دهیم. این کد ۴۰ کدکلمه دارد که ثابت می شود کمترین فاصله آن برابر با ۴ است.

در بسیاری از کاربردهای فنی (نظیر دیسک فشرده)، دو کد به کار می روند. این کدها به روشی باهم همکاری می کنند. برخی اوقات، هدف ما مقابله با خطاهای گروهی است. بسیاری از اوقات، خطاهای بیشتری نسبت به آنچه از کمترین فاصله انتظار می رود، می تواند 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 بینداریم. حاصل ضرب یک کد همینگ گسترش یافته  $[8, 4, 4]$  با یک کد همینگ گسترش یافته  $[16, 11, 4]$  را در نظر بگیرید. این حاصل ضرب تا ۷ خطا را می تواند تصحیح کند. حال فرض کنید یک کلمه دریافتی، یعنی یک ماتریس  $16$  در  $8$ ، 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 به طوری که بتوانیم آن را اصلاح کنیم. اما، هنگامی که ما سطرها را کدگشایی می کنیم، سیزده تا تصحیح می شود و سه تا از بدهای آن تشخیص داده می شود. حال اعلام می کنیم که این سطرها پاک شده اند. هنگامی که ما ستون ها را کدگشایی می کنیم، با کلمات خطادار روبه رو نخواهیم شد، اما تمامی آنها دارای سه پاک شده می باشند. از آنجا که کد ستونی دارای فاصله ۴ است، می توانیم این پاک شده ها را اصلاح نماییم. در پایان، تمامی ۱۴ خطا تصحیح شده اند.

کدهایی که در عمل کاربرد دارند، تغییراتی را بر روی این ایده به کار می برند. در یک دیسک فشرده، دو کد، هر یک با فاصله ۵، با هم همکاری می کنند. برای یکی از آنها، کدگشا تنها کلمات با حداکثر یک خطا را تصحیح می کند؛ در غیر این صورت، اعلام می شود که کلمه پاک شده است. در پایان، ثابت می شود که کارایی این زوج کد هم کار افزایش می یابد.

مثال بیان شده در بالا را تعمیم می دهیم تا دنباله ای از کدهایی را که توسط الیاس<sup>۱۷</sup> در سال ۱۹۵۴ تعریف شده اند معرفی نماییم. با کد همینگ گسترش یافته  $C_1$  با طول  $2^m = n_1$  شروع می کنیم. فرض کنید این کدها بر روی یک کانال دوتایی متقارن با احتمال خطای  $p$  به کار رفته اند که در آن  $p < \frac{1}{4}$ . برای  $C_2$ ، کد همینگ گسترش یافته با طول  $2^{m+1}$  را در نظر می گیریم. تعریف کنید  $C_1$  و  $V_1$  و  $V_2$  حاصل ضرب مستقیم  $C_1$  و  $C_2$  باشد. این روش را ادامه می دهیم: اگر  $V_i$  تعریف شده باشد، آنگاه  $V_{i+1}$  حاصل ضرب مستقیم  $V_i$  و کد همینگ گسترش یافته  $C_{i+1}$  با طول  $2^{m+i}$  می باشد. طول  $V_i$  را با  $n_i$  و بعد آن را با  $k_i$  نمایش می دهیم. سرانجام،  $E_i$  را تعداد متوسط خطا در هر بلوک در کلمات  $V_i$  پس از کدگشایی قرار دهید.

<sup>۱۷</sup>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  $i \rightarrow \infty$  به  $E_i$  به صفر میل می‌کند. از رابطه بازگشتی برای  $n_i$  و  $k_i$  داریم:

$$n_i = 2^{mi + \frac{1}{4}i(i-1)} \quad ; \quad k_i = n_i \prod_{j=0}^{i-1} \left(1 - \frac{m+j+1}{2^{m+j}}\right).$$

بنابراین، اگر  $R_i$  نمایش نرخ  $V_i$  باشد، آن‌گاه:

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

زمانی که  $i \rightarrow \infty$ ؛ بنابراین، دنباله‌ای از کدها را خواهیم داشت که طول آنها به  $\infty$  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،  $d_i/n_i \rightarrow 0$  وقتی  $i \rightarrow \infty$ .

## ۴.۵ کدهای رید-مولر

حال دسته‌ای از کدهای دوتایی مرتبط با هندسه متناهی را توصیف می‌کنیم. این کدها برای اولین بار توسط مولر<sup>۱۸</sup> (۱۹۵۴) و رید<sup>۱۹</sup> (۱۹۵۴) به کار 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 یک پارچه‌ای 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<sup>۲۰</sup> (۱۸۷۸)).

<sup>۱۸</sup>D. E. Muller

<sup>۱۹</sup>I. S. Reed

<sup>۲۰</sup>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  $k$  در پایه  $p$  باشند؛ یعنی  $0 \leq n_i \leq p-1$  و  $0 \leq k_i \leq p-1$ ؛ در این صورت:

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

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

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

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

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

□

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  $i$  کوچک‌ترین اندیس  $i$  باشد به طوری که  $b_i \neq 0$ ؛ بنابراین:

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

اثبات. برای  $l = 0$  اثبات واضح است. استقرا را به کار می‌بریم. فرض کنید قضیه برای  $l < 2^n$  درست است. حال قرار دهید  $2^n \leq l < 2^{n+1}$ ؛ در این صورت 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 در نظر می‌گیریم:

(۱) اگر  $P_1(x) = 0$ ، آن گاه  $w(P(x)) = 2w(P_2(x))$  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  $P_1(x) \neq 0$ ، آن گاه 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.

در ابتدا برخی نمادگذاری‌ها و تعاریف را بیان می‌کنیم. نقاط  $AG(m, 2)$  را در نظر بگیرید؛ یعنی  $\mathbb{F}_2^m$

به‌عنوان بردارهای ستونی و پایه استاندارد با عناصر  $u_0, u_1, \dots, u_{m-1}$ . فرض کنید نمایش دوتایی  $j$  به‌صورت  $j = \sum_{i=0}^{m-1} \xi_{ij} 2^i$ ،  $0 \leq j < 2^m$ ، باشد.

تعریف می‌کنیم  $x_j := \sum_{i=0}^{m-1} \xi_{ij} u_i$ . 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  $i$ امین سطر  $E$  است؛ یعنی تابع مشخصه  $A_i$ . بردار  $v_i$  یک کلمه در  $\mathbb{F}_2^n$  است؛ معمولاً می‌نویسیم  $1 := (1, 1, \dots, 1)$  برای تابع مشخصه  $AG(m, 2)$ ؛

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

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

(۴) اگر  $S \subset \{0, 1, \dots, m-1\}$ ، آن گاه تعریف می کنیم:

$$C(S) := \{j = \sum_{i=0}^{m-1} \xi_{ij} 2^i \mid i \notin S \implies \xi_{ij} = 0 \ (0 \leq i < m)\}.$$

لم ۴.۴.۵. فرض کنید  $l = \sum_{i=0}^{m-1} \xi_{ij} 2^i$  و  $i_1, \dots, i_s$  مقادیری از  $i$  باشند که در آن  $\xi_{il} = 0$ . اگر:

$$v_{i_1} v_{i_2} \cdots v_{i_s} = (a_{l,0}, a_{l,1}, \dots, a_{l,n-1}),$$

آن گاه:

$$(x+1)^l = \sum_{j=0}^{n-1} a_{l,j} x^{n-1-j}.$$

(در اینجا، به طور معمول، یک حاصل ضرب بدون هیچ عاملی ( $s=0$ )، برابر با 1 تعریف شده است).

اثبات. با استناد به قضیه ۱.۴.۵، ضریب دوجمله‌ای  $\binom{n-1}{j}$  برابر با ۱ است اگر و تنها اگر  $\xi_{ij} = 1$  برای هر  $i$  که  $\xi_{il} = 0$ . همچنین با استناد به تعریف ۳.۴.۵ قسمت‌های (۱)، (۲) و (۳) داریم  $a_{l,j} = 1$  اگر و تنها اگر  $\xi_{ij} = 1$  برای  $i = i_1, \dots, i_s$ .

مطالب زیر نشان می‌دهد که چگونه می‌توان  $v_{i_1}, \dots, v_{i_s}$  را به طور هندسی تفسیر نمود.

لم ۵.۴.۵. اگر  $i_1, i_2, \dots, i_s$  متفاوت باشند، آن گاه:

(۱)  $v_{i_1} v_{i_2} \cdots v_{i_s}$  تابع مشخصه  $(m-s)$ -سطح  $A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_s}$  است.

(۲) وزن  $w(v_{i_1} \cdots v_{i_s})$  از بردار  $v_{i_1} \cdots v_{i_s}$  در  $\mathbb{F}_2^m$  برابر با  $2^{m-s}$  است.

(۳) تابع مشخصه  $\{x_j\}$ ، یعنی زامین بردار پایه  $\mathbb{F}_2^m$ ، برابر است با:

$$e_j = \prod_{i=0}^{m-1} \{v_i + (1 + \xi_{ij})1\}$$

(۴) بردارهای  $v_{i_1} \cdots v_{i_s}$  ( $0 \leq s \leq m$ ) یک پایه از  $\mathbb{F}_2^m$  هستند.



(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 در نظر بگیرید. برای هر  $i$  که  $\xi_{ij} = 0$  ما  $i$  امین سطر  $E$ ، یعنی  $v_i$ ، را با مکمل آن  $1 + v_i$  جایگزین می‌کنیم؛ در این صورت اگر سطرهاى ماتریس جدید را ضرب کنیم، بردار حاصل ضرب شامل درایه ۱ تنها در مکان  $j$  خواهد بود، چون تمامی ستون‌های ممکن تنها یک بار رخ می‌دهند. به عنوان یک مثال  $\{x_{14}\}$  را در جدول زیر در نظر بگیرید. چون  $14 = 0 + 2 + 2^2 + 2^3$  می‌بینیم که  $1 + \xi_{ij} = 1$  تنها اگر  $i = 0$  (در اینجا  $j = 14$ )؛ بنابراین، در این جدول، ما سطر متناظر با  $v_0$  را مکمل می‌کنیم و سپس ضرب می‌کنیم تا  $v_1 \ v_2 \ v_3$  را  $(v_0 + 1)$  را بیابیم که برداری سطری است که دارای تنها یک ۱ در چهاردهمین مکان است.

(۴)  $\sum_{s=0}^m \binom{m}{s} = 2^m = n$  بردار  $v_{i_1} \cdots v_{i_s}$  وجود دارند. این نتیجه از (۳) به دست می‌آید. از آنجا که چند جمله‌ای‌های  $(x+1)^l$  مستقل هستند، می‌توانیم لم ۴.۴.۵ را نیز به کار ببریم.

□

جدول زیر لم ۴.۴.۵ را تشریح می‌کند؛ برای مثال،  $v_0 v_2$  متناظر با  $10 = 2^2 - 2^0 = 15$  است؛ بنابراین،  $(x+1)^{10} = x^{10} + x^8 + x^2 + 1$ .

$v_{i_1} \ v_{i_2} \ \cdots \ v_{i_s}$	ضرایب $(x+1)^l =$ مولفه‌ها	$l = n - 1 - \sum 2^{i_s}$
۱	۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱	$15 = 1111$
$v_0$	۰ ۱ ۰ ۱ ۰ ۱ ۰ ۱ ۰ ۱ ۰ ۱ ۰ ۱ ۰ ۱	$14 = 1110$
$v_1$	۰ ۰ ۱ ۱ ۰ ۰ ۱ ۱ ۰ ۰ ۱ ۱ ۰ ۰ ۱ ۱	$13 = 1101$
$v_2$	۰ ۰ ۰ ۰ ۱ ۱ ۱ ۱ ۰ ۰ ۰ ۰ ۱ ۱ ۱ ۱	$11 = 1011$
$v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۱ ۱ ۱ ۱ ۱ ۱ ۱	$7 = 0111$
$v_0 \ v_1$	۰ ۰ ۰ ۱ ۰ ۰ ۱ ۰ ۰ ۱ ۰ ۰ ۱ ۰ ۰ ۱	$12 = 1100$
$v_0 \ v_2$	۰ ۰ ۰ ۰ ۰ ۱ ۰ ۱ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۰ ۱	$10 = 1010$
$v_0 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۰ ۱ ۰ ۱ ۰ ۱	$6 = 0110$
$v_1 \ v_2$	۰ ۰ ۰ ۰ ۰ ۰ ۱ ۱ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۱	$9 = 1001$
$v_1 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۱ ۱ ۱ ۱ ۱ ۱	$5 = 0101$
$v_2 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۱ ۱ ۱	$3 = 0011$
$v_0 \ v_1 \ v_2$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱	$8 = 1000$
$v_0 \ v_1 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۰ ۰ ۱	$4 = 0100$
$v_0 \ v_2 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۰ ۱	$2 = 0010$
$v_1 \ v_2 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱ ۱ ۱	$1 = 0001$
$v_0 \ v_1 \ v_2 \ v_3$	۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۰ ۱	$0 = 0000$

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 به عنوان پایه است،  $r$  امین مرتبه کد دوتایی رید-مولر نامیده می شود (RM کد؛ با نماد  $\mathcal{R}(r, m)$ ).

حالت خاص  $\mathcal{R}(0, m)$  کد تکرار است. از لم ۵.۴.۵ قسمت (۱) می بینیم که تابع منطقی  $x = (x_0, \dots, x_{m-1})$  که در آن  $x_{i_1} x_{i_2} \cdots x_{i_s}$  ثابت می کند که  $\mathbb{F}_2^m$  دارای مقدار ۱ است اگر و تنها اگر  $x \in A_{i_1} \cap \cdots \cap A_{i_s}$  بنابراین،  $\mathcal{R}(r, m)$  شامل دنباله هایی با مقادیر داده شده توسط چند جمله ای هایی بر حسب  $x_0, \dots, x_{m-1}$  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).  $\square$

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  $v_{j_1} \cdots v_{j_t}$  به ترتیب بردارهای پایه  $\mathcal{R}(r, m)$  و  $\mathcal{R}(m-r-1, m)$  باشند؛ در این صورت  $s+t < m$ ؛ بنابراین، حاصل ضرب 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 حاصل ضرب دارای وزن زوج می باشد، یعنی بردارهای اصلی از دو پایه، متعامد هستند.

$\square$

نتیجه گیری ۸.۴.۵.  $\mathcal{R}(m-2, m)$  یک کد همینگ گسترش یافته  $[n, n-m-1]$  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  $C = \mathcal{R}(m-1, m)$  و  $A$  یک  $1$ -سطح در  $AG(m, 2)$  باشد؛ در این صورت تابع مشخصه  $A$  در  $C$  می‌باشد.

اثبات. فرض کنید  $f = \sum_{j=0}^{n-1} f_j e_j$  تابع مشخصه  $A$  باشد. با استفاده از تعریف ۳.۴.۵ و لم ۵.۴.۵ داریم:

$$e_j = \sum_{s=0}^m \sum_{\substack{(i_1, \dots, i_s) \\ j \in C(i_1, \dots, i_s)}} v_{i_1} v_{i_2} \cdots v_{i_s};$$

بنابراین:

$$f = \sum_{s=0}^m \sum_{(i_1, \dots, i_s)} \left( \sum_{j \in C(i_1, \dots, i_s)} f_j \right) v_{i_1} v_{i_2} \cdots v_{i_s}.$$

در اینجا، مجموع داخلی، تعداد نقاط موجود در اشتراک  $A$  و  $s$ -سطح:

$$L = \{x_j \in AG(m, 2) \mid j \in C(i_1, \dots, i_s)\},$$

را شمارش می‌کند. اگر  $s > m-1$ ، 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.  $\square$

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. در اصطلاح علمی توابع منطقی،  $\mathcal{R}(r, m)$  مجموعه چند جمله‌ای‌هایی برحسب  $x_0, x_1, \dots, x_{m-1}$  با درجه کمتری 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، در نظر بگیریم. این جای‌گشت‌ها تشکیل یک گروه می‌دهند که معروف به گروه خودریختی  ${}^{22}C$  (با نماد:  $Aut(G)$ ) می‌باشند؛ برای مثال، اگر  $C$  کد تکرار باشد، آن‌گاه  $Aut(C) = S_n$ .

قضیه ۱۰.۴.۵.  $AGL(m, 2) \subset Aut(\mathcal{R}(r, m))$ .

اثبات. این یک نتیجه فوری از قضیه ۹.۴.۵ و این واقعیت است که  $AGL(m, 2)$  یک  $k$ -سطح را به یک  $k$ -سطح تصویر می‌کند.  $\square$

تذکر ۱۰.۴.۵ خواننده باید متوجه باشد که ما  $AGL(m, 2)$  را روی  $AG(m, 2)$  به عنوان گروهی از جای‌گشت‌های  $n$  مکان در نظر گرفتیم که توسط عناصر  $AG(m, 2)$  شمارش شده‌اند.

بدون پرداختن به جزئیات، به طور خلاصه یک روش کدگشایی برای کدهای RM بیان می‌کنیم که گسترشی از کدگشایی منطقی است. فرض کنید  $C = \mathcal{R}(r, m)$ . به وسیله قضیه ۸.۴.۵ و ۹.۴.۵، تابع مشخصه هر  $(r+1)$ -سطحی در  $AG(m, 2)$  یک بردار بررسی‌توازن برای  $C$  است. برای یک  $r$ -سطح داده شده  $A$ ، تعداد  $1 - 2^{m-r}$ ،  $(r+1)$ -سطح مجزا شامل  $A$  وجود دارد. نقطه‌ای که در  $A$  نباشد، متعلق به دقیقاً یکی از این  $(r+1)$ -سطح می‌باشد. هریک از این  $(r+1)$ -سطح شامل تقاطعی از  $A$  است و دقیقاً برابر با تعداد نقاطی است که در  $A$  نباشند.

حال، بیایید به بررسی توازن‌ها نگاهی بیندازیم. فرض کنید یک کلمه دریافتی شامل کمتر از  $2^{m-r-1}$  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  $1 - 2^{m-r}$  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  $r < 2^{m-r-1}$ ، آن‌گاه (۲) نسبت به (۱) دارای احتمال بیشتری است و در غیر این صورت (۱) دارای احتمال بیشتری است. این بدان معناست که یافتن توازن تعداد خطاها در مکان‌های هر  $r$ -سطحی امکان‌پذیر است؛ بنابراین، با به‌کارگیری روشی مشابه، همان موارد برای  $(r-1)$ -سطوح برقرار است و الی آخر. پس از  $r+1$  مرحله، خطاها مشخص شده‌اند. این روش، کدگشایی اکثریت چند مرحله‌ای<sup>۲۳</sup> نامیده می‌شود.

## ۴.۶ کدهای کرداک

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

<sup>۲۳</sup> multistep majority decoding

<sup>۲۴</sup> Kerdock codes

کد رید-مولر مرتبه اول متناظر با آن است. دقت کنید که  $\mathcal{R}(2, m)$ ، خود اجتماعی از هم مجموعه‌های  $\mathcal{R}(1, m)$  است که هر هم مجموعه متناظر با یک فرم درجه دوم به صورت زیر است:

$$Q(v) := \sum_{0 \leq i < j < m} q_{ij} v_i v_j. \quad (4)$$

متناظر با  $Q$ ، یک شکل دوخطی متناوب  $B$  به صورت:

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

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:

$$\sum_{i=0}^{h-1} v_{2i} v_{2i+1} + L(v), \quad (5)$$

واقع شود که در آن  $L$  خطی است و  $2h$  رتبه  $B$  است. در واقع، با نگاهی به آن می‌توان دید که  $v_{2h}$  یا  $L(v) = 0$ .

لم ۱.۴.۶. تعداد نقاط  $\mathbb{F}_2^{2h} \ni (x_0, x_1, \dots, x_{2h-1})$ ، که در آن  $\sum_{i=0}^{h-1} x_{2i} x_{2i+1} = 0$ ، برابر با  $2^{2h-1} + 2^{h-1}$  است.

اثبات. اگر  $x_0 = x_2 = \dots = x_{2h-2} = 0$ ، آن گاه  $2^h$  انتخاب برای  $(x_1, \dots, x_{2h-1})$  وجود دارد. در غیر این صورت،  $2^{h-1}$  انتخاب وجود دارد؛ بنابراین، تعداد صفرها برابر با  $2^{h-1} + (2^h - 1)2^{h-1}$  است.  $\square$

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 سادگی  $2^5$  با رتبه  $n$  باشد، آن گاه هم مجموعه  $\mathcal{R}(1, m)$  تعیین شده توسط  $Q(v)$ ، دارای  $2^m$  کلمه با وزن  $2^{m/2-1} - 2^{m-1}$  و  $2^m$  کلمه با وزن  $2^{m/2-1} + 2^{m-1}$  است.

(دقت کنید که این مطلب باعث می‌شود تا اگر  $Q$  دارای رتبه‌ای کمتر از  $m$  باشد، آن گاه هم مجموعه متناظر دارای کمترین-وزن کمتری باشد).

به وضوح، اجتماعی از هم مجموعه‌های  $\mathcal{R}(r, m)$ ، کدی با کمترین-فاصله حداکثر  $2^{m/2-1} - 2^{m-1}$  خواهد بود. می‌خواهیم کد  $C$  را با استفاده از اجتماع هم مجموعه‌های متناظر با فرم‌های درجه دوم  $Q_1, \dots, Q_l$  (با فرم‌های سادگی  $B_1, \dots, B_l$ ) بسازیم. برای یافتن کمترین-فاصله این کد، باید کدهای

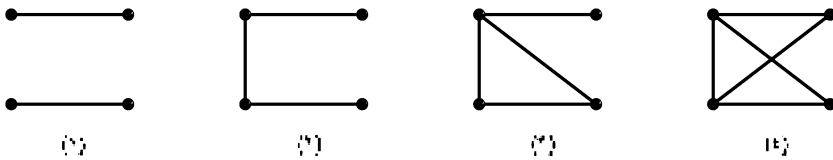
متناظر با هم مجموعه‌های تعریف شده توسط فرم‌های  $Q_i - Q_j$  ( $i \neq j$ ) را در نظر بگیریم و کمترین-وزن آنها را بیابیم. بهترین حالتی که می‌توانیم به آن دست یابیم این است که هر تفاضل  $Q_i - Q_j$  متناظر با یک فرم سادگی با رتبه ماکسیمال باشد که یک فرم سادگی نامنفرد است. چون فرم‌های سادگی متناظر با ماتریس‌های 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  $2^{m/2-1} - 2^{m-1}$  باشد، آن‌گاه  $l \leq 2^{m-1}$ .

تعریف ۳.۴.۶. فرض کنید  $m$  زوج باشد. یک مجموعه از  $2^{m-1}$  ماتریس سادگی با اندازه  $m$  به طوری که تفاضل هر دو عضو متمایز، نامنفرد است یک مجموعه کرداک نامیده می‌شود.

تعریف ۴.۴.۶. فرض کنید  $m$  زوج باشد. فرض کنید  $l = 2^{m-1}$  و  $Q_1, \dots, Q_l$  یک مجموعه کرداک باشد. کد غیرخطی  $\mathcal{K}(m)$  با طول  $n = 2^m$  شامل هم‌مجموعه‌های  $\mathcal{R}(1, m)$ ، متناظر با فرم‌های  $Q_i$ ،  $1 \leq i \leq l$ ، کد کرداک نامیده می‌شود.

نشان دادن این که دراصل چنین کدهایی وجود دارند، یک مساله غیربديهی است که مربوط به هندسه  $\mathbb{F}_2^m$  (ر.ک. مرجع [۱۱]) است. ما تنها یک مثال می‌آوریم. فرض کنید  $m = 4$ . اگر  $Q$  فرم مربعی  $\sum_{i=0}^3 q_{ij} x_i x_j$  باشد، آن‌گاه  $Q$  را با یک گراف با رئوس  $x_0, \dots, x_3$  با یال  $\{x_i, x_j\}$  نمایش می‌دهیم اگر و تنها اگر  $q_{ij} = 1$ .

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



افرازهای  $(12)(34)$ ،  $(13)(24)$  و  $(14)(23)$  را به صورت دوری منظم کنید. از شش گراف نوع (۲)، با گرفتن دو ضلع از یک زوج از این افرازاها 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 سادگی نامنفرد است. در این روش،  $2^8 = 256 = 8 \cdot 2^5$  کلمه از یک کد  $(6, 2^8, 16)$  را می‌یابیم، که درواقع همان کد نورداستروم-راینسن در بخش ۴.۴ است.

در حالت کلی،  $\mathcal{K}(m)$  یک کد  $(2^m, 2^{2m}, 2^{m-1} - 2^{m/2-1})$  است؛ بنابراین، تعداد کلمات آن به طور قابل توجهی بزرگ‌تر از  $\mathcal{R}(1, m)$  است، اگر چه کمترین-فاصله آن کمی کوچک‌تر است.

## ۴.۷ پیشنهادها

برای دیدن جزئیات درباره کاربردهای کدهای هادامارد در سفرهای مارینر، به مرجع [۵۶] مراجعه کنید. کدهای گلی توسط گلی<sup>۲۶</sup> 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<sup>۲۷</sup> و ونلینت<sup>۲۸</sup> [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  $n = 2^m$ . نشان دهید که کد رید-مولر  $\mathcal{R}(1, m)$  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  $\{x, 2x\}$  از کدکلمات به وزن ۵، زیرمجموعه‌ای از مکان‌هایی که  $x_i \neq 0$  را در نظر بگیرید. نشان دهید که این ۶۶ مجموعه تشکیل یک  $(1, 5, 11) - 4$  طرح می‌دهند.
- ۳.۴.۸. فرض کنید  $S$  ماتریس پالی مرتبه ۱۱ باشد و  $A = \frac{1}{3}(S + I + J)$ . سطرهاى  $A$  را در نظر بگیرید و تمامی ۵۵ مجموع هر دو سطر متمایز  $A$  و مکمل‌های این بردارها را در نظر بگیرید. نشان دهید که حاصل یک کد  $(3, 132, 11)$  است.
- ۴.۴.۸. یک کد  $(8, 36, 17)$  بسازید.
- ۵.۴.۸. ساختار کانوی<sup>۲۹</sup> از  $\mathcal{G}_{24}$  را در نظر بگیرید. سپس زیرگروه شامل ماتریس‌های  $A$  به شکل  $(B, B, B)$  را در نظر بگیرید که در آن  $B$  یک ماتریس  $4$  در  $2$  است. نشان دهید که ماتریس‌های  $B$  کلمات یک کد هم‌ارز با کد همینگ گسترش‌یافته  $[4, 8]$  هستند.

<sup>۲۶</sup>M. J. E. Golay

<sup>۲۷</sup>P. J. Cameron

<sup>۲۸</sup>J. H. vanLint

<sup>۲۹</sup>Conway

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

۷.۴.۸. ماتریس های  $I, J$  و  $P$  از اندازه ۲ همانند ۱ را در نظر بگیرید؛ تعریف کنید:

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

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

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

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

۹.۴.۸. نشان دهید  $(u, u+v)$ -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 می کند. 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 به صورت برداری که از جانشینی ۰ ها در  $x$  با  $-1$  به دست آمده، تعریف می کنیم. در مساله ۱.۴.۷ دیدیم که این نگاشت تحدید شده بر روی  $\mathcal{R}(1, m)$ ، بردارهای  $\pm a_1, \pm a_2, \dots, \pm a_n$  را نتیجه می دهد که در آن سطرهای یک ماتریس هادامارد می باشند. با به کارگیری این مطالب، نشان دهید که اگر  $x \in \mathbb{F}_2^n$ ، آن گاه کدکلمه  $c \in \mathcal{R}(1, m)$  وجود دارد؛ به طوری که  $d(x, c) \leq (n - \sqrt{n})/2$ .

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



۱۱.۴.۸. فرض کنید  $H$  ماتریس بررسی توازن یک کد همینگ گسترش یافته سه تایی  $[۴, ۲]$  باشد و  $I$  و  $J$  به ترتیب ماتریس های همانی و ماتریس تماماً ۱ از مرتبه ۴ باشند. نشان دهید:

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

کد  $C$  را که یک کد  $[۱۲, ۶]$  با کمترین-فاصله ۶ است، تولید می کند و این؛ یعنی کدی معادل با کد گلی سه تایی گسترش یافته.

## 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 به عنوان الفبا مجموعه  $Q$  با  $q$  سمبل را در نظر گرفته و تعریف می‌کنیم  $\theta := (q - 1)/q$ . نمادگذاری در اینجا همانند بخش ۳.۱ است. فرض می‌کنیم  $q$  انتخاب شده است و سپس یک کد  $(n, *, d)$  را به صورت 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  $(n, M + 1, d)$  نباشد، ماکسیمال نامیده می‌شود.

**تعریف ۱.۵.۱.** {یک کد  $(n, M, d)$  موجود باشد.  $A(n, d) := \max\{M \mid$  کد  $C$  به طوری که  $|C| = A(n, d)$  بهینه<sup>۱</sup> نامیده می‌شود.

برخی از مولفین، جمله “بهینه” را برای کدهای  $[n, k]$  با  $d = n - k + 1$  به کار می‌برند (مساله ۲.۳.۸ را ببینید). چنین کدهایی بنابر تعریف ۱.۵.۱ (با ۱.۵.۲ مقایسه کنید) بهینه هستند. معمولاً کدهای  $[n, k, n - k + 1]$ ، کدهای تفکیک‌پذیر با بیشترین فاصله<sup>۲</sup> (کدهای MDS) نامیده می‌شوند.

<sup>۱</sup> optimal

<sup>۲</sup> maximum distance separable codes

مطالعه اعداد  $A(n, d)$  به عنوان مساله‌ای اساسی در نظریه ترکیبیاتی کدگذاری در نظر گرفته شده است. در فصل ۲، آموختیم که کدهای خوب طولانی هستند، یا به طور دقیق‌تر، برای یک کانال با احتمال خطای خاص  $p$ ، می‌توانیم احتمال خطا را با مشاهده دنباله‌ای از کدها با افزایش طول  $n$ ، کاهش داد. به وضوح، تعداد متوسط خطای یک کلمه دریافتی برابر با  $np$  است؛ بنابراین، اگر می‌خواهیم این خطاها را تصحیح کنیم، باید  $d$  را حداقل با سرعت  $2np$  افزایش دهیم. این مطلب، اهمیت عدد  $\alpha(\delta)$  که به صورت زیر تعریف می‌شود، روشن می‌سازد.

### تعریف ۲.۵.۱.

$$\alpha(\delta) := \limsup_{n \rightarrow \infty} n^{-1} \log_q A(n, \delta n).$$

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 (به عنوان تابعی از  $n$ ). از تعریف ۲.۵.۱ دیده می‌شود که ما به معکوس تابع  $\alpha$  علاقه‌مند هستیم.

توابع  $A$  و  $\alpha$  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:

$$A(n, 2l - 1) = A(n + 1, 2l)$$

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

$$V_q(n, r) := |B_r(x)| = \sum_{i=0}^r \binom{n}{i} (q-1)^i. \quad (1)$$

(با شرط ۶.۳.۱ مقایسه کنید).

به منظور مطالعه تابع  $\alpha$ ، نیاز به توسیعی از تابع آنتروپی تعریف شده توسط ۴.۱.۴ را داریم. تابع آنتروپی  $H_p$  روی  $[\circ, \theta]$ ، که  $\theta := (q-1)/q$ ، به صورت:

$$H_q(\circ) := \circ, \quad (2)$$

$$H_q(x) := x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x), \quad \circ < x \leq \theta$$

تعریف می‌شود. دقت کنید که  $H_q(x)$  وقتی  $x$  از  $\theta$  تا  $\theta$  تغییر می‌کند، از  $\theta$  تا  $\theta$  افزایش می‌یابد.

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

$$\lim_{n \rightarrow \infty} n^{-1} \log_q V_q(n, [\lambda n]) = H_q(\lambda).$$

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

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

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<sup>۳</sup>، ولادوت<sup>۴</sup> و زینک<sup>۵</sup> [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  $B_{d-1}(c)$  با  $c \in C$  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  $c$  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 این که  $C$  خطی باشد، همان‌طور که قضیه زیر نشان می‌دهد، یک محدودیت اساسی نمی‌باشد.

<sup>۳</sup> Tsfasman

<sup>۴</sup> Vlăduț

<sup>۵</sup> 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  $z = ax + y$  (که در آن  $a \in Q, y \in C_{k-1}$ ) یک کدکلمه در  $C_k$  باشد؛ در این صورت:

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

□

کدهای موجود در مساله ۱۴.۳.۸ مثالی از قضیه ۶.۵.۱ می‌باشند.

**مثال ۷.۵.۱.** فرض کنید  $q = 2, n = 13, d = 5$ ؛ بنابراین، از رابطه ۱ داریم  $V_2(13, 4) = 1093$  و از این رو  $A(13, 5) \geq \lfloor 8192/1093 \rfloor = 8$ . در واقع قضیه ۶.۵.۱ وجود یک کد  $[13, 3, 5]$  را ضمانت می‌کند. به وضوح، این، یک کد خیلی خوب نمی‌باشد؛ زیرا با استفاده از قضیه ۷.۴.۵، سه بار پنجره کردن  $\mathcal{R}(1, 4)$  یک کد  $[13, 5, 5]$  را به دست می‌دهد و در واقع 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<sup>۶</sup> (یا کران گیلبرت-ورشامو<sup>۷</sup>) معروف است. حال بیایید نگاهی به کران متناظر برای  $\alpha$  بیندازیم.

**قضیه ۸.۵.۱.** (کران گیلبرت مجانبی<sup>۸</sup>). 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:

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

□

<sup>۶</sup> Gilbert bound

<sup>۷</sup> Varshamov

<sup>۸</sup> Asymptotic Gilbert Bound

## ۵.۲ کران‌های بالایی

در این بخش، تعدادی از کران‌های بالایی برای  $A(n, d)$  را مطرح می‌کنیم که به حق به دست 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 پنچر کردن یک کد  $(n, M, d)$  به اندازه  $d - 1$  بار، یک کد  $(n - d + 1, M, 1)$  به دست می‌آید؛ یعنی  $M$  کلمه پنچر شده متمایز می‌باشند. بنابراین،  $M \leq q^{n-d+1}$ . از این رو قضیه زیر را که به کران سینگلتون<sup>۹</sup> 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 این صورت داریم  $A(13, 5) \leq 512$ .  
فرم مجانبی قضیه ۱.۵.۲ به صورت 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 کد کلمه متفاوت حاصل می‌گردد. فرض کنید  $C$  یک کد  $(n, M, d)$  باشد. لیستی از کلمات  $C$  را می‌سازیم. یک ستون از این لیست را در نظر بگیرید. فرض کنید  $j$ امین سمبل  $Q$ ،  $m_j$  بار،  $0 \leq j \leq q - 1$ ، در این ستون رخ دهد. سهم این ستون در مجموع فاصله تمامی زوج کد کلمات متفاوت، برابر با  $\sum_{j=0}^{q-1} m_j(M - m_j)$  است. چون  $\sum_{j=0}^{q-1} m_j = M$ ، از نامساوی کشی-شوارتز داریم:

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

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

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

در اینجا ما کران معروف پلانکین<sup>۱۰</sup> را اثبات نموده‌ایم.

<sup>۹</sup> Singleton bound

<sup>۱۰</sup> Plotkin

قضیه ۴.۵.۲. برای  $q \geq 2, q, n, d \in \mathbb{N}$  و  $\theta = 1 - q^{-1}$  داریم:

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

### مثال ۵.۵.۲

(۱) فرض کنید  $q = 2, n = 13, d = 5$ ؛ در این صورت  $\theta = \frac{1}{2}$ . برای این که بتوانیم قضیه ۴.۵.۲ را به کار گیریم، کد  $(13, M, 5)$  را در نظر بگیرید و آن را چهار بار کوتاه نمایید تا یک کد  $(9, M', 5)$  با  $M' \geq 2^{-4}M$  حاصل گردد. با استفاده از کران پلاتکین داریم  $M' \leq 5 / (5 - 4 \cdot \frac{1}{2}) = 10$ ؛ بنابراین،  $M \leq 160$ ؛ یعنی  $A(13, 5) \leq 160$ . یک کران بهتر می تواند به این صورت به دست آید که در ابتدا از قضیه ۳.۵.۱ استفاده نموده تا به دست آوریم  $A(13, 5) = A(14, 6)$  و سپس استدلال فوق را تکرار نموده تا به دست آوریم  $A(14, 6) \leq 2^3 \cdot 6 / (6 - 5 \cdot \frac{1}{2}) = 96$ .

(۲) قرار دهید  $q = 3, n = 13, d = 9$ ؛ در این صورت  $\theta = \frac{2}{3}$  و کران پلاتکین باعث می گردد تا برای کدهای سه تایی داشته باشیم  $A(13, 9) \leq 27$ . دوگان کد همینگ سه تایی را در نظر بگیرید (تعریف ۱.۳.۳ را ببینید). این کد دارای ماتریس مولد زیر است:

$$G = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

ستون های این ماتریس، نقاط  $PG(2, 3)$  هستند. این مکان ها، که در آن  $G(a_1, a_2, a_3)$  دارای یک صفر می باشد، متناظر با نقاط  $PG(2, 3)$  بر روی خط تصویری با معادله  $a_1x_1 + a_2x_2 + a_3x_3 = 0$  هستند؛ یعنی اگر  $a \neq 0$ ، آن گاه دقیقاً چهار تا از این موقعیت ها وجود دارد؛ بنابراین، هر کد کلمه مخالف با صفر دارای وزن ۹ می باشد. از این رو این یک کد خطی است که در قضیه ۴.۵.۲ و در حالت تساوی صدق می کند.

از اثبات قضیه ۴.۵.۲ می توان دید که تساوی تنها زمانی امکان پذیر است که تمامی زوج کد کلمات متمایز در واقع دارای فاصله یکسان باشند. چنین کدی یک کد هم فاصله<sup>۱۱</sup> نامیده می شود. ما مجدداً یک نتیجه مجانبی را نتیجه می گیریم.

قضیه ۶.۵.۲. (کران پلاتکین مجانبی)؛ داریم:

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

$$\alpha(\delta) \leq 1 - \delta/\theta, \quad \text{اگر } 0 \leq \delta < \theta.$$

<sup>۱۱</sup>equidistant

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

کران پایین که توسط گریسمر<sup>۱۲</sup> (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، در واقع ممکن است فرض کنیم این سطر به‌صورت  $(111\dots 100\dots 0)$  با  $d$  تا ۱ است. هر سطر دیگر، حداقل دارای  $\lfloor d/q \rfloor$  مولفه در اولین  $d$  مکان است که یکسان می‌باشند؛ بنابراین، کد باقی‌مانده نسبت به اولین سطر، یک کد  $[n-d, k-1, d']$  با  $d' \geq \lfloor d/q \rfloor$  است؛ در این صورت با به‌کارگیری استقرا، قضیه زیر را داریم.

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

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

### مثال ۸.۵.۲

(۱) فرض کنید  $q = 2$ ،  $n = 13$  و  $d = 5$ . چون  $\sum_{i=0}^5 \lfloor 5/2^i \rfloor = 13$  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. در واقع، 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  $\sum_{i=0}^2 \lfloor 9/3^i \rfloor = 14$  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

<sup>۱۲</sup>J. H. Griesmer



(۱۱۰۰۰۱۰۰۰۰۰۰) دارای وزن ۹ در اولین سطر ماتریس مولد است؛ بنابراین، مشابه اثبات کران گریسمر، کد باقی مانده یک کد  $[5, 3, 3]$  سه تایی می باشد. ماتریس مولد چنین کدی به صورت زیر است:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & a & b \\ 0 & 0 & 1 & c & d \end{pmatrix},$$

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

یکی از آسان ترین کران ها، تعمیم شرط ۶.۳.۱ است که به کران همینگ یا کران گوی پوششی<sup>۱۳</sup> معروف است.

**قضیه ۹.۵.۲.** اگر  $q, n, e \in \mathbb{N}$  و  $q \geq 2$  و  $d = 2e + 1$ ، آنگاه:

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

**اثبات.** گوی های  $B_e(c)$  که در آن  $c$  متعلق به یک کد  $(n, M, 2e + 1)$  است، مجزا می باشند؛ بنابراین،  
 $M \cdot V_q(n, e) \leq q^n$

□

**مثال ۱۰.۵.۲.** فرض کنید  $q = 2$ ،  $n = 13$  و  $d = 5$ ؛ در این صورت از:

$$V_2(13, 2) = 1 + 13 + 78 = 92,$$

$$A(13, 5) \leq \lfloor 2^{13} / 92 \rfloor = 89$$

یک کد کامل را به این صورت تعریف کرده ایم که در تساوی رابطه ۹.۵.۲ صدق کند. در فصل ۷ به این سوال باز می گردیم.

**قضیه ۱۱.۵.۲.** (کران همینگ مجانبی) داریم:

$$\alpha(\delta) \leq 1 - H_q\left(\frac{1}{q}\delta\right).$$

<sup>۱۳</sup>sphere packing bound

اثبات.  $A(n, \lceil \delta n \rceil) \leq A(n, 2 \lceil \frac{1}{q} \delta n \rceil - 1) \leq q^n / V_q(n, \lceil \frac{1}{q} \delta n \rceil - 1)$ . پس نتیجه از لم ۴.۵.۱ حاصل می‌شود.  $\square$

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<sup>۱۴</sup> 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.  $x_0$  را طوری انتخاب کنید که  $|(x_0 + A) \cap c|$  ماکسیمال باشد؛ در این صورت:

$$\begin{aligned} |(x_0 + A) \cap c| &\geq q^{-n} \sum_{x \in Q^n} |(x + A) \cap c| \\ &= q^{-n} \sum_{x \in Q^n} \sum_{a \in A} \sum_{c \in C} |\{x + a\} \cap \{c\}| \\ &= q^{-n} \sum_{a \in A} \sum_{c \in C} 1 = q^{-n} |A| \cdot |c|. \end{aligned}$$

$\square$

حال فرض کنید  $C$  یک کد  $(n, M, d)$  و  $A$  همان  $B_r(o)$  باشد. بدون از دست دادن کلیت، فرض کنیم که نقطه  $x_0$  از این لم برابر با صفر باشد. کد  $A \cap C$  را در نظر بگیرید. این یک کد  $(n, K, d)$  با  $K \geq MV_q(n, r)/q^n$  است. کلمات این کد را به‌عنوان سطرهاى یک ماتریس  $K$  در  $n$  لیست می‌کنیم. فرض کنید  $m_{ij}$  تعداد وقوع سمبل  $j$  در ستون  $i$ ام این ماتریس باشد. می‌دانیم:

$$\sum_{j=0}^{q-1} m_{ij} = K \quad (1)$$

$$\sum_{i=1}^n m_{i0} := S \geq K(n - r) \quad (2)$$

زیرا هر سطر این ماتریس دارای وزن حداکثر  $r$  است؛ بنابراین:

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

$$\cdot \sum_{i=1}^n m_{i0}^2 \geq n^{-1} \left( \sum_{i=1}^n m_{i0} \right)^2 = n^{-1} S^2 \quad (۴)$$

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 به دست می‌آوریم  $S \geq q^{-1}nK$ ؛ داریم  $K^2 r(2 - (r/\theta n)) \leq \sum_{i=1}^n \sum_{j=0}^{q-1} m_{ij} (K - m_{ij})$ . 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 کمترین مساوی  $r$  باشند که در آن  $r \leq \theta n$  آن‌گاه:

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

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

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

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 به کار ببریم 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  $d > \theta n$  و  $r = \theta n$  کران پلانکین را نتیجه می‌دهد.

مثال ۱۵.۵.۲. فرض کنید  $q = 2$ ،  $n = 13$  و  $d = 5$ ؛ بنابراین،  $\theta = \frac{1}{5}$ . اگر ما  $A(14, 6)$  در رابطه ۱۴.۵.۲ را تخمین بزنیم، آنگاه بهترین نتیجه به دست 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، به طور مجانبی کران الیاس بهترین نتیجه از این بخش است.

قضیه ۱۶.۵.۲. (کران الیاس مجانبی): داریم:

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

$$\alpha(\delta) = 0, \quad \theta \leq \delta < 1$$

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:

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

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

□

کران بعدی نیز بر پایه ایده مشاهده زیر مجموعه‌ای از کدکلمات است. در این حالت، کدکلمات با یک وزن ثابت  $w$  را در نظر می‌گیریم.

در ابتدا باید تعدادهای معینی را مطالعه کنیم که مشابه با  $A(n, d)$  هستند. خود را به حالت  $q = 2$  محدود می‌کنیم.

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

لم ۱۸.۵.۲. داریم:

$$A(n, 2k - 1, w) = A(n, 2k, w) \leq \lfloor \frac{n}{w} \lfloor \frac{n-1}{w-1} \lfloor \dots \lfloor \frac{n-w+k}{k} \rfloor \dots \rfloor \rfloor.$$

اثبات. کلمات با وزن یکسان، دارای فاصله زوج  $A(n, 2k, w) = A(n, 2k - 1, w)$  می‌باشند. فرض کنید کد  $C$  با  $|c| = K$  صادق در شرایط ما باشد. کلمات  $C$  را به عنوان سطرهای یک ماتریس بنویسید. هر ستون این ماتریس دارای حداکثر  $A(n - 1, 2k, w - 1)$  سمبل ۱ است؛ بنابراین،

$$Kw \leq nA(n - 1, 2k, w - 1); \text{ یعنی:}$$

$$A(n, 2k, w) \leq \lfloor \frac{n}{w} A(n - 1, 2k, w - 1) \rfloor.$$

چون  $A(n, 2k, k - 1) = 1$ ، نتیجه با استفاده از استقرا ثابت می‌شود.  $\square$

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 به کار رفته‌اند، که به کران جانسون<sup>۱۵</sup> معروف است.

قضیه ۱۹.۵.۲. فرض کنید  $q = 2$ ،  $n, e \in \mathbb{N}$  و  $d = 2e + 1$ ؛ در این صورت:

$$A(n, d) \leq \frac{2^n}{\sum_{i=0}^e \binom{n}{i} + \frac{\binom{n}{e+1} - \binom{d}{e} A(n, d, d)}{\lfloor \frac{n}{e+1} \rfloor}}$$

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، می‌باشد؛ بنابراین:

$$M \sum_{i=0}^e \binom{n}{i} + N_{e+1} \leq 2^n.$$

به منظور تخمین  $N_{e+1}$ ، کد کلمه دلخواه  $c$  را در نظر 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  $\binom{n}{e}$  کلمه به وزن  $e + 1$  است. چون  $\binom{n}{e+1}$  کلمه با وزن  $e + 1$  وجود دارد، حداقل  $\binom{n}{e+1} - \binom{n}{e} A(n, d, d)$  آنها دارای فاصله  $e + 1$  تا  $C$  می‌باشند. با تغییر دادن  $c$ ،  $M \{ \binom{n}{e+1} - \binom{n}{e} A(n, d, d) \}$  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 در نظر بگیرید؛ مجدداً آن را  $0$  می‌نامیم. کدکلمات با فاصله  $e + 1$  تا  $0$  دارای فاصله متقابل بزرگتر یا مساوی  $2e + 1$  هستند اگر و تنها اگر آنها دارای عناصر  $1$  در مکان‌های متفاوت باشند؛ بنابراین، حداکثر  $\lfloor n/(e+1) \rfloor$  از چنین کدکلماتی وجود دارد. این مطلب به ما تخمین مورد نظر برای  $N_{e+1}$  را می‌دهد.  $\square$

از لم ۱۸.۵.۲، با در نظر 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:

$$|c| \left\{ \sum_{i=0}^e \binom{n}{i} + \frac{\binom{n}{e}}{\lfloor \frac{n}{e+1} \rfloor} \left( \frac{n-e}{e+1} - \lfloor \frac{n-e}{e+1} \rfloor \right) \right\} \leq 2^n, \quad (3)$$

که شکل اصلی کران جانسون است.

مثال ۲۰.۵.۲. فرض کنید  $q = 2$ ،  $n = 13$  و  $d = 5$ ؛ یعنی  $e = 2$ ؛ در این صورت:

$$A(13, 5, 5) \leq \lfloor \frac{13}{5} \lfloor \frac{12}{4} \lfloor \frac{11}{3} \rfloor \rfloor \rfloor = 23$$

و کران جانسون باعث می‌شود تا:

$$A(13, 5) \leq \lfloor \frac{2^{13}}{1 + 13 + 78 + \frac{286 - 10 \cdot 23}{4}} \rfloor = 77.$$

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 به حال شناخته شده‌اند، بر پایه روشی هستند که توسط دلسارت<sup>۱۶</sup> (۱۹۷۳) توسعه داده شد. ایده کار، به دست 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 به شدت به خواص چندجمله‌ای‌های کراچوک تکیه کنیم.

به منظور 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 این صورت، به طور معمول،  $\langle x, y \rangle$  نمایش ضرب داخلی  $\sum_{i=1}^n x_i y_i$  برای  $x, y \in Q^n$  می‌باشد.

لم ۱.۵.۳. فرض کنید  $\omega$  یک  $q$ امین ریشه واحد در  $\mathbb{C}$  باشد و  $x \in Q^n$  یک کلمه مشخص با وزن  $i$  باشد؛ در این صورت:

$$\sum_{\substack{y \in Q^n \\ w(y) = k}} \omega^{\langle x, y \rangle} = K_k(i).$$

اثبات. ممکن است فرض کنیم  $x = (x_1, x_2, \dots, x_i, 0, 0, \dots, 0)$  که در آن مختصات  $x_1$  تا  $x_i$  برابر ۰ نمی‌باشد.  $k$  موقعیت را انتخاب کنید،  $h_1, h_2, \dots, h_k$ ؛ به طوری که  $0 < h_1 < h_2 < \dots < h_j \leq i < h_{j+1} < \dots < h_k \leq n$  (با وزن  $D$  فرض کنید مجموعه تمام کلمات (با وزن

<sup>۱۶</sup>P. Delsarte

( $k$ ) باشد که مختصات ناصفر آنها در این مکان‌ها می‌باشد؛ در این صورت با استفاده از لم ۲۷.۱.۱ داریم:

$$\begin{aligned} \sum_{y \in D} w^{\langle x, y \rangle} &= \sum_{y_{h_1} \in Q \setminus \{0\}} \dots \sum_{y_{h_k} \in Q \setminus \{0\}} w^{x_{h_1} y_{h_1} + \dots + x_{h_k} y_{h_k}} \\ &= (q-1)^{k-j} \prod_{i=1}^j \sum_{y \in Q \setminus \{0\}} w^{x_{h_i} y} = (-1)^j (q-1)^{k-j}. \end{aligned}$$

□

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:

$$A_i := M^{-1} |\{(x, y) \mid x \in C, y \in C, d(x, y) = i\}|.$$

دنباله  $(A_i)_{i=0}^n$ ، توزیع فاصله<sup>۱۷</sup> یا توزیع داخلی<sup>۱۸</sup>  $C$  نامیده می‌شود.

دقت کنید که اگر  $C$  خطی پایا 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  $k \in \{0, 1, \dots, n\}$ .

اثبات. با توجه به لم ۱.۵.۳ داریم:

$$\begin{aligned} M \sum_{i=0}^n A_i K_k(i) &= \sum_{i=0}^n \sum_{(x, y) \in C^2} \sum_{\substack{\mathbf{z} \in Q^n \\ d(x, y) = i \\ w(\mathbf{z}) = k}} w^{\langle x-y, \mathbf{z} \rangle} \\ &= \sum_{\mathbf{z} \in Q^n} \left| \sum_{x \in C} w^{\langle x, \mathbf{z} \rangle} \right|^2 \geq 0. \\ & \quad w(\mathbf{z}) = k \end{aligned}$$

□

<sup>۱۷</sup>distance distribution

<sup>۱۸</sup>inner distribution



قضیه ۴.۵.۳. فرض کنید  $q, n, d \in \mathbb{N}$  و  $q \geq 2$ ؛ در این صورت:

$$A(n, d) \leq \max \left\{ \sum_{i=0}^n A_i \mid A_0 = 1, A_i = 0 \quad 1 \leq i < d \right\},$$

$$A_i \geq 0, \sum_{i=0}^n A_i K_k(i) \geq 0 \quad k \in \{0, 1, \dots, n\} \text{ برای } \{.$$

اگر  $q = 2$  و  $d$  زوج باشد، آنگاه ممکن است برای  $i$  زوج، فرض کنیم  $A_i = 0$ .

اثبات. با به کارگیری لم ۳.۵.۳، توزیع فاصله یک کد  $(n, M, d)$  در نامساوی  $\sum_{i=0}^n A_i K_k(i) \geq 0$  صدق می کند. به وضوح  $A_i$ ها نامنفی هستند و  $A_0 = 1$ ، برای  $1 \leq i < d$  علاوه بر این با استفاده از لم

$$3.5.3 \text{ داریم } \sum_{i=0}^n A_i = M^{-1} |c^T| = M$$

ادعای آخر در مساله ۶.۴.۸ آمده است.

مثال ۵.۵.۳ همانند چند مثال قبل، می خواهیم تا  $A(14, 6) = A(13, 5)$  را برای  $q = 2$  تخمین بزنیم. برای توزیع فاصله یک کد  $(14, M, 6)$ ، ممکن است فرض کنیم:

$$A_0 = 1, A_1 = A_2 = A_3 = A_4 = A_5 = A_6 = A_7 = A_8 = A_9 = A_{10} = A_{11} = A_{12} = 0,$$

$$A_6 \geq 0, A_7 \geq 0, A_{10} \geq 0, A_{12} \geq 0, A_{14} \geq 0.$$

برای اینها، نامساوی های زیر از لم ۳.۵.۳ را داریم (مقادیر  $K_k(i)$  با به کارگیری رابطه ۱۴ یافت شده اند).

$$14 + 2A_7 - 2A_8 - 6A_{10} - 10A_{12} - 14A_{14} \geq 0;$$

$$91 - 5A_7 - 5A_8 + 11A_{10} + 43A_{12} + 91A_{14} \geq 0;$$

$$374 - 12A_7 + 12A_8 + 4A_{10} - 100A_{12} - 374A_{14} \geq 0;$$

$$1001 + 9A_7 + 9A_8 - 39A_{10} + 121A_{12} - 1001A_{14} \geq 0;$$

$$2002 + 30A_7 - 30A_8 + 38A_{10} - 22A_{12} - 2002A_{14} \geq 0;$$

$$2003 - 5A_7 - 5A_8 + 27A_{10} - 165A_{12} + 3003A_{14} \geq 0;$$

$$3432 - 40A_7 + 40A_8 - 72A_{10} + 264A_{12} - 3432A_{14} \geq 0.$$

حال باید یک کران بالا برای  $M = 1 + A_7 + A_8 + A_{10} + A_{12} + A_{14}$  بیابیم. ثابت می شود که این

مساله برنامه‌ریزی خطی دارای جواب یکتاست؛ یعنی:

$$A_7 = 42, A_8 = 7, A_{10} = 14, A_{12} = A_{14} = 0.$$

بنابراین،  $M \leq 64$ . در بخش ۴.۴ یک کد  $(5, 64, 13)$  به نام  $Y$  را ساختیم؛ بنابراین، اینک ثابت نموده‌ایم که  $A(13, 5) = 64$ .

حال قضیه ۴.۵.۳ را به صورت دیگری تبدیل می‌کنیم که نسبت به فرم اصلی، دارای مزیت‌هایی است. خواننده آشنا با برنامه‌ریزی خطی تصدیق می‌کند که ما داریم از قضیه دوگانگی<sup>۱۹</sup> استفاده می‌کنیم (ر.ک. مرجع [۳۲]).

قضیه ۶.۵.۳. فرض کنید  $\beta(x) = 1 + \sum_{k=1}^n \beta_k K_k(x)$  یک چندجمله‌ای با  $\beta_k \geq 0$  ( $1 \leq k \leq n$ ) باشد؛ به طوری که برای  $j = d, d+1, \dots, n$  داریم  $\beta(j) \leq 0$ ؛ در این صورت  $A(n, d) \leq \beta(0)$ .

اثبات. فرض کنید  $A_0, A_1, \dots, A_n$  در شرایط قضیه ۴.۵.۳ صدق کند؛ یعنی:

$$K_k(0) + \sum_{i=d}^n A_i K_k(i) \geq 0. \quad (k = 0, 1, \dots, n; A_i \geq 0, i = d, d+1, \dots, n)$$

بنابراین، شرطی که روی  $\beta$  قرار دادیم، باعث می‌گردد تا  $\sum_{i=d}^n A_i \beta(i) \leq 0$ ؛ یعنی:

$$-\sum_{i=d}^n A_i \geq \sum_{k=1}^n \sum_{i=d}^n A_i K_k(i) \geq -\sum_{k=1}^n \beta_k K_k(0) = 1 - \beta(0),$$

بنابراین:

$$1 + \sum_{i=d}^n A_i \leq \beta(0).$$

□

مزیت قضیه ۶.۵.۳ این است که هر چندجمله‌ای  $\beta$  صادق در شرایط قضیه، کرانی برای  $A(n, d)$  را القا می‌کند که برای به دست آوردن این کران، باید در قضیه ۴.۵.۳ جواب بهینه برای دستگاه نامعادلات را یافت.

مثال ۷.۵.۳. فرض کنید  $q = 2$  و  $n = 2l + 1$  و  $d = l + 1$ . سعی می‌کنیم تا کرانی برای  $A(n, d)$  با در نظر گرفتن  $\beta(x) = 1 + \beta_1 K_1(x) + \beta_2 K_2(x) = 1 + \beta_1(n - 2x) + \beta_2(2x^2 - 2nx + \frac{1}{2}n(n-1))$  بیابیم.  $\beta_1$  و  $\beta_2$  را طوری انتخاب کنید که در آن  $\beta(d) = \beta(n) = 0$ . داریم  $\beta_2 = 1/n$ ,  $\beta_1 = (n+1)/2n$ ؛ بنابراین،

<sup>۱۹</sup>duality theorem

شرایط قضیه ۶.۵.۳ برقرار است؛ بنابراین، داریم  $2l+2 = \beta(0) = 1 + \beta_1 n + \beta_2 \binom{n}{2}$  این مطلب، مشابه کران پلاتکین ۴.۵.۲ است.

بهترین کران برای  $\alpha(\delta)$  که در حال حاضر مشهور است، توسط مک‌الیس، ردمیچ<sup>۲۰</sup>، رامسی<sup>۲۱</sup>، و ولج<sup>۲۲</sup> (۱۹۷۷؛ مرجع [۵۰]) مطرح شده است. در اینجا این بهترین کران را مطرح نمی‌کنیم، اما یک نتیجه کمی ضعیف‌تر (که در واقع برای  $0.273 < \delta < 1$  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:

$$\alpha(\delta) \leq H_2\left(\frac{1}{q} - \sqrt{\delta(1-\delta)}\right).$$

اثبات. عدد صحیح  $t$  با شرط  $1 \leq t \leq \frac{1}{q}n$  و عدد حقیقی  $a$  در بازه  $[0, n]$  را در نظر می‌گیریم. چند جمله‌ای  $\alpha(x)$  را به صورت زیر تعریف کنید:

$$\alpha(x) := (a-x)^{-1} \{K_t(a)K_{t+1}(x) - K_{t+1}(a)K_t(x)\}^2.$$

با به کارگیری رابطه ۱۶ از فصل ۱ داریم:

$$\alpha(x) = \frac{2}{t+1} \binom{n}{t} \{K_t(a)K_{t+1}(x) - K_{t+1}(a)K_t(x)\} \sum_{k=0}^t \frac{K_k(a)K_k(x)}{\binom{n}{k}}. \quad (4)$$

فرض کنید  $\alpha(x) = \sum_{k=0}^{2t+1} \alpha_k K_k(x)$  توسعه 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  $a \leq d$ ، آن‌گاه تنها چیزی که باید چک کنیم این است که آیا  $\alpha_i \geq 0$ ،  $(i = 1, \dots, n)$ ،  $a_0 > 0$ . اگر  $x_i^{(k)}$  نمایش کوچکترین صفر  $K_k$  باشد، آن‌گاه می‌دانیم که  $x_i^{(t+1)} < x_i^{(t)} < 0$  (با رابطه ۱۷ از فصل ۱ مقایسه کنید).

به منظور ساده‌کردن محاسبات زیر،  $t$  را طوری انتخاب می‌کنیم که  $x_i^{(t)} < a$  و  $x_i^{(t)}$  و  $x_i^{(t+1)}$  طوری انتخاب می‌کنیم که  $K_t(a) = -K_{t+1}(a) > 0$ . نتیجه ۴ بیان می‌کند که  $\alpha(x)$  به شکل  $\sum_{k,l} c_{kl} K_k(x)K_l(x)$  است؛ که در آن تمامی ضرایب  $c_{kl}$  ناصفر می‌باشند. از ۱۸ نتیجه می‌شود که تمامی  $\alpha_i$  ناصفر می‌باشند. علاوه بر این،  $\alpha_0 = -[2/(t+1)] \times \binom{n}{t} K_t(a)K_{t+1}(a) > 0$ . پس در حقیقت می‌توانیم

<sup>۲۰</sup>E. R. Rodemich

<sup>۲۱</sup>H. C. Rumsey

<sup>۲۲</sup>L. R. Welch

قضیه ۶.۵.۳ را به کار ببریم؛ داریم:

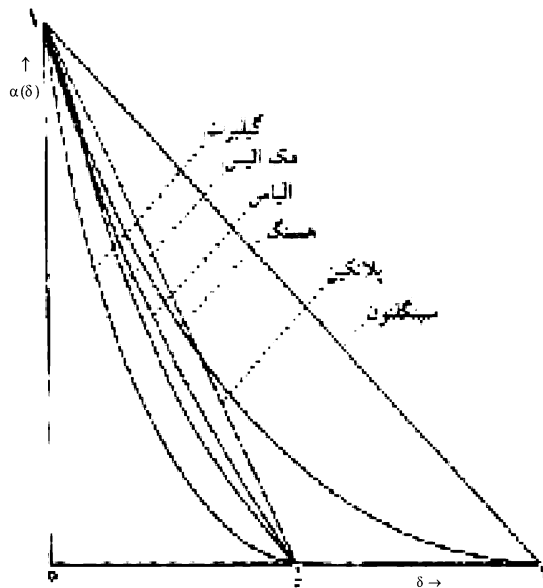
$$A(n, d) \leq \beta(\circ) = \frac{\alpha(\circ)}{\alpha_\circ} = \frac{(n+1)^2}{2a(t+1)} \binom{n}{t}. \quad (5)$$

برای تکمیل اثبات، نیاز داریم درباره مکان صفرهای  $x^{(t)}$  مطالب بیشتری بدانیم. می‌توان دید که اگر  $0 < \tau < \frac{1}{2}$ ،  $n \rightarrow \infty$  و  $t/n \rightarrow \tau$ ، آنگاه  $x^{(t)}/n \rightarrow \frac{1}{2} - \sqrt{\tau(1-\tau)}$ . در نتیجه می‌توانیم رابطه ۵ را برای  $n \rightarrow \infty$  و  $d/n \rightarrow \delta$  با دنباله‌ای از مقادیر  $t$  که  $t/n \rightarrow \frac{1}{2} - \sqrt{\delta(1-\delta)}$  به کار بگیریم. با گرفتن لگاریتم در رابطه ۵ و تقسیم بر  $n$  ادعای قضیه به دست می‌آید (برای مشاهده اثبات حکمی درباره  $x^{(t)}$  خواننده را به یکی از منابع درباره چندجمله‌ای‌های متعامد [۴۶] یا [۵۰] ارجاع می‌دهیم).  $\square$

## ۵.۴ پیشنهادها

برای مشاهده مطالبی درباره کدهای تعریف شده با استفاده از هندسه جبری و برای بهبود کران گیلبرت، به مرجع [۷۳] ارجاع می‌دهیم. برای نمونه بخش ۶.۸ را ببینید.

در شکل ۵.۱، کران‌های مجانبی به دست آمده در این بخش را مقایسه نموده‌ایم.



شکل ۵.۱: مقایسه برخی کران‌های مجانبی معروف با یکدیگر.

این شکل، کران‌های مطرح شده توسط لون‌اشتین<sup>۲۳</sup> (۱۹۷۹؛ مرجع [۴۰]) و سیدل‌نیکف<sup>۲۴</sup> (۱۹۷۵)؛ مرجع [۶۳]) را شامل نمی‌شود؛ زیرا این کران‌ها به اندازه نتایج به دست آمده توسط مک‌الیس در مرجع

<sup>۲۳</sup>V. I. Levenshtein

<sup>۲۴</sup>M. Sidelnikov

[۵۰] خوب نیستند و به دست آوردن آنها نسبتاً مشکل می‌باشد. بهترین کران ذکر شده در فوق به صورت زیر است:

$$\alpha(\delta) \leq \min\{1 + g(u^2) - g(u^2 + 2\delta u + 2\delta) \mid 0 \leq u \leq 1 - 2\delta\}, \quad (6)$$

که در آن:

$$g(x) := H_2\left(\frac{1 - \sqrt{1-x}}{2}\right).$$

برای مشاهده اثباتی از آن، خواننده را به منابع [۵۰] یا [۵۲] ارجاع می‌دهیم. برای مقادیر بسیار کوچک  $\delta$ ، کران الیاس بهتر از کران موجود در قضیه ۸.۵.۳ است، اما به خوبی کران ۶ نمی‌باشد.

در مقاله‌ای توسط بست (۱۹۷۷؛ مرجع [۶])، 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 اضافه نمودن نامساوی‌هایی (نظیر نامساوی بدیهی  $A_{n-1} + A_n \leq 1$ ) 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 بررسی توازن خود تعریف شود، استفاده نموده و نشان دهید که یک کد  $[n, k, d]$  روی  $\mathbb{F}_q$  وجود دارد، اگر  $q^{n-k} < V_q(n-1, d-2)$ . این مطلب را با قضیه ۶.۵.۱ مقایسه کنید.

۲.۵.۵.  $A(10, 5)$  را برای  $q = 2$  تعیین کنید.

۳.۵.۵. فرض کنید  $q = 2$ . نشان دهید اگر در قضیه ۴.۵.۲ طرف راست عدد صحیح فرد  $l$  باشد، آنگاه  $A(n, d) \leq l - 1$ .

۴.۵.۵. اگر  $q = 2$ ، آنگاه کران‌هایی برای  $A(17, 8)$  بیابید.

۵.۵.۵. ماتریس مولدی برای دوگان کد  $[۳۱, ۵]$  همینگ دوتایی در نظر 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 گریسر 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  $A(n - ۲, ۲k, w - ۲)$  نشان  $|c| = [n(n - ۱)/w(w - ۱)] \times A(n - ۲, ۲k, w - ۲)$  باشد. 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  $C_1$  یک کد دوتایی با طول  $n$  تعریف شده به‌صورت زیر باشد:

$$C_l := \{(c_0, c_1, \dots, c_{n-1}) \mid \sum_{i=0}^{n-1} c_i = w, \sum_{i=0}^{n-1} i c_i \equiv l \pmod{n}\},$$

که در آن اعمال جمع روی  $\mathbb{Z}$  انجام گرفته‌اند. نشان دهید:

$$A(n, ۴, w) \sim \frac{n^{w-1}}{w!}, \quad (n \rightarrow \infty).$$

۹.۵.۵. فرض کنید  $q = ۲$ . نشان دهید:  ${}^{(n)}A(n, ۲k) \leq ۲^n A(n, ۲k, w)$ .

۱۰.۵.۵

(۱) نشان دهید  $A(n, ۲k, w) \leq (1 - \frac{w}{k}(1 - \frac{w}{k}))^{-1}$ ، 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  $x + 1 \in C$ . نشان دهید قرار دادن  $k = ۲$  در رابطه ۳.۵.۳، کران زیر را نتیجه می‌دهد:

$$M \leq \frac{\lambda d(n - d)}{n - (n - ۲d)^2}.$$

(این کران با نام کران گری<sup>۲۵</sup> شناخته می‌شود).

۱۲.۵.۵. نشان دهید کد  $(۳, ۲۰, ۸)$  از بخش ۴.۴، بهینه است (اثبات مشکل است؛ بخش ۵.۴ را ببینید).

## فصل ۶

# کدهای دوری

### ۶.۱ تعاریف

در بخش ۴.۵، گروه خودریختی  $Aut(C)$  از کد  $C$  را تعریف نمودیم. متنناظر 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 متنناظر 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 ۱.۶.۱. یک کد خطی  $C$  دوری نامیده می‌شود، اگر:

$$\forall (c_0, c_1, \dots, c_{n-1}) \in C [(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C].$$

این تعریف با به‌کارگیری ماتریس‌های تک‌جمله‌ای به جای جای‌گشت‌ها، هم‌چنان که در ادامه می‌آید، گسترش می‌یابد. اگر برای هر کد کلمه  $(c_0, c_1, \dots, c_{n-1})$ ، کلمه  $(\lambda c_{n-1}, c_0, \dots, c_{n-2})$  (در اینجا  $\lambda$  مقداری ثابت است) نیز در  $C$  باشد، آن‌گاه این کد، یک کد پایادوری<sup>۱</sup> (و نادوری<sup>۲</sup> اگر  $\lambda = -1$ ) نامیده

<sup>۱</sup> constacyclic

<sup>۲</sup> 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، یک ریختی زیر، بین  $\mathbb{F}_q^n$  و یک گروه از چندجمله‌ای‌ها می‌باشد. مضارب  $x^n - 1$  تشکیل یک ایده آل اصلی در حلقه چندجمله‌ای  $\mathbb{F}_q[x]$  می‌دهد. حلقه کلاس باقی مانده  $\mathbb{F}_q[x]/(x^n - 1)$  شامل مجموعه‌ای از چندجمله‌ای‌های:

$$\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{F}_q, 0 \leq i < n\},$$

به عنوان یک دستگاه نماینده‌ها است. به وضوح،  $\mathbb{F}_q^n$  با این حلقه یک ریخت می‌باشد (تنها به عنوان یک گروه جمعی در نظر گرفته شده است). در ادامه، هم‌چنین ساختار ضربی را که اینک معرفی کردیم؛ یعنی حاصل ضرب چندجمله‌ای‌ها در پیمانۀ  $(x^n - 1)$ ، به کار خواهیم برد. از اینجا به بعد، از همسانی زیر استفاده خواهیم کرد:

$$(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n \Leftrightarrow a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1), \quad (1)$$

و اغلب از کد کلمه  $c$  به عنوان کد کلمه  $c(x)$  با به کارگیری رابطه ۱ صحبت خواهیم نمود. با توسیع این مطلب، یک کد خطی را به عنوان زیر مجموعه‌ای از  $\mathbb{F}_q[x]/(x^n - 1)$  تفسیر می‌کنیم.

قضیه ۲.۶.۱. یک کد خطی  $C$  در  $\mathbb{F}_q^n$  دوری است اگر و تنها اگر  $C$  در  $\mathbb{F}_q[x]/(x^n - 1)$  یک ایده آل باشد. اثبات.

(۱) اگر  $C$  در  $\mathbb{F}_q[x]/(x^n - 1)$  دوری باشد و  $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$  یک کد کلمه باشد، آن‌گاه  $xc(x)$  نیز یک کد کلمه خواهد بود؛ یعنی:

$$(c_{n-1}, c_0, \dots, c_{n-2}) \in C.$$

(۲) برعکس، اگر  $C$  دوری باشد، آن‌گاه برای هر کد کلمه  $c(x)$ ، کد کلمه  $xc(x)$  نیز در  $C$  است؛ بنابراین،  $x^i c(x)$  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 ایده آل است.

قرارداد ۳.۶.۱. از اینجا به بعد، تنها کدهای دوری به طول  $n$  روی  $\mathbb{F}_q$  با شرط  $(n, q) = 1$  را در نظر می‌گیریم. برای مشاهده برخی مباحث تئوری در مورد کدهای دوری دودویی با طول زوج می‌توان به بخش ۶.۱۰ 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<sup>۳</sup> این کد دوری نامیده می‌شود. چندجمله‌ای مولد یک عامل  $x^n - 1$  است (چون در غیر این صورت، 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 ۳.۶.۱، 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 به صورت مضارب  $g(x)$  در پیمانه  $(x^n - 1)$ ، بیابیم.

مثال ۴.۶.۱. 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 به ترتیب دارای ابعاد ۳، ۳، ۴ و ۴ هستند؛ برای مثال، با در نظر 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 ۵.۶.۱. کد دوری تولیدشده توسط  $f_i(x)$ ، یک کد دوری ماکسیمال<sup>۴</sup> می‌باشد (چون یک ایده‌آل ماکسیمال می‌باشد) و با  $M_i^+$  نمایش داده می‌شود. کد تولیدشده توسط  $(x^n - 1)/f_i(x)$ ، کد دوری می‌نیمال<sup>۵</sup> نامیده می‌شود و با  $M_i^-$  نمایش داده می‌شود. کدهای دوری می‌نیمال، کدهای دوری تحویل‌ناپذیر<sup>۶</sup> نیز نامیده می‌شوند.

<sup>۳</sup> generator matrix

<sup>۴</sup> maximal cyclic code

<sup>۵</sup> minimal cyclic code

<sup>۶</sup> irreducible cyclic code

تعریف ۱.۶.۱ تضمین می‌کند که گروه خودریختی یک کد دوری  $C$ ، شامل گروه دوری تولیدشده توسط جای‌گشت:

$$i \rightarrow i + 1 \pmod n,$$

است. اما، چون  $a(x^q) = a(x)^q$  متعلق به همان کدی است که  $a(x)$  متعلق به آن است، می‌بینیم که جای‌گشت  $\pi_q$  تعریف شده، به صورت  $\pi_q(i) = qi \pmod n$ ، یعنی  $x \rightarrow x^q$ ، نیز یک کد دوری را به خودش تصویر می‌کند. اگر  $m$  از مرتبه  $q$  در پیمانه  $n$  باشد، آن‌گاه دو جای‌گشت  $i \rightarrow i + 1$  و  $\pi_q$  یک گروه با مرتبه  $mn$  مشمول در  $Aut(C)$  تولید می‌کنند.

## ۶.۲ ماتریس مولد و چندجمله‌ای بررسی

فرض کنید  $g(x)$ ، چندجمله‌ای مولد یک کد دوری  $C$  به طول  $n$  باشد. اگر  $g(x)$  دارای درجه  $n - k$  باشد، آن‌گاه کدکلمات  $g(x)$ ،  $xg(x)$ ،  $\dots$ ،  $x^{k-1}g(x)$  به وضوح تشکیل یک پایه برای  $C$  می‌دهند؛ یعنی  $C$  یک کد  $[n, k]$  است؛ بنابراین، اگر  $g(x) = g_0 + g_1x + \dots + g_{n-k}x^{n-k}$ ، آن‌گاه:

$$G = \begin{pmatrix} g_0 & g_1 & & g_{n-k} & \circ & \circ & \circ \\ \circ & g_0 & & g_{n-k-1} & g_{n-k} & \circ & \circ \\ \circ & \circ & & & & & \circ \\ \circ & \circ & & & & & g_{n-k} \end{pmatrix},$$

یک ماتریس مولد برای  $C$  است. معنای آن این است که ما یک دنباله اطلاعاتی  $(a_0, a_1, \dots, a_{k-1})$  را به صورت  $aG$  کد می‌کنیم که به شکل چندجمله‌ای:

$$(a_0 + a_1x + \dots + a_{k-1}x^{k-1})g(x),$$

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  $(a_0, a_1, \dots, a_{k-1})$  به صورت زیر کد می‌شود:

$(a_0, a_1, \dots, a_{k-1})x^{n-k}$  را بر  $g(x)$  تقسیم نموده و باقی‌مانده را از  $(a_0, a_1, \dots, a_{k-1})x^{n-k}$  کم نمایید که در نتیجه 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 اعمال است.

چون  $g(x)$  یک عامل  $x^n - 1$  است، چندجمله‌ای  $h(x) = h_0 + h_1x + \dots + h_kx^k$  وجود دارد؛ به طوری که  $g(x)h(x) = x^n - 1$  در  $(\mathbb{F}_q[x])$ . در حلقه  $\mathbb{F}_q[x]$  داریم  $g(x)h(x) = 0$  یعنی  $g_0h_i + g_1h_{i-1} + \dots + g_{n-k}h_{i-n+k} = 0$  برای  $i = 0, 1, \dots, n-1$ . در نتیجه:

$$H := \begin{pmatrix} 0 & 0 & 0 & h_k & \dots & h_1 & h_0 \\ 0 & 0 & h_k & & & h_1 & h_0 \\ \vdots & & & & & & \vdots \\ h_k & 0 & h_1 & h_0 & 0 & & 0 \end{pmatrix},$$

یک ماتریس بررسی توازن برای کد  $C$  است. ما  $h(x)$  را چندجمله‌ای بررسی  $C$  می‌نامیم. کد  $C$  شامل تمامی  $c(x)$  هایی است که  $c(x)h(x) = 0$ . 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  $g(x) = (x^n - 1)/f_i(x)$  را در نظر بگیرید، که در آن  $f_i(x)$  دارای درجه  $k$  می‌باشد. اگر  $a(x)$  و  $b(x)$ ، دو کدکلمه در  $M_i^-$  باشند به طوری که  $a(x)b(x) = 0$ ، آن‌گاه یکی از آنها باید بر  $f_i(x)$  بخش پذیر باشد؛ بنابراین، برابر با  $0$  است. چون  $M_i^-$  دارای هیچ عامل صفری نیست، یک میدان است؛ یعنی یک ریخت با  $\mathbb{F}_q^k$ . مخصوصاً، اگر قرار دهیم  $n = 2^k - 1$  و  $f_i(x)$  یک چندجمله‌ای اولیه از درجه  $k$  باشد، یک مثال جالب به دست می‌آید. در این حالت،  $n$  شیفیت 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  $2^{k-1}$  است (با استفاده از ۵.۳.۸). به عنوان یک نتیجه، می‌بینیم که برای هر عامل اولیه  $f(x)$  از  $x^n - 1$  (که در آن  $n = 2^k - 1$ )، چندجمله‌ای  $(x^n - 1)/f(x)$  دارای دقیقاً  $2^{k-1}$  ضریب مساوی با  $1$  است. یک نمونه با  $k = 3$  در مثال ۴.۶.۱ آورده شده است.

### ۶.۳ صفرهای یک کد دوری

فرض کنید  $x^n - 1 = f_1(x) \dots f_t(x)$  و  $\beta_i$  یک صفر از  $f_i(x)$  در میدان گسترش یافته‌ای از  $\mathbb{F}_q$  باشد. از این رو  $f_i(x)$  چندجمله‌ای می‌نیمال  $\beta_i$  است؛ بنابراین، کد ماکسیمال  $M_i^+$  چیزی نیست جز مجموعه چندجمله‌ای های  $c(x)$  به طوری که  $c(\beta_i) = 0$ . بنابراین، در حالت کلی، یک کد دوری می‌تواند با استفاده از این شرط این که تمامی کدکلمات دارای صفرهای مشخص شده‌ای هستند، تعیین شود. در

واقع، کافی است تا یک صفر  $\beta_i$  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  $\alpha_s, \dots, \alpha_2, \alpha_1$  شروع کنیم و یک کد  $C$  را به این صورت (تعریف کنیم که  $c(x) \in C$  اگر و تنها اگر  $c(\alpha_i) = 0$  برای  $i = 1, 2, \dots, s$ ، در این صورت  $C$  دوری است و چندجمله‌ای مولد  $C$ ، کوچک‌ترین مضرب مشترک چندجمله‌ای‌های  $\alpha_0, \alpha_1, \dots, \alpha_s$  است. فرض کنید که تمامی این صفرها متعلق به  $\mathbb{F}_{q^m}$  است (که می‌توانیم آن را به صورت یک فضای برداری  $\mathbb{F}_q^m$  نمایش دهیم). برای هر  $i$  می‌توانیم ماتریس  $m$  در  $n$  را با نمایش‌های برداری  $(\alpha_i, \alpha_i^2, \dots, \alpha_i^{n-1})$  به‌عنوان ستون‌ها در نظر 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  $c = (c_0, c_1, \dots, c_{n-1})$  بدان معنی است که  $c(\alpha_i) = 0$  برای  $i = 1, 2, \dots, s$ . سطرهای  $H$  لزوماً مستقل نمی‌باشند. ممکن است یک ماتریس بررسی‌توازن را از  $H$  با حذف برخی سطرها به دست 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  $\beta$  را یک ریشه  $n$ ام واحد در  $\mathbb{F}_{q^m}$  در نظر بگیرید. علاوه‌براین، فرض کنید  $(m, q - 1) = 1$ . در این صورت کد دوری:

$$C := \{c(x) : c(\beta) = 0\},$$

هم‌ارز با یک کد همینگ  $[n, n - m]$  روی  $\mathbb{F}_q$  است.

اثبات. چون:

$$n = (q - 1)(q^{m-2} + 2q^{m-3} + \dots + m - 1) + m,$$

داریم  $(n, q - 1) = (m, q - 1) = 1$ ؛ بنابراین،  $\beta^{i(q-1)} \neq 1$  برای  $i = 1, 2, \dots, n - 1$ ؛ یعنی  $\beta^i \notin \mathbb{F}_q$  برای  $i = 1, 2, \dots, n - 1$ . در نتیجه ستون‌های ماتریس  $H$ ، که در آن نمایش‌های  $(1, \beta, \beta^2, \dots, \beta^{n-1})$  به‌صورت بردارهایی در  $\mathbb{F}_q^m$  می‌باشند، دو به دو روی  $\mathbb{F}_q$  مستقل خطی هستند. بنابراین،  $H$  ماتریس بررسی‌توازن یک کد همینگ  $[n, n - m]$  است.  $\square$

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  $\mathbb{F}_{2^3}$  است. اگر  $\alpha$  یک عضو اولیه در این میدان باشد، آن‌گاه  $\alpha^{12} = \alpha^7$  و  $\beta := \alpha^7$  یک ریشه ۹ام اولیه

واحد می باشد. با استفاده از قضیه ۱۸.۱.۱ چندجمله‌ای—می‌نیمال  $\beta$  دارای ریشه‌های  $\beta, \beta^2, \beta^4, \beta^8$ ،  $\beta^{16} = \beta^7$  و  $\beta^{14} = \beta^5$  است. این چندجمله‌ای باید  $1 + x^3 + x^6 = (x^2 - 1)/(x^9 - 1)$  باشد (ارجاع به رابطه ۲۴.۱.۱)؛ بنابراین:

$$(x^9 - 1) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1) = f_1(x)f_2(x)f_3(x).$$

کد  $M_3^+$  دارای ستون‌های دوجه دو مستقل در  $H$  می‌باشد؛ یعنی کمترین—فاصله بزرگ‌تر یا مساوی ۳ است. چون  $M_i^+$  به وضوح شامل کدکلمات:

$$(c_0c_1c_2 \quad c_0c_1c_2 \quad c_0c_1c_2),$$

است، فوراً می‌بینیم که  $d = 3$ . کد  $M_i^-$  دارای چندجمله‌ای توازن  $1 + x^3 + x^6$  است، بنابراین، یک کد  $[6, 9]$  است. چون  $1 - x^3$  یک کدکلمه است، این فاصله برابر با ۲ است. اگر ما  $\mathbb{F}_3$  را با چندجمله‌ای  $1 + x + x^6$  بسازیم و سپس ماتریس  $H$  با ابعاد ۱۲ در ۹ را برای کد  $M_3^-$ ، با استفاده از روشی که قبلاً آن را در قضیه ۱.۶.۳ تشریح نمودیم، تشکیل دهیم، آنگاه این ماتریس تنها دارای ۶ سطر به صورت یک سطر تمام صفر، یک سطر تمام ۱، سطر  $(110 \quad 110 \quad 110)$  و چهار سطر  $(011 \quad 011 \quad 011)$  خواهد بود؛ بنابراین، با توجه به آن، یک ماتریس بررسی توازن ۳ در ۹ داریم. البته از  $1 + x^3 + x^6$  یک ماتریس بررسی توازن هم‌ارز با  $(I \quad I \quad I)$  داریم. خواننده می‌تواند مثال‌های با وضوح کمتر را به روشی مشابه حل نماید.

مثال ۳.۶.۳. چندجمله‌ای  $1 - x^8$  روی  $\mathbb{F}_3$  را در نظر بگیرید. اگر  $\beta$  یک ۸ امین ریشه واحد باشد، آنگاه  $\beta^9 = \beta$ ؛ بنابراین،  $1 - x^8$  باید حاصل ضرب  $(x - 1), (x + 1)$  و سه چندجمله‌ای تحویل‌ناپذیر از درجه ۲ باشد. با جای‌گذاری ۰، ۱، ۲ در  $x^2 + ax + b$ ، می‌بینیم که تنها چندجمله‌ای‌های تحویل‌ناپذیر از درجه ۲ در  $\mathbb{F}_3[x]$  به صورت  $x^2 + 1, x^2 + x + 1, x^2 + 2x + 2$  و  $x^2 + x^2 + 2$  هستند؛ بنابراین، تجزیه  $1 - x^8$  را می‌دانیم. کد دوری با ماتریس مولد  $g(x) := (x^2 + 1)(x^2 + x + 2)$  دارای کمترین—فاصله کمتر یا مساوی ۴ است، چون  $g(x)$  دارای وزن ۴ است. در بخش ۶.۶، روشی آسان برای اثبات این‌که ۴ کمترین—فاصله این کد است، ارائه خواهیم داد.

## ۶.۴ خودتوان یک کد دوری

در بسیاری از کاربردها، مزیت جای‌گزین کردن چندجمله‌ای مولد یک کد دوری با یک چندجمله‌ای  $c(x)$  که خودتوان<sup>۷</sup> نام دارد، اثبات شده است. قضیه زیر، این تعریف را دربر گرفته است.

<sup>۷</sup> idempotent

قضیه ۱.۶.۴. فرض کنید  $C$  یک کد دوری باشد؛ در این صورت یک کدکلمه منحصر به فرد  $c(x)$  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  $g(x)h(x) = x^n - 1$  در  $\mathbb{F}_q[x]$ . چون  $x^n - 1$  دارای هیچ ریشه مضاعفی نمی‌باشد، داریم  $(g(x), h(x)) = 1$ ؛ بنابراین، چندجمله‌ای‌های  $a(x)$  و  $b(x)$  وجود دارند؛ به طوری که  $a(x)g(x) + b(x)h(x) = 1$ . حال تعریف کنید:

$$c(x) := a(x)g(x) = 1 - b(x)h(x).$$

به وضوح  $c(x)$  یک کدکلمه در  $C$  می‌باشد. علاوه بر این، اگر  $p(x)g(x)$  یک کدکلمه در  $C$  باشد، آن‌گاه:

$$c(x)p(x)g(x) = p(x)g(x) - b(x)h(x)p(x)g(x)$$

$$\equiv p(x)g(x) \pmod{(x^n - 1)}.$$

چون  $c(x)$  یک عضو همانی برای  $C$  می‌باشد، بنابراین، یکتاست.  $\square$

چون  $c^2(x) = c(x)$ ، این کدکلمه خودتوان<sup>۸</sup> می‌باشد. البته، عناصر دیگری در  $C$  می‌توانند وجود داشته باشند به طوری که با مربع خودشان برابر باشند، اما تنها یکی از اینها عضو همانی کد است. چون هر کدکلمه می‌تواند به صورت  $v(x)c(x)$  نوشته شود؛ یعنی مضربی از  $c(x)$ ، می‌بینیم که  $c(x)$  ایده آل  $C$  را تولید می‌کند.

بیاید تجزیه  $x^n - 1 = f_1(x) \cdots f_t(x)$  را یک بار دیگر در نظر بگیریم. حال قرار می‌دهیم  $q = 2$ . از قضیه ۱۸.۱.۱ می‌دانیم که این عوامل متناظر با افراز مجموعه  $\{0, 1, \dots, n-1\}$  به هم مجموعه‌های دایره‌بر<sup>۹</sup>:  $\{0\}$ ،  $\{1, 2, 4, \dots, 2^r\}$ ،  $\dots$ ،  $\{a, 2a, \dots, 2^s a\}$  می‌باشند که در آن  $s$  کمترین توانی است که  $a(2^{s+1} - 1) \equiv 0 \pmod{n}$ . در مثال ۲.۶.۳ این تجزیه برابر  $\{0\}$ ،  $\{1, 2, 4, 8, 7, 5\}$  و  $\{3, 6\}$  با  $n = 9$  است. از طرف دیگر، واضح است که اگر یک خودتوان  $c(x)$  شامل جمله  $x^i$  باشد، آن‌گاه شامل جمله  $x^{2^i}$  نیز هست؛ بنابراین، یک خودتوان باید مجموعی از خودتوان‌ها به شکل  $x^a + x^{2a} + \dots + x^{2^s a}$  باشد، که در آن  $\{a, 2a, \dots, 2^s a\}$  یکی از هم مجموعه‌های دایره‌بر است. چون دقیقاً  $2^t$  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  $x^n - 1$  تولید کنیم.

<sup>۸</sup> idempotent

<sup>۹</sup> cyclotomic cosets

کمی جلوتر، این نظریه را تعمیم می‌دهیم. مجدداً خود را روی  $q = 2$  محدود می‌کنیم. در ابتدا مشاهده می‌کنید که از اثبات قضیه ۱.۶.۴ 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 ۲.۶.۴. خودتوان یک کد دوری تحویل‌ناپذیر  $M_i^-$ ، یک خودتوان اولیه  $1^\circ$  نامیده شده و با  $\theta_i(x)$  نشان داده می‌شود؛ برای مثال، در ۴.۶.۱ چندجمله‌ای  $g(x) = x^6 + x^5 + x^3 + 1$  یک خودتوان اولیه است.

فرض کنید  $\alpha$  یک  $n$  امین ریشه اولیه واحد در یک میدان گسترش یافته  $\mathbb{F}_2$  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، به طوری 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  $\{a, 2a, \dots\}$  باشد. چنین خودتوان اولیه‌ای اغلب با  $\theta_a$  نمایش داده می‌شود؛ یعنی در تعریف ۲.۶.۴ اندیس  $i$  از نماینده‌های هم‌مجموعه‌های دایره‌بر متفاوت انتخاب شده است؛ برای مثال، در نظر بگیرید  $n = 15$  و  $\alpha$  را ریشه‌ای از  $x^4 + x + 1$  در نظر بگیرید؛ در این صورت، خودتوان اولیه متعلق به کد دوری می‌نیمال با چندجمله‌ای بررسی  $x^4 + x + 1$  با  $\theta_1$  نمایش داده می‌شود و در این حالت  $\theta_{-1}$  متناظر با عناصر ناصفر  $\alpha^{-1}, \alpha^{-2}, \alpha^{-4}, \alpha^{-8}$  است؛ یعنی با چندجمله‌ای بررسی  $1 + x^3 + x^4$ . در ادامه، اگر چنین  $\alpha$  ای را ثابت فرض نکرده باشیم، آن‌گاه برای سادگی کدهای دوری تحویل‌ناپذیر را به صورت  $M_1^-, M_2^-, \dots, M_t^-$  می‌شماریم.

قضیه ۳.۶.۴. اگر  $C_1$  و  $C_2$  کدهای دوری با خودتوان‌های  $c_1(x)$  و  $c_2(x)$  باشند، آن‌گاه:

$$(1) \quad C_1 \cap C_2 \text{ دارای خودتوان } c_1(x)c_2(x) \text{ می‌باشد؛}$$

$$(2) \quad C_1 + C_2, \text{ یعنی مجموعه تمامی کلمات } a + b \text{ با } a \in C_1 \text{ و } b \in C_2, \text{ دارای خودتوان } c_1(x) + c_2(x) + c_1(x)c_2(x) \text{ است.}$$

اثبات.

(۱) یک نتیجه بدیهی از قضیه ۱.۶.۴ است.



(۲) به طریق مشابه نتیجه می‌شود، چرا که به‌وضوح  $c_1(x)c_2(x) + c_2(x) + c_1(x)$  در  $C_1 + C_2$  است و مجدداً به آسانی 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:

$$(۱) \quad \theta_i(x)\theta_j(x) = 0 \quad \text{اگر } i \neq j$$

$$(۲) \quad \sum_{i=1}^t \theta_i(x) = 1$$

$$(۳) \quad 1 + \theta_{i_1}(x) + \theta_{i_2}(x) + \dots + \theta_{i_r}(x) \quad \text{خودتوان کد با مولد } f_{i_1}(x)f_{i_2}(x)\dots f_{i_r}(x) \text{ است.}$$

اثبات.

$$(۱) \quad \text{از قضیه ۳.۶.۴ قسمت (۱) نتیجه می‌شود؛ زیرا } M_i^- \cap M_j^- = \{0\}$$

(۲) از قضیه ۳.۶.۴ قسمت (۲) و قضیه ۴.۶.۴ قسمت (۱) نتیجه می‌شود؛ زیرا  $M_1^- + M_2^- + \dots + M_t^-$  مجموعه تمامی کلمات به طول  $n$  است؛ و سرانجام:

(۳) با مشاهده این که چندجمله‌ای توازن  $M_{i_1}^- + \dots + M_{i_r}^-$  برابر با  $f_{i_1}(x)f_{i_2}(x)\dots f_{i_r}(x)$  است، نتیجه می‌شود.

□

با به‌کارگیری این قضایا، یافتن خودتوان‌های اولیه کار زیاد سختی نیست؛ در این صورت فرد روش آسانی برای یافتن خودتوان‌های یک کد دارد، اگر مولد کد به صورت  $f_{i_1}f_{i_2}\dots f_{i_t}$  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 در نظر بگیرید. فرض کنید  $g(x)h(x) = x^n - 1$ . 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 این صورت برابر با  $0$  است. به عنوان یک مثال؛ کد کمترین به طول ۱۵ با چندجمله‌ای توازن  $x^4 + x + 1$  را در نظر بگیرید. خودتوان  $\theta_1$  برابر با  $(x^4 + x + 1)/(x^{15} - 1)$  است.

تناظر زیر بین خودتوان‌ها، تمرین مفید دیگری است. مثال بالا می‌تواند به عنوان یک توصیف به کار رود. فرض کنید  $f(x)$  یک مقسوم‌علیه  $x^n - 1$  باشد که در آن  $n = 2^k - 1$ . فرض کنید  $\alpha$  یک عضو اولیه از  $\mathbb{F}_{2^k}$  طوری باشد که  $f(\alpha) = 0$ . خودتوان‌های اولیه  $\theta_1, \dots, \theta_{n-1}$ ، متناظر با هم مجموعه‌های دایره‌بر  $\{1, 2, \dots, 2^{k-1}\}$ ، به ترتیب  $\{-1, -2, \dots, -2^{k-1}\}$  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  $l = 0, 1, \dots, n-1$  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 حاصل ضرب داخلی برابر با  $0$  است، مگر این که  $\alpha^{l+2^j} = 1$ ؛ بنابراین،  $\varphi(\alpha^l) = 1$  اگر برای یک مقدار  $j$  داشته باشیم  $l = -2^j$  و در غیر این صورت  $\varphi(\alpha^l) = 0$ . این مطلب، ادعا را ثابت می‌کند.

خودتوان‌ها در بسیاری جاها به کار رفته‌اند، به طور نمونه در شمارنده‌های وزنی. ما در این موضوع وارد نشده، اما خواننده را به مراجع [۴۲] و [۴۶] ارجاع می‌دهیم. نظریه‌ای که در این بخش به آن پرداختیم، به طور خاص قضیه ۴.۶.۴، حالت خاصی از نظریه عمومی خودتوان‌ها برای جبرهای شبه-ساده است. خواننده را به مرجع [۱۶] ارجاع می‌دهیم.

## ۶.۵ نمایش‌های دیگر کدهای دوری

چندین روش دیگر برای نمایش کدهای دوری به غیر از روش استاندارد که در بخش ۶.۱ 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 به کار می‌گیرد (ارجاع به تعریف ۲۵.۱.۱).

قضیه ۱.۶.۵. فرض کنید  $k$  رتبه ضربی  $p$  در پیمانه  $n$  باشد؛ یعنی  $q = p^k$  و  $\beta$  یک  $n$ امین ریشه اولیه واحد باشد، آن گاه مجموعه:

$$V := \{c(\xi) := (Tr(\xi), Tr(\xi\beta), \dots, Tr(\xi\beta^{n-1})) \mid \xi \in \mathbb{F}_q\},$$

یک کد دوری تحویل ناپذیر  $[n, k]$  روی  $\mathbb{F}_p$  است.

اثبات. با به کارگیری قضیه ۲۶.۱.۱،  $V$  یک کد خطی است. سپس، مشاهده می کنید که  $c(\xi\beta^{-1})$  یک شیفت دوری  $c(\xi)$  می باشد. بنابراین،  $V$  یک کد دوری است. چون  $\beta$  متعلق به هیچ زیرمیدانی از  $\mathbb{F}_q$  نیست، می دانیم که  $\beta$  یک ریشه از یک چندجمله ای تحویل ناپذیر  $h(x) = h_0 + h_1x + \dots + h_kx^k$  از درجه  $k$  است. اگر  $c(\xi) = (c_0, c_1, \dots, c_{n-1})$  آن گاه:

$$\sum_{i=0}^k c_i h_i = Tr(\xi h(\beta)) = Tr(\circ) = \circ,$$

یعنی، یک معادله بررسی توازن برای کد  $V$  داریم.

چون  $h(x)$  تحویل ناپذیر است، می بینیم که  $x^k h(x^{-1})$  چندجمله ای بررسی برای  $V$  است؛ بنابراین،  $V$  یک کد  $[n, k]$  دوری تحویل ناپذیر است.  $\square$

حال یک نمونه گسسته از تبدیل فوریه را معرفی خواهیم نمود که در نظریه کدگذاری همیشه از آن به عنوان چندجمله ای ماتسون-سولومن<sup>۱۱</sup> تعبیر می شود. فرض کنید  $\beta$  یک  $n$ امین ریشه اولیه واحد در میدان گسترش یافته  $\mathcal{F}$  از  $\mathbb{F}_q$  باشد. فرض کنید  $T$  مجموعه چندجمله ای های روی  $\mathcal{F}$  با درجه حداکثر  $n-1$  باشد. نگاشت  $\Phi: T \rightarrow T$  را به صورت زیر تعریف می کنیم. فرض کنید  $a(x) \in T$ . در این صورت  $A(X) = (\Phi a)(X)$  به صورت زیر تعریف شده است:

$$A(X) := \sum_{j=1}^n a(\beta^j) X^{n-j}. \quad (2)$$

اگر  $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$  آن گاه چندجمله ای  $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  چندجمله ای ماتسون-سولومن بردار  $\mathbf{a}$  نامیده می شود.

لم ۲.۶.۵. معکوس  $\Phi$  برابر با:

$$a(x) = n^{-1}(\Phi A)(x^{-1}) \bmod x^n - 1,$$

است.

<sup>۱۱</sup>Mattson-Solomon polynomial

اثبات.

$$A(\beta^k) = \sum_{j=1}^n \sum_{i=0}^{n-1} a_i \beta^{ij} \beta^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=1}^n \beta^{(i-k)j} = na_k.$$

□

فرض کنید  $\circ$  حاصل ضرب چندجمله‌ای‌ها در پیمانه  $1 - x^n$  باشد و  $*$  به صورت زیر تعریف شده باشد:

$$\left(\sum a_i x^i\right) * \left(\sum b_i x^i\right) := \sum a_i b_i x^i.$$

در این صورت به آسانی دیده می‌شود که  $\Phi$  یک یک‌ریختی از حلقه  $(T, +, \circ)$  به روی حلقه  $(T, +, *)$  می‌باشد.

حال بیایید این چندجمله‌ای‌ها را برای مطالعه کدهای دوری به کار گیریم.

لم ۳.۶.۵. فرض کنید  $V$  یک کد دوری روی  $\mathbb{F}_q$  تولیدشده توسط:

$$g(x) = \prod_{k \in K} (x - \beta^k),$$

باشد. فرض کنید  $K \subset \{1, 2, \dots, d-1\}$  و  $\mathbf{a} \in V$ ; در این صورت 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 ۴.۶.۵. اگر  $r$  تا  $n$ مین 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 ۳.۶.۵ است.

□

هم‌چنین می‌توانیم ارتباطی بین کدهای دوری و نظریه دنباله‌های بازگشتی خطی<sup>۱۲</sup> که مطالب گسترده‌ای درباره آن وجود دارد (ر.ک. مرجع [۶۱])، برقرار سازیم. یک دنباله بازگشتی خطی با عناصر در  $\mathbb{F}_q$  توسط یک دنباله اولیه  $a_0, a_1, \dots, a_{k-1}$  و یک رابطه بازگشتی:

$$a_l + \sum_{i=1}^k b_i a_{l-i} = 0, \quad (l \geq k), \quad (3)$$

<sup>۱۲</sup>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  $\beta$  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  $\beta_1, \beta_2, \dots, \beta_k$  در یک میدان گسترش یافته  $\mathbb{F}_q$  است؛ در این صورت اگر  $c_1, c_2, \dots, c_k$  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 به گونه‌ای انتخاب نماییم که  $a_0, a_1, \dots, a_{k-1}$  دارای مقادیر مشخص شده باشند. این مقادیر برای حل یک دستگاه با  $k$  معادله خطی کاربرد دارد، که در آن دترمینان ضرایب، دترمینان واندرموند:

$$\begin{pmatrix} 1 & 1 & 1 \\ \beta_1 & \beta_2 & \beta_k \\ \beta_1^2 & \beta_2^2 & \beta_k^2 \\ \dots & \dots & \dots \\ \beta_1^{k-1} & \beta_2^{k-1} & \beta_k^{k-1} \end{pmatrix} = \prod_{i>j} (\beta_i - \beta_j) \neq 0. \quad (4)$$

است؛ بنابراین، می‌توانیم در واقع دنباله مورد نیاز را بیاییم.

فرض کنید  $h(x)$  یک عامل  $x^n - 1$  است (مجدداً  $(n, q) = 1$ )؛ در این صورت دنباله بازگشتی خطی، متناوب با دوره تناوب عاملی از  $n$  است. حال تمامی دنباله‌های جزئی  $(a_0, a_1, \dots, a_{n-1})$  را در نظر بگیرید، که در آن  $(a_0, a_1, \dots, a_{n-1})$  متعلق به  $\mathbb{F}_q^k$  می‌باشد؛ در این صورت ما یک کد  $[n, k]$  دوری با  $x^k h(x^{-1})$  به عنوان چندجمله‌ای بررسی داریم؛ بنابراین:

$$C = \{(a_0, \dots, a_{n-1}) \mid a_l = \sum_{i=1}^k c_i \beta_i^l (0 \leq l < n), (c_1, c_2, \dots, c_k) \in \mathbb{F}_q^k\},$$

نمایش دیگری از یک کد دوری می‌باشد.

## ۶.۶ کدهای BCH

یک کلاس مهم از کدهای دوری، که هنوز در عمل بسیار به کار می‌رود، توسط بویس<sup>۱۳</sup> و چادوری<sup>۱۴</sup> (۱۹۶۰) و به طور مستقل توسط هکنگم<sup>۱۵</sup> کشف شد. این کدها به کدهای BCH معروف هستند.

تعریف ۱.۶.۶. یک کد دوری به طول  $n$  روی  $\mathbb{F}_q$ ، کد BCH با فاصله طراحی شده<sup>۱۶</sup>  $\delta$  می‌باشد، اگر مولد آن  $g(x)$  کوچک‌ترین مضرب مشترک چندجمله‌ای‌های  $\beta^l, \beta^{l+1}, \dots, \beta^{l+\delta-2}$  برای یک  $l$  باشد که در آن  $\beta$  یک  $n$ امین ریشه اولیه واحد است. معمولاً قرار می‌دهیم  $l = 1$  (برخی اوقات به آن، یک کد BCH

<sup>۱۳</sup>R. C. Bose

<sup>۱۴</sup>D. K. Ray-Chaudhuri

<sup>۱۵</sup>Hocquenghem

<sup>۱۶</sup>designed distance

با مفهوم کم‌عرض<sup>۱۷</sup> اطلاق می‌شود). اگر  $n = q^m - 1$ ، یعنی  $\beta$  یک عضو اولیه  $\mathbb{F}_{q^m}$  باشد، آن‌گاه کد BCH، اولیه نامیده می‌شود.

اصطلاح "فاصله طراحی شده" توسط قضیه زیر تشریح شده است.

قضیه ۲.۶.۶. کمترین فاصله یک کد BCH با فاصله طراحی شده  $d$  حداقل برابر با  $d$  است.

اثبات اول. به روشی مشابه با بخش ۶.۳، ماتریس  $m(d-1)$  در  $n$ ،  $H$  را تشکیل می‌دهیم:

$$H := \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \beta^{(n-1)(l+1)} \\ \dots & \dots & \dots & \dots \\ 1 & \beta^{l+d-2} & \beta^{2(l+d-2)} & \beta^{(n-1)(l+d-2)} \end{pmatrix},$$

که در آن هر درایه به‌عنوان یک بردار ستونی به طول  $m$  روی  $\mathbb{F}_q$  تعبیر می‌شود. کلمه  $c$  در کد BCH قرار دارد اگر و تنها اگر  $cH^T = 0$ .  $m(d-1)$  سطر  $H$  لزوماً مستقل نیستند.  $d-1$  ستون دلخواه از  $H$  را در نظر گرفته و فرض کنید  $\beta^{i_1}, \dots, \beta^{i_{d-1}}$  عناصر بالای این ستون‌ها باشند. دترمینان زیرماتریس  $H$ ، به دست آمده در این روش، مجدداً یک دترمینان و اندرمنند (ارجاع به رابطه ۴) با مقدار  $\beta^{(i_1 + \dots + i_{d-1})l} \prod_{r>s} (\beta^{i_r} - \beta^{i_s})$  است، چون  $\beta$  یک  $m$ امین ریشه واحد است. بنابراین، هر  $d-1$  ستون  $H$  به‌طور خطی مستقل می‌باشند؛ بنابراین، یک کد کلمه  $c \neq 0$  دارای وزن بزرگ‌تر یا مساوی  $d$  است.

اثبات دوم. قرار می‌دهیم  $l = 1$ . با به‌کارگیری لم ۳.۶.۵، درجه چندجمله‌ای ماتسون-سولومن کد کلمه  $c$ ، حداکثر  $n-d$  است؛ بنابراین، در قضیه ۴.۶.۵ داریم  $r \leq n-d$ ؛ یعنی  $w(c) \geq d$ .

□

تذکر ۳.۶.۶. معمولاً قضیه ۲.۶.۶، کران BCH نامیده می‌شود. از اینجا به بعد، معمولاً کدهای BCH با مفهوم کم‌عرض را در نظر می‌گیریم. اگر با  $l = 0$  به جای  $l = 1$  شروع کنیم، آن‌گاه زیرکد با وزن زوج از کد با مفهوم کم‌عرض را در نظر گرفته‌ایم.

<sup>۱۷</sup>a narrow-sense BCH code

مثال ۴.۶.۶. فرض کنید  $m = 5$ ,  $n = 31$ ,  $q = 2$  و  $d = 8$ . فرض کنید  $\alpha$  یک عضو اولیه از  $\mathbb{F}_{32}$  باشد. چند جمله‌ای  $\alpha$ —می‌نیمال برابر است با:

$$(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}).$$

به روش مشابه چند جمله‌ای  $\alpha$ —می‌نیمال  $m_3(x)$  را داریم؛ اما:

$$m_5(x) = (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^9)(x - \alpha^{18}) = m_9(x).$$

ثابت می‌شود  $g(x)$  کوچک‌ترین مضرب مشترک  $m_1(x)$ ,  $m_3(x)$ ,  $m_5(x)$ ,  $m_7(x)$  و  $m_9(x)$  است؛ بنابراین، کمترین—فاصله کد BCH اولیه با فاصله طراحی شده ۸ (که به وضوح 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<sup>۱۸</sup> و ویلسن<sup>۱۹</sup> در مرجع [۷۶] آمده است. بهبودهای اخیر قضیه ۲.۶.۶ نتیجه این روش می‌باشد.

اگر  $A = \{\alpha^{i_1}, \dots, \alpha^{i_l}\}$  مجموعه  $n$  امین ریشه‌های واحد باشد؛ به طوری که برای یک کد دوری به طول  $n$  داشته باشیم:

$$c(x) \in C \Leftrightarrow \forall \xi \in A [c(\xi) = 0],$$

آن‌گاه خواهیم گفت  $A$  یک مجموعه تعریف  $2^\circ$  برای  $C$  است. اگر  $A$  بزرگ‌ترین مجموعه تعریف برای  $C$  باشد، آن‌گاه  $A$  را کامل<sup>۲۱</sup> می‌نامیم.

تعریف ۵.۶.۶  $M(A)$  یا  $M(\alpha^{i_1}, \dots, \alpha^{i_l})$  را ماتریسی با اندازه  $l$  در  $n$  تعریف می‌کنیم که سطر  $k$ ام آن به صورت  $1, \alpha^{i_k}, \alpha^{2i_k}, \dots, \alpha^{(n-1)i_k}$  باشد؛ یعنی:

$$M(\alpha^{i_1}, \dots, \alpha^{i_l}) = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{i_l} & \alpha^{2i_l} & \dots & \alpha^{(n-1)i_l} \end{pmatrix}.$$

$M(A)$  را ماتریس بررسی توازن 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).

<sup>۱۸</sup>J. H. van Lint

<sup>۱۹</sup>R. M. Wilson

<sup>۲۰</sup>defining set

<sup>۲۱</sup>complete

تعریف ۶.۶.۶. مجموعه  $A = \{\alpha^{i_1}, \dots, \alpha^{i_l}\}$ ، مجموعه متوالی  ${}^{۲۲}$  به طول  $n$  نامیده می‌شود، اگر  $n$  امین ریشه واحد  $\beta$  و توان  $i$  وجود داشته باشد، به طوری که  $A = \{\beta^i, \beta^{i+1}, \dots, \beta^{i+l-1}\}$ . بنابراین، قضیه ۲.۶.۶ بیان می‌کند که اگر یک مجموعه تعریف  $A$  برای یک کد دوری شامل یک مجموعه متوالی به طول  $l - 1$  باشد، آن‌گاه کمترین فاصله حداقل برابر با  $d$  است. یک نتیجه از اثبات قضیه ۲.۶.۶، لم زیر است.

لم ۷.۶.۶. اگر  $A$  یک مجموعه متوالی به طول  $l$  باشد، آن‌گاه زیرماتریس  $M(A)$ ، حاصل از در نظر گرفتن  $l$  ستون دلخواه، دارای رتبه  $l$  است. در ادامه نتیجه زیر از این لم را به کار خواهیم برد.

نتیجه‌گیری ۸.۶.۶. اگر  $\beta$  یک  $n$  امین ریشه اولیه واحد باشد و

$$i_1 < i_2 < \dots < i_k = i_1 + t - 1,$$

آن‌گاه اگر هر  $t$  ستون  $M(\beta^{i_1}, \beta^{i_2}, \dots, \beta^{i_k})$  را در نظر بگیریم، ماتریس به دست آمده دارای رتبه  $k$  می‌باشد.

حال نماد زیر را معرفی می‌کنیم:

$$AB := \{\xi\eta \mid \xi \in A, \eta \in B\}$$

در ادامه، عمل‌گر حاصل ضربی برای ماتریس‌ها در نظر می‌گیریم که در موقعیت خاصی که این ماتریس‌ها، ماتریس بررسی توازن به شکل  $M(A)$  تعریف شده در ۵.۶.۶ هستند، به کار خواهد رفت.

تعریف ۹.۶.۶. ماتریس  $A * B$  ماتریسی است که سطرهای آن تمامی حاصل ضرب‌های  $ab$  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 در نظر بگیرید.

لم ۱۰.۶.۶. اگر یک ترکیب خطی از تمام ستون‌های  $A * B$  با ضرایب ناصفر برابر با  $0$  باشد، آن‌گاه:

$$\text{rank}(A) + \text{rank}(B) \leq n.$$

<sup>۲۲</sup>consecutive set



اثبات. اگر ضرایب موجود در این ترکیب خطی برابر با  $\lambda_j$  ( $j = 1, \dots, n$ ) باشند، آن گاه ستون  $j$ ام  $B$  را در  $\lambda_j$  ضرب کنید. این کار، ماتریس  $B'$  با رتبه مشابه با رتبه  $B$  را تولید خواهد کرد. شرط لم بیان می کند که هر سطر  $A$  دارای ضرب داخلی صفر با هر سطر  $B'$  است. چون این مطلب ایجاب می کند  $\square$   $rank(A) + rank(B') \leq n$  آنچه را می خواستیم، انجام داده ایم.

حال در موقعیتی هستیم که قضیه ای را بیان کنیم که ما را قادر به یافتن کمترین—فاصله تعداد زیادی از کدهای دوری می سازد. اگر  $c$  یک کد کلمه در یک کد دوری باشد، آن گاه محل  $c$  از  $I$  مجموعه مکان های مختصات  $i$  است؛ به طوری که  $c_i \neq 0$ . اگر  $A$  یک ماتریس باشد، آن گاه  $A_I$  معرف زیرماتریس حاصل از حذف مکان هایی است که متعلق به  $I$  نیستند.

قضیه ۱۱.۶.۶. فرض کنید  $A$  و  $B$  ماتریس هایی با درایه هایی از یک میدان  $\mathbb{F}$  باشند. فرض کنید  $A * B$  یک ماتریس بررسی توازن برای کد  $C$  روی  $\mathbb{F}$  باشد. اگر  $I$  محل کد کلمه ای در  $C$  باشد، آن گاه:

$$rank(A_I) + rank(B_I) \leq |I|.$$

اثبات. این مطلب نتیجه فوری از لم ۱۰.۶.۶ است.  $\square$

این قضیه را به صورت زیر به کار خواهیم برد. لم ۷.۶.۶ به ما اجازه خواهد داد تا درباره رتبه ماتریس های مناسب از نوع  $A_I$ ، به ترتیب  $B_I$ ، چیزی بگوییم. اگر مجموع این رتبه ها بیشتر از  $|I|$ ، برای هر زیرمجموعه  $I$  از  $\{1, 2, \dots, n\}$  با اندازه کمتر از  $\delta$ ، باشد، آن گاه این کد دارای کمترین—فاصله حداقل  $\delta$  است.

مثال ۱۲.۶.۶. در اینجا روشی را با استفاده از اثبات کران معروف به روس<sup>۲۴</sup> تشریح می کنیم. این کران بیان می کند که اگر  $A$  یک مجموعه تعریف برای یک کد دوری با کمترین—فاصله  $d_A$  باشد و اگر  $B$  مجموعه ریشه های  $n$ ام واحد باشد، به طوری که کوچک ترین مجموعه متوالی که شامل  $B$  است دارای اندازه کمتر یا مساوی  $|B| + d_A - 2$  باشد، آن گاه کد با مجموعه تعریف  $AB$  دارای کمترین—فاصله  $d \geq |B| + d_A - 1$  است.

برای اثبات این مطلب، در ابتدا مشاهده می کنید که:

$$rank(M(A)_I) = \begin{cases} |I|, & \text{برای } |I| < d_A \\ \geq d_A - 1, & \text{برای } |I| \geq d_A \end{cases}$$

<sup>۲۳</sup>support

<sup>۲۴</sup>Roos bound

نتیجه ۸.۶.۶ اطلاعاتی در مورد رتبه زیرماتریس‌های  $M(A)$  به ما آرایه می‌دهد؛ یعنی:

$$\text{rank}(M(B)_I) \geq \begin{cases} 1, & |I| < d_A \\ |I| - d_A + 2, & d_A \geq |I| \geq |B| + d_A - 2 \end{cases}$$

حال قضیه ۱۱.۶.۶ را به کار می‌بریم. از مطلب بالا داریم:

$$\text{rank}(M(A)_I) + \text{rank}(M(B)_I) > |I|. \quad |I| < |B| + d_A - 2 \text{ برای}$$

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 ۱۳.۶.۶. این کران توسط روس<sup>۲۵</sup> [۸۰] معرفی شده است. حالت خاصی که  $B$  یک مجموعه متوالی است، توسط هارتمن<sup>۲۶</sup> و تزینگ<sup>۲۷</sup> در سال ۱۹۷۲، مرجع [۳۳]، اثبات شده است.

مثال ۱۴.۶.۶. کد دوری  $C$  به طول ۳۵ با مولد:

$$g(x) = m_1(x)m_5(x)m_7(x),$$

را در نظر بگیرید. اگر  $\alpha$  یک ۳۵امین ریشه اولیه واحد باشد، آنگاه مجموعه تعریف  $C$  شامل مجموعه  $\{23, 22, 21, 20, 11, 10, 9, 8, 7\}$  را در نظر بگیرید. این مجموعه می‌تواند به صورت  $AB$  نوشته شود، که در آن  $A = \{\alpha^i \mid i = 7, 8, 9, 10\}$  و  $B = \{\beta^j \mid j = 0, 3, 4\}$  با  $\beta = \alpha^{12}$  (نیز یک ۳۵امین ریشه اولیه واحد). مجموعه  $A$ ، مجموعه تعریف یک کد دوری با کمترین فاصله  $d_A = 5$  است. مجموعه  $B$  مشمول در مجموعه متوالی با اندازه ۵ است. شرط روی  $|B|$  از مثال ۱۲.۶.۶ برقرار است. در نتیجه  $C$  دارای کمترین فاصله حداقل  $7 = 5 + 3 - 1$  است. این مقدار در واقع کمترین فاصله این کد است. توجه دارید که کران BCH تنها نشان می‌دهد که کمترین فاصله حداقل برابر ۶ است. قبل از آرایه یکی از زیباترین مثال‌ها از روش خود، حالت خاصی از یک قضیه را که توسط مک‌الیس<sup>۲۸</sup> بیان شده است، اثبات می‌کنیم.

<sup>۲۵</sup>C. Roos

<sup>۲۶</sup>C. R. P. Hartmann

<sup>۲۷</sup>K. K. Tzeng

<sup>۲۸</sup>R. J. McEliece

لم ۱۵.۶.۶. فرض کنید  $C$  یک کد دودویی دوری به طول  $n$  با مجموعه تعریف کامل  $R$  باشد. فرض کنید حاصل ضرب هر دو ریشه  $m$ م واحدی که در  $R$  نباشند، برابر با ۱ نباشد؛ در این صورت وزن هر کدکلمه در  $C$  بر ۴ بخش پذیر است.

اثبات. واضح است که  $1 \in R$  و برای هر ریشه  $m$ م واحد  $\gamma$  داریم  $\gamma \in R$  یا  $\gamma^{-1} \in R$ . فرض کنید  $c(x) = x^{i_1} + x^{i_2} + \dots + x^{i_k}$  یک کدکلمه باشد. چون  $1 \in R$ ،  $k$  باید زوج باشد. از آنجا که  $c(x)c(x^{-1})$  برای هر  $m$ مین ریشه واحد، صفر است نتیجه می گیریم که آن برابر با چندجمله ای صفر است. اگر  $x^{i-j} = x^{l-m}$ ، آن گاه  $x^{j-i} = x^{m-l}$ ؛ یعنی در حاصل ضرب  $c(x)c(x^{-1})$ ، هر بار چهار جمله حذف می شوند.  $k$  جمله برابر با ۱ وجود دارد؛ بنابراین،  $k(k-1) \equiv 0 \pmod{4}$ . بنابراین،  $4 | k$ .  $\square$

نتیجه ای از لم ۱۵.۶.۶ این است که دوگان کد  $C$  از کد BCH اولیه با طول ۱۲۷ و فاصله طراحی شده ۱۱ دارای کمترین فاصله بخش پذیر 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 کوتاه شده کد رید-مولر  $R(2, 7)$  است، کمترین فاصله آن حداکثر برابر ۳۲ می باشد. حال نشان خواهیم داد که روش بیان شده در بالا نشان می دهد  $d \geq 30$ ، بنابراین، با اثبات این مطلب در واقع نشان داده ایم که  $d = 32$ .

مثال ۱۶.۶.۶. فرض کنید  $R$  مجموعه تعریف  $C$  باشد. توجه دارید که  $R$  شامل مجموعه های  $\{\alpha^i \mid 81 \leq i \leq 95\}$ ،  $\{\alpha^i \mid 98 \leq i \leq 111\}$  و  $\{\alpha^i \mid 113 \leq i \leq 127\}$  است که در آن  $\alpha$  یک ریشه ۱۲۷ام اولیه واحد است. فرض کنید:

$$A = \{\alpha^i \mid 83 \leq i \leq 95\} \cup \{\alpha^i \mid 98 \leq i \leq 111\},$$

$$B = \{\beta^j \mid j = -7, 0, 1\}, \quad \beta = \alpha^{17}.$$

در این صورت  $R \supseteq AB$ . مجموعه  $A$  شامل ۱۴ توان متوالی  $\alpha$  است؛ بنابراین، زیرمجموعه ای از یک مجموعه از ۲۹ توان متوالی  $\alpha$  است، با توان های  $\alpha^{96}$  و  $\alpha^{97}$  که از دست رفته اند؛ بنابراین، از لم ۷.۶.۶ و نتیجه ۸.۶.۶ داریم:

$$\text{rank}(M(A)_I) \geq \begin{cases} |I|, & \text{برای } 1 \leq |I| \leq 14 \\ 14, & \text{برای } 14 \leq |I| \leq 16 \\ |I| - 2, & \text{برای } 17 \leq |I| \leq 29 \end{cases}$$

با روشی مشابه، داریم:

$$\text{rank}(M(B)_I) \geq \begin{cases} |I|, & 1 \leq |I| \leq 2, \\ 2, & 2 \leq |I| \leq 8, \\ 3, & |I| \geq 9. \end{cases}$$

با به کارگیری قضیه ۱۱.۶.۶ مجموعه  $I$  با شرط  $|I| < 3^0$  می تواند محمل یک کدکلمه در  $C$  باشد.

این مطلب توسط ونلینت و ویلسن در مرجع [۷۶] نشان داده شده است که روش تشریح شده در بالا، کمترین-فاصله دقیق برای تمامی کدهای دوری دودویی با طول کمتر از ۶۳، با تنها دومورد استثنا، را می دهد.

یافتن کمترین-فاصله واقعی یک کد BCH در حالت کلی یک مساله مشکل است. اما، مطلبی در اینجا می تواند 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.  $\mathbb{F}_{2^k}$  را به عنوان فضای  $\mathbb{F}_2^k$  و  $U$  را زیرفضایی با بعد  $l$  در نظر بگیرید. تعریف می کنیم  $\sum_i(U) := \sum_{x \in U} x^i$ .

لم ۱۷.۶.۶. اگر  $i$  دارای کمتر از  $l$  یک در بسط دودویی خود باشد، آن گاه  $\sum_i(U) = 0$ .

اثبات. استقراء را به کار می گیریم. حالت  $l = 1$  بدیهی است. فرض کنید ادعا برای یک مقادیر  $l$  درست باشد و فرض کنید  $V$  دارای بعد  $l + 1$  باشد و  $V = U \cup (U + b)$  که در آن  $U$  دارای بعد  $l$  است؛ در این صورت:

$$\sum_i(V) = \sum_i(U) + \sum_{x \in U} (x + b)^i = \sum_{v=0}^{i-1} \binom{i}{v} b^{i-v} \sum_v(U).$$

اگر بسط دودویی  $i$  دارای حداکثر  $l$  یک باشد، آن گاه 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.  $\square$

قضیه ۱۸.۶.۶. کد BCH دودویی اولیه  $C$  با طول  $n = 2^m - 1$  و فاصله طراحی شده  $\delta = 2^l - 1$  دارای کمترین-فاصله  $\delta$  است.

اثبات. فرض کنید  $U$  یک زیرفضای  $l$  بعدی از  $\mathbb{F}_{2^m}$  باشد. بردار  $c$  را که دارای یک‌هایی دقیقاً در مکان‌های متناظر با عناصر ناصفر  $U$  است، در نظر بگیرید؛ یعنی:

$$c(x) = \sum_{j: \alpha^j \in U \setminus \{0\}} x^j.$$

فرض کنید  $1 \leq i \leq 2^l - 1$ ؛ در این صورت بسط دودویی  $i$  دارای کمتر از  $l$  عدد یک می باشد. علاوه بر این  $c(\alpha^i) = \sum_i(U)$ ؛ بنابراین، با استفاده از لم ۱۷.۶.۶ داریم  $c(\alpha^i) = 0$  برای  $1 \leq i < 2^l - 1$ ؛  
 یعنی  $c(x)$  کد کلمه ای در  $C$  است. □

نتیجه گیری ۱۹.۶.۶. یک کد BCH اولیه با فاصله طراحی شده  $\delta$  دارای فاصله  $d \leq 2\delta - 1$  است.

اثبات. در قضیه ۱۸.۶.۶، مقدار  $l$  را طوری در نظر بگیرید که  $2^{l-1} \leq \delta \leq 2^l - 1$ . کد موجود در قضیه ۱۸.۶.۶ زیرکدی از این با فاصله طراحی شده  $\delta$  است. □

اگرچه این مطلب خیلی مشکل نیست، زمان بسیار زیادی از ما می گیرد تا تخمین های قابل قبولی برای بعد واقعی یک کد BCH ارایه دهیم. در حالت دودویی، تخمین  $2^m - 1 - mt$  در حالت  $\delta = 2t + 1$  را داریم که به وضوح برای مقادیر به اندازه کافی بزرگ  $t$  ضعیف می باشد، اگرچه این تخمین برای مقادیر کوچک  $t$  (نسبت به  $m$ )، دقیق می باشد؛ خواننده علاقه مند را به مرجع [۴۶] ارجاع می دهیم. با ترکیب این تخمین ها، می توان به آسانی نشان داد که کدهای BCH اولیه با طول بزرگ، در مفهوم فصل ۵ کدهای بدی می باشند؛ یعنی اگر  $C_v$  یک کد  $[n_v, k_v, d_v]$  BCH اولیه برای  $v = 1, 2, \dots$  باشد و  $n_v \rightarrow \infty$ ، آن گاه  $k_v/n_v \rightarrow 0$  یا  $d_v/n_v \rightarrow 0$ .

در بخش ۶.۱ اشاره کردیم که گروه خودریختی یک کد دوری به طول  $n$  روی  $\mathbb{F}_q$  نه تنها شامل جای گشت های دوری است، بلکه شامل  $\pi_q$  نیز می باشد. برای کدهای BCH می توانیم بیشتر از این اثبات نماییم. یک کد BCH اولیه  $C$  با طول  $n = q^m - 1$  روی  $\mathbb{F}_q$  با فاصله طراحی شده  $d$  را در نظر بگیرید، یعنی  $\alpha, \alpha^2, \dots, \alpha^{d-1}$  صفرهای تعیین شده کدکلمات هستند که  $\alpha$  یک عضو اولیه از  $\mathbb{F}_{q^m}$  است.

مکان های سمبل های موجود در کدکلمات را با  $X_i$  ( $i = 0, 1, \dots, n-1$ ) نشان می دهیم که  $X_i = \alpha^i$ . این کد را با  $\bar{C}$  با اضافه نمودن یک بررسی توازن سراسری توسعه می دهیم. این مکان اضافی را با  $\infty$  نشان می دهیم و قراردادهای قبلی درباره قواعد حساب با سمبل  $\infty$  را در نظر می گیریم. کدکلمه  $(c_0, c_1, \dots, c_\infty)$  را با  $c_0 + c_1x + \dots + c_{n-1}x^{n-1} + c_\infty x^\infty$  معرفی می کنیم و قراردادهای بیشتر  $1^\infty := 1, \alpha^\infty := 0$  برای  $i \not\equiv 0 \pmod n$  را در نظر می گیریم.

حال نشان خواهیم داد که  $\bar{C}$  تحت جای گشت های گروه جای گشتی آفین  $AGL(1, q^m)$  عمل کننده روی مکان ها، پایاست (بخش ۱.۱ را نیز ببینید). این گروه شامل جای گشت های:

$$P_{u,v}(X) := uX + v, \quad (u \in \mathbb{F}_{q^m}, v \in \mathbb{F}_{q^m}, u \neq 0)$$

است. این گروه، ۲-ترایا<sup>۳</sup> است. در ابتدا مشاهده می‌کنید که  $P_{\alpha, \circ}$  شیفت دوری روی مکان‌های  $C$  است و  $\infty$  را ثابت نگه می‌دارد. فرض کنید  $(c_0, c_1, \dots, c_{n-1}, c_\infty) \in \bar{C}$  و  $P_{u,v}$  کلمه جای‌گشتی  $(c'_0, c'_1, \dots, c'_\infty)$  را به دست دهد؛ در این صورت برای  $0 \leq k \leq d-1$  داریم:

$$\begin{aligned} \sum_i c'_i \alpha^{ik} &= \sum_i c_i (u\alpha^i + v)^k = \sum_i c_i \sum_{l=0}^k \binom{k}{l} u^l \alpha^{il} v^{k-l} \\ &= \sum_{l=0}^k \binom{k}{l} u^l v^{k-l} \sum_i c_i (\alpha^l)^i = 0 \end{aligned}$$

زیرا مجموع داخلی برای  $0 \leq l \leq d-1$  برابر با ۰ است؛ چرا که  $c \in \bar{C}$ ؛ بنابراین، قضیه زیر را داریم.

**قضیه ۲۰.۶.۶.** 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 ۲۱.۶.۶.** 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 در نظر بگیریم؛ بنابراین،  $\bar{C}$  دارای کلمات با کمترین-وزن با یک ۱ در آخرین مکان بررسی است.  $\square$

## ۶.۷ کدگشایی کدهای BCH

مجدداً یک کد BCH با طول  $n$  روی  $\mathbb{F}_q$  با فاصله طراحی شده  $\delta = 2t+1$  را در نظر بگیرید و  $\beta$  را یک ریشه  $n$ ام واحد در  $\mathbb{F}_{q^m}$  فرض کنید. کدکلمه  $C(x)$  را در نظر گرفته و فرض کنید کلمه دریافتی برابر با:

$$R(x) = R_0 + R_1 x + \dots + R_{n-1} x^{n-1},$$

باشد. فرض کنید  $E(x) := R(x) - C(x) = E_0 + E_1 x + \dots + E_{n-1} x^{n-1}$  بردار خطا باشد. تعریف می‌کنیم:

$$M := \{i \mid E_i \neq 0\},$$

مکان‌هایی که یک خطا رخ می‌دهد

$$e := |M|,$$

تعداد خطاها

$$\sigma(z) := \prod_{i \in M} (1 - \beta^i z),$$

که ما آن را چندجمله‌ای تشخیص-خطا می‌نامیم

$$\omega(z) := \sum_{i \in M} E_i \beta^i z \prod_{j \in M \setminus \{i\}} (1 - \beta^j z).$$

واضح است که اگر بتوانیم  $\sigma(z)$  و  $\omega(z)$  را بیابیم، آنگاه خطاها می‌توانند تصحیح شوند. در واقع یک خطا در مکان  $i$  رخ می‌دهد اگر و تنها اگر  $\sigma(\beta^{-i}) = 0$  و در آن حالت، خطا برابر است با  $E_i = -\omega(\beta^{-i})\beta^i/\sigma'(\beta^{-i})$ . از اینجا به بعد فرض می‌کنیم  $e \leq t$  (اگر  $e > t$  ما انتظار نداریم که بتوان خطاها را تصحیح نمود). مشاهده می‌کنید که:

$$\begin{aligned} \frac{\omega(z)}{\sigma(z)} &= \sum_{i \in M} \frac{E_i \beta^i z}{1 - \beta^i z} = \sum_{i \in M} E_i \sum_{l=1}^{\infty} (\beta^i z)^l \\ &= \sum_{l=1}^{\infty} z^l \sum_{i \in M} E_i \beta^{li} = \sum_{l=1}^{\infty} z^l E(\beta^l), \end{aligned}$$

که در آن تمامی محاسبات با سری‌های توانی روی  $\mathbb{F}_q^m$  می‌باشد. برای  $1 \leq l \leq 2t$  داریم  $E(\beta^l) = R(\beta^l)$ ؛ یعنی گیرنده  $2t$  مختصات اول در طرف راست را می‌داند؛ بنابراین،  $\omega(z)/\sigma(z)$  در پیمانه  $z^{2t+1}$  معلوم است. ادعا می‌کنیم که گیرنده باید چندجمله‌ای‌های  $\sigma(z)$  و  $\omega(z)$  را به گونه‌ای تعیین نماید که  $\deg \omega(z) \leq \deg \sigma(z)$  و  $\deg \sigma(z)$  به اندازه کافی تحت شرط زیر کوچک باشد:

$$\frac{\omega(z)}{\sigma(z)} = \sum_{l=1}^{2t} z^l R(\beta^l) \pmod{z^{2t+1}}. \quad (5)$$

فرض کنید  $S_l := R(\beta^l)$  برای  $l = 1, \dots, 2t$  و  $\sigma(z) = \sum_{i=0}^e \sigma_i z^i$ ؛ در این صورت:

$$\omega(z) \equiv \left( \sum_{l=1}^{2t} S_l z^l \right) \left( \sum_{i=0}^e \sigma_i z^i \right) = \sum_k \left( \sum_{i+l=k} S_l \sigma_i \right) \pmod{z^{2t+1}}.$$

از آنجایی که  $\omega(z)$  دارای درجه کمتر یا مساوی  $e$  است؛ داریم:

$$\sum_{i+l=k} S_l \sigma_i = 0, \quad e+1 \leq k \leq 2t.$$

این یک دستگاه با  $2t - e$  معادله خطی برای متغیرهای نامعین  $\sigma_1, \dots, \sigma_e$  (می‌دانیم  $\sigma_0 = 1$ ) است. فرض کنید  $\tilde{\sigma}(z) = \sum_{i=0}^e \tilde{\sigma}_i z^i$  (که در آن  $\tilde{\sigma}_0 = 1$ ) چندجمله‌ای با کمترین درجه یافت شده توسط حل این معادلات باشد (می‌دانیم حداقل جواب  $\sigma(z)$  وجود دارد). برای  $e+1 \leq k \leq 2t$  داریم:

$$0 = \sum_l S_{k-l} \tilde{\sigma}_l = \sum_{i \in M} \sum_l E_i \beta^{(k-l)i} \tilde{\sigma}_l = \sum_{i \in M} E_i \beta^{ik} \tilde{\sigma}(\beta^{-i}).$$

می‌توانیم طرف راست را به عنوان دستگاهی از معادلات خطی برحسب  $E_i \tilde{\sigma}(\beta^{-i})$  با ضرایب  $\beta^{ik}$  تعبیر کنیم. بنابراین، درمینان ضرایب مجدداً و اندر موند است، پس مخالف صفر است؛ بنابراین،  $E_i \tilde{\sigma}(\beta^{-i}) = 0$ ؛ چون  $i \in M$ ،  $E_i \neq 0$ ؛ بنابراین،  $\tilde{\sigma}(z) = \sigma(z)$ ؛ یعنی  $\tilde{\sigma}(z)$  را؛ یعنی  $\tilde{\sigma}(z) = \sigma(z)$ ؛ در واقع 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 در نظر گرفته‌ایم، می‌باشد. چنین الگوریتمی (با کاربرد) توسط برلیکمپ<sup>۳۱</sup> (مراجع [۲] و [۲۴]) طراحی شد و اغلب به‌عنوان کدگشای برلیکمپ<sup>۳۲</sup> از آن یاد می‌شود.

اگر ما چند جمله‌ای (معلوم) طرف راست رابطه ۵ را  $S(z)$  بنامیم و تعریف کنیم  $G(z) := z^{2t+1}$ ، آن‌گاه این رابطه به‌صورت زیر در می‌آید:

$$S(z)\sigma(z) \equiv \omega(z) \pmod{G(z)}. \quad (6)$$

نیاز داریم تا جوابی از این هم‌نهستی با  $\sigma$  از درجه کم‌تر یا مساوی  $t$  و  $\omega$  از درجه کم‌تر از درجه  $\sigma$  را بیابیم. این جواب (یکتا)، احتمال تصحیح خطا را تعیین می‌کند. در بخش ۹.۵، با هم‌نهستی مشابهی مواجه می‌شویم.

## ۶.۸ کدهای رید-سولومن

یکی از ساده‌ترین مثال‌های کدهای BCH، یعنی حالت  $n = q - 1$ ، ثابت شده که دارای کاربردهای بسیاری است.

تعریف ۱.۶.۸. یک کد رید-سولومن<sup>۳۳</sup> (کد RS) یک کد BCH اولیه با طول  $n = q - 1$  روی  $\mathbb{F}_q$  است. مولد چنین کدی دارای شکلی به‌صورت  $g(x) = \prod_{i=1}^{d-1} (x - \alpha^i)$  است که در آن  $\alpha$  یک عضو اولیه از  $\mathbb{F}_q$  است.

با استفاده از کران BCH (قضیه ۲.۶.۶)، کمترین-فاصله یک کد RS با این مولد  $g(x)$  حداقل برابر  $d$  می‌باشد. با مراجعه به بخش ۶.۲، این کد دارای بعد  $k = n - d + 1$  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<sup>۳۴</sup> رخ دهند (یعنی چندین خطای نزدیک به هم). این حالت اغلب در عمل رخ می‌دهد (مخابرات، نوارهای ضبط‌صوت، 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  $\mathbb{F}_{2^m}$  تعبیر شده‌اند، رخ داده‌اند. اگر اینها با استفاده از

<sup>۳۱</sup>E. R. Berlekamp

<sup>۳۲</sup>Berlekamp-decoder

<sup>۳۳</sup>Reed-solomon

<sup>۳۴</sup>bursts



کد RS کد شوند، آن‌گاه یک دسته پشت سر هم از خطاها (به صورت 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  $\alpha$  یک عضو اولیه از  $\mathbb{F}_q$  باشد. به‌طور معمول،  $a = (a_0, a_1, \dots, a_{k-1})$  را با  $a(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1} = a(x)$  یکی در نظر می‌گیریم؛ در این صورت:

$$C = \{(c_0, c_1, \dots, c_{n-1}) \mid c_i = a(\alpha^i), 0 \leq i < n, a \in \mathbb{F}_q^k\},$$

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  $i = 1, 2, \dots, n - k$ ؛ 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. در اینجا  $\mathbb{F}_{q^m}$  را به‌عنوان الفبا در نظر گرفته و  $n$  عضو متمایز را از این میدان اختیار می‌کنیم؛ گیریم  $\alpha_1, \alpha_2, \dots, \alpha_n$ . فرض کنید  $v = (v_1, v_2, \dots, v_n)$  برداری از  $\mathbb{F}_{q^m}^n$  با درایه‌های ناصفر باشد و می‌نویسیم  $a := (\alpha_1, \alpha_2, \dots, \alpha_n)$ .

**تعریف ۲.۶.۸.** کد رید-سولومن گسترش‌یافته<sup>۳۵</sup>  $GRS_k(a, v)$  شامل تمامی  $(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n))$  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

<sup>۳۵</sup>generalized Reed-Solomon code

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  $Q := (1, 0)$  را به‌عنوان نقطه خاصی بر روی این خط بررسی می‌داریم. نقاط باقی‌مانده شامل  $(0, 1)$  و  $(\alpha^i, 1)$  ( $0 \leq i < q-1$ ) به‌عنوان مختصات می‌باشند که در آن  $\alpha$  مجدداً یک عضو اولیه از  $\mathbb{F}_q$  را نمایش می‌دهد. حال آن دسته از کسرهای گویای  $a(x, y)/y^l$  را که  $l < k$  در نظر 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  $P_0, P_1, \dots, P_{q-1}$ ) و در نظر گرفتن آن به‌صورت کدکلمات  $f(P_0), \dots, f(P_{q-1})$  که در آن  $f$  متعلق به فضای  $K$  است، معادل است. این توابع به‌صورتی انتخاب شده‌اند که در واقع 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<sup>۳۶</sup> با مرتبه حداکثر  $k-1$  است.

ساده‌ترین مثال‌های کدهای هندسه جبری این ساختار را با جانشین نمودن خط تصویری با منحنی تصویری در یک فضای تصویری تعمیم می‌دهد. کدهای هندسه جبری را در فصل ۱۰ مطالعه می‌کنیم. حال نگاهی به کدهای MDS به‌طور کلی می‌اندازیم. اگر  $C$  یک کد  $[n, k]$  با کمترین-فاصله  $d = n - k + 1$  باشد، آن‌گاه  $C$  بر روی هر  $k$  مکانی متقارن است (ارجاع به مساله ۲.۳.۸).

**قضیه ۳.۶.۸.** دوگان یک کد MDS نیز یک کد MDS است.

**اثبات.** فرض کنید  $G = (I_k \ P)$  ماتریس مولد کد  $C$  باشد. چون  $C$  دارای کمترین-فاصله  $d$  است، هر مجموعه از  $d-1 = n-k$  ستون ماتریس بررسی توازن  $H := (-P^T \ I_{n-k})$  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  $[n, n-k, k+1]$  است؛ یعنی یک کد MDS.  $\square$

فرض کنید  $C$  یک کد  $[n, k, d]$  با  $d = n - k + 1$  باشد. اگر مجموعه‌ای از  $d$  مکان را در نظر بگیریم و به زیرکد  $C$  با صفرهایی در سایر مکان‌ها، نگاه کنیم، این زیرکد دارای بعدی بزرگ‌تر یا مساوی  $1 = k - (n - d)$  است. چون این زیرکد دارای کمترین-فاصله  $d$  است، باید دارای بعدی دقیقاً برابر با  $1$  باشد. در نتیجه برای  $d' > n \geq d'$  با تخصیص مجموعه‌ای از  $d'$  مکان و در نظر گرفتن کدکلمات به‌صورتی که در سایر مکان‌ها برابر با صفر باشند، زیرکدی از  $C$  با بعد  $d' - d + 1$  تعریف خواهد شد. این نتیجه را به‌صورت یک لم فرمول‌بندی می‌کنیم.

لم ۴.۶.۸. برای  $n \geq d' \geq d = n - k + 1$ ، 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  $d' - d + 1$  است.

ما این لم و یک فرم مشابه از فرمول معکوس موبیوس ۴.۱.۱ را برای یافتن شمارنده وزنی یک کد MDS به کار خواهیم برد. در ابتدا 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:

$$\mu(S, T) := (-1)^{|T| - |S|}.$$

قضیه ۶.۶.۸. فرض کنید  $N$  یک مجموعه تعریف باشد و فرض کنید  $f$  یک تابع تعریف شده 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.

$$\sum_{S \subset T} \mu(S, T) g(S) = \sum_{S \subset T} \mu(S, T) \sum_{R \subset S} f(R)$$

$$= \sum_{R \subset T} f(R) \sum_{R \subset S \subset T} \mu(S, T),$$

و نتیجه از تساوی زیر حاصل می‌شود:

$$\sum_{R \subset S \subset T} \mu(S, T) = \sum_{j=0}^{|T|-|R|} \binom{|T|-|R|}{j} (-1)^j = (1-1)^{|T|-|R|} = \begin{cases} 0, & R \neq T \\ 1, & R = T \end{cases}$$

□

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  $d = n - k + 1$  باشد. اگر شمارنده وزنی  $C$  برابر با  $1 + \sum_{i=d}^n A_i z^i$  باشد، آن‌گاه:

$$A_i = \binom{n}{i} (q-1) \sum_{j=0}^{i-d} (-1)^j \binom{i-1}{j} q^{i-j-d} \quad (i = d, d+1, \dots, n).$$

اثبات. اگر  $R$  زیرمجموعه‌ای از  $N := \{0, 1, \dots, n-1\}$  باشد،  $f(R)$  را تعداد کدکلمات  $(c_0, c_1, \dots, c_{n-1})$  تعریف کنید به طوری که  $i \in R \Leftrightarrow c_i \neq 0$ . اگر  $g$  را مانند قضیه ۶.۶.۸ تعریف کنیم، آنگاه با استفاده از لم ۴.۶.۸ داریم:

$$g(S) = \begin{cases} 1, & \text{اگر } |S| \leq d-1 \\ q^{|S|-d+1}, & \text{اگر } n \geq |S| \geq d \end{cases}$$

با به کارگیری تعریف  $f$ ، داریم  $A_i = \sum_{R \subset N, |R|=i} f(R)$ ؛ بنابراین، کاربرد قضیه ۶.۶.۸ نتیجه می‌دهد:

$$\begin{aligned} A_i &= \sum_{R \subset N, |R|=i} \sum_{S \subset R} \mu(S, R) g(S) \\ &= \binom{n}{i} \left\{ \sum_{j=0}^{d-1} \binom{i}{j} (-1)^{i-j} + \sum_{j=d}^i \binom{i}{j} (-1)^{i-j} q^{j-d+1} \right\} \\ &= \binom{n}{i} \sum_{j=d}^i \binom{i}{j} (-1)^{i-j} (q^{j-d+1} - 1). \end{aligned}$$

حال اگر ما  $j$  را با  $i-j$  جای‌گزین نموده، سپس تساوی  $\binom{i}{j} = \binom{i-1}{j-1} + \binom{i-1}{j}$  را به کار ببریم، نتیجه حاصل می‌شود.  $\square$

قضیه ۷.۶.۸، محدودیت زیر را روی اندازه الفبای یک کد MDS مطرح می‌کند.

قضیه ۸.۶.۸ اگر یک کد MDS روی  $\mathbb{F}_q$  به طول  $n$  و بعد  $k$  وجود داشته باشد، آنگاه  $q \geq n - k + 1$  یا  $k \leq 1$ .

اثبات. فرض کنید  $d = n - k + 1$ . با استفاده از قضیه ۷.۶.۸ برای  $d < n$  داریم  $0 \leq A_{d+1} = \binom{n}{d+1} (q-1)(q-d)$ .  $\square$

چون دوگان یک کد MDS نیز MDS است (قضیه ۳.۶.۸)، نتیجه زیر را داریم:

نتیجه‌گیری ۹.۶.۸ اگر یک کد MDS روی  $\mathbb{F}_q$  با طول  $n$  و بعد  $k$  وجود داشته باشد، آنگاه  $q \geq k + 1$  یا  $d = n - k + 1 \leq 2$ .

## ۶.۹ کدهای باقی‌مانده مربعی

در این بخش، کدهایی را در نظر خواهیم گرفت که طول کلمه  $n$  یک عدد اول فرد باشد. الفبای  $\mathbb{F}_q$  باید در این شرط صدق کند:  $q$  یک باقی‌مانده مربعی در پیمانه  $n$  باشد؛ یعنی  $q^{(n-1)/2} \equiv 1 \pmod{n}$ . به‌طور

معمول  $\alpha$  یک ریشه  $n$ ام اولیه واحد را در یک توسیع میدان  $\mathbb{F}_q$  نشان خواهد داد. بعداً ثابت می‌شود که نیاز داریم تا  $\alpha$  در یک شرط اضافی صدق کند. تعریف می‌کنیم:

$$R_o := \{i^{\vee} \bmod n \mid i \in \mathbb{F}_n, i \neq o\}, \quad \mathbb{F}_n \text{ مانده‌های مربعی در}$$

$$R_{\wedge} := \mathbb{F}_n^* \setminus R_o, \quad \mathbb{F}_n \text{ مجموعه عناصر غیرمربعی در}$$

$$g_o(x) := \prod_{r \in R_o} (x - \alpha^r), \quad g_{\wedge}(x) := \prod_{r \in R_{\wedge}} (x - \alpha^r).$$

چون شرط کرده‌ایم که  $q \bmod n$  در  $R_o$  باشد، چندجمله‌ای‌های  $g_o(x)$  و  $g_{\wedge}(x)$  هردو دارای ضرایبی در  $\mathbb{F}_q$  هستند (مراجعه به قضیه ۱۸.۱.۱)؛ علاوه‌براین:

$$x^n - 1 = (x - 1)g_o(x)g_{\wedge}(x).$$

**تعریف ۱.۶.۹.** کدهای دوری به طول  $n$  روی  $\mathbb{F}_q$  با مولدهای  $g_o(x)$ ، به ترتیب  $(x - 1)g_o(x)$  هردو کدهای باقی‌مانده مربعی  $^{۳۷}$  (کدهای QR) نامیده می‌شوند.

ما تنها کدهای QR گسترش‌یافته در حالت دودویی را در نظر خواهیم گرفت که تعریف آن مشابه تعریف ۶.۳.۲ است. چنین کدی با اضافه‌نمودن یک بررسی‌توازن سراسری به کد با مولد  $g_o(x)$  به دست می‌آید.

در مورد سایر میدان‌ها، تعریف کد گسترش‌یافته معمولاً به صورتی است که اگر  $n \equiv -1 \pmod{4}$ ، آن‌گاه کد گسترش‌یافته خوددوگان باشد، و به ترتیب، اگر  $n \equiv 1 \pmod{4}$ ، آن‌گاه دوگانِ توسیع کد با مولد  $g_{\wedge}(x)$  باشد (ر.ک. [۴۶]). در حالت دودویی، کد با مولد  $(x - 1)g_o(x)$  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  $G$  به دست می‌آوریم. اگر چنین کاری را پس از اضافه‌نمودن یک ستون تمام صفر به  $G$  انجام دهیم، ماتریس مولدی برای کد گسترش‌یافته به دست می‌آوریم.

در حالت دودویی این شرط که  $q$  باقی‌مانده مربعی در پیمانه  $n$  باشد، به معنی  $n \equiv \pm 1 \pmod{8}$  می‌باشد (ارجاع به بخش ۱.۱). جای‌گشت  $\pi_j : i \rightarrow ij \bmod n$  با عمل کردن روی مکان‌های کدکلمات، کد با مولد  $g_o(x)$  را به خودش تصویر می‌کند، اگر  $j \in R_o$  و به کد با مولد  $g_{\wedge}(x)$  تبدیل می‌کند، اگر  $j \in R_{\wedge}$ ؛ بنابراین، کدهای با مولدهای  $g_o(x)$ ، به ترتیب  $g_{\wedge}(x)$ ، هم ارز می‌باشند. اگر  $n \equiv -1 \pmod{4}$ ، آن‌گاه  $-1 \in R_{\wedge}$  و در آن حالت تبدیل  $x \rightarrow x^{-1}$ ، کدکلمه‌ای از کد با مولد  $g_o(x)$  را به کدکلمه‌ای از کد با مولد  $g_{\wedge}(x)$  تصویر می‌کند.

قضیه ۲.۶.۹. اگر  $c = c(x)$  کدکلمه‌ای در کد QR با مولد  $g_0(x)$  بوده و  $c(1) \neq 0$  و  $w(c) = d$ ، آن‌گاه:

$$(۱) \quad d^2 \geq n$$

$$(۲) \quad \text{اگر } n \equiv -1 \pmod{4} \text{، آن‌گاه } d^2 - d + 1 \geq n$$

$$(۳) \quad \text{اگر } n \equiv -1 \pmod{8} \text{ و } q = 2 \text{، آن‌گاه } d \equiv 3 \pmod{4}$$

اثبات.

(۱) چون  $c(1) \neq 0$ ، چندجمله‌ای  $c(x)$  بر  $(x-1)$  بخش‌پذیر نیست. با استفاده از جای‌گشت مناسب  $\pi_j$  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  $1 + x + x^2 + \dots + x^{n-1}$  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 حاصل ضرب  $c(x)\hat{c}(x)$  حذف شوند، آنها چهارتایی حذف می‌شوند. از این‌رو برای یک  $a \geq 0$  داریم  $n = d^2 - d + 1 - 4a$ .  $\square$

ثابت خواهد شد که خودتوان یک کد دوری، معرفی شده در بخش ۶.۴، ابزار نیرومندی در تجزیه و تحلیل کدهای QR است.

قضیه ۲.۶.۹. برای انتخاب مناسبی از ریشه  $n$ ام اولیه واحد  $\alpha$ ، چندجمله‌ای:

$$\theta(x) := \sum_{r \in R_0} x^r,$$

خودتوان کد دودویی QR با مولد  $g_0(x)$  است، اگر  $n \equiv 1 \pmod{8}$  و خودتوان کد QR با مولد  $g_0(x)$  است، اگر  $n \equiv -1 \pmod{8}$ .

اثبات. به‌وضوح  $\theta(x)$  یک چندجمله‌ای خودتوان است؛ بنابراین،  $\theta(\alpha) = \theta(\alpha)^2$ ؛ یعنی  $\theta(\alpha) = 0$  یا  $\theta(\alpha) = 1$ . با اثباتی مشابه داریم  $\theta(\alpha^i) = \theta(\alpha)$ ، اگر  $i \in R_0$  و  $\theta(\alpha^i) + \theta(\alpha) = 1$ ، اگر  $i \in R_1$ . "انتخاب مناسب"  $\alpha$  طوری است که  $\theta(\alpha) = 0$  (خواننده باید خود را قانع کند که این که تمامی عناصر اولیه  $\mathbb{F}_q$  در رابطه  $\theta(\alpha) = 0$  صدق کنند، غیرممکن می‌باشد). انتخاب ما ایجاب می‌کند تا  $\theta(\alpha^i) = 0$ ، اگر  $i \in R_0$  و  $\theta(\alpha^i) = 1$ ، اگر  $i \in R_1$ . سرانجام داریم  $\theta(\alpha^n) = (n-1)/2$ . به این ترتیب، حکم ثابت می‌شود.  $\square$

با کمک  $\theta$ ، اکنون ماتریس  $C$  با درایه‌های  $0$  و  $1$  را (معروف به ماتریس گردشی  $^{38}$ )، با در نظر گرفتن کلمه  $\theta$  به‌عنوان سطر اول و تمامی شیفتهای دوری به‌عنوان سایر سطرها، می‌سازیم. فرض کنید  $c := (0 \dots 0)$ ، اگر  $n \equiv 1 \pmod{8}$  و  $c := (1 \dots 1)$ ، اگر  $n \equiv -1 \pmod{8}$ ؛ داریم:

$$G := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ c^T & & C & \end{pmatrix}.$$

از قضیه ۳.۶.۹ نتیجه می‌شود که سطرهای  $G$  (که به‌وضوح مستقل نمی‌باشند)، کد QR دودویی گسترش‌یافته با طول  $n+1$  را تولید می‌کنند. حال مکان‌های مختصات کدکلمات این کد را با نقاط خط تصویری مرتبه  $n$ ، یعنی  $1, \dots, n-1, \infty$ ، شماره‌گذاری می‌کنیم. بررسی توازن سراسری در ابتدا و دارای شماره  $\infty$  است. قراردادهای معمول را درباره عمل‌گرهای ریاضی شامل  $\infty$  در نظر می‌گیریم. گروه  $PSL(2, n)$  شامل تمامی تبدیل‌های  $x \rightarrow (ax+b)/(cx+d)$  با  $a, b, c, d$  متعلق به  $\mathbb{F}_n$  و  $ad-bc = 1$  است. بررسی این‌که این گروه، تولید شده توسط تبدیلات  $S: x \rightarrow x+1$  و  $T: x \rightarrow -x^{-1}$  است، مشکل نمی‌باشد. به‌وضوح  $S$  روی مکان‌های متفاوت از  $\infty$  یک شیفتهای دوری است و  $\infty$  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، هر دو  $S$  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  $n+1$ ، شامل  $PSL(2, n)$  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]).

نتیجه‌گیری ۵.۶.۹ یک کلمه با کمترین-وزن در یک کد QR دودویی، در شرایط قضیه ۲.۶.۹ صدق می‌کند.

اثبات. اثبات مشابه با اثبات نتیجه ۲۱.۶.۶ است. در این حالت از این واقعیت که  $PSL(2, n)$  تعدی است، استفاده می‌کنیم؛ بنابراین، کمترین-وزن، عددی فرد می‌باشد.  $\square$

مثال ۶.۶.۹. (a) فرض کنید  $q = 2$  و  $n = 7$ ؛ داریم:

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

$g_0(x)$  را به‌عنوان مولد می‌گیریم. انتخاب  $\alpha$  صادق در قضیه ۳.۶.۹ ایجاب می‌کند که  $x + x^2 + x^4$  نیز یک مولد باشد؛ بنابراین،  $g_0(x) = 1 + x + x^3$ . البته این کد، کد همینگ [۷, ۴] (کامل) است (بخش ۳.۳ و قضیه ۲.۳.۳ را ببینید). زیرکد با وزن زوج متناظر، در مثال ۴.۶.۱ بررسی شده است. (b) فرض کنید  $q = 2$  و  $n = 23$ ؛ داریم:

$$x^{23} - 1 = (x - 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$$

$$\times (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1).$$

مجدداً  $g_0(x)$  را مضربی از  $\theta(x)$  می‌گیریم که برابر است با:

$$x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1.$$

با استفاده از نتیجه ۵.۶.۹، کد QR متناظر  $C$  دارای کمترین-فاصله  $d \geq 7$  است.

چون  $\sum_{i=0}^3 \binom{23}{i} = 2^{11}$  و  $|c| = 2^{12}$ ، نتیجه می‌شود که  $d$  برابر با ۷ است و با استفاده از ۶.۳.۱،  $C$  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 ۶.۱۳).

## ۶.۱۰ کدهای دوری دودویی با طول $2n$ ( $n$ فرد)

فرض کنید  $n$  فرد باشد و  $x^n - 1 = f_1(x)f_2(x)\cdots f_t(x)$  تجزیه  $x^n - 1$  به عوامل تحویل‌ناپذیر در  $\mathbb{F}_2[x]$  باشد.



تعریف می‌کنیم  $g_1(x) = f_1(x) \cdots f_k(x)$  و  $g_2(x) = f_{k+1}(x) \cdots f_l(x)$  که در آن  $k < l < t$ . فرض کنید  $r_1 := \deg g_1$  و  $r_2 := \deg g_2$ .

فرض کنید  $C_1$  کد دوری به طول  $n$  و بعد  $n - r_1$  با مولد  $g_1(x)$  باشد و فرض کنید  $C_2$  کد دوری به طول  $n$  و بعد  $n - r_2$  با مولد  $g_2(x)$  باشد. همچنین فرض کنید  $d_i$  کمترین-فاصله  $C_i$  ( $i = 1, 2$ ) باشد. به وضوح  $d_2 \geq d_1$ .

در ادامه کد دوری  $C$  با طول  $2n$ ، بعد  $2n - r_1 - r_2$  و مولد  $g(x) := g_1^2(x)g_2(x)$  را مورد مطالعه قرار خواهیم داد. ادعا می‌کنیم که این کد دارای ساختار زیر است:

فرض کنید  $a = (a_0, a_1, \dots, a_{n-1}) \in C_1$  و  $c = (c_0, c_1, \dots, c_{n-1}) \in C_2$ . تعریف کنید  $b := a + c$ . چون  $n$  فرد است، می‌توانیم کلماتی را به صورت:

$$w := (a_0, b_1, a_2, \dots, b_{n-2}, a_{n-1}, b_0, a_1, \dots, a_{n-2}, b_{n-1})$$

تعریف کنیم که متعلق به  $C$  می‌باشند و با این روش تمامی کلمات  $C$  را می‌یابیم؛ (ادعای اخیر از مباحث بعد نتیجه می‌شود). برای تشریح این مطلب، به صورت زیر عمل می‌کنیم. بنویسید:

$$\begin{aligned} a(x) &= a_0 + a_1x + \dots + a_{n-1}x^{n-1} \\ &= (a_0 + a_2x^2 + \dots + a_{n-1}x^{n-1}) + x(a_1 + \dots + a_{n-2}x^{n-2}) \\ &= a_e(x^2) + xa_o(x^2), \end{aligned}$$

و به طور مشابه برای  $c(x)$  و  $b(x)$ ؛ در این صورت دو نمایش (یکسان) زیر را برای چندجمله‌ای  $w(x)$  متناظر با کد کلمه  $w$  داریم:

$$w(x) = \{a_e(x^2) + x^{n+1}a_o(x^2)\} + \{xb_o(x^2) + x^n b_e(x^2)\}, \quad (7)$$

و

$$w(x) = \{a(x) + x(x^n + 1)a_o(x^2)\} + \{b(x) + (x^n + 1)b_e(x^2)\}. \quad (8)$$

هر دو جمله در رابطه ۸، بر  $g_1(x)$  بخش‌پذیر هستند. از رابطه ۷ می‌بینیم که اولین جمله تنها شامل توان‌های زوج  $x$  و دومی تنها شامل توان‌های فرد  $x$  می‌باشد. چون  $g_1(x)$  شامل عوامل تکراری نمی‌باشد، هر دو جمله در واقع بر  $g_1^2(x)$  بخش‌پذیر هستند.

از رابطه ۸ داریم:

$$w(x) = (x^n + 1)a(x) + c(x) + (x^n + 1)c_e(x^2),$$

به طوری که هر جمله بر  $g_2(x)$  بخش پذیر است.

چون  $b = a + c$ ، کلمه  $aw$  جای گشتی از کلمه  $|a|a + c|$  است (ارجاع به رابطه ۳). پس قضیه زیر را اثبات کرده ایم:

قضیه ۱.۶.۱۰. فرض کنید  $C_1$  یک کد دوری دودویی با طول  $n$  (فرد) با مولد  $g_1(x)$  باشد و فرض کنید  $C_2$  یک کد دوری دودویی با طول  $n$  با مولد  $g_2(x)$  باشد؛ در این صورت کد دوری دودویی  $C$  با طول  $2n$  با مولد  $g_1^2(x)g_2(x)$  هم ارز با مجموع  $|u|u + v|$  از  $C_1$  و  $C_2$  می باشد؛ بنابراین،  $C$  دارای کمترین فاصله  $\min\{2d_1, d_2\}$  می باشد.

کدهای دودویی دوری خوب زیادی با طول زوج وجود ندارند. اما، قضیه زیر وجود کلاسی از مثال های بهینه را نشان می دهد.

قضیه ۲.۶.۱۰. زیرکد با وزن زوج از یک کد همینگ دودویی کوتاه شده، دوری است (تحت یک ترتیب مناسب از سمبل ها).

اثبات. دیدن این امر مشکل نمی باشد که تفاوتی در این که کد روی چه مکانی کوتاه شده، نیست (تمامی کدهای حاصل، هم ارز می باشند). فرض کنید  $n = 2^s - 1$ . هم چنین فرض کنید که  $m_1(x)$  معرف چند جمله ای مینیمال یک عضو اولیه  $\alpha$  از  $\mathbb{F}_2$  باشد؛ در این صورت  $m_1(x)$  چند جمله ای مولد یک کد همینگ  $[n, n - s]$  دودویی است و  $(x + 1)m_1(x)$  چند جمله ای مولد زیرکد با وزن زوج از آن است. در قضیه ۱.۶.۱۰ قرار دهیم  $g_1(x) = (x + 1)$  و  $g_2(x) = m_1(x)$ ؛ در این صورت ما یک کد دوری  $C$  با طول  $2n$ ، بعد  $2n - s - 2$  و کمترین فاصله ۴ می یابیم. از ساختار  $|u|u + v|$  نتیجه می شود که تمام وزن های  $C$  زوج هستند؛ بنابراین،  $C$  شامل یک ماتریس بررسی توازن با یک سطر بالایی تماماً ۱ و ستون های مجزا می باشد. از این رو  $C$  هم ارز با زیرکد با وزن زوج از یک کد همینگ کوتاه شده است.  $\square$

مشاهده می کنیم که روش های متفاوتی برای اثبات قضیه قبل وجود دارد. ما مشتق هسه<sup>۳۹</sup> (فصل ۱ را ببینید) را به کار خواهیم برد. مولد  $C$  شامل ۱ به عنوان یک ریشه با تکرار ۲ و  $\alpha$  یک ریشه با تکرار ۱ است. این بدان معناست که اگر  $c(x) = \sum c_i x^i$  یک کد کلمه باشد، آن گاه:

$$\sum c_i = 0, \quad \sum i c_i = 0, \quad \sum c_i \alpha^i = 0;$$

یعنی:

$$H_1 := \begin{pmatrix} 1 & 1 & 1 & & 1 & 1 & 1 & & 1 & 1 \\ 0 & 1 & 0 & & 0 & 1 & 0 & & 0 & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} & \alpha^n & \alpha^{n+1} & & \alpha^{2n-2} & \alpha^{2n-1} \end{pmatrix},$$

یک ماتریس بررسی توازن برای  $C$  است؛ در اینجا سطر دوم با به کارگیری خاصیت مشتق هسه و ریشه‌های مضاعف به دست آمده است. دقت کنید که  $\alpha^n = 1$ . در اینجا ماتریس  $H_1$  شامل تمامی ستون‌های ممکن با یک ۱ در بالا، به جز  $(1000 \dots 0)^T$  و  $(1100 \dots 0)^T$  است؛ یعنی این کد در واقع هم‌ارز با زیرکد با وزن زوج از یک کد همینگ کوتاه شده است.

## ۶.۱۱ کدهای رید-مولر گسترش یافته

ما کلاسی از کدهای دوری (گسترش یافته) روی  $\mathbb{F}_q$  را تعریف خواهیم نمود که هم‌ارز با کدهای رید-مولر در حالت  $q = 2$  هستند. در ابتدا ایده وزن همینگ را به اعداد صحیحی که به صورت دستگاه اعداد  $q$  تایی نوشته می‌شوند، تعمیم می‌دهیم.

تعریف ۱.۶.۱۱. اگر  $q$  یک عدد صحیح بزرگ‌تر یا مساوی ۲ باشد و برای  $0 \leq \xi_i < q$  و  $i = 0, 1, \dots, m-1$  داشته باشیم  $j = \sum_{i=0}^{m-1} \xi_i q^i$ ، در این صورت تعریف می‌کنیم  $w_q(j) := \sum_{i=0}^{m-1} \xi_i$ . دقت کنید که این مجموع در  $\mathbb{Z}$  رخ داده است. کلاس جدیدی از این کدها به صورت زیر تعریف شده است.

تعریف ۲.۶.۱۱. کد کوتاه شده رید-مولر گسترش یافته (کد GRM) از مرتبه  $r$ ام با طول  $n = q^m - 1$  روی  $\mathbb{F}_q$ ، کد دوری با مولد زیر است:

$$g(x) := \prod_{j=0}^{(r)} (x - \alpha^j),$$

که در آن  $\alpha$  یک عضو اولیه در  $\mathbb{F}_{q^m}$  است و اندیس بالایی  $(r)$  نشان می‌دهد که حاصل ضرب بر روی اعداد صحیح  $j$  می‌باشد که در آن  $0 \leq j < q^m - 1$  و  $0 \leq w_q(j) < (q-1)m - r$ .

کد GRM از مرتبه  $r$ ام با طول  $q^m$  دارای ماتریس مولد  $G^*$  است که از ماتریس مولد  $G$  از کد GRM کوتاه شده با الحاق یک ستون تماماً صفر و سپس یک سطر تماماً یک، به دست آمده است.

دقت کنید که مجموعه توان‌ها در این تعریف از کدهای GRM کوتاه شده، در واقع تحت ضرب بر  $q$  بسته است. فرض کنید  $h(x)$  چند جمله‌ای بررسی کد کوتاه شده GRM از مرتبه  $r$  باشد؛ در این صورت دوگان این کد شامل چند جمله‌ای  $h^*(x)$  به عنوان مولد است، که در آن  $h^*(x)$  از  $h(x)$  با تخصیص مرتبه توان‌های  $x$  به دست آمده است. آن با روشی مشابه با  $g(x)$ ، در اینجا با شرط  $0 < w_q(j) \leq r$ ، تعریف شده است.

تعمیم زیر از قضیه ۸.۴.۵ را داریم.

قضیه ۳.۶.۱۱. دوگان کد GRM مرتبه  $r$  ام 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 بعدها 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 ۴.۶.۱۱. فرض کنید  $C_1$  و  $C_2$  کدهای دوری به طول  $n$  روی  $\mathbb{F}_q$  با چندجمله‌ای‌های بررسی  $f_1(x) := \prod_{i=1}^{k_1} (x - \alpha_i)$ ، به ترتیب، باشند. فرض کنید  $C$  کد دوری با همان طول باشد به طوری که چندجمله‌ای بررسی آن شامل تمامی حاصل ضرب‌های  $\alpha_i \beta_j$  به عنوان ریشه‌های خود باشد؛ در این صورت  $C$  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 ۶.۵، به کار می‌بریم. می‌دانیم که مختص‌های  $a$  و  $b$  می‌توانند به صورت 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 به کار رفته در این بخش را توجیه می‌کند.

قضیه ۵.۶.۱۱. 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 ۶.۴.۵ و ۲.۶.۱۱، 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  $\alpha^j$  است که  $w_2(j) \leq r$ . ریشه‌های چندجمله‌ای بررسی کد کوتاه‌شده RM از مرتبه ۱، شامل توان‌های  $\alpha^j$  با شرط  $w_2(j) = 1$  هستند. حال قضیه با توجه به فرض استقرا، تعریف ۶.۴.۵ و لم ۴.۶.۱۱ اثبات می‌شود. □

ما این بخش را با قضیه‌ای درباره وزن‌های کدهای RM تمام می‌کنیم. این، کاربرد دیگری از قضیه ۵.۶.۸ است.

**قضیه ۶.۶.۱۱.** فرض کنید  $F = F(x_1, x_2, \dots, x_m)$  چند جمله‌ای با درجه  $r$  تعریف شده روی  $\mathbb{F}_2^m$  باشد. اگر تک جمله‌ای‌های  $G$  تشکیل زیرمجموعه‌ای از تک جمله‌ای‌های  $F$  را دهند، می‌نویسیم  $G \subset F$ .  $v(G)$  را تعداد متغیرهایی تعریف می‌کنیم که مشمول در  $G$  نباشند و تعداد تک جمله‌ای‌های  $G$  را با  $|G|$  نمایش می‌دهیم. اگر  $N(f)$  تعداد ریشه‌های  $F$  در  $\mathbb{F}_2^m$  باشند، آنگاه:

$$N(F) = 2^{m-1} + \sum_{G \subset F} (-1)^{|G|} 2^{|G|+v(G)-1}.$$

**اثبات.** برای هر  $G \subset F$ ،  $f(G)$  را تعداد نقاطی در  $\mathbb{F}_2^m$  تعریف می‌کنیم که تمامی تک جمله‌ای‌های  $G$ ، دارای مقدار صفر باشند و سایر تک جمله‌ای‌های  $F$  دارای مقدار ۱. به وضوح داریم:

$$\sum_{H \subset G} f(H) = 2^{v(F-G)}$$

(زیرا این مقدار برابر با تعداد نقاطی از زیرفضای آفین  $\mathbb{F}_2^m$  تعریف شده به صورت  $x_{i_1} = x_{i_2} = \dots = x_{i_v} = 1$  است، که در آن متغیرهایی واقع در  $F - G$  هستند). از قضیه ۶.۶.۸ نتیجه می‌شود:

$$f(G) = \sum_{H \subset G} \mu(H, G) 2^{v(F-G)}.$$

علاوه بر این:

$$N(F) = \sum_{G \subset F, |F-G| \equiv 0 \pmod{2}} f(G).$$

چون  $\sum_{G \subset F} f(G) = 2^m$  داریم:

$$\begin{aligned} N(F) &= 2^{m-1} + \frac{1}{2} \sum_{G \subset F} (-1)^{|F-G|} f(G) \\ &= 2^{m-1} + \frac{1}{2} \sum_{G \subset F} (-1)^{|F-G|} \sum_{H \subset G} \mu(H, G) 2^{v(F-H)} \\ &= 2^{m-1} + \frac{1}{2} \sum_{H \subset F} (-1)^{|F-G|} 2^{v(F-H)} \sum_{H \subset G \subset F} 1 \\ &= 2^{m-1} + \frac{1}{2} \sum_{H \subset F} (-1)^{|F-G|} 2^{v(F-H)} 2^{|F-H|} \\ &= 2^{m-1} + \frac{1}{2} \sum_{G \subset F} (-1)^{|G|} 2^{v(G)+|G|}. \end{aligned}$$

حال این مطلب را روی کدهای RM به کار می‌بریم.

قضیه ۷.۶.۱۱. وزن‌های کدکلمات در  $\mathcal{R}(r, m)$  بر  $2^{\lceil m/r \rceil - 1}$  بخش پذیر 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  $2^m - N(F)$  است. اگر  $G \subset F$  و  $G$  دارای درجه  $d$  باشد، آن‌گاه  $d \leq |G|$ . یعنی  $v(G) \geq m - |G|$ . چون:

$$v(G) + \left\lceil \frac{m - v(G)}{d} \right\rceil \geq \left\lceil \frac{m}{d} \right\rceil,$$

نتیجه با توجه به قضیه ۶.۶.۱۱ حاصل می‌شود. □

## ۶.۱۲ پیشنهادها

خواننده‌ای که علاقه‌مند به مشاهده تابع اثر و خودتوان‌های با وزن زیاد، به کاررفته در اثبات‌ها است، باید فصل ۱۵ مرجع [۴۶] 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-آچیا<sup>۴۰</sup> را یادآوری می‌کنیم که به یک قضیه عمیق در نظریه اعداد توسط ویل<sup>۴۱</sup> 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 ۶.۹ است، خواننده را به مقاله‌ای توسط ون‌لینت<sup>۴۲</sup> و مک‌ویلیامز<sup>۴۳</sup> (۱۹۷۸؛ مرجع [۴۵]) ارجاع می‌دهیم.

## ۶.۱۳ مسائل

۱.۶.۱۳. نشان دهید که کد همینگ [۴, ۲] سه‌تایی، یک کد نادوری می‌باشد.

۲.۶.۱۳. خودتوان یک کد همینگ [۱۵, ۱۱] دودویی را تعیین کنید.

<sup>۴۰</sup>Carlitz-Uchiyama

<sup>۴۱</sup>A. Weil

<sup>۴۲</sup>J. H. van Lint

<sup>۴۳</sup>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 طراحی شده ۵ را بسازید.

۵.۶.۱۳. فرض کنید  $\alpha$  یک عضو اولیه از  $\mathbb{F}_{2^5}$ ، صادق در رابطه  $\alpha^5 = \alpha^2 + 1$  باشد. یک کد BCH کم‌عرض با طول ۳۱ با فاصله طراحی شده ۵، مورد استفاده قرار گرفته است. بردار زیر را دریافت کرده‌ایم:

$$(111 \ 0111 \ 0101 \ 1101 \ 0000 \ 1111 \ 0110 \ 1001)$$

این پیام را با استفاده از روش موجود در بخش ۶.۷ کدگشایی کنید.

۶.۶.۱۳. فرض کنید  $m$  عددی فرد باشد و  $\beta$  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 به طوری 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 به معنای زیر توسعه دهید. فرض کنید  $e > 2$ ،  $n$  یک عدد اول باشد به طوری که  $e \mid (n-1)$  و  $q$  توانی از یک عدد اول باشد و  $q^{(n-1)/e} \equiv 1 \pmod{n}$ . به جای به‌کارگیری عناصر مربعی در  $\mathbb{F}_n$ ، توان‌های  $e$ ام 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.

۱۲.۶.۱۳. فرض کنید  $m$  یک عدد فرد باشد،  $n = 2^m - 1$  و  $\alpha$  یک عضو اولیه از  $\mathbb{F}_{2^m}$  باشد. فرض کنید  $g(x)$  یک مقسوم علیه از  $x^n - 1$  باشد، به طوری که  $g(\alpha) = g(\alpha^5) = 0$ . به دوروش زیر ثابت کنید که کد دوری دودویی با مولد  $g(x)$  دارای کمترین فاصله بزرگتر یا مساوی ۴ است:

الف) با به کارگیری یک قضیه از این فصل.

ب) با نشان دادن این که روابط  $1 + \xi + \eta = 0$  و  $1 + \xi^5 + \eta^5 = 0$  وقتی که  $\xi$  و  $\eta$  متعلق به  $\mathbb{F}_{2^m}$  هستند، غیرممکن است.

ج) با به کارگیری ایده موجود در (ب) نشان دهید که در واقع داریم  $d \geq 5$ .

۱۳.۶.۱۳. نشان دهید که کد گلی سه تایی دارای یک نمایش نادوری است.

۱۴.۶.۱۳. با استفاده از قضیه ۲.۶.۹، کد  $QR [31, 16]$  دارای  $d \geq 7$  است در حالی که کران BCH تنها ایجاب می کند که  $d \geq 5$ . نشان دهید که روش  $AB$  از بخش ۶.۶ نیز ایجاب می کند که  $d \geq 7$ .



## فصل ۷

# کدهای کامل و کدهای به طور یکنواخت

## بسته بندی شده

### ۷.۱ قضیه لوید

در این فصل، توجه خود را به روی کدهای دودویی محدود خواهیم کرد. برای به دست 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 ارائه خواهیم داد. قضیه مربوطه در ابتدا توسط لوید<sup>۱</sup> (۱۹۵۷) (در واقع برای  $q = 2$ ) با به کارگیری روش‌های تحلیلی اثبات شد. از آن روز به بعد 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 سیتکویک<sup>۲</sup> و ون‌لینت<sup>۳</sup> (۱۹۷۷؛ مرجع [۱۷]) ارائه شده است.

<sup>۱</sup> S. P. Lloyd

<sup>۲</sup> D. M. Cvetković

<sup>۳</sup> J. H. van Lint

تعریف ۱.۷.۱. ماتریس مربعی  $A_k$  با اندازه  $2^k$  به صورت زیر تعریف شده است. سطرها و ستون‌ها را با نمایش دودویی از  $0$  تا  $2^k - 1$  شماره گذاری کنید. درایه  $A_k(i, j)$  برابر  $1$  است اگر نمایش‌های  $i$  و  $j$  دارای فاصله همینگ  $1$  باشد، در غیر این صورت  $A_k(i, j) = 0$ .  
از تعریف ۱.۷.۱ فوراً می‌بینیم که:

$$A_{k+1} = \begin{pmatrix} A_k & I \\ I & A_k \end{pmatrix}. \quad (1)$$

لم ۲.۷.۱. مقادیر ویژه  $A_k$  برابر با  $2j - k + 1$  ( $0 \leq j \leq k$ ) با تکرار  $\binom{k}{j}$  هستند.

اثبات. اثبات بر پایه استقراست. برای  $k = 1$  به آسانی حکم ثابت می‌شود. فرض کنید بردار ستونی  $x$  بردار ویژه  $A_k$  متناظر با مقدار ویژه  $\lambda$  باشد؛ در این صورت با توجه به تعریف ۱ داریم:

$$A_{k+1} \begin{pmatrix} x \\ x \end{pmatrix} = (\lambda + 1) \begin{pmatrix} x \\ x \end{pmatrix},$$

$$A_{k+1} \begin{pmatrix} x \\ -x \end{pmatrix} = (\lambda - 1) \begin{pmatrix} x \\ -x \end{pmatrix},$$

□ حال اثبات با توجه به خواص شناخته شده از ضرایب دوجمله‌ای، نتیجه می‌شود.

مهم‌ترین قسمت مشکل این بخش از نظر تکنیکی، تعیین مقادیر ویژه ماتریس‌های سه قطری<sup>۴</sup> است که در اثبات قضیه رخ می‌دهد. برای کاهش نمادگذاری، تعریف زیر را به کار می‌بریم.

تعریف ۳.۷.۱. ماتریس  $Q_e = Q_e(a, b)$  سه قطری به صورت زیر است:

$$(Q_e)_{i,i} := a, \quad 0 \leq i \leq e,$$

$$(Q_e)_{i,i+1} := b - i, \quad 0 \leq i \leq e - 1,$$

$$(Q_e)_{i,i-1} := i, \quad 1 \leq i \leq e,$$

علاوه بر این تعریف می‌کنیم:

$$P_e := P_e(a, b) := \begin{pmatrix} & & & & 1 \\ & & & & 1 \\ & & & & \vdots \\ & & & & 1 \\ \hline & & & & 1 \\ \circ & \circ & \dots & \circ & e & 1 \end{pmatrix}.$$

<sup>۴</sup> tridiagonal matrices

دترمینان این ماتریس‌ها با  $\bar{Q}_e$ ، به ترتیب  $\bar{P}_e$  نمایش داده می‌شود.

لم ۴.۷.۱. فرض کنید  $\Psi_e(x)$  چندجمله‌ای کراچوک  $K_e(x-1; n-1, 2)$  تعریف شده در تعریف ۱.۱.۲ (فصل ۱) و رابطه ۱۹ (فصل ۱) باشد؛ در این صورت:

$$\bar{P}_e(2y-n, n) = (-1)^e e! \Psi_e(y).$$

اثبات. با اضافه نمودن تمام ستون‌ها به ستون آخر و سپس توسیع نسبت به سطر آخر داریم:

$$\bar{Q}_e = (a+e)\bar{Q}_{e-1} - e(a+b)\bar{P}_{e-1}.$$

با بسط  $\bar{P}_e$  نسبت به سطر آخر داریم:

$$\bar{P}_e = \bar{Q}_{e-1} - e\bar{P}_{e-1}.$$

با ترکیب این روابط، رابطه بازگشتی زیر برای  $\bar{P}_e$  ایجاد می‌شود:

$$\bar{P}_{e+1} = (a-1)\bar{P}_e - e(b-a)\bar{P}_{e-1}. \quad (2)$$

بررسی این ادعا که این لم برای  $e=1$  و  $e=2$  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:

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{1k} \\ A_{21} & A_{22} & A_{2k} \\ \dots & \dots & \dots \\ A_{k1} & A_{k2} & A_{kk} \end{pmatrix},$$

که در آن  $A_{ij}$  دارای اندازه  $m_i$  در  $m_j$ ،  $i = 1, 2, \dots, k$ ،  $j = 1, 2, \dots, k$  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 این صورت هر مقدار ویژه  $B$  نیز یک مقدار ویژه  $A$  می‌باشد.

اثبات. فرض کنید  $Bx = \lambda x$  که در آن  $x = (x_1, x_2, \dots, x_k)^T$  را به صورت زیر تعریف کنید:

$$y^T := (x_1, x_1, \dots, x_1, x_2, x_2, \dots, x_2, \dots, x_k, x_k, \dots, x_k),$$

□ که در آن هر  $x_i$  به اندازه  $m_i$  بار تکرار می شود. با استفاده از تعریف  $B$ ، واضح است که  $Ay = \lambda y$ . حال به سراغ قضیه ای اساسی می رویم که نتایج مهمی را دربر دارد.

قضیه ۶.۷.۱. اگر یک کد کامل دودویی  $e$ -تصحیح کننده خطا با طول  $n$  وجود داشته باشد، آن گاه  $\Psi_e(x)$  دارای  $e$  ریشه متمایز در میان اعداد صحیح  $1, 2, \dots, n$  است.

اثبات. این واقعیت که ریشه ها متمایز هستند، یک خاصیت معروف از چندجمله ای های کراچوک است (ارجاع به رابطه ۱۷). برای نشان دادن این که آنها مقادیر صحیح هستند، فرض می کنیم که  $C$  کد خواسته شده در قضیه باشد. ماتریس  $A_n$  را در نظر بگیرید (ارجاع به تعریف ۱.۷.۱). سطرها و ستون های آن را به صورت زیر ثبت کنید. در ابتدا سطرها و ستون ها را با یک عدد متناظر با یک کدکلمه در نظر بگیرید. سپس آنها را به طور متوالی با اعداد متناظر با کلمات موجود در  $C_i := \{x \in \mathbb{F}_2^n \mid d(x, c) = i\}$ ،  $1 \leq i \leq e$  در نظر بگیرید. چون  $C$  کامل است، این باعث ایجاد افزای  $A_n$  به بلوک هایی مانند آنچه در لم ۵.۷.۱ آمد، می گردد. اکنون داریم:

$$B = \begin{pmatrix} \circ & n & \circ & \circ & \circ \\ ۱ & \circ & n-۱ & \circ & \circ \\ \circ & ۲ & \circ & n-۲ & \circ \\ \dots & & & & \dots \\ \circ & & & \circ & e-۱ & \circ & n-e+۱ \\ \circ & & & \circ & \circ & e & n-e \end{pmatrix}.$$

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 لم های ۲.۷.۱، ۴.۷.۱ و ۵.۷.۱ حاصل می گردد.

اثبات داده شده در این بخش، هیچ دیدی درباره ادامه کار نمی دهد (برای مثال آیا ریشه های  $\Psi_e$  دارای یک معنای ترکیبیاتی است؟)، اما دارای این مزیت است که کاملاً مقدماتی می باشد (به جز برای اطلاعات اجتناب ناپذیری از خواص چندجمله ای های کراچوک). در بخش ۷.۵، قضیه ۶.۷.۱ را برای یافتن تمامی کدهای کامل به کار می بریم.

## ۷.۲ چند جمله‌ای مشخصه یک کد

کد دودویی  $C$  با طول  $n$  را در نظر 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<sup>۵</sup> را به صورت زیر داریم:

$$A_C(z) := \sum_{i=0}^n A_i z^i = |c|^{-1} \sum_{u,v \in C} z^{d(u,v)}. \quad (۳)$$

حتی برای به دست آوردن اطلاعات بیشتر درباره فاصله‌ها، در اینجا توزیع خارجی<sup>۶</sup> را ماتریسی مانند  $B$  تعریف می‌کنیم (سطرها با عناصر  $\mathbb{F}_q^n$  و ستون‌ها با  $0, 1, \dots, n$  اندیس‌گذاری شده‌اند)، به طوری که:

$$B(x, i) := |\{c \in C \mid d(x, c) = i\}|. \quad (۴)$$

سطری از  $B$  که با  $x$  اندیس‌گذاری شده، با  $B(x)$  نمایش داده می‌شود. مشاهده می‌کنید که:

$$(A_0, A_1, \dots, A_n) = |c|^{-1} \sum_{x \in C} B(x), \quad (۵)$$

و

$$x \in C \Leftrightarrow B(x, 0) = 1. \quad (۶)$$

تعریف ۱.۷.۲. کد  $C$  یک کد منظم<sup>۷</sup> نامیده می‌شود، اگر تمامی سطرها  $B$  دارای یک ۱ در مکان ۰ برابر باشند. این کد کاملاً منظم<sup>۸</sup> 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. به منظور مطالعه ماتریس  $B$ ، در ابتدا تعدادی جبر معرفی می‌کنیم (به تعریف ۱۱.۱.۱ مراجعه شود).

<sup>۵</sup> distance enumerator

<sup>۶</sup> outer distribution

<sup>۷</sup> regular code

<sup>۸</sup> completely regular

تعریف ۲.۷.۲. اگر  $G$  یک گروه جمعی باشد و  $\mathbb{F}$  یک میدان باشد، آن گاه جبر گروهی  ${}^9 \mathbb{F}G$  (یا بهتر  $(\mathbb{F}G, \oplus, *)$ ) یک فضای برداری روی  $\mathbb{F}$  با عناصر  $G$  به عنوان پایه است که در آن جمع  $\oplus$  و ضرب  $*$  به صورت زیر تعریف شده اند:

$$\sum_{g \in G} \alpha(g)g * \sum_{h \in G} \beta(h)h := \sum_{k \in G} \left( \sum_{g+h=k} \alpha(g)\beta(h) \right) k.$$

برخی مولفین، معرفی یک سمبل اضافی  $z$  و به کارگیری ضرب صوری به صورت زیر را ترجیح می دهند:

$$\sum_{g \in G} \alpha(g)z^g * \sum_{h \in G} \beta(h)z^h := \sum_{k \in G} \left( \sum_{g+h=k} \alpha(g)\beta(h) \right) z^k.$$

ما  $G$  را طوری خواهیم گرفت که برابر با  $\mathbb{F}_2^u$  و  $\mathbb{R} = \mathbb{C}$  باشد. این جبر را با  $A$  نمایش می دهیم. برای گیج نشدن درباره جمع در  $G$  با جمع عناصر  $A$ ، عناصر جمع گروهی را به صورت  $\sum_{x \in \mathcal{R}} \alpha(x)x$  می نویسیم. اگر  $S$  زیرمجموعه ای از  $\mathcal{R}$  باشد، آن گاه این زیرمجموعه را با عنصر  $\sum_{x \in S} x$  در  $A$  هم سان در نظر می گیریم (ما آن را نیز با  $S$  نمایش می دهیم). در اینجا نمادهای زیر را برای مجموعه کلمات با وزن ثابت، به ترتیب گوی های حول صفر، تعریف می کنیم:

$$Y_i := \{x \in \mathcal{R} \mid w(x) = i\}, \tag{۷}$$

$$S_j := \{x \in \mathcal{R} \mid w(x) \leq j\}. \tag{۸}$$

اگر  $C$  کدی با توزیع خارجی  $B$  باشد، آن گاه قراردادی که در بالا مطرح کردیم، ایجاب می کند 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  $(D(x, j) = \sum_{i \leq j} B(x, i))$ ، آن گاه داریم:

$$S_j * C := \sum_{x \in \mathcal{R}} D(x, j)x. \tag{۱۰}$$

فرض کنید  $\chi$  سرشت  $\mathbb{F}_2$  با  $\chi(1) = -1$  باشد. برای هر  $u \in \mathcal{R}$ ، نگاشت  $\chi_u : \mathcal{R} \rightarrow \mathbb{C}$  را به صورت:

$$\forall v \in \mathcal{R} [\chi_u(v) := \chi(\langle u, v \rangle) = (-1)^{\langle u, v \rangle}], \tag{۱۱}$$

<sup>9</sup> group algebra

تعریف می‌کنیم؛ یعنی  $\chi_u(v) = 1$  اگر  $u \perp v$  و  $1 -$  در غیر این صورت. این نگاشت را به تابع خطی بر روی جبر گروهی  $A$  به صورت زیر گسترش می‌دهیم.

$$\chi_u \left( \sum \alpha(x)x \right) := \sum \alpha(x) \chi_u(x). \quad (12)$$

دو ادعای زیر، فوراً از تعریف ما نتیجه می‌شوند. اثبات آنها را به صورت تمرین‌هایی آسان برعهده خواننده می‌گذاریم.

$$\forall u \in \mathcal{R} \forall A \in \mathcal{R} \forall B \in \mathcal{R} [\chi_u(A * B) := \chi(A) \chi_u(B)], \quad (13)$$

$$(\chi_\circ(S) = 2^n, \quad \forall u \neq \circ [\chi_u(S) = \circ]) \Leftrightarrow S = S_n. \quad (14)$$

نتیجه لم ۱.۵.۳ (در اینجا داریم  $q = 2$ ) می‌تواند به صورت زیر نوشته شود:

$$\chi_u(Y_k) = K_k(w(u)). \quad (15)$$

از این نتیجه می‌شود که اگر  $w(u) = x$  آن‌گاه:

$$\chi_u(S_j) = \sum_{k=\circ}^j K_k(x) = \Psi_j(x). \quad (16)$$

(به رابطه ۱۹ مراجعه شود).

فرض کنید  $C$  یک کد باشد. اعداد زیر را در نظر می‌گیریم.

$$C_j := |c|^{-1} \sum_{u \in Y_j} \chi_u(C).$$

این اعداد را قبلاً دیده‌ایم. اگر  $C$  یک کد خطی باشد، آن‌گاه اثبات قضیه ۲.۳.۵ به ما نشان می‌دهد که  $C_j$ ، تعداد کلمات به وزن  $j$  در  $C^\perp$  است. اگر  $C$  خطی نباشد، آن‌گاه هنوز می‌توانیم اعداد  $C_j$  را در نظر بگیریم و اثبات قضیه ۲.۳.۵ را ادامه دهیم تا دریابیم که  $C_j(1-z)^j(1+z)^{n-j}$  که  $\sum_{j=\circ}^n |c|^{-1} 2^{-n}$  شمارنده وزنی کد  $C$  است. این رابطه مابین شمارنده وزنی و اعداد  $C_j$ ، تعریف شده با کمک  $\chi$ ، یک شکل غیرخطی از رابطه مک‌ویلیمز است.

در اینجا دنباله دومی از اعداد را مجدداً با به‌کارگیری سرشت  $\chi$  تعریف می‌کنیم.

تعریف ۳.۷.۲. اعداد مشخصه<sup>۱</sup>  $B_j$  ( $0 \leq j \leq n$ ) از کد  $C$  به صورت زیر تعریف شده‌اند:

$$B_j := |c|^{-2} \sum_{u \in Y_j} |\chi_u(C)|^2.$$

<sup>۱</sup>characteristic numbers

همان طور که قبلاً دیدیم،  $B_j$  تعداد کلمات به وزن  $j$  در کد  $C^\perp$  است، اگر  $C$  یک کد خطی باشد. فرض کنید  $N(C) := \{j \mid 1 \leq j \leq n, B_j \neq 0\}$ . چند جمله ای مشخصه  $F_C$  از کد  $C$  به صورت زیر تعریف شده است:

$$F_C(x) := 2^{n|C|^{-1}} \prod_{j \in N(C)} \left(1 - \frac{x}{j}\right). \quad (17)$$

قضیه ۴.۷.۲. فرض کنید  $\alpha_n, \dots, \alpha_1, \alpha_0$  ضرایب موجود در توسیع کراچوک  $F_C$  باشند؛ در این صورت در  $A$  داریم:

$$\chi_u \left( \sum \alpha_i Y_i * C \right) = S_n.$$

اثبات. فرض کنید  $w(u) = j, u \in \mathcal{R}$ . با استفاده از روابط ۱۳ و ۱۵ داریم:

$$\chi_u \left( \sum \alpha_i Y_i * C \right) = \chi_u \left( \sum \alpha_i Y_i \right) \chi_u(C) = \chi_u(C) \sum \alpha_i K_i(j) = \chi_u(C) F_C(j).$$

اگر  $u \neq 0$ ، آن گاه طرف راست معادله فوق با استفاده از تعریف  $F_C$  برابر با صفر است. اگر  $u = 0$ ، آن گاه طرف راست برابر با  $2^n$  است. حال، حکم با توجه به رابطه ۱۴ اثبات می شود.  $\square$

نتیجه گیری ۵.۷.۲. اگر  $\alpha_n, \dots, \alpha_1, \alpha_0$  ضرایب موجود در توسیع کراچوک  $F_C$  باشند و  $u \in \mathcal{R}$ ، آن گاه:

$$\sum_{i=0}^n \alpha_i B(u, i) = 1.$$

اثبات. رابطه ۹ را به کار ببرید.  $\square$

تعریف ۶.۷.۲. عدد  $s := |N(C)|$ ، فاصله بیرونی  $C$  نامیده می شود.

توجه دارید که اگر  $C$  خطی باشد، آن گاه  $s$  تعداد وزن های ناصفر واقع در  $C^\perp$  است. این نام که تاحدی عجیب است، توسط نتیجه ۵.۷.۲ که نشان می دهد شعاع پوششی  $\rho(C)$  از یک کد (بخش ۳.۴ را ببینید) حداکثر برابر با  $s$  است، تا اندازه کمی توجیه می شود.



### ۷.۳ کدهای به طور یکنواخت بسته‌بندی شده

در این بخش، کدهایی را در نظر 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  $A$  داریم  $S_e * C = S_n$ . حال کدهای  $C$  با  $d \geq 2e + 1$  و  $\rho(C) = e + 1$  را در نظر می‌گیریم (اگر  $d = 2e + 3$ ، آن‌گاه این بدان معناست که  $C$  کامل است). این گوی‌های 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  $g \geq 2e + 1$  به طور یکنواخت بسته‌بندی شده<sup>۱۲</sup> 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 این صورت کدکلمات با فاصله  $e + 1$  تا  $u$  دارای وزن  $e + 1$  می‌باشند. چون آنها باید دارای فاصله‌های متقابل بزرگ‌تر یا مساوی  $2e + 1$  باشند؛ در نتیجه:

$$r \leq \frac{n}{e+1}. \quad (18)$$

حال فرض کنیم  $e + 1$ ،  $n + 1$  را عاد نکند. کدی که در آن  $r = \lfloor n/(e + 1) \rfloor$  تقریباً کامل<sup>۱۳</sup> نامیده می‌شود. به آسانی می‌توان چک نمود که این بدان معناست که  $C$  در کران جانسون (۳) در حالت تساوی صدق می‌کند. در مقاله‌ای که توسط گوتالز<sup>۱۴</sup> و ون تیلبرگ<sup>۱۵</sup> مرجع [۲۵] آمده است، تعریف ۱.۷.۳ با جانشینی  $r$  با دو عدد، وابسته به این که  $e + 1$  یا  $\rho(u, C) = e$ ، تعمیم داده شده است.

قضیه ۲.۷.۳. کد  $C$  با  $\rho(C) = e + 1$  و  $d \geq 2e + 1$  به طور یکنواخت بسته‌بندی شده با پارامتر  $r$  است اگر و تنها اگر در  $A$  داشته باشیم:

$$\{Y_0 \oplus Y_1 \oplus \dots \oplus Y_{e-1} \oplus \frac{1}{r}(Y_e \oplus Y_{e+1})\} * C = S_n.$$

اثبات. این مطلب با توجه به روابط ۳، ۹ و تعریف ۱.۷.۳ نتیجه می‌شود. □

<sup>۱۲</sup>uniformly packed

<sup>۱۳</sup>nearly perfect

<sup>۱۴</sup>J. M. Goethals

<sup>۱۵</sup>H. C. A. van Tilborg

قضیه ۳.۷.۳. کد  $C$  با  $\rho(C) = e + 1$  و  $d \geq 2e + 1$  به طور یکنواخت بسته بندی شده با پارامتر  $r$  است اگر و تنها اگر چند جمله ای مشخصه دارای درجه  $s = e + 1$  و ضرایب کراچوک:

$$\alpha_0 = \alpha_1 = \dots = \alpha_{e-1} = 1, \quad \alpha_e = \alpha_{e+1} = \frac{1}{r},$$

باشد.

اثبات.

(۱) قسمت اگر با توجه به قضیه ۴.۷.۲ و قضیه ۲.۷.۳ نتیجه می شود.

(۲) فرض کنید  $C$  به طور یکنواخت بسته بندی شده باشد. می دانیم 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  $\alpha_0 = \alpha_1 = \dots = \alpha_{e-1} = 1$ ،  $\alpha_e = \alpha_{e+1} = 1/r$ . اگر

$w(u) = j \neq 0$ ،  $u \in \mathcal{R}$  و  $\chi_u(C) \neq 0$ ؛ در این صورت با استفاده از روابط ۱۳ و ۱۴ و قضیه

۲.۷.۳ داریم  $F(j) = 0$ . حال با استفاده از رابطه ۱۷ نتیجه می شود که  $F_C(x)$ ،  $F(x)$  را عاد

می کند؛ بنابراین،  $s = e + 1$  و  $F(x) = aF_C(x)$  برای یک مقدار  $a$ . با جانشینی  $x = 0$  داریم

$a = 1$  (مجدداً با به کارگیری قضیه ۲.۷.۳).  $\square$

قضیه زیر فرمول بندی متفاوتی از قضیه ۳.۷.۳ است.

قضیه ۴.۷.۳. اگر کد به طور یکنواخت بسته بندی شده  $C$  با  $\rho(C) = e + 1$  و  $d \geq 2e + 1$  موجود باشد،

آن گاه چند جمله ای:

$$F(x) := \sum_{i=0}^{e-1} K_i(x) + \frac{1}{r} [K_e(x) + K_{e+1}(x)]$$

دارای  $e + 1$  ریشه صحیح مجزا در بازه  $[1, n]$  می باشد و  $F(0) = 2^n |c|^{-1}$ .

در ابتدا مشاهده می کنید که  $C$  یک کد کامل است؛ یعنی  $d = 2e + 3$ ؛ در این صورت 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  $F(0)$  می تواند به صورت زیر نوشته شود:

$$|c| \left\{ \sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r} \binom{n+1}{e+1} \right\} = 2^n, \quad (19)$$

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.

در واقع رابطه ۱۹ در حالت کلی درست است، اگر  $r$  را به عنوان 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 این که یک کد داده شده با استفاده از این تعریف به طور یکنواخت بسته بندی شده است، کار آسانی نیست.

در اینجا حالت خاصی را در نظر می گیریم؛ یعنی یک کد خطی با  $e = 1$ . برای این که  $C$  به طور یکنواخت فشرده باشد، چند جمله ای 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  $w_1$  و  $w_2$  رخ می دهد. حال فرض کنید که  $C^\perp$  چنین کد دو-وزنی با شمارنده وزنی:

$$A_{C^\perp}(z) = 1 + N_1 z^{w_1} + N_2 z^{w_2},$$

باشد. رابطه مک ویلیامز (ارجاع به بخش ۷.۲) را در نظر بگیرید و برای  $(1+z)^{n-x}(1-z)^x$  (ارجاع به رابطه ۷) رابطه زیر را جانشین کنید:

$$\sum_{k=0}^{\infty} K_k(x) z^k.$$

چون فرض کرده ایم که  $C$  دارای کمترین-فاصله  $d \geq 3$  است، با به دست آوردن ضرایب  $z^0$ ،  $z^1$  و  $z^2$  سه معادله به صورت زیر داریم:

$$1 + N_1 + N_2 = 2^n |c|^{-1},$$

$$K_k(0) + N_1 K_k(\omega_1) + N_2 K_k(\omega_2) = 0, \quad (k = 1, 2).$$

با استفاده از تعریف داریم  $F_C(0) = 2^n |c|^{-1}$  و  $F_C(\omega_1) = F_C(\omega_2) = 0$ ؛ در این صورت برای ضرایب  $\alpha_0$ ،  $\alpha_1$  و  $\alpha_2$  در توسعه کراچوک  $F_C(x)$  با استفاده از رابطه ۱۱ داریم:

$$\alpha_0 + \alpha_1 n + \alpha_2 \binom{n}{2} = 2^n |c|^{-1},$$

$$\alpha_0 + \alpha_1 (n - 2\omega_i) + \alpha_2 \{2\omega_i^2 - 2n\omega_i + \binom{n}{2}\} = 0, \quad (i = 1, 2).$$

ما این معادلات را با معادلات متناظر با  $N_1$  و  $N_2$  مقایسه می کنیم. این مطلب نشان می دهد که  $\alpha_0 = 1$ . تعریف می کنیم:

$$r := 2(n+1)\omega_1 - 2\omega_1^2 - \frac{1}{2}n(n+1).$$

در این صورت نتیجه می شود که  $\alpha_1 = \alpha_2 = 1/r$  اگر  $\omega_1 + \omega_2 = n + 1$ ؛ بنابراین، مشخصه سازی زیر را از کدهای ۱-تصحیح کننده خطای به طور یکنواخت بسته بندی شده داریم:

قضیه ۵.۷.۳. کد خطی  $C$  با  $\rho(C) = 2$  و  $d \geq 3$  به طور یکنواخت بسته بندی شده است اگر و تنها اگر  $C^\perp$  یک کد دو-وزنی با وزن های  $w_1$  و  $w_2$  صادق در رابطه  $w_1 + w_2 = n + 1$  باشد.

در مرجع [۲۵] نشان داده شده است که اگر ما تعریف کلی تر کدهای به طور یکنواخت بسته بندی شده را بپذیریم، آنگاه می توانیم محدودیت  $w_1 + w_2 = n + 1$  را حذف کنیم. این قضیه نیز برای  $e > 1$  با  $e + 1$  وزن در  $C^\perp$  به جای دو تا، درست است.

### ۷.۴ مثال هایی از کدهای به طور یکنواخت بسته بندی شده

۱.۷.۴. یک کد هادامارد (ارجاع به بخش ۴.۱)

کد هادامارد  $(12, 24, 6)$  را در نظر بگیرید. این کد را برای به دست آوردن کد  $C(11, 24, 5)$  پنچر کنید. واضح است که هر کلمه  $z$  می تواند دارای فاصله ۲ یا ۳ تا حداکثر چهار کد کلمه باشد و اگر این رخ دهد، آنگاه وضعیت زیر را داریم (پس از تغییر علامت به نماد  $\pm$  و ضرب مناسب ستون ها در  $-1$ ):

$$z = \quad - - \quad + + + \quad + + + \quad + + + ,$$

$$x_1 = \quad + + \quad + + + \quad + + + \quad + + + ,$$

$$x_2 = \quad - - \quad - - - \quad + + + \quad + + + ,$$

$$x_3 = \quad - - \quad + + + \quad - - - \quad + + + ,$$

$$x_4 = \quad - - \quad + + + \quad + + + \quad - - - ,$$

این بدان معناست که ماتریس هادامارد اصلی از مرتبه ۱۲ دارای چهار سطر  $(+, x_1), (-, x_2), (-, x_3), (-, x_4)$  است. بردار سطری  $(-4, -4, -4, 0, 0, \dots, 0)$  ترکیب خطی از این چهار سطر است؛ بنابراین، باید به سطرهای باقی مانده ماتریس هادامارد عمود باشد که به وضوح غیرممکن است. از این نتیجه می شود که کلمه  $z$  دارای فاصله ۲ یا ۳ تا حداکثر سه کد کلمه است. از رابطه ۱۹ نتیجه می شود که مقدار متوسط کد کلمات با فاصله ۲ یا ۳ تا کد کلمه  $z$  با  $\rho(z, C) > 1$  برابر سه است؛ بنابراین، این تعداد همواره برابر با سه است. از این رو  $C$  به طور یکنواخت بسته بندی شده با  $r = 3$  است. در این مثال،  $C$  غیرخطی است.

توجه دارید که در این مثال،  $e + 1, n + 1$  را عادی می کند؛ بنابراین، رابطه ۱۹ برقرار است، اما برابر با ۳ نیست. این کد یک کد تقریباً کامل نمی باشد.

## ۲.۷.۴. یک کد RM پنچر شده

فرض کنید  $V$  فضای برداری با  $\mathbb{F}_2$  بعدی روی  $\mathbb{F}_2$  باشد. فرض کنید  $W$  مجموعه با ۳۵ نقطه  $x$  در  $V \setminus \{0\}$  روی فرم درجه ۲ با معادله  $x_1x_2 + x_3x_4 + x_5x_6 = 0$  باشد. این بردارها را به عنوان ستون‌هایی از یک ماتریس  $6 \times 35$ ،  $G$  در نظر بگیرید. مانند بخش ۴.۵، می‌بینیم که  $\lambda$  امین سطر  $G$ ، تابع مشخصه اشتراک  $W$  و ابرصفحه‌هایی با معادله  $x_i = 1$  ( $1 \leq i \leq 6$ ) است؛ بنابراین، وزن یک ترکیب خطی  $a^T G$  ( $a \in V$ )، 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 این که  $a = 0$ ). با جانشین کردن و استفاده از تبدیل آفین:

$$y_2 = x_2, \quad y_3 = x_3 + a_4 x_2, \quad y_4 = x_4 + a_3 x_2,$$

$$y_5 = x_5 + a_6 x_2, \quad y_6 = x_6 + a_5 x_2,$$

(که معکوس‌پذیر است) می‌بینیم که باید تعداد جواب‌های معادله زیر را بشماریم:

$$(1 + a_2 + a_3 a_4 + a_5 a_6) y_2 + y_3 y_4 + y_5 y_6 = 0.$$

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  $G$  به عنوان ماتریس بررسی توازن است، دارای دوگان  $C^\perp$ ، یک کد دو-وزنی با وزن‌های ۱۶ و ۲۰، است. چون کد  $C$  تصویری است، داریم  $d \geq 3$ . با استفاده از ملاحظه زیر (رابطه ۶.۷.۲) داریم  $\rho(C) = 2$ ؛ بنابراین، با استفاده از ۵.۷.۳،  $C$  به طور یکنواخت بسته‌بندی شده با  $r = 10$  است (با استفاده از ۱۹). روش مشابه در ابعاد بالاتر کار می‌کند.

## ۳.۷.۴. کدهای پریاراتا

در سال ۱۹۶۸، پریاراتا<sup>۱۶</sup> مرجع [۵۷] کلاسی از کدهای غیرخطی ۲-تصحیح‌کننده خطا را طراحی نمود که ثابت شده است آنها دارای خواص بسیار جالبی هستند. تعریف او بر پایه 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 پریاراتا توسط باکر<sup>۱۷</sup> و ویلسن<sup>۱۸</sup> و مولف این کتاب (ر.ک. مرجع [۷۲]) است.

<sup>۱۶</sup>F. P. Preparata

<sup>۱۷</sup>R. D. Baker

<sup>۱۸</sup>R. M. Wilson

در زیر،  $m$  ( $m \geq 3$ ) فرد است و  $n = 2^m - 1$ . ما کد  $\bar{T}$  با طول  $2^{m+1} = 2n + 2$  را تعریف خواهیم کرد. کلمات، توسط زوج‌های  $(X, Y)$  توصیف می‌شوند که در آن  $X \subset \mathbb{F}_{2^m}$  و  $Y \subset \mathbb{F}_{2^m}$ . به طور معمول، زوج  $(X, Y)$  را به عنوان تابع مشخصه متناظر تفسیر می‌کنیم که یک  $(0, 1)$ -بردار با طول  $2^{m+1}$  است.

تعریف ۴.۷.۴. کد پاراتای گسترش یافته  $\bar{T}$  با طول  $2^{m+1}$ ، شامل کدکلمات توصیف شده توسط تمامی زوج‌های  $(X, Y)$  صادق در روابط زیر است:

$$(1) \quad |X| \text{ زوج است، } |Y| \text{ زوج است.}$$

$$(2) \quad \sum_{x \in X} x = \sum_{y \in Y} y$$

$$(3) \quad \sum_{x \in X} x^2 + (\sum_{x \in X} x)^2 = \sum_{y \in Y} y^2$$

کد  $T$  با صرف نظر کردن از مختصات متناظر با مکان‌های صفر در اولین نیمه، به دست آمده است.

در ابتدا نشان می‌دهیم که  $T$  دارای  $2^{2n-2m}$  کلمه است. می‌توانیم  $X$  صادق در شرط (۱) را به  $2^n$  طریق انتخاب کنیم. سپس مشاهده می‌کنیم که چون  $m$  فرد است، چند جمله‌ای مینیمال  $m_2(x)$  برای  $\mathbb{F}_{2^m}$  دارای درجه  $m$  است. بنابراین، کد BCH با طول  $n$  و فاصله طراحی شده ۵ دارای بعد  $n - 2m$  است. این مطلب در ادامه ایجاب می‌کند که برای  $X$  داده شده، معادلات (۲) و (۳) دارای  $2^{n-2m}$  جواب  $Y \subset \mathbb{F}_{2^m}^*$  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  $\bar{T}$  دارای کمترین-فاصله ۶ است. از تعریف ۴.۷.۴ قسمت (۱) می‌بینیم که کمترین-فاصله، زوج است و هم‌چنین این که اگر  $(X, Y)$  در دو شرط فوق صدق کند، آنگاه  $(Y, X)$  نیز چنین است. فرض کنید دو کلمه  $(X, Y_1)$  و  $(X, Y_2)$  را داریم و قرار دهید  $Y := Y_1 \Delta Y_2$ ؛ در این صورت از تعریف ۴.۷.۴ قسمت (۲) داریم:

$$\sum_{y \in Y} y = \sum_{y \in Y} y^2 = 0,$$

یعنی با استفاده از کران BCH داریم  $|Y| \geq 5$ ؛ بنابراین، در این حالت دو کلمه دارای فاصله بزرگ‌تر یا مساوی ۶ هستند. تنها مطلبی که باقی می‌ماند این است که احتمال  $(X_1, Y_1)$  و  $(X_2, Y_2)$  را به شرط زیر در نظر بگیریم:

$$|X_1 \Delta X_2| = |Y_1 \Delta Y_2| = 2.$$

فرض کنید  $X_1 \Delta X_2 = \{\alpha, \beta\}$  و  $Y_1 \Delta Y_2 = \{\gamma, \delta\}$  و فرض کنید  $s + \alpha$  مجموع عناصر در  $X_1$  باشد. در

این صورت، قسمت (۲) و (۳) از ۴.۷.۴ ایجاب می‌کنند:

$$\alpha + \beta = \gamma + \delta,$$

$$s^2(\alpha + \beta) + s(\alpha + \beta)^2 = \gamma^3 + \delta^3.$$

از اینها داریم  $(s + \gamma)^3 + (s + \delta)^3 = 0$ ؛ 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 پریاراتای  $T$  با طول  $1 - 2^{m+1}$  ( $m \geq 3$  فرد است)  $|T| = 2^k$  که در آن  $k = 2^{m+1} - 2m - 2$  و کمترین-فاصله برابر با ۵ است.

از رابطه ۱۹ در می‌یابیم که مقدار متوسط  $r$  برای کد  $T$  برابر  $(2^{m+1} - 1)/3$  است و سپس رابطه ۱۸ ایجاب می‌کند که  $r$  ثابت بوده و برابر  $(2^{m+1} - 1)/3$  است؛ یعنی  $T$  تقریباً کامل است.

اگر در تعریف ۴.۷.۴ در نظر بگیریم  $m = 3$ ، آنگاه کد نرداستروم-رایینسن 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  $2^t + 1 := s$  جای‌گزین کنیم که در آن نیاز داریم  $x \rightarrow x^s$  و  $x \rightarrow x^{s-2}$  نگاشت‌های  $1-1$  از  $\mathbb{F}_m$  به خودش باشند؛ در این صورت قسمت اول استدلال مربوط به کمترین-فاصله با استدلال مربوط به قضیه ۵.۶.۶ جای‌گزین می‌شود. این مطلب را به صورت 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  $2^{m+1}$  است. با توجه به این مطلب و یک استدلال شمارشی نتیجه می‌گیریم که اگر ما  $T$  را در نظر بگیریم و آن را به تمامی کلمات با فاصله ۳ تا  $T$  اضافه کنیم، کد همینگ با طول  $2^{m+1} - 1$  را به دست می‌آوریم. در قضیه ۷.۷.۴ یک ساختار مستقیم ارائه می‌دهیم.

**قضیه ۷.۷.۴** اجتماع کد پریاراتای  $T$  با طول  $1 - 2^{m+1}$  ( $m$  فرد) و مجموعه کلمات دارای فاصله ۳ با  $T$ ، برابر کد همینگ با طول  $n$  است.

**اثبات.** چون  $T$  در رابطه ۳ صدق می‌کند، می‌دانیم که  $|T| \cdot \frac{n-1}{3}$  کلمه دارای فاصله ۳ با  $T$  وجود دارد. بنابراین، اجتماع  $C$  شامل  $2^{n-m-1}$  کلمه است که به اندازه کد همینگ با طول  $n$  است.

حال تعریف می‌کنیم  $\bar{T} := C_0$  و برای  $\alpha \in \mathbb{F}_m^*$ ،  $C_\alpha$  را کد به دست آمده توسط اضافه نمودن کلمه متناظر با  $(\{0, \alpha\}, \{0, \alpha\})$  به کلمات  $C_0$  تعریف می‌کنیم. به وضوح هر  $C_\alpha$  تنها شامل بردارهای با وزن زوج است. اگر وزن ۲ رخ دهد، آنگاه  $C_0$  شامل کلمه‌ای متناظر با  $X = \{0, \alpha\}$ ،  $Y = \{0, \alpha, \beta, \gamma\}$

خواهد بود که با تعریف ۴.۷.۴ قسمت (۲) در تناقض است. بنابراین، هر  $C_\alpha$  دارای کمترین-فاصله ۴ است. از اثبات قضیه ۲۲ نتیجه می شود که  $C_\alpha$  ها دوبه دو مجزا هستند ( $\alpha \in \mathbb{F} := \mathbb{F}_{2^m}$ ). ادعا می کنیم 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 معادله ای از نوع  $x^3 = \alpha$  منجر می گردد که امکان پذیر است، زیرا  $m$  فرد است. از این پارامترها و خطی بودن، نتیجه می گیریم که  $\bar{H}$ ، کد همینگ گسترش یافته با طول  $n + 1$  است. این مطلب، ادعا درباره  $C$  را اثبات می کند.  $\square$

توجه دارید که از قضیه ۷.۷.۴ نتیجه می شود که ترکیبات خطی کد کلمات کد پرپاراتا، مشمول در کد همینگ است.

## ۷.۵ قضایای عدم وجود

این مطلب توسط تیتاوینین<sup>۱۹</sup> [۶۸] و ون لینت<sup>۲۰</sup> [۴۱] نشان داده شده است که کدهای گلی تنها کدهای کامل غیربیدیهی  $e$ -تصحیح کننده خطا با  $e > 1$  روی الفبای دلخواه  $Q$  هستند، به طوری که  $|Q|$  توانی از یک عدد اول است. برای  $e > 2$ ، محدودیت روی  $Q$  می تواند به صورتی که توسط بست<sup>۲۱</sup> [۷] و هونگ<sup>۲۲</sup> [۷۴] نشان داده شده است، حذف گردد، اما اثبات آن بسیار مشکل تر می باشد. برای  $e = 1$ ، کدهای همینگ را دیده ایم. هم چنین مثال هایی از کدهای کامل غیرخطی با  $e = 1$  وجود دارد (ارجاع به مساله ۴.۷.۷).

در سال ۱۹۷، تیلبرگ<sup>۲۳</sup> [۶۹] نشان داد که کدهای به طور یکنواخت بسته بندی شده  $e$ -تصحیح کننده خطا با  $e > 3$  وجود ندارند و آنهایی که  $e \leq 3$  همگی شناخته شده اند. در این بخش، برخی ایده ها مربوط به روش به کار رفته برای اثبات این نتایج را ارائه خواهیم داد. کافی است تا حالت دودویی را در نظر بگیریم.

قضیه ۱.۷.۵. اگر  $C$  یک کد دودویی کامل  $e$ -تصحیح کنه خطا با  $e > 1$  باشد، آن گاه  $C$  یک کد تکرار یا یک کد گلی دودویی است.

اثبات. با استفاده از قضیه لوید (۶.۷.۱)، چند جمله ای  $\Psi_e$  دارای ریشه های  $x_1 < x_2 < \dots < x_e$  می باشد که اعداد صحیحی در بازه  $[1, n]$  هستند. با استفاده از تعریف  $\Psi_e$  و رابطه (۱۲)، توابع متقارن

<sup>۱۹</sup>A. Tietäväinen

<sup>۲۰</sup>J. H. van Lint

<sup>۲۱</sup>M. R. Best

<sup>۲۲</sup>Y. Hong

<sup>۲۳</sup>van Tilborg



مقدماتی از درجه ۱ و ۲ از ریشه‌ها شناخته شده هستند:

$$\sum_{i=1}^e x_i = \frac{1}{4} e(n+1), \quad (20)$$

$$\sum_{i < j} x_i x_j = \frac{1}{44} e(e-1) \{3n^2 + 3n + 2e + 2\}. \quad (21)$$

مشاهده می‌کنید که رابطه ۲۰ نیز از رابطه ۶ نتیجه می‌شود که نشان می‌دهد:

$$x_{e-i+1} = n+1 - x_i. \quad (22)$$

از روابط ۲۰ و ۲۱ داریم:

$$\sum_{i=1}^e \sum_{j=1}^e (x_i - x_j)^2 = \frac{1}{4} e^2 (e-1) \left\{ n - \frac{2e-1}{3} \right\}. \quad (23)$$

برای یافتن حاصل ضرب 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 ۶.۳.۱ با رابطه ۱۲ (فصل ۱) داریم:

$$\prod_{i=1}^e x_i = e! 2^l, \quad \text{برای یک مقدار صحیح } l. \quad (24)$$

در روشی مشابه،  $\Psi_e(1)$  و  $\Psi_e(2)$  را محاسبه می‌کنیم که به روابط زیر منجر می‌شود:

$$\prod_{i=1}^e (x_i - 1) = 2^{-e} (n-1)(n-2) \cdots (n-e), \quad (25)$$

$$\prod_{i=1}^e (x_i - 2) = 2^{-e} (n-1-2e)(n-2) \cdots (n-e). \quad (26)$$

حال نتیجه درباره  $x_1, x_2, \dots, x_e$  را از این روابط استخراج می‌کنیم. فرض کنید  $A(x)$  بزرگ‌ترین مقسوم‌علیه فرد  $x$  باشد. در این صورت 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 به طوری که  $A(x_i) = A(x_j)$ ؛ بنابراین،  $2x_i \leq 2x_j$  و از این رو  $2x_1 \leq x_e$ . حال رابطه ۲۳ ایجاب می‌کند:

$$x_e - x_1 \geq \frac{1}{3} (n+1). \quad (27)$$

اگر ما  $x_e$  و  $x_1$  را ثابت نگه داریم، آنگاه سمت چپ رابطه ۲۳ دارای کمترین مقدار است، اگر:

$$x_2 = x_3 = \cdots = x_{e-1} = \frac{1}{3} (x_1 + x_e).$$

با جانشین نمودن این مقادیر در رابطه ۲۳، داریم:

$$(x_e - x_1)^2 \leq \frac{1}{4} e(e-1) \left( n - \frac{2e-1}{3} \right), \quad (28)$$

که ما آن را با رابطه ۲۷ ترکیب می‌کنیم. نتیجه به صورت زیر است:

$$n + 1 \leq \frac{9}{4} e(e-1). \quad (29)$$

حال روابط ۲۵ و ۲۶ را در نظر بگیرید. چون اگر  $x \in \mathbb{N}$ ، آن‌گاه  $(x-1)(x-2)$  همواره زوج است، داریم:

$$(n-1-2e)(n-1)(n-2)^2(n-3)^2 \cdots (n-e)^2 \equiv 0 \pmod{2^{2e}}. \quad (30)$$

اگر  $e = \frac{1}{4}(n-1)$ ، آن‌گاه این مطلب بدیهی است؛ یعنی  $C$  کد تکراری است. فرض کنید  $e < \frac{1}{4}(n-1)$ . نیز  $2^\alpha$  را بزرگ‌ترین توان ۲ در هر عامل  $n-j$  در طرف چپ رابطه ۳۰ در نظر بگیرید که شامل  $n-1-2e$  باشد؛ در این صورت بزرگ‌ترین توان ۲ که طرف چپ رابطه ۳۰ را عادی می‌کند حداکثر برابر با  $2^{2\alpha+2e-2}$  است که ایجاب می‌کند  $\alpha \geq \frac{1}{4}e + 1$ .

بنابراین:

$$n > 2^{1+(1/3)e}. \quad (31)$$

اگر  $e$  بزرگ باشد، آن‌گاه رابطه ۳۱ متناقض با رابطه ۲۹ است. مقادیر کوچک  $e$  که به واسطه رابطه ۲۹، مقادیر کوچک  $n$  را ایجاب می‌کند، به آسانی بررسی می‌شوند. در واقع، 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. در واقع،  $e = 3$  می‌تواند حتی کاملاً بدون استفاده از قضیه لویید مورد بحث واقع شود. این مطلب در مساله ۱.۷.۷ نشان داده شده است.  $\square$

دلیل به کار رفته برای نشان دادن این‌که تمامی کدهای به‌طور یکنواخت بسته‌بندی شده، 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 بسته‌بندی شده را لیست می‌کند.

اثبات. با تعمیم قضیه لوید شروع می‌کنیم؛ یعنی قضیه ۴.۷.۳. در روندی دقیقاً مشابه با روشی که رابطه ۲۸، به ترتیب رابطه ۳۱، را ثابت کردیم، داریم:

$$x_{e+1} - x_1 \leq (e+1) \left( \frac{n+1}{2} \right)^{1/2}, \quad (32)$$

$$n > 2^{e/2}. \quad (33)$$

دلیلی که منجر به رابطه ۲۷ گردد باید تغییر کند. در روشی متفاوت، ریشه‌ها را به صورت  $y_1, y_2, \dots, y_{e+1}$  شماره‌گذاری می‌کنیم که در آن  $y_j = A(y_j) 2^{\alpha_j}$  و  $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_{e+1}$ . از طرف دیگر داریم (با نوشتن  $(a, b)$  برای ب.م.م  $a$  و  $b$ ):

$$\begin{aligned} \prod_{i=1}^e \frac{|y_i - y_{i+1}|}{y_i} &\geq \prod_{i=1}^e \frac{(y_i, y_{i+1})}{y_i} = \prod_i \frac{(A(y_i), A(y_{i+1})) 2^{\alpha_i}}{y_i} \\ &\geq \prod_{i=1}^e \frac{1}{A(y_i)} \geq \frac{1}{A(y_1, \dots, y_{e+1})} = \frac{A(|c|)}{A(r)A((e+1)!)} \\ &\geq \frac{1}{rA((e+1)!)}. \end{aligned}$$

در اینجا، معادله آخر از رابطه ۱۹ نتیجه می‌شود. از طرف دیگر، داریم:

$$\begin{aligned} \prod_{i=1}^e \frac{|y_i - y_{i+1}|}{y_i} &\leq \frac{(x_{e+1} - x_1)^e}{y_1 \dots y_e} \leq \frac{n(x_{e+1} - x_1)^e}{x_1 x_2 \dots x_{e+1}} \\ &= \frac{1}{n(x_{e+1} - x_1)^e} r(e+1)! \cdot \frac{2^{e+1}|c|}{2^n}. \end{aligned}$$

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:

$$(x_{e+1} - x_1)^e \geq \frac{(e+1)}{A((e+1)!)} \frac{1}{2^{e+1}} (n-1)(n-2) \dots (n-e+1). \quad (34)$$

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 می‌کند. حالات  $e=1$  و  $e=2$  به آسانی و به‌طور مستقیم توسط قضیه ۴.۷.۳ می‌توانند مورد بحث قرار گیرند. به‌عنوان یک نتیجه، حالات متناهی بسیاری به‌طور مجزا بررسی شده‌اند. ما جزئیات (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 به طور یکنواخت بسته بندی شده.

توصیف	نوع	$ c $	$n$	$e$
$\{0, 1\}^n$	کامل	$2^n$	$n$	۰
کد همینگ (و سایر کدها)	کامل	$2^{n-m}$	$2^m - 1$	۱
کد همینگ کوتاه شده	تقریباً کامل	$2^{n-m}$	$2^m - 2$	۱
رجوع به ۱.۷.۷				
رجوع به ۲.۷.۴	به طور یکنواخت فشرده	$2^{n-2m}$	$2^{2m-1} \pm 2^{m-1} - 1$	۱
کد پریاراتا	تقریباً کامل	$2^{n+1-4m}$	$2^{2m} - 1$	۲
کد $BCH$ (رجوع به ۲.۷.۷)	به طور یکنواخت فشرده	$2^{n-4m-2}$	$2^{2m+1} - 2$	۲
رجوع به ۱.۷.۴	به طور یکنواخت فشرده	۲۴	۱۱	۲
کد گلی	کامل	۲۱۲	۲۳	۳
کد تکرار	کامل	۲	$2e + 1$	$e$
$\{0\}$	کامل	۱	$e$	$e$

## ۷.۶ پیشنهادها

کدهای کامل به چندین روش تعمیم یافته اند (برای مثال متریک های دیگری به جز فاصله همینگ، الفباهای ترکیب شده). برای یک بررسی (شامل بسیاری از منابع) خواننده باید به مرجع [۴۴] مراجعه کند. نسخه تغییر یافته ای از اثبات عدم وجود تیتاوا این می تواند در منبع [۴۶] و نیز بسیاری از منابع دیگر یافت شود.

کامل ترین اطلاعات درباره کدهای به طور یکنواخت بسته بندی شده می تواند در مرجع [۶۹] یافت شود. برای مشاهده ارتباط با نظریه طرح <sup>۲۴</sup>، به مراجع [۱۱] و [۴۶] ارجاع می دهیم.

مساله امکان وجود کدهای ۲-تصحیح کننده خطای شناخته نشده بر روی الفباهای  $Q$ ، در حالتی که  $|Q|$  توانی از یک عدد اول نباشد، به نظر بسیار مشکل می آید، اما غیرممکن نیست. حالت  $e = 1$  امیدوارکننده به نظر می رسد.

بسیاری از ایده ها و روش هایی که در این بخش به کار رفته اند (برای مثال بخش ۷.۲) توسط دلسارت <sup>۲۵</sup> مطرح شده اند.

<sup>۲۴</sup> design theory

<sup>۲۵</sup>P. Delsarte

۱.۷.۷. نشان دهید کد همینگ دودویی کوتاه شده  $[2^m - 2, 2^m - m - 2]$  تقریباً کامل است.

۲.۷.۷. فرض کنید  $C$  کد BCH دودویی با طول  $n = 2^{2m+1} - 1$  و با فاصله طراحی شده ۵ باشد. با استفاده از محاسبه صریح تعداد کدکلمات با فاصله ۳ تا کدکلمه  $u$  با  $\rho(u, C) \geq 2$  نشان دهید  $C$  به طور یکنواخت بسته بندی شده با پارامتر  $r = \frac{1}{4}(n - 1)$  است.

۳.۷.۷. نشان دهید که یک کد تقریباً کامل  $C$  وجود دارد به طوری که  $\bar{C}$  کد نرد-استروم است.

۴.۷.۷. فرض کنید  $H$ ، کد همینگ  $[7, 4]$  دودویی باشد.  $f$  را روی  $H$  با  $f(0) = 0$  و  $f(c) = 1$  اگر  $c \neq 0$  تعریف کنید. فرض کنید  $C$  کد با طول ۱۵ با کدکلمات:

$$(x, x + c, \sum_{i=1}^7 x_i + f(c)), \quad c \in H, x \in \mathbb{F}_2^7.$$

باشد. نشان دهید  $C$  کامل است و  $C$  هم ارز با یک کد خطی نیست.

۵.۷.۷. نشان دهید که یک کد کامل دودویی ۲-تصحیح کننده خطا بدیهی است.

۶.۷.۷. فرض کنید  $C$  یک کد به طور یکنواخت بسته بندی شده با طول  $n$ ،  $e = 1$  و  $r = 6$  باشد. نشان دهید  $n = 27$  و یک ساختار از  $C$  را ارائه دهید.

۷.۷.۷. در مثال ۳.۳.۳ دیدیم که خطوط  $PG(2, 2)$ ، کد همینگ  $[7, 4]$  را تولید می کند. کد گسترش یافته برابر یک کد  $[8, 4, 4]$  است. یک نفر ممکن است امید داشته باشد که با به کارگیری  $PG(2, q)$ ، می توان کد  $C$  روی  $\mathbb{F}_q$  را با طول  $q^2 + q + 2$ ،  $d = 4$  و  $|c| = q^{n-4}$  بیابد. این در واقع مثالی از یک کد به طور یکنواخت بسته بندی شده در حالت کلی تر است (ر.ک. مرجع [۲۵]). حالت  $q = 3$  و  $|c| = 3^1$  را در نظر بگیرید. نشان دهید چنین کدی وجود ندارد.

راهنمایی: زوج های  $(x, c)$  را به دوروش با  $x \in \mathbb{F}_3^4$  و  $c \in C$  و  $d(x, c) = 2$  شمارش کنید.  $A_4$  و سپس  $A_5$  را محاسبه کنید.

۸.۷.۷. الفبای  $\mathbb{Z}_m$  ( $m$  فرد) با فاصله لی را در نظر بگیرید. یک کد کامل تصحیح کننده یک خطا با طول  $n = \frac{1}{4}(m^2 - 1)$  بسازید.

# فصل ۸

## کدهای روی $\mathbb{Z}_4$

### ۸.۱ کدهای چهارتایی

در سال ۱۹۹۴ (مرجع [۸۸]) را به عنوان راهنمایی برای این فصل مشاهده کنید) نشان داده شد که چندین کد دودویی معروف را با ساخت یک کد روی الفبای  $\mathbb{Z}_4$  و سپس تصویر کردن مختصات آن به  $\mathbb{Z}_2^2$  می توان ساخت. در ابتدا کدهای روی  $\mathbb{Z}_4$  را در حالت کلی مطالعه می کنیم.

تعریف ۱.۸.۱. اگر  $C$  یک زیرگروه جمعی از  $\mathbb{Z}_4^n$  باشد، آن گاه  $C$  را یک کد بلوکی خطی به طول  $n$  روی  $\mathbb{Z}_4$  یا یک کد چهارتایی<sup>۱</sup> می نامیم.

اگرچه  $C$  یک  $\mathbb{Z}_4$ -مدول است و یک فضای برداری نیست، ما اصطلاح نظریه کدگذاری را دنبال کرده و از کلمه "خطی" به صورت نامناسب استفاده می کنیم.

ضرب داخلی  $\langle a, b \rangle$  از دو کلمه  $\mathbb{Z}_4^n$ ، به طور معمول تعریف می شود. می توانیم کد دوگان  $C^\perp$  را به شکل مشابه با تعریف ۴.۳.۲، معرفی نماییم.

به طور معمول، ما دو کد را هم ارز<sup>۲</sup> می نامیم، اگر یکی را از دیگری بتوان با جای گشت مکان های مختصات به دست آورد. برخی اوقات این تعریف با تغییر مجاز علامت ها در بعضی مکان ها، تعمیم داده می شود؛ (این تغییر، سمبل ۱ را به جای ۳ جایگزین می کند و برعکس).

<sup>۱</sup> quaternary

<sup>۲</sup> equivalent

در تعمیم مفهوم ماتریس مولد، باید دقت کنیم. در ابتدا یک مثال می آوریم.

مثال ۲.۸.۱. زیرگروه جمعی از  $\mathbb{Z}_4^3$  را که شامل تمامی کلمات  $(x, x, x)$  و  $(y, y + 2, y + 2)$  ( $x, y \in \mathbb{Z}_4$ ) باشد، در نظر بگیرید. می توانیم این کد چهارتایی را به عنوان مجموعه ترکیبات خطی  $a(1, 1, 1) + b(0, 2, 2)$  در نظر بگیریم که در آن  $a \in \mathbb{Z}_4$  و  $b \in \mathbb{Z}_2$  (جمع به پیمانه ۴). در حالت کلی، یک کد چهارتایی، حاصل ضرب مستقیم زیرکدهای با مرتبه ۴ یا ۲ است (گروه های دوری جمعی از مرتبه ۴ یا ۲). این مطلب نشان دهنده آن است که یک کد هم ارز با ماتریس مولد به شکل زیر است:

$$G := \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{pmatrix} \quad (1)$$

که در آن درایه های  $A$  و  $C$  برابر با ۰ و ۱ و درایه های  $B$  متعلق به  $\mathbb{Z}_4$  هستند. یک کد کلمه، به شکل  $aG$  می باشد که در آن  $a_1$  تا  $a_{k_1}$  متعلق به  $\mathbb{Z}_4$  و  $a_{k_1+1}$  تا  $a_{k_1+k_2}$  متعلق به  $\mathbb{Z}_2$  می باشند. کد دوگان  $C^\perp$  دارای ماتریس مولدی به شکل زیر است:

$$H := \begin{pmatrix} -B^T - C^T A^T & C^T & I_{n-k_1-k_2} \\ 2A^T & 2I_{k_2} & 0 \end{pmatrix} \quad (2)$$

با دنبال کردن بحث کدهای خطی از فصل ۳، اکنون باید به شمارنده های وزنی نگاهی بیندازیم. به عنوان مقدمه ای بر این فصل، این مطالب در بخش ۳.۶ مورد بحث قرار گرفته اند. شمارنده وزنی متقارن یک کد در  $\mathbb{Z}_4^n$  و شمارنده وزن لی را تعریف نمودیم. نتیجه مهم، این واقعیت بود که شمارنده های وزن لی یک کد و دوگان آن در روابط مک و ویلیامز صدق می کنند.

## ۸.۲ کدهای دودویی به دست آمده از کدهای روی $\mathbb{Z}_4$

یک نگاشت طبیعی  $\phi$  از  $\mathbb{Z}_4$  به  $\mathbb{Z}_2$  وجود دارد که فاصله لی در  $\mathbb{Z}_4$  را به فاصله همینگ تصویر می کند و به صورت زیر است:

$$\phi(0) = (0, 0), \quad \phi(1) = (0, 1), \quad \phi(2) = (1, 1), \quad \phi(3) = (1, 0)$$

در اینجا این نگاشت را به کدهای متعلق به  $\mathbb{Z}_4^3$  تعمیم می‌دهیم. برای سادگی در نمادگذاری، در ادامه سه تابع از  $\mathbb{Z}_4$  به  $\mathbb{Z}_2$  را به صورت 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، به صورت  $(\beta(i), \alpha(i))$  است. به علاوه  $\gamma(i) = \alpha(i) + \beta(i)$ . نگاشت  $\phi$  تعریف شده در بالا، به طور بدیهی به  $\mathbb{Z}_4^3$  تعمیم داده می‌شود.

### تعریف ۱.۸.۲

$$\phi(C) := (\beta(c), \gamma(c)), \quad (c \in \mathbb{Z}_4^3).$$

این نگاشت، نگاشت گری<sup>۳</sup> 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. در ادامه، همیشه  $C'$  معرف تصویر دودویی کد چهارتایی  $C$  می‌باشد.

مثال ۲.۸.۲. کد چهارتایی  $C$  با طول ۳ تولید شده توسط  $(1, 1, 3)$  و  $(0, 2, 2)$  را در نظر بگیرید (اینها سطرهای  $G$  در رابطه ۱ با  $k_1 = k_2 = 1$  هستند). سهم سطر اول در تصویر دودویی، ترکیبات خطی  $(001110)$  و  $(110001)$  می‌باشد. سطر دوم فقط  $(011011)$  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:

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

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 به شکل

<sup>۳</sup> Gray map



زیر است:

$$G' := \begin{pmatrix} I_{k_1} & A & \alpha(B) & I_{k_1} & A & \alpha(B) \\ \circ & I_{k_2} & C & \circ & I_{k_2} & C \\ \circ & \circ & \beta(B) & I_{k_1} & A & \gamma(B) \end{pmatrix}. \quad (3)$$

در حالت کلی،  $C'$  خطی نمی‌باشد، زیرا  $\phi$  یک نگاشت خطی نیست. مهم‌ترین مساله برای ما این است که نگاشت  $\phi$  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 پریپاراتا<sup>۴</sup> 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 در واقع دوگان یکدیگر هستند؛ بنابراین، ما  $\mathbb{Z}_4$ -دوگانگی را به صورت 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 این که  $C$  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 ۳.۳.۶ و قضیه ۴.۳.۶، داریم:

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

□

در اینجا شرایط لازم و کافی را برای این که یک کد دودویی، تصویر دودویی یک کد چهارتایی باشد، اثبات خواهیم نمود. در ابتدا مشاهده می‌کنید که  $\phi(-C) = (\gamma(C), \beta(C))$ . این مطلب نتیجه می‌دهد که یک کد  $\mathbb{Z}_4$ -خطی توسط جای‌گشت  $\sigma$  به صورت  $(n, 2n), \dots, (2, n+2), (1, n+1)$ ، ثابت می‌باشد. این جای‌گشت، دو نیمه هر کدکلمه را با یکدیگر جابه‌جا می‌کند.

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:

$$(۱) \quad \alpha(a) + \beta(a) + \gamma(a) = ۰$$

$$(۲) \quad \alpha(a)\alpha(b) = ۱ \text{ اگر و فقط اگر } a \text{ و } b \text{ فرد باشند؛}$$

(۳)  $\beta(a + b) = \beta(a) + \beta(b) + \epsilon$  که در آن  $\epsilon = ۱$  اگر و فقط اگر  $a$  و  $b$  هر دو فرد باشند (در غیر این صورت  $\epsilon = ۰$ ) و  $\gamma$  نیز به طور 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، به طوری 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 در نظر بگیرید. هر کدکلمه، دارای فرم  $a = (x, x + \epsilon)$  است که در آن  $\epsilon = ۰$  یا  $\epsilon = ۱$  (از طول  $2^m - 1$ ). اگر  $b = (y, y + \epsilon)$  دومین کدکلمه باشد، آن‌گاه  $(a + \sigma(a))(b + \sigma(b)) = ۰$  یا  $(a + \sigma(a))(b + \sigma(b)) = ۱$ ؛ بنابراین، با استفاده از قضیه ۶.۸.۲، کد  $\mathcal{R}(1, m)$ ،  $\mathbb{Z}_4$ -خطی است. اگر حالت  $m = ۳$  را در نظر بگیریم، آن‌گاه کد چهارتایی متناظر، دارای ماتریس مولدی به شکل زیر است:

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

از  $G$  و ماتریس ۱، بردارهای پایه استاندارد برای  $\mathcal{R}(1, m)$  را پیدا می‌کنیم. اکنون کدهای خطی دودویی را در نظر 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:

$$a, b \in C \Rightarrow \Psi(\alpha(a)\alpha(b)) \in C.$$

اثبات. با دو بار به کار بردن لم ۵.۸.۲ داریم:

$$\phi(a + b + \Psi(\alpha(a)\alpha(b))) = \phi(a) + \phi(b).$$

□

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 به طول  $n = 2^m$  برای  $m \geq 5$   $\mathbb{Z}_4$ -خطی نیست.

قضیه ۹.۸.۲. کد  $\mathcal{R}(m-2, m)$  برای  $m \geq 5$   $\mathbb{Z}_4$ -خطی نیست.

اثبات. فرض کنید  $C$  یک کد چهارتایی به طول  $2^{m-1}$  باشد که تصویر دودویی آن شامل کد همینگ دودویی گسترش‌یافته  $H_m$  به طول  $n = 2^m$  است. فرض کنید  $G$  از رابطه ۱، ماتریس مولد  $C$  باشد. بخش بالایی را  $G_{k_1}$  و بخش پایینی را  $2G_{k_2}$  می‌نامیم. چون  $H_m$  یک کد با وزن زوج است،  $G_{k_1}$  سطرهایی با تعدادی زوج از درایه‌های فرد دارد؛ تعریف می‌کنیم:

$$G'_{k_1} := (I_{k_1} \quad A \quad \alpha(B)).$$

کد دودویی  $H'$  که توسط  $G'_{k_1}$  تولید شده را مطالعه می‌کنیم. توجه کنید که  $2G'_{k_1}$  و  $2G_{k_2}$  زیرکدی از  $C$  را که تنها شامل کلمات با مختصات زوج است، تولید می‌کند. به‌وضوح  $1 - 2^{m-1} \leq k_1 + k_2$ . چون  $2^{m-1} - m = 2k_1 + k_2$ ، می‌بینیم که  $H'$  دارای بعد حداقل  $2^{m-1} - m$  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 در نظر گرفته و ممکن است

فرض کنیم که سایر بردارهای پایه، دارای مکان‌های ناصفری مجزا از مکان‌های ناصفر 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 پنجر می‌کنیم. ما مولد یک کد دودویی به طول  $2a - 2^{m-1}$  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، به آسانی دیده می‌شود که کلمات با وزن ۴ در یک کد گسترش‌یافته همینگ تشکیل یک طرح  $(1, 4, 2^m) - 3$  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.  $\square$

### ۸.۳ حلقه‌های گالوا روی $\mathbb{Z}_4$

می‌خواهیم مفهوم کدهای دوری را برای کدهای روی  $\mathbb{Z}_4$  تعمیم دهیم. برای این کار، به اندکی از جبر نیاز داریم. برای کدهای دوری به طول  $n$  روی  $\mathbb{F}_2$ ، به یک میدان گسترش‌یافته که شامل ریشه  $m$ ام واحد باشد نیاز داریم. موقعیت فعلی مشابه است. ما باید یک توسیع از  $\mathbb{Z}_4$  را به واسطه ریشه  $m$ ام واحد در نظر بگیریم. چنین توسیعی را حلقه گالوا<sup>۵</sup> می‌نامیم.

ما نیاز به برخی پیش زمینه‌ها در مورد چندجمله‌ای‌های تحویل‌ناپذیر در  $\mathbb{Z}_4[x]$  داریم. چندجمله‌ای  $f(x)$  در  $\mathbb{Z}_2[x]$  را در نظر بگیرید و آن را به صورت  $f(x) = a(x^2) - xb(x^2)$  بنویسید (که در آن ما علامت منفی را به کار می‌بریم، زیرا محاسبات مختصری را روی  $\mathbb{Z}_4$  انجام خواهیم داد). نگاشت  $\phi$  را به صورت:

$$\phi(f)(x) = F(X) := \pm(a(x)^2 - xb(x)^2) \in \mathbb{Z}_4[x],$$

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. به وضوح نگاشت معکوس، همان  $f(x) \equiv F(x) \pmod{2}$  می‌باشد.

با انجام یک محاسبه جزیی می‌توان چک نمود که  $\phi(fg) = \phi(f)\phi(g)$ . چون هم  $\phi$  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 به صورت حاصل ضرب  $f_1(x)f_2(x)\cdots f_l(x)$  از چندجمله‌ای‌های تحویل‌ناپذیر

<sup>۵</sup> Galois Ring

در  $\mathbb{Z}_2[x]$  نوشت، آن‌گاه  $F_1(x)F_2(x)\cdots F_l(x)$  که در آن  $F_i := \phi(f_i)$ ، تجزیه منحصر به فرد  $x^n - 1$  در  $\mathbb{Z}_2[x]$  می‌باشد. عامل تحویل‌ناپذیر  $h(x)$  از درجه  $m$ ، چندجمله‌ای ابتدایی پایه<sup>۶</sup> در  $\mathbb{Z}_2[x]$  نامیده می‌شود. این روش توسعه دادن<sup>۷</sup> یک چندجمله‌ای تحویل‌ناپذیر در  $\mathbb{Z}_2[x]$  به یک چندجمله‌ای تحویل‌ناپذیر در  $\mathbb{Z}_2[x]$  (با نگاهت  $\phi$ ) به روش گرافت<sup>۸</sup> معروف است (ر.ک. مرجع [۹۹]). این مطلب یک مورد خاص از یک نتیجه، معروف به لم هنسل<sup>۹</sup> است (ر.ک. مرجع [۹۳]).

مثال ۱.۸.۳. چندجمله‌ای اولیه  $f(x) = x^3 + x + 1$  به عنوان عاملی از  $x^7 - 1$  را در نظر بگیرید. با نمادگذاری به کار رفته در بالا، داریم  $a(x) = 1$  و  $b(x) = -1 - x$ ، بنابراین،  
 $F(x) = x^3 + 2x^2 + x - 1 \equiv x^3 + x + 1 \pmod{2}$ . در این روش، تجزیه زیر را داریم:

$$x^7 - 1 = (x^3 + 2x^2 + x - 1)(x^3 - x^2 + 2x - 1)(x - 1),$$

که دو عامل اول، چندجمله‌ای‌های اولیه پایه در  $\mathbb{Z}_2[x]$  هستند.

تعریف ۲.۸.۳. حلقه گالوا  $GR(\mathcal{F}, m)$  به صورت  $\mathbb{Z}_2[\xi]$  تعریف شده است که در آن  $\xi$  ریشه‌ای از  $h(x)$  است (چون  $\xi$   $m$  ریشه واحد است؛ داریم  $(\mathbb{Z}_2[\xi] = \frac{\mathbb{Z}_2[x]}{(h(x))})$ ).  
 دقت می‌کنید که مجدداً داریم:

$$h(x) = x^3 + 2x^2 + x - 1 = (x - \xi)(x - \xi^2)(x - \xi^4).$$

مشابه مثال ۱.۹.۱، می‌توان عناصر  $GR(\mathcal{F}, m)$  را به صورت چندجمله‌ای‌های با درجه کمتر از  $m$  بر حسب  $\xi$  با ضرایب در  $\mathbb{Z}_2$ ، نشان داد.

مثال ۳.۸.۳. برای  $GR(\mathcal{F}, m)$ ، تولید شده توسط  $x^3 + 2x^2 + x - 1$ ، جدول زیر را برای مجموعه  $\{0, 1, \xi, \xi^2, \xi^3, \dots, \xi^6\}$  داریم. در اینجا:

$$C = \sum_{i=0}^2 a_i \xi^i, \quad (\xi^3 = 1 + 3\xi + 2\xi^2).$$

چنین جدولی به ما نمی‌گوید که چگونه عناصری از  $GR(\mathcal{F}, m)$  را که در مجموعه:

<sup>۶</sup> basic primitive polynomial

<sup>۷</sup> lifting

<sup>۸</sup> Graeff's method

<sup>۹</sup> Hensel

$c$	$a_0$	$a_1$	$a_2$
۰	۰	۰	۰
۱	۱	۰	۰
$\xi$	۰	۱	۰
$\xi^2$	۰	۰	۱
$\xi^3$	۱	۳	۲
$\xi^4$	۲	۳	۳
$\xi^5$	۳	۳	۱
$\xi^6$	۱	۲	۱

$$\tau := \{0, 1, \xi, \xi^2, \dots, \xi^{n-1}\},$$

نیستند، بیان کنیم. با مشاهده نمایش  $\xi^i$  به صورت چندجمله‌ای با درجه کمتر از  $m$  نسبت به  $\xi$ ، می‌بینیم که  $2\xi^i = 2$  نتیجه می‌دهد که  $\xi^i = 1$  یعنی  $\xi = 1$ . از این رو اگر  $t$  در  $\tau$  تغییر کند، آن‌گاه همه عناصر  $2t$  متمایز هستند.

$4^m$  مجموع به شکل  $a + 2b$  را در نظر بگیرید که  $a$  و  $b$  در مجموعه  $\tau$  قرار دارند. اگر  $a + 2b = a' + 2b'$  آن‌گاه  $2a = 2a'$ ؛ بنابراین،  $a = a'$  و از این رو  $b = b'$ ؛ پس، مجموع‌های  $a + 2b$  همگی متفاوت هستند؛ بنابراین، آنها تمامی عناصر  $GR(4, m)$  را نمایش می‌دهند. مجموعه  $\tau$ ، مجموعه مربع‌های عناصر  $GR(4, m)$  است.

برای یافتن نمایش یک عنصر داده‌شده، از لم زیر استفاده می‌کنیم.

لم ۴.۸.۳. داریم:

$$(x + y)^{2^k} \equiv x^{2^k} + 2x^{2^{k-1}}y^{2^{k-1}} + y^{2^k} \pmod{4}.$$

اثبات. برای  $k = 1$  اثبات بدیهی است. با مربع کردن هر دو طرف، نتیجه با استقرای اثبات می‌شود.  $\square$

بنابراین، اگر  $a \in \tau$ ،  $b \in \tau$  و  $c = a + 2b$ ، آن‌گاه:

$$c^{2^m} = a^{2^m} = a.$$

از این رو، نگاشت  $\tau : c \mapsto a$  با ضابطه:

$$\tau(c) = c^{2^m}, \quad (c \in GR(4, m), n = 2^m - 1), \quad (4)$$

داده شده است. همین که  $a$  معرفی شد،  $b$  از  $c = a + 2b$  نتیجه می‌شود.

به‌وضوح  $\tau(cd) = \tau(c)\tau(d)$  و با استفاده از لم ۴.۸.۳ داریم:

$$\tau(c + d) = \tau(c) + \tau(d) + 2(cd)^{2^{m-1}}.$$

اکنون می‌توانیم ساختار حلقه  $R := GR(\mathbb{F}, m)$  را تشریح کنیم. ایده آل ماکسیمال منحصر به فرد در  $R$ ، مجموعه  $2\tau$  است. حاصل ضرب هر دو عنصر در این مجموعه برابر با صفر است (بنابراین، در  $R$  مقسوم علیه‌های صفر وجود دارد). مجموعه باقی‌مانده،  $R^* := \frac{R}{(2\tau)}$ ، از عناصر معکوس پذیر تشکیل شده است. آنها تشکیل یک گروه ضربی از مرتبه  $2^m(2^m - 1)$  می‌دهند. این گروه، یک حاصل ضرب مستقیم از گروه دوری  $H$  از مرتبه  $n$  است که توسط  $\xi$  تولید شده و گروه  $\varepsilon$  که شامل عناصری به شکل  $1 + 2t, t \in \tau$  است، می‌باشد؛ (اینها یک‌ه‌های اصلی  $R$  هستند).

برای دانستن ساختار  $\varepsilon$ ، توجه کنید که اگر  $t_i$  و  $t_j$  در  $\tau$  باشند، آنگاه  $t_i + t_j = a_{ij} + 2b_{ij}$  که در آن  $a_{ij}, b_{ij} \in \tau$ ؛ بنابراین،  $(1 + 2t_i)(1 + 2t_j) = 1 + 2a_{ij}$ . علاوه بر این، نمایش جمعی  $a_{ij}$  (مانند جدول مثال ۳.۸.۳)، در پیمانه ۲ با مجموع نمایش‌هایی از  $t_i$  و  $t_j$  برابر است. در پیمانه ۲، عناصر موجود در این جدول، گروه جمعی  $F_{2^m}$  هستند؛ بنابراین،  $\varepsilon$  با این گروه یک‌ریخت است. هر عضو  $R^*$  دارای یک نمایش منحصر به فرد به شکل  $\xi^r(1 + 2t)$  که  $0 \leq r < n, t \in \tau$ ، است. عناصر با  $r$  ثابت، یک کلاس باقی‌مانده از حلقه  $\frac{R}{(2\tau)} = \frac{R}{(2\tau)}$  را تشکیل می‌دهند و  $2\tau$  کلاس متناظر با صفر است. فرض کنید  $\theta$  یک ریشه از  $h_2(x)$  باشد؛ یعنی یک عنصر اولیه از  $F_{2^m}$ . قبلاً دیده‌ایم که این جدول برای مقادیر  $\xi^r$ ، به پیمانه ۲، یک جدول جمعی برای  $F_{2^m}$  با مولد  $\theta$  است. در نتیجه، نگاشت  $\mu$  که  $\tau^r$  را به  $\theta^r$  و صفر را به صفر تصویر می‌کند، یک یک‌ریختی از حلقه کلاسی باقی‌مانده  $\frac{R}{(2\tau)}$  روی میدان  $F_{2^m}$  است.

در زیر، به این یک‌ریختی و به این مطلب که  $2\xi^r = 2\xi^s$  نتیجه می‌دهد  $r = s$  را، نیاز خواهیم داشت. همچنین، به تعدادی از نتایج وابستگی میان توان‌های  $\xi^r$  نیاز پیدا می‌کنیم. این مطالب را در قالب یک لم بیان می‌کنیم.

لم ۵.۸.۳ فرض کنید  $m \geq 2$ . در نظر بگیرید  $GR(\mathbb{F}, m) = \mathbb{Z}_\mathbb{F}[\xi]$  با  $\xi^n = 1$  (برای  $n = 2^m - 1$ )؛ داریم:

$$(۱) \quad \pm \xi^j \pm \xi^k \quad \text{برای } 0 \leq j < k < n \text{، معکوس پذیر است.}$$

$$(۲) \quad \text{برای } i, j, k \text{ متمایز در بازه } [0, n-1] \text{ داریم } \xi^i - \xi^j \neq \pm \xi^k.$$

(۳) اگر  $m \geq 3$  و  $i \neq j, k \neq l$  در بازه  $[0, m-1]$ ، آن گاه:

$$\xi^i - \xi^j = \xi^k - \xi^l \Rightarrow i = k, j = l.$$

(۴) اگر  $m \geq 3$  و  $m$  فرد باشد، آن گاه:

$$\xi^i + \xi^j + \xi^k + \xi^l = 0 \Rightarrow i = j = k = l.$$

اثبات.

(۱) اگر  $\pm \xi^j \pm \xi^k = 2\lambda$  برای یک  $\lambda \in R$ ، آن گاه با مربع نمودن دو طرف معادله  $\pm \xi^j = \pm \xi^k + 2\lambda$  داریم  $j = k$ .

(۲) یک معادله از این نوع می تواند به  $\xi^b = \xi^a + 1$  تقلیل یابد. دو طرف را به توان  $2^m$  رسانده و لم ۴.۸.۳ را به کار می بریم. داریم  $2\xi^{a \cdot 2^{m-1}} = 0$  که یک تناقض است.

(۳) یک معادله از این نوع می تواند به  $\xi^b + \xi^c = \xi^a + 1$  تقلیل یابد. با به کار بردن لم ۴.۸.۳، داریم  $2(\xi^b + \xi^c)^{2^{m-1}} = 2(\xi^a)^{2^{m-1}}$ ؛ بنابراین،  $\xi^a = \xi^{b+c}$ . این معادله به صورت  $2(\xi^b - 1)(\xi^c - 1) = 0$  در می آید و ما این حالت را در مرحله (۱) انجام داده ایم.

(۴) در اینجا، لازم است که با  $F_{2^m}$  کار کنیم. ما یک ریختی  $\mu$  را به کار می بریم. اگر چهار توان  $\xi$  جمع شود و صفر گردند، رابطه مشابهی وجود دارد که یکی از توان ها برابر با ۱ است. علاوه بر این، چون  $\xi^n = 1$  ممکن است فرض کنیم که بقیه توان ها زوج هستند. پس داریم:

$$\xi^{2a} + \xi^{2b} = -\xi^{2c} - 1.$$

با رساندن دو طرف به توان  $2^m$  و به کار بردن لم ۴.۸.۳، داریم:

$$2(\xi^{2a} + \xi^{a+b} + \xi^{2b}) = 2\xi^c.$$

از این معادله نمی توانیم نتیجه ای را در  $R$  به دست آوریم، اما این مطلب مفهومی در  $F_{2^m}$  دارد. نگاشت  $\mu$  را به کار برده و می نویسیم  $x := \theta^a$ ،  $y := \theta^b$  و  $z := \theta^c$ . از معادله آخر نتیجه می گیریم که  $x^2 + xy + y^2 = z$ . معادله اصلی ایجاب می کند 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 این که  $m$  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  $c = (c_0, c_1, \dots, c_{n-1})$  را با چند جمله‌ای  $c(x) := c_0 + c_1x + \dots + c_{n-1}x^{n-1}$  از حلقه  $\mathcal{R} = \mathbb{Z}_4[x]/(x^n - 1)$  همسان در نظر می‌گیریم. هر چیزی تعمیم نمی‌یابد! دامنه تجزیه یکتا نمی‌باشد؛ یعنی برخی از چند جمله‌ای‌ها در  $\mathcal{R}$  را می‌توان به صورت حاصل ضرب عوامل تحویل‌ناپذیر به بیشتر از یک صورت نوشت. این مطلب روی بحث ما تاثیری نخواهد داشت.

به طور معمول، کدها را با معرفی ماتریس مولد یا ماتریس بررسی توازن 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 بررسی توازن آن اضافه می‌کنیم. این کار، به طول  $\mathbb{Z}_4$ -کد یک عدد اضافه می‌کند، اما تصویر دودویی آن به اندازه دو سبمل طولانی‌تر می‌شود.

مثال ۱.۸.۴. کد دوری چهارتایی  $C$  به طول  $n = 2^m - 1$  با مولد  $(2\xi^{n-1} \quad 2\xi \quad 2)$  را در نظر بگیرید. این کد یک کد بدیهی است، یک کد دودویی درون آن پنهان است. تمامی کدکلمات تصویر دودویی آن به شکل  $(c, c)$  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 به صورت زیر را در نظر بگیرید:

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2\xi & 2\xi^{n-1} \end{pmatrix}.$$

هر دوی  $C$  و  $C'$  دارای  $2^{m+2}$  کدکلمه هستند. تصاویر دودویی آنها دارای طول  $2^{m+1}$  بوده و به وضوح 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  $2^m$   $n+1 = 2^m$  (فرد  $m$ ) با ماتریس بررسی توازن زیر را در نظر بگیرید:

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \xi & \xi^{n-1} \end{pmatrix},$$

که در آن  $\xi$  یک  $n$ امین 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 در نظر می‌گیریم. برای موقعیت‌های متناظر که در آن یک مختصات ناصفر در خط اول وجود دارد، معادلات مشابه با یک جمله کم‌تر باید در نظر 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 این صورت 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  $i, j, k$ . با استفاده 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 به طوری 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  $4^{n-m-1}$  کد کلمه است. حال نگاهی به تصویر دودویی  $C_m$  می‌اندازیم. آن یک کد دودویی با طول  $2^{m+1}$  است، با تعداد  $2^k$  عضو که در آن  $k = 2^{m+1} - 2m - 2$  و کمترین-فاصله آن حداقل ۶ است. از بخش ۷.۴ می‌بینیم که اگر ما این کد دودویی را کوتاه کنیم، آن‌گاه یک کد با طول  $2^{m+1} - 1$  با پارامترهای یکسان با یک کد پریاراتا به دست می‌آوریم! بنابراین، یک کد تقریباً کامل است و از این‌رو دارای شمارنده وزنی مشابه با کد پریاراتا با طول یکسان است. مولفین در مرجع [۸۸]،  $C'_m$  را یک کد "پریاراتا" نامیده‌اند، چرا که آن با کد موجود در بخش ۷.۴ هم‌ارز نمی‌باشد.

حال بیایید دوگان کد  $C_m^\perp$  را در نظر بگیریم. این کد، ماتریس  $H$  را به عنوان 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 پریاراتای 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 [۴۶] را ببینید. حال می‌دانیم که کد دودویی که تصویر کد روی  $\mathbb{Z}_4$  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  $\mathbb{Z}_4$ -کدها هستند که ما آنرا در اینجا مورد بحث قرار دادیم.

مثالی از یک کد دودویی خوب می‌آوریم که تصویر دودویی  $\mathbb{Z}_4$ -کدی است که دوری بوده، اما خطی نیست.

مثال ۳.۸.۴. به بردار  $(11100)$  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) چهار جفت 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 به همراه سه‌تای دیگر که توسط جای‌گذاری ۱۱۱ با ۱۱۳ یا برخی جای‌گشت‌ها و ۰۰ با ۰۲، ۲۰ با ۲۲ به دست آمده‌اند، می‌گیریم. ادعا می‌کنیم که انتخاب  $11120, 31100, 13102, 11322$  دارای این خاصیت است که این چهار بردار، منفی آنها و تمامی شیفت‌های دوری تشکیل یک  $\mathbb{Z}_4$ -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 نادر این فاصله شمرده می‌شود یا مختصات دیگر فاصله ۶ را به دست می‌دهد. یک زوج ۳-۱ نیز به اندازه ۲ تا در این فاصله شرکت می‌کند. دو کد کلمه 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  $o_2 = o'_2$  و  $o_3 = o'_3$  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 در نظر 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 ۶ 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  $\mathcal{R}(2, m)$  یک کد  $\mathbb{Z}_4$ -خطی است.

۳.۸.۵. فرض کنید  $c = \xi^i + 2\xi^j$  عنصری از  $GR(4, m)$  باشد. معکوس آن را بیابید.

۴.۸.۵. شمارنده وزنی کد نرداستروم-رابینسن را در نظر بگیرید. نشان دهید که آن با تبدیل مک‌ویلیمز خود برابر است.

۵.۸.۵. کد پریاراتا  $\mathcal{P}$  از قضیه ۵.۷.۴ را در نظر بگیرید. تعداد کلمات با وزن ۵ و ۶ را تعیین کنید. از این استفاده نموده، شمارنده وزنی کد پریاراتای گسترش‌یافته به طول ۱۶ را بیابید.

۶.۸.۵. 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  $m \geq 5$  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 بررسی توازن یک کد BCH (کم عرض) را آن چنان که در اثبات قضیه ۲.۶.۶ آمده است، در نظر بگیرید؛ یعنی:

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \dots & \beta^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \beta^{d-1} & \beta^{2(d-1)} & \dots & \beta^{(d-1)(n-1)} \end{pmatrix},$$

که در آن  $\beta$  یک  $n$ امین ریشه اولیه واحد در  $\mathbb{F}_{q^m}$  است و هر درایه به صورت برداری ستونی با طول  $n$  روی  $\mathbb{F}_q$  تفسیر می شود؛ وجود  $\beta$  نتیجه می دهد  $n \mid (q^m - 1)$ .

با به کارگیری این واقعیت که هر زیرماتریس  $H$  تشکیل شده با در نظر گرفتن  $d - 1$  ستون، یک ماتریس و اندر موند 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 داشته اند که اگر ما  $H$  را با ماتریس زیر جایگزین کنیم، هنوز هم دلیل مشابهی می تواند کارساز باشد:

$$\hat{H} = \begin{pmatrix} h_0 \beta_0 & h_1 \beta_1 & \dots & h_{n-1} \beta_{n-1} \\ \vdots & \vdots & \dots & \vdots \\ h_0 \beta_0^{d-1} & h_1 \beta_1^{d-1} & \dots & h_{n-1} \beta_{n-1}^{d-1} \end{pmatrix},$$

که در آن  $h_j \in \mathbb{F}_{q^m}^*$  و  $\beta_i$ ها عناصر متفاوتی از  $\mathbb{F}_{q^m}^*$  باشند. اگر  $h_j \in \mathbb{F}_q$  ( $0 \leq j \leq n-1$ )، آن گاه 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، آن گاه جملات  $h_j \beta_j^t$  به‌عنوان بردارهای ستونی روی  $\mathbb{F}_q$  می‌توانند با درایه‌های اولیه تفاوت بسیار داشته باشند.

دوروش در تعمیم کدهای BCH به این طریق را در نظر خواهیم گرفت. آنچه که ما را در واقع 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 حالی که ثابت شده است کدهای BCH با طول بزرگ، بد هستند.

## ۹.۲ کدهای گاپا

فرض کنید  $(c_0, c_1, \dots, c_{n-1})$  کد کلمه‌ای در یک کد BCH با فاصله طراحی شده  $d$  (طول کلمه  $n$ ) یک ریشه اولیه  $n$ ام واحد) باشد؛ در این صورت با استفاده از تعریف داریم  $\sum_{i=0}^{n-1} c_i (\beta^j)^i = 0$  برای  $0 \leq j \leq d-1$ . می‌خواهیم تا این شرط را به‌روش دیگری بنویسیم. مشاهده می‌کنید که:

$$\frac{z^n - 1}{z - \beta^{-i}} = \sum_{k=0}^{n-1} z^k (\beta^{-i})^{n-1-k} = \sum_{k=0}^{n-1} \beta^{i(k+1)} z^k. \quad (1)$$

این نتیجه می‌دهد که برای یک چندجمله‌ای  $p(z)$  داریم:

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \beta^{-i}} = \frac{z^{d-1} p(z)}{z^n - 1}. \quad (2)$$

اگر  $g(z)$  چندجمله‌ای دلخواه باشد و  $g(\gamma) \neq 0$ ، آن گاه  $1/(z - \gamma)$  را چندجمله‌ای یکتایی در پیمانه  $g(z)$  تعریف می‌کنیم، به طوری که  $(z - \gamma) \cdot 1/(z - \gamma) \equiv 1 \pmod{g(z)}$ ؛ یعنی:

$$\frac{1}{z - \gamma} = \frac{-1}{g(\gamma)} \cdot \left( \frac{g(z) - g(\gamma)}{z - \gamma} \right). \quad (3)$$

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  $L = \{\gamma_0, \gamma_1, \dots, \gamma_{n-1}\}$  به طوری که  $|L| = n$  و  $g(\gamma_i) \neq 0$  برای  $0 \leq i \leq n-1$ . کد گاپای<sup>۱</sup>

<sup>۱</sup> Goppa code

$\Gamma(L, g)$  را با چند جمله‌ای گاپای<sup>۲</sup>  $g(z)$  به صورت مجموعه کدکلمات  $c = (c_0, c_1, \dots, c_{n-1})$  روی  $\mathbb{F}_q$  تعریف می‌کنیم، به طوری که:

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \gamma_i} \equiv 0 \pmod{g(z)}. \quad (۴)$$

مشاهده می‌کنید که کدهای گاپا، خطی هستند.

مثال ۲.۹.۲. با توجه به ملاحظات مقدماتی، می‌بینیم که اگر ما چند جمله‌ای گاپای  $g(z) = z^{d-1}$  و  $L := \{\beta^{-i} \mid 0 \leq i \leq n-1\}$  را در نظر بگیریم که در آن یک ریشه  $n$ ام اولیه واحد در  $\mathbb{F}_{q^m}$  است، کد گاپای  $\Gamma(L, g)$  حاصل شده، یک کد BCH کم‌عرض با فاصله طراحی شده  $d$  است (ارجاع به مساله ۲.۹.۸).

به منظور برقراری رابطه با بخش ۹.۱، سعی می‌کنیم تا یک ماتریس بررسی توازن مناسب برای  $\Gamma(L, g)$  بیابیم. از روابط ۴ و ۳ می‌بینیم که:

$$\left( \frac{1}{g(\gamma_0)} \cdot \frac{g(z) - g(\gamma_0)}{(z - \gamma_0)}, \dots, \frac{1}{g(\gamma_{n-1})} \cdot \frac{g(z) - g(\gamma_{n-1})}{(z - \gamma_{n-1})} \right),$$

که در آن هر درایه به صورت یک بردار ستونی تعبیر می‌شود، به یک معنا، یک ماتریس بررسی توازن است. فرض کنید  $h_j := g(\gamma_j)^{-1}$  و بنابراین،  $h_j \neq 0$ . اگر  $g(z) = \sum_{i=0}^t g_i z^i$ ، آن‌گاه در روشی مشابه با رابطه ۱ داریم:

$$\frac{g(z) - g(x)}{z - x} = \sum_{i+j \leq t-1} g_{i+j+1} x^j z^i.$$

با صرف نظر کردن از عوامل  $z^i$ ، به عنوان ماتریس بررسی توازن برای  $\Gamma(L, g)$  داریم:

$$\begin{pmatrix} h_0 g_t & h_{n-1} g_t \\ h_0 (g_{t-1} + g_t \gamma_0) & h_{n-1} (g_{t-1} + g_t \gamma_{n-1}) \\ \vdots & \vdots \\ h_0 (g_1 + g_2 \gamma_0 + \dots + g_t \gamma_0^{t-1}) & h_{n-1} (g_1 + g_2 \gamma_{n-1} + \dots + g_t \gamma_{n-1}^{t-1}) \end{pmatrix}.$$

با استفاده از یک تبدیل خطی، ماتریسی را که می‌خواستیم، می‌یابیم؛ یعنی:

$$H = \begin{pmatrix} h_0 & h_{n-1} \\ h_0 \gamma_0 & h_{n-1} \gamma_{n-1} \\ \vdots & \vdots \\ h_0 \gamma_0^{t-1} & h_{n-1} \gamma_{n-1}^{t-1} \end{pmatrix}.$$

<sup>۲</sup> Goppa polynomial

(در اینجا این واقعیت را به کار 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 بررسی توازن  $H$  با روشی دقیقاً مشابه با کدهای BCH، نتیجه می‌شود.  $\square$

مثال داده شده ۲.۹.۲ نشان می‌دهد که کران BCH (برای کدهای BCH کم‌عرض) حالت خاصی از قضیه ۳.۹.۲ است.

به منظور 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 در نظر 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  $\gamma_0, \gamma_1, \dots, \gamma_{n-1}$  و در آن حالت قطب‌ها مرتبه ۱ می‌باشند.

یک کد روی  $\mathbb{F}_{q^m}$  با در نظر گرفتن کدکلمات به صورت  $n$ -تایی:

$$(\text{Res}_{\gamma_0} f, \text{Res}_{\gamma_1} f, \dots, \text{Res}_{\gamma_{n-1}} f)$$

تعریف شده است که در آن باقی‌مانده  $f(z)$  در نقطه  $\gamma_i$  به صورت معمول تعریف شده است. کد گاپای  $\Gamma(L, g)$  زیرمیدان زیرکد (روی  $\mathbb{F}_q$ ) این کد است.

ماتریس بررسی توازن  $H$  تعریف شده در بالا را در نظر بگیرید. این موقعیت را با تعریف ۲.۶.۸ مقایسه کنید که در آن در نظر گرفته‌ایم  $v := (h_0, h_1, \dots, h_{n-1})$  و  $a := (\gamma_0, \gamma_1, \dots, \gamma_{n-1})$ .  $k = t$  می‌بینیم که  $H$  ماتریس مولد کد  $GRS_k(a, v)$  است. بنابراین، کد گاپای  $\Gamma(L, g)$  زیرمیدان زیرکد دوگان یک کد رید-سولومن گسترش یافته است.

بنابراین، تا اینجا دیده‌ایم که کدهای تعریف شده به وسیله چند جمله‌ای‌ها مانند تعریف ۲.۶.۸ و کدهایی که با استفاده از باقی‌مانده‌ها 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 به دست 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:

$$\mathcal{R}^* := \left\{ \xi(z) = \sum_{i=0}^{n-1} \frac{b_i}{z - \gamma_i} \mid (b_0, b_1, \dots, b_{n-1}) \in \mathcal{R} \right\},$$

و فاصله دو تابع گویای  $\xi(z)$  و  $\eta(z)$  را به صورت زیر تعریف می‌کنیم:

$$d(\xi(z), \eta(z)) := \|\xi(z) - \eta(z)\|,$$

که در آن  $\|\xi(z)\|$  معرف درجه مخرج است و  $\xi(z)$  به صورت  $n(z)/d(z)$  با  $(n(z), d(z)) = 1$  است. به آسانی دیده می‌شود که این تابع فاصله است و در واقع نگاشت  $(b_0, \dots, b_{n-1}) \rightarrow \sum_{i=0}^{n-1} b_i/(z - \gamma_i)$  یک یک‌ریختی از  $\mathcal{R}$  به  $\mathcal{R}^*$  است. ما این اصطلاح را برای مطالعه کدهای گاپا با در نظر گرفتن سمت چپ رابطه ۴ به عنوان عضوی از  $\mathcal{R}^*$  به کار خواهیم برد؛ یعنی رابطه ۳ را به کار نخواهیم برد. اگر  $\xi(z) = n(z)/d(z)$  متنظر با یک کدکلمه ناصفر باشد، آن‌گاه  $\deg d(z) \geq \deg n(z) + 1$ . شرط  $\xi(z) \equiv 0 \pmod{g(z)}$  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 به صورت  $n(z)/d(z)$  بنویسیم که در آن  $d(z)$  برابر با حاصل ضرب تمام  $n$  عامل‌های  $(z - \gamma_i)$  است، آن‌گاه می‌توانیم تخمین خود در مورد 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 بررسی توازن 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 به کار ببریم. ضریب  $z^{n-s-1}$  در مخرج  $n(z)$  برابر با  $(-1)^s \sum_{i=0}^{n-1} b_i \gamma_{j_1} \gamma_{j_2} \dots \gamma_{j_s}$  است (که در آن  $\sum$  نشان می‌دهد که  $j_v \neq i$  برای  $v = 1, 2, \dots, s$ ). 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 بررسی توازن، 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  $(1 + sm) - n - tm$  و کمترین-فاصله حداقل  $t + s + 2$  را داریم. چگونه این حالت با زمانی که  $g(z)$  را با چند جمله‌ای گاپای دیگری با درجه  $t + s$  جای‌گزین می‌کنیم، مقایسه می‌گردد؟ اولین روش، دارای این مزیت است که  $\sum_{i=0}^{n-1} b_i \gamma_i^q = 0$ ؛ بنابراین، در مرحله  $q$  ما مطمئن هستیم که بعد کاهش نمی‌یابد.

قضیه ۱.۹.۳. فرض کنید  $q = 2$  و فرض کنید  $g(z)$  دارای هیچ ریشه تکراری نباشد؛ در این صورت  $\Gamma(L, g)$  دارای کمترین-فاصله حداقل  $2t + 1$  است (که در آن  $t = \deg g(z)$ ).

اثبات. فرض کنید  $(c_0, c_1, \dots, c_{n-1})$  یک کدکلمه باشد؛ تعریف کنید  $f(z) = \prod_{i=0}^{n-1} (z - \gamma_i)^{c_i}$ ؛ در این صورت  $\xi(z) = \sum_{i=0}^{n-1} c_i / (z - \gamma_i) = f'(z)/f(z)$  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 در واقع داشته باشیم  $g^2(z)$  عاد کند  $f'(z)$  را؛ بنابراین، استدلال قبلی ایجاب می‌کند که  $d \geq 2t + 1$ .

البته می‌توان قضیه ۱.۹.۳ را با موضوع مشترک با یک کد BCH ترکیب نمود.

## ۹.۴ رفتار مجانبی کدهای گاپا

در بخش ۶.۶ اشاره کردیم که کدهای BCH اولیه با طول بزرگ، بد هستند. این واقعیت با قضیه ۹.۶.۶ در ارتباط است. کازامی<sup>۳</sup> (۱۹۶۹؛ 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 زیر دنباله‌ای از کدهای  $C_i$  با طول  $n_i$  بعد  $k_i$  و فاصله  $d_i$  باید  $\liminf(k_i/n_i) = 0$  یا  $\liminf(d_i/n_i) = 0$ . 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. در ابتدا پارامترهای  $n = q^m$  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  $c = (c_0, c_1, \dots, c_{n-1})$  کلمه دلخواهی با وزن  $d > j$  باشد؛ یعنی کلمه‌ای که نمی‌خواهیم در  $\Gamma(L, g)$  باشد. چون  $\sum_{i=0}^{n-1} c_i / (z - \gamma_i)$  دارای شمارنده با درجه حداکثر  $1 - j$  است، حداکثر  $\lfloor (j-1)/t \rfloor$  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  $\sum_{j=1}^{d-1} \lfloor (j-1)/t \rfloor (q-1)^j \binom{n}{j}$  چندجمله‌ای تحویل‌ناپذیر با درجه  $t$  را خارج کنیم. این تعداد کمتر از  $(d/t)V_q(n, d-1)$  است (ارجاع به رابطه ۱). با استفاده از رابطه ۴، تعداد چندجمله‌ای‌های تحویل‌ناپذیر با درجه  $t$  روی  $\mathbb{F}_q^m$  از  $(1/t)q^{mt}(1 - q^{-(1/2)mt+mn})$

<sup>۳</sup> T. Kasami

تجاوز می‌کند؛ بنابراین، یک شرط کافی برای وجود کد  $\Gamma(L, g)$  که ما به دنبال آن هستیم این است که:

$$\frac{d}{t} V_q(n, d-1) < \frac{1}{t} q^{mt} (1 - q^{-(1/2)mt+n}). \quad (5)$$

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،  $mt \rightarrow \infty$  و  $d/n \rightarrow \infty$ . 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 گپای منظر، دارای نرخ اطلاعات مایل به  $1 - H_q(\delta)$  باشند. این همان کران گیلبرت (قضیه ۸.۵.۱) است.  $\square$

## ۹.۵ کدگشایی کدهای گپا

کدگشای برلیکمپ برای کدهای BCH که آنرا در انتهای بخش ۶.۷ بیان کردیم، نیز می‌تواند کدهای گپا را کدگشایی نماید. برای نشان دادن این مطلب، در روشی مشابه با بخش ۶.۷ پیش خواهیم رفت. فرض کنید  $(C_0, C_1, \dots, C_{n-1})$  کدکلمه‌ای در  $\Gamma(L, g)$ ، آن‌چنان که در تعریف ۱.۹.۲ آمد، باشد و فرض کنید بردار  $(R_0, R_1, \dots, R_{n-1})$  را دریافت کنیم. ما بردار خطا را با  $(E_0, E_1, \dots, E_{n-1}) = R - C$  نشان می‌دهیم. فرض کنید  $M := \{i \mid E_i \neq 0\}$ . درجه  $g(x)$  را با  $t$  نشان می‌دهیم و فرض کنیم که  $|M| = e < \frac{1}{t}$ . مجدداً با به‌کارگیری قرارداد ۳، چندجمله‌ای  $S(x)$  که هم‌رفت نامیده می‌شود، به صورت زیر تعریف می‌گردد:

$$S(x) \equiv \sum_{i=0}^{n-1} \frac{E_i}{x - \gamma_i} \pmod{g(x)}. \quad (6)$$

مشاهده می‌کنید که  $S(x)$  می‌تواند توسط گیرنده با به‌کارگیری  $R$  و رابطه ۴ محاسبه شود. حال ما چندجمله‌ای تشخیص-خطا<sup>۴</sup>  $\sigma(z)$  و یک چندجمله‌ای همراه  $\omega(z)$  را به روشی مشابه با بخش ۶.۷ تعریف می‌کنیم (اما در این لحظه با به‌کارگیری خود مکان‌ها به جای معکوس آنها).

$$\sigma(z) := \prod_{i \in M} (z - \gamma_i), \quad (7)$$

$$\omega(z) := \sum_{i \in M} E_i \prod_{j \in M \setminus \{i\}} (z - \gamma_j). \quad (8)$$

<sup>۴</sup> 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.

$$S(z)\sigma(z) \equiv \sum_{i=0}^{n-1} \frac{E_i}{z-\gamma_i} \prod_{i \in M} (z - \gamma_i) \equiv \omega(z) \pmod{g(z)}. \tag{۹}$$

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، به طوری که:

$$S(z)\sigma_1(z) \equiv \omega_1(z) \pmod{g(z)}. \tag{۱۰}$$

این نتیجه می‌دهد که:

$$\omega_1(z)\sigma(z) - \omega(z)\sigma_1(z) \equiv 0 \pmod{g(z)}.$$

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

بیاپید نگاه دیگری به کدهای گاپا بیندازیم. در نظر بگیرید  $L = \{1, \beta, \beta^2, \dots, \beta^{n-1}\}$  که در آن  $\beta$  یک ریشه  $n$ ام اولیه واحد در  $\mathbb{F}_{2^m}$  و  $g(z)$  یک چندجمله‌ای مناسب است. فرض کنید  $(a_0, a_1, \dots, a_{n-1}) \in \Gamma(L, g)$ . مشابه رابطه ۲، چندجمله‌ای ماتسون-سولومن  $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  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 در نظر بگیرید (با استفاده از لم ۲.۶.۵). طرف چپ معادله، یک چندجمله‌ای با درجه کمتری 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  $1$  جای‌گزین نماییم، چون روی  $\mathbb{F}_2$  کار می‌کنیم؛ بنابراین، سمت چپ برابر با چندجمله‌ای  $X^{n-1} \circ A(X)$

است (با به کارگیری نماد موجود در بخش ۶.۵)؛ زیرا این چندجمله‌ای نیز دارای درجه کمتر یا مساوی  $n - 1$  است و همان مقادیر را در ریشه‌های  $n$ ام واحد می‌پذیرد؛ بنابراین، قضیه زیر را اثبات کرده‌ایم.

**قضیه ۱.۹.۶.** اگر  $L = \{1, \beta, \dots, \beta^{n-1}\}$  که در آن یک ریشه  $n$ ام اولیه واحد در  $\mathbb{F}_m$  است و  $1 = (g(z), z^n - 1)$ ، آن‌گاه کد گپای دودویی  $\Gamma(L, g)$  شامل کلمات  $(a_0, a_1, \dots, a_{n-1})$  است که در آن چندجمله‌ای ماتسون-سولومن  $A(X)$  از  $a(x)$  در رابطه زیر صدق می‌کند:

$$X^{n-1} \circ A(X) \equiv 0 \pmod{g(X)}.$$

در قضیه ۲.۶.۶، کران BCH را با کمک قضیه ۴.۶.۵ و با به کارگیری این واقعیت که چندجمله‌ای ماتسون-سولومن یک کدکلمه دارای درجه به اندازه کافی کوچک است، ثابت کردیم. برای کدهای گپای، استدلال مشابهی کار می‌کند. چندجمله‌ای  $g(X)$  دارای درجه  $t$  است و  $1 = (g(X), X^n - 1)$ ؛ بنابراین، از قضیه ۱.۹.۶ نتیجه می‌شود که حداکثر  $n - 1 - t$  تا ریشه‌های  $n$ ام 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 به کار رفته، ما را مطمئن می‌سازد که چندجمله‌ای ماتسون-سولومن یک کدکلمه شامل تعداد کمی ریشه‌های  $n$ ام واحد به عنوان ریشه‌های خود است. این ایده، توسط چین<sup>۵</sup> و چُی<sup>۶</sup> (۱۹۷۵؛ مرجع [۱۳]) به روش زیر به کار رفته است.

**تعریف ۲.۹.۶.** فرض کنید  $(T, +, \circ)$  همان باشد که در بخش ۶.۵ با  $\mathcal{F} = \mathbb{F}_q^m$  و  $S = \mathbb{F}_q[x] \pmod{x^n - 1}$  آورده شد. فرض کنید  $P(X)$  و  $G(X)$  دو چندجمله‌ای در  $T$  باشند، به طوری که  $1 = (P(X), X^n - 1) = (G(X), X^n - 1)$ . کد BCH گسترش یافته (GBCH کد) با طول  $n$  روی  $\mathbb{F}_q$  با زوج چندجمله‌ای  $(P(X), G(X))$  به صورت زیر تعریف می‌شود:

$$\{a(x) \in S \mid P(X) \circ (\Phi a)(X) \equiv 0 \pmod{G(X)}\}.$$

یک GBCH به وضوح خطی است.

**قضیه ۳.۹.۶.** کمترین-فاصله یک کد GBCH در تعریف ۲.۹.۶ حداقل برابر با  $1 + \deg G(X)$  می‌باشد.

<sup>۵</sup> R. T. Chien

<sup>۶</sup> D. M. Choy

اثبات. قضیه ۴.۶.۵ را به کار می‌بریم. عامل مشترک  $f(X)$  از  $\Phi a$  و  $X^n - 1$ ، عاملی از  $P(X) \circ (\Phi a)(X)$  هم هست. اما  $(G(X), f(X)) = 1$ ؛ بنابراین، درجه  $f(X)$  باید حداکثر برابر با  $n - 1 - \deg G(X)$  باشد.  $\square$

توجه دارید که کدهای گاپای خاصی که در قضیه ۱.۹.۶ مطرح شدند، مثال‌هایی از کدهای GBCH هستند. اگر در نظر بگیریم  $P(X) = X^{n-1}$  و  $G(X) = X^{d-1}$ ، آن‌گاه یک کد BCH به دست می‌آوریم. کدهای GBCH شامل یک ماتریس بررسی توازن شبیه  $\hat{H}$  از بخش ۸.۱ هستند. برای نشان دادن این مطلب، چند جمله‌ای‌های  $p(x) = (\Phi^{-1}P)(x) = \sum_{i=0}^{n-1} p_i x^i$  و  $g(x) = (\Phi^{-1}G)(x) = \sum_{i=0}^{n-1} g_i x^i$  را در نظر می‌گیریم. با استفاده از لم ۲.۶.۵، تمامی ضرایب  $p(x)$  و  $g(x)$ ، ناصفر هستند، چون ریشه‌های  $n$ م 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 ۲.۹.۶، چند جمله‌ای  $B(X)$  با درجه حداکثر  $n - 1 - \deg G(X)$  وجود دارد، به طوری که:

$$P(X) \circ A(X) = B(X)G(X) = B(X) \circ G(X).$$

تعریف کنید  $b(x) := (\Phi^{-1}B)(x) = \sum_{i=0}^{n-1} b_i x^i$ ؛ در این صورت داریم:

$$p(x) * a(x) = b(x) * g(x),$$

یعنی:

$$\sum_{i=0}^{n-1} p_i a_i x^i = \sum_{i=0}^{n-1} b_i g_i x^i.$$

بنابراین، به دست آورده‌ایم  $b_i = p_i g_i^{-1} a_i$  ( $0 \leq i \leq n-1$ ). فرض کنید  $h_i := p_i g_i^{-1}$  و تعریف کنید:

$$H := \begin{pmatrix} h_0 & h_1 \beta & h_{n-1} \beta^{n-1} \\ h_0 & h_1 \beta^2 & h_{n-1} \beta^{2(n-1)} \\ \vdots & \vdots & \vdots \\ h_0 & h_1 \beta^t & h_{n-1} \beta^{t(n-1)} \end{pmatrix}.$$

فرض کنید  $1 \leq j \leq t = \deg G(X)$ ؛ در این صورت  $B_{n-j} = 0$ . با به کارگیری رابطه ۲ داریم:

$$B_{n-j} = b(\beta^j) = \sum_{i=0}^{n-1} b_i \beta^{ij} = \sum_{i=0}^{n-1} h_i a_i \beta^{ij}.$$

بنابراین،  $aH^T = 0$ . برعکس، اگر  $aH^T = 0$ ، آن‌گاه داریم که درجه  $B(X)$  حداکثر برابر  $n - 1 - t$  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<sup>۷</sup> نامیده می‌شوند. این کدها که در این فصل مورد بحث قرار گرفتند، موارد خاصی، وابسته به انتخاب  $h_i$  و  $\beta_i$ ، هستند. اولین زیرکلاس جالب، به نظر می‌رسد که کلاس کدهای اسریواستاوا<sup>۸</sup> که توسط اسریواستاوا<sup>۹</sup> در سال ۱۹۶۷ (منتشر نشده) معرفی شده است، باشد. برلیکمپ<sup>۱۰</sup> [۲] امکان آنها را تشخیص داد و مطالعه بیشتر در این زمینه را پیشنهاد داد. کدهای متناوب توسط هلگرت<sup>۱۱</sup> (۱۹۷۴؛ مرجع [۳۵]) معرفی شد. جالب‌ترین مطلبی که در مورد کدهای گاپا ثابت شد، توسط خود گاپا<sup>۱۲</sup> [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<sup>۱۳</sup> و زیمرمن<sup>۱۴</sup> [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  $\mathbb{F}_{2^4}$  باشد (فرض کنید  $\alpha^4 + \alpha + 1 = 0$ ). فرض کنید  $g(z) := z^2 + 1$ . کد دودویی گاپای  $\Gamma(L, g)$  را بررسی کنید.

۲.۹.۸. فرض کنید  $\alpha$  یک ریشه  $n$ ام اولیه واحد در  $\mathbb{F}_{2^m}$  باشد و فرض کنید  $L := \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ . 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  $L = \mathbb{F}_{q^m} \setminus \{0\}$ ،  $n = q^m - 1$ . فرض کنید  $C_1$  کد BCH با طول  $n$  روی  $\mathbb{F}_q$  به دست آمده با در نظر گرفتن  $d_1 = \delta$  در تعریف ۱.۶.۶ باشد. هم‌چنین فرض کنید  $C_2$  یک کد گاپای  $\Gamma(L, g)$  باشد. نشان دهید  $C_1 \cap C_2$  دارای کمترین-فاصله  $d \geq d_1 + d_2 - 1$  است که در آن  $d_2 := 1 + \deg g$ .

<sup>۷</sup> alternate codes

<sup>۸</sup> Srivistava codes

<sup>۹</sup> J. N. Srivistava

<sup>۱۰</sup> E. R. Berlekamp

<sup>۱۱</sup> H. J. Helgert

<sup>۱۲</sup> V. D. Goppa

<sup>۱۳</sup> K. K. Tzeng

<sup>۱۴</sup> K. P. Zimmerman

۴.۹.۸. کد GBCH با زوج چندجمله‌ای  $(P(X), G(X))$  را در نظر بگیرید که  $G(X)$  دارای درجه  $t$  باشد. نشان دهید که چندجمله‌ای  $\hat{P}(X)$  وجود دارد به طوری 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  $x^2 + x + 1$  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. در واقع، 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<sup>۱</sup>، ولادوت<sup>۲</sup> و زینک<sup>۳</sup> [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<sup>۴</sup> 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

<sup>۱</sup> Tsfasman

<sup>۲</sup> Vlăduț

<sup>۳</sup> Zink

<sup>۴</sup> G. van der Geer

کدگشایی سروکار زیادی نخواهیم داشت، بنابراین، در این روش‌ها وارد نمی‌شویم. در واقع، تنها روش کدگشایی که به طور گسترده در عمل به کار رفت (برای کدهای بلوکی)، یکی از روش‌هایی است که در بخش ۶.۷ 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 به دست می‌آید. برای مشاهده شرحی درباره این روی‌کرد، خواننده را به مرجع [۹۰] ارجاع می‌دهیم.

در بخش ۶.۹ دیدیم که ممکن است کدهای رید-سولومن را با در نظر گرفتن نقاط با مختص‌های متعلق به  $\mathbb{F}_q$  روی خط تصویری (شاید روی بستار جبری  $\mathbb{F}_q$ ) تعریف نماییم. کدکلمات، با در نظر گرفتن توابع گویا با یک قطب از مرتبه محدود در یک نقطه خاص و به دست آوردن مقادیر این توابع در نقاط داده شده به صورت مختص‌ها، تعریف شده‌اند. در بخش ۹.۲، کدهای گاوا را با محاسبه باقی‌مانده‌های توابع معین در نقاط داده شده تعریف کردیم. این مجموعه از توابع توسط شرط‌هایی بر روی ریشه‌ها و قطب‌های آنان محدود شده‌اند. این دورویکرد همان چیزی است که آن را در این فصل توسعه خواهیم داد. ما باید خم‌های جبری را مطالعه کنیم، روشی برای توصیف این محدودیت‌ها بر روی مجموعه توابعی که به کار 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 در نظر می‌گیریم، نتیجه کاملاً متفاوت خواهد بود). فرض کنید  $\mathbb{A}^n$  معرف فضای آفین  $n$ -بعدی باشد (با مختص‌های  $(x_1, x_2, \dots, x_n)$ ). به طور مشابه،  $\mathbb{P}^n$  فضای تصویری  $n$ -بعدی خواهد بود (با مختص‌های همگن  $(x_1, x_2, \dots, x_n)$ . در ابتدا 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<sup>۵</sup> معروف است. مجموعه‌های بسته<sup>۶</sup>، مجموعه‌هایی با ریشه‌های ایده‌آل‌های  $a$  از  $k[x_1, x_2, \dots, x_n]$  هستند؛ یعنی:

$$B = V(a) := \{(x_1, x_2, \dots, x_n) \in \mathbb{A}^n \mid f(x_1, x_2, \dots, x_n) = 0, \quad f \in a \text{ تمامی}\}.$$

<sup>۵</sup> Zariski topology

<sup>۶</sup> closed set

همواره فرض می‌کنیم  $a$  رادیکال<sup>۷</sup> است؛ یعنی  $a$  شامل تمامی چندجمله‌ای‌هایی است که روی  $B$  صفر می‌شوند (یک ایده آل  $a$ ، رادیکال نامیده می‌شود، اگر برای هر  $n \in \mathbb{N}$ ،  $f^n \in a$  نتیجه دهد  $f \in a$ ). یک زیرمجموعه بسته  $B$ ، تحویل‌ناپذیر<sup>۸</sup> نامیده می‌شود، اگر  $B$  را نتوان به صورت اجتماع دو زیرمجموعه بسته سره از  $B$  نوشت. مجموعه  $V(a)$  تحویل‌ناپذیر است، اگر و تنها اگر  $a$  یک ایده آل اول باشد. یک مجموعه باز<sup>۹</sup> مکمل یک مجموعه بسته است.

مثال ۱.۱۰.۱. در صفحه آفین، ایده آل اصلی تولید شده توسط  $x^2 - y^2$  را در نظر بگیرید. مجموعه بسته متناظر، اجتماع دو خط با معادلات  $y = x$ ، به ترتیب  $y = -x$ ، 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.

ایده آل اول  $p$  در حلقه  $k[x_1, x_2, \dots, x_n]$  را در نظر بگیرید. مجموعه  $\chi$  از ریشه‌های  $p$  یک چندگونای آفین<sup>۱۰</sup> نامیده می‌شود.

مثال ۲.۱۰.۱. در فضای ۳ بعدی، گوی واحد را در نظر بگیرید؛ یعنی مجموعه با معادله  $x^2 + y^2 + z^2 = 1$ . در اصطلاح خودمان، این یک چندگویای آفین شامل ریشه‌های ایده آل  $p$  تولید شده توسط چندجمله‌ای  $1 - x^2 - y^2 - z^2$  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  $\chi$  خواهند بود. این مطلب دلیل معرفی حلقه زیر است.

تعریف ۳.۱۰.۱. حلقه  $k[x_1, x_2, \dots, x_n]/p$ ، حلقه مختصات<sup>۱۱</sup>  $k[\chi]$  از متغیر  $\chi$  نامیده می‌شود.

حلقه مختصات، یک دامنه صحیح<sup>۱۲</sup> است، چون  $p$  یک ایده آل 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<sup>۱۳</sup>  $\chi$  گفته می‌شود. بعد متغیر  $\chi$ ، درجه متعالی  $k(\chi)$  روی  $k$  است. اگر این بعد برابر ۱ باشد، آن گاه  $\chi$  یک خم

<sup>۷</sup> radical

<sup>۸</sup> irreducible

<sup>۹</sup> open set

<sup>۱۰</sup> affine variety

<sup>۱۱</sup> coordinate ring

<sup>۱۲</sup> integral domain

<sup>۱۳</sup> function field

جبری نامیده می‌شود.

مثال ۵.۱۰.۱. در صفحه آفین روی میدان  $k$ ، سهمی  $\chi$  با معادله  $y^2 = x$  را در نظر می‌گیریم. در این مثال، حلقه مختصات  $k[\chi]$  شامل تمامی عبارتهایی به شکل  $A + By$  می‌باشد، که در آن  $A$  و  $B$  متعلق به  $k[x]$  هستند و  $y$  در رابطه  $y^2 = x$  صدق می‌کند. در این مثال، حلقه مختصات  $k(\chi)$  شامل تمامی عبارتهای به شکل  $A + By$  است، که در آن  $A$  و  $B$  در  $k[x]$  هستند و  $y$  در رابطه  $y^2 = x$  صدق می‌کند. بنابراین،  $k(\chi)$  یک توسیع جبری  $k(x)$  به وسیله 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 به کار ببریم. این بدان معناست که تنها مطلبی که منطقی به نظر می‌آید، مطالعه توابع گویاست به طوری که صورت و مخرج کسر، چندجمله‌ای‌های همگنی با درجه یکسان باشند. یک متغیر تصویری  $\chi$ ، مجموعه صفر در  $\mathbb{P}^n$  از یک ایده آل اول همگن  $p$  در  $k[x_0, x_1, \dots, x_n]$  است. زیرحلقه  $R(\chi)$  از  $k(x_0, x_1, \dots, x_n)$  شامل کسرهای  $f/g$  را در نظر بگیرید که در آن  $f$  و  $g$  چندجمله‌ای‌های همگن با درجه یکسان هستند و  $g \notin p$ ؛ در این صورت  $R(\chi)$  دارای ایده آل ماکسیمال یکتای  $M(\chi)$  است که شامل تمامی  $f/g$ هایی 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  $\chi$  یک آفین یا یک متغیر تصویری باشد. فرض کنید  $P$  یک نقطه روی  $\chi$  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 این صورت خارج قسمت  $\phi = f/g$ ، تعریف شده روی  $U$ ، منظم<sup>۱۴</sup> 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  $\chi$  تصویری باشد، آن‌گاه هیچ تابع منظمی روی  $\chi$  وجود ندارد مگر توابع ثابت.

تعریف ۶.۱۰.۱. حلقه موضعی<sup>۱۵</sup>  $O_P$  (که برخی اوقات با  $O_P(\chi)$  نشان داده می‌شود) از نقطه  $P$  روی متغیر  $\chi$ ، مجموعه توابع گویا روی  $\chi$  است که منظم می‌باشند.

خواننده آشنا با اصطلاح جبری، تشخیص خواهد داد که این در واقع یک "حلقه موضعی" به معنای جبری است؛ یعنی شامل یک ایده آل ماکسیمال است که در واقع این ایده آل همان مجموعه  $m_P$  از توابع در  $O_P$  است که در  $P$  صفر هستند.

یک متغیر آفین می‌تواند در یک متغیر تصویری به روش زیر نشانده شود. اگر  $f \in k[x_1, x_2, \dots, x_n]$

<sup>۱۴</sup>regular

<sup>۱۵</sup>local ring

آن‌گاه ما به  $f$  تابع همگن زیر را تخصیص می‌دهیم:

$$f^*(x_0, x_1, \dots, x_n) := x_0^l f(x_1/x_0, \dots, x_n/x_0),$$

که در آن  $l$  از درجه  $f$  است.

فرض کنید  $\phi$  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 این صورت  $p^*$  یک متغیر تصویری  $\chi^*$  در  $\mathbb{P}^n$  تعریف می‌کند. تعریف می‌کنیم  $\chi_*^* := \{(x_0, x_1, \dots, x_n) \in \chi^* \mid x_0 \neq 0\}$ ؛ در این صورت  $\chi$  یک ریخت با  $\chi^*$  تحت نگاشت  $(x_1, \dots, x_n) \rightarrow (1 : x_1 : \dots : x_n)$  است. نقاط  $(x_0 : x_1 : \dots : x_n) \in \chi^*$  با  $x_0 = 1$  نقاط در بی‌نهایت<sup>۱۶</sup>  $\chi$  نامیده می‌شوند. علاوه بر این، میدان تابعی  $k(\chi)$  و  $k(\chi^*)$  تحت نگاشت  $f/g \rightarrow f^*x_0^m/g^*$  که در آن  $m$  برابر با  $\deg(g) - \deg(f)$  است، یک ریخت می‌باشند.

مثال ۷.۱۰.۱. در  $\mathbb{P}^2$  با مختص‌های  $(x : y : z)$ ، متغیر  $\chi$  تعریف شده به صورت  $xz - y^2 = 0$  را در نظر بگیرید (این، همان سهمی مثال ۵.۱۰.۱ است، در اینجا با یک نقطه در بی‌نهایت یعنی  $(Q := (1 : 0 : 0))$  تابع  $(y^2 + z^2)/(xz + z^2)$  در نقطه  $(0 : 0 : 1)$   $P$  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  $(x^2 + y^2)/z^2$  که در  $P$  برابر با صفر است، می‌تواند به صورت حاصل ضرب  $y^2/z^2$  و  $(y^2 + z^2)/z^2$  نوشته شود، که در آن دومین عامل منظم است و در  $P$  صفر نیست. اگر با توپولوژی معمولی داشته باشیم  $k = \mathbb{C}$ ، در این صورت 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 آن را یک پارامتر موضعی خواهیم نامید.

مثال‌های موجود در پایان این پاراگراف، آنچه را گفتیم توضیح می‌دهند، اما باید در ابتدا تمامی اصطلاحاتی را که نیاز داریم، معرفی کنیم. از اینجا به بعد، تنها خم‌ها را در نظر می‌گیریم. خمی در  $\mathbb{A}^2$ ، تعریف شده به صورت یک معادله  $F(x, y) = 0$  را در نظر 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<sup>۱۷</sup> یا نامنفرد<sup>۱۸</sup> 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:

$$d_P F := F_x(a, b)(x - a) + F_y(a, b)(y - b).$$

<sup>۱۶</sup>points at infinity

<sup>۱۷</sup>simple

<sup>۱۸</sup>nonsingular

در این صورت مماس  $T_P$  در  $P$  به صورت  $d_P F = 0$  تعریف می‌شود. این نماد، شناخته شده 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  $d_P G := G_x(a, b)(x - a) + G_y(a, b)(y - b)$  خوش تعریف 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 این صورت از قاعده حاصل ضرب مشتق، می‌بینیم که  $m_P^2$  هسته این نگاشت است. بدون اثبات بیان می‌کنیم که این در واقع هسته است؛ بنابراین،  $m_P/m_P^2$  یک ریخت 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 این که فضای  $k$ -بعدی  $m_P/m_P^2$  دارای بعد ۱ است، تعریف کنیم. از اینجا به بعد، تنها خم‌های نامنفرد (خم‌های هموار نیز نامیده می‌شوند) را در نظر می‌گیریم؛ یعنی خم‌هایی که در آن تمامی نقاط نامنفرد هستند. این محدودیت دارای نتیجه زیر است. فرض کنید  $P$  یک نقطه از  $\chi$  باشد. به خواننده یادآوری می‌کنیم که ایده آل 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  $m_P$  به کار می‌بریم؛ در این صورت می‌توانیم هر عضو  $z$  از  $O_P$  را به طور یکتا به صورت  $z = ut^m$  بنویسیم، که در آن  $u$  یک عنصر یکه است و  $m \in \mathbb{N}_0$ . تابع  $t$  یک پارامتر موضعی یا پارامتر یکنواخت‌کننده<sup>۱۹</sup> 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  $m = \text{ord}_P(z) = v_P(z)$  (برای خواننده‌هایی که با این اصطلاح آشنایی دارند،  $O_P$  یک حلقه ارزیابی گسسته<sup>۲۰</sup> است و عناصر  $1 = v_P(t)$  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  $-m < v_P(z) = 0$ ، آن‌گاه گوییم  $z$  در  $P$  شامل یک قطب<sup>۲۱</sup> 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  $a \neq 0$ ،  $a \in k$  و  $v_P(z') > m$ . با این روش، می‌توان نشان داد که  $z$  می‌تواند به صورت یک سری لوران بیان شود. بعداً ما این مطلب را برای تعریف "مانده"<sup>۲۲</sup>  $z$  به کار خواهیم برد.

<sup>۱۹</sup>uniformizing parameter<sup>۲۰</sup>discrete valuation ring<sup>۲۱</sup>pole<sup>۲۲</sup>residue

مثال ۸.۱۰.۱. فرض کنید  $\chi$  دایره‌ای در  $\mathbb{A}^2$  با معادله  $x^2 + y^2 = 1$  باشد و فرض کنید  $P = (1, 0)$ ،  $\text{char}(k) \neq 2$ . هم‌چنین فرض کنید  $z = z(x, y) = 1 - x$ . 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  $dx = x - 1$  روی  $T_P$  برابر صفر است، بنابراین،  $x$  یک پارامتر موضعی در  $P$  نیست. روی  $\chi$  داریم  $1 - x = y^2 / (1 + x)$  و تابع  $1 / (1 + x)$  در  $O_P$  یک‌ه است. در مثال ۷.۱۰.۱، یک موقعیت مشابه را برای  $\mathbb{P}^2$  می‌بینیم.

مثال ۹.۱۰.۱. یک بار دیگر سهمی موجود در مثال ۷.۱۰.۱ را در نظر بگیرید. فرض کنید  $Q$  نقطه در بی‌نهایت باشد؛ یعنی  $Q = (1 : 0 : 0)$ . میدان  $k(\chi)$  شامل کسرهای  $(A_l + B_{l-1}y) / (C_l + D_{l-1}y)$  است که در آن، ضرایب، چندجمله‌ای‌های همگنی با درجه  $l$  (به ترتیب  $l - 1$ ) نسبت به  $x$  و  $z$  هستند و  $y$  در رابطه  $y^2 = xz$  صدق می‌کند. چنین تابعی در  $Q$  منظم است اگر ضریب  $C_l$  در  $x^l$  صفر نباشد. به آسانی دیده می‌شود که  $y/x$  نیز یک پارامتر موضعی در  $Q$  است. درباره رفتار تابع  $g := (z^2 + xyz) / x^3$  در  $Q$  چه می‌توان گفت؟ روی  $\chi$  داریم:

$$\frac{z^2 + xyz}{x^3} = \left(\frac{y}{x}\right)^2 \left(\frac{x^2 + yz}{x^2}\right).$$

دومین عامل در طرف راست معادله فوق 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  $\chi$  یک خم روی  $k$  باشد، آن‌گاه نقاط روی  $\chi$  که تمام مختص‌های آنها در  $\mathbb{F}_q$  است، نقاط گویا<sup>۲۳</sup> نامیده می‌شوند (مانند این اصطلاح را برای خم‌های روی  $k$  با معادلاتی که دارای تمام ضرایب در  $\mathbb{F}_q$  است، به کار خواهیم برد). سه مثال دیگر می‌آوریم.

مثال ۱۱.۱۰.۱. فرض کنید  $\mathbb{P}$  خط تصویری روی  $k$  باشد. یک پارامتر موضعی در نقطه  $P = (1 : 0)$  برابر  $y/x$  است. تابع گویای  $(x^2 - y^2) / y^2$  شامل یک قطب مرتبه ۲ در  $P$  است. اگر  $k$  دارای مشخصه ۲ نباشد، آن‌گاه  $(1 : 1)$  و  $(-1 : 1)$  ریشه‌هایی با تکرار ۱ هستند.

<sup>۲۳</sup>rational points

مثال ۱۲.۱۰.۱. خم مسطح با معادله  $x^2y + y^2z + z^2x = 0$  چهارتایی کلاین<sup>۲۴</sup> نامیده می‌شود. این خم را روی بستار جبری  $\mathbb{F}_2$  در نظر می‌گیریم. نگاهی به چند تا از زیرمیدان‌ها بیندازید. روی  $\mathbb{F}_2$ ، نقاط گویا برابر با  $(0:0:0)$ ،  $(1:0:0)$  و  $(0:1:0)$  هستند. اگر ما به  $\mathbb{F}_4$  برویم، آن‌گاه دو نقطه گویای بیشتر وجود دارند؛ یعنی  $(1:\alpha:1+\alpha)$  و  $(1:1+\alpha:\alpha)$  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 به صورت  $\mathbb{F}_2(\xi)$  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 در نظر بگیریم  $z = 1$ . اگر  $y = \xi^i$  ( $0 \leq i \leq 6$ )، آن‌گاه می‌نویسیم  $x = \xi^{2i}\eta$ . با جانشین نمودن آن در معادله، داریم  $\eta^3 + \eta + 1 = 0$ ؛ یعنی  $\eta$  یکی از عناصر  $\xi$ ،  $\xi^2$  یا  $\xi^4$  است؛ بنابراین، در مجموع ۲۴ نقطه گویا روی  $\mathbb{F}_8$  داریم.

مثال ۱۳.۱۰.۱. فرض کنید  $\chi$  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 ۱ یا ۰ 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 در نظر بگیریم. مشکلی را در نظر می‌گیریم که مجدداً پیش می‌آید. عبارت  $f := x/(y+z)$  به‌نظر یک تابع کاملاً منطقی به نظر می‌آید و در واقع روی بیشتر  $\chi$  چنین است. اما در  $Q$ ، این کسر معنی نمی‌دهد. ما باید یک شکل هم‌ارز برای  $f$  نزدیک  $Q$  بیابیم. روی  $\chi$  داریم:

$$\frac{x}{y+z} = \frac{x(y^2 + yz + z^2)}{y^3 + z^3} = t^{-2} \cdot \frac{y^2 + yz + z^2}{z^2},$$

که در آن دومین عامل سمت راست معادله فوق، منظم است و در  $Q$  صفر نیست. با استفاده 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 در نظر 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

<sup>۲۴</sup>Klein quartic



تکرارها شمرده شوند، آن‌گاه تعداد ریشه‌ها برابر با  $m$  است. در اینجا قضیه‌ای، معروف به قضیه بزوت<sup>۲۵</sup>، را بیان می‌کنیم که تعمیمی از این مساله به چندجمله‌ای‌های چند متغیره است. ما تنها حالت دو متغیره را در نظر می‌گیریم؛ یعنی خم‌های مسطح. مجدداً فرض کنیم که خواننده می‌داند چگونه تکرارها با نقاط مشترک دو خم مسطح 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  $l$  به ترتیب  $m$  را در نظر می‌گیریم. فرض می‌کنیم  $F$  و  $G$  شامل یک عامل مشترک غیربدیهی نباشند؛ یعنی این خم‌ها شامل یک مولفه در اشتراک خود نمی‌باشند. حالتی را در نظر 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 در نظر 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 بستر  $\mathbb{F}_2$  با معادله  $x^2 + y^2 = 1$  و خط با معادله  $x = y$  تلاقی نمی‌کنند. اما هنگامی که آنها به‌طور تصویری در نظر گرفته می‌شوند، خم  $\chi$  از مثال ۱۳.۱۰.۱ را داریم و خواننده به آسانی می‌تواند بررسی کند که  $\chi$  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 در نظر بگیرید. فرض کنید  $P_1, P_2, \dots, P_n$  نقاطی روی خم مسطح تعریف شده توسط معادله  $G(x, y) = 0$  باشند؛ یعنی  $G(P_i) = 0$  برای  $1 \leq i \leq n$ . کد  $C$  را به صورت زیر تعریف می‌کنیم.

$$C := \{(F(P_1), F(P_2), \dots, F(P_n)) \mid F \in \mathbb{F}_q[x, y], \deg(F) \leq l\}.$$

ما  $d$  را برای کمترین-فاصله این کد به کار خواهیم برد و (به‌طور معمول)  $k$  را بعد می‌نامیم (با میدانی که اخیراً در این بخش در نظر گرفته شد، اشتباه نگردد).

<sup>۲۵</sup>Bézout's

قضیه ۱۶.۱۰.۱. فرض کنید  $lm < n$ . برای کمترین فاصله  $d$  و بعد  $k$  از  $C$ ، داریم:

$$d \geq n - lm,$$

$$k = \begin{cases} \binom{l+2}{2} & \text{اگر } l < m \\ lm + 1 - \binom{m-1}{2} & \text{اگر } l \geq m. \end{cases}$$

اثبات. تکین‌هایی به شکل  $x^\alpha y^\beta$  با  $\alpha + \beta \leq 1$  تشکیل یک پایه از  $V_l$  می‌دهند؛ بنابراین،  $V_l$  دارای بعد  $\binom{l+2}{2}$  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  $F = 0$  و  $G = 0$  به ترتیب دارای درجه  $l' > l$  و  $m$  هستند و آنها شامل  $n$  نقطه مشترک  $P_1, P_2, \dots, P_n$  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  $k = \binom{l+2}{2}$  و اگر  $l \geq m$ ، آن‌گاه:

$$k = \binom{l+2}{2} - \binom{l-m+2}{2} = lm + 1 - \binom{m-1}{2}.$$

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،  $d \geq n - lm$ .  $\square$

## ۱۰.۲ مقسوم‌علیه‌ها

در ادامه،  $\chi$  یک خم تصویری هموار روی  $k$  است.

تعریف ۱۰.۱۰.۲.

(۱) یک مقسوم‌علیه<sup>۲۶</sup>، یک جمع صوری  $D = \sum_{P \in X} n_P P$  است به طوری که  $n_P \in \mathbb{Z}$  و برای همه به جز یک تعداد متناهی از نقاط  $P$  داریم  $n_P = 0$ .

(۲)  $Div(\chi)$  یک گروه جمعی از مقسوم‌علیه‌ها با جمع صوری است (گروه آبدلی آزاد روی  $\chi$ )؛

<sup>۲۶</sup>divisor

(۳) یک مقسوم علیه  $D$ ، موثر<sup>۲۷</sup> نامیده می‌شود اگر تمام ضرایب  $n_P$  نامنفی باشند (نماد  $(D \succeq 0)$ ؛

(۴) درجه<sup>۲۸</sup>  $\deg(D)$  از مقسوم علیه  $D$  برابر با  $\sum n_P$  است.

فرض کنید  $v_P = ord_P$  یک ارزیابی گسسته تعریف شده برای توابع روی  $\chi$  در بخش ۱۰.۱ باشد.

تعریف ۲.۱۰.۲. اگر  $f$  یک تابع گویا روی  $\chi$  باشد که هم‌ارز با تابع صفر نیست، آن‌گاه مقسوم علیه  $f$  را به صورت زیر تعریف می‌کنیم:

$$(f) := \sum_{P \in \chi} v_P(f)P.$$

بنابراین، در یک معنا، مقسوم علیه  $f$  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 به طوری که صورت و مخرج دارای درجه یکسانی هستند و چون  $k$  از نظر جبری بسته است، به طور محسوس، روشن است که  $f$  شامل تعداد یکسانی ریشه به عنوان قطب است، اگر به درستی شمارش شود. ما اثباتی ارائه نمی‌دهیم اما نتیجه‌ای را به صورت قضیه بیان می‌کنیم.

قضیه ۳.۱۰.۲. درجه یک مقسوم علیه از یک تابع گویا برابر با صفر است.

مقسوم علیه یک تابع گویا یک مقسوم علیه اصلی<sup>۲۹</sup> نامیده می‌شود.

تعریف ۴.۱۰.۲. دو مقسوم علیه  $D$  و  $D'$  به طور خطی هم‌ارز<sup>۳۰</sup> نامیده می‌شوند اگر و تنها اگر  $D - D'$  یک مقسوم علیه 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 تعیین شده 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 مقسوم علیه روی یک خم  $\chi$  باشد. یک فضای برداری  $\mathcal{L}(D)$  روی  $k$  را به صورت زیر تعریف می‌کنیم:

$$\mathcal{L}(D) := \{f \in k(\chi)^* : (f) + D \succeq 0\} \cup \{0\}.$$

<sup>۲۷</sup>effective

<sup>۲۸</sup>degree

<sup>۲۹</sup>principal divisor

<sup>۳۰</sup>linearly equivalent

توجه دارید که اگر  $D = \sum_{i=1}^r n_i P_i - \sum_{j=1}^s m_j Q_j$  که  $n_i, m_j > 0$  آن گاه  $\mathcal{L}(D)$  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 به صورت  $g = D - D'$  باشد، آن گاه نگاشت  $f \rightarrow fg$  نشان می‌دهد که  $\mathcal{L}(D)$  و  $\mathcal{L}(D')$  یک‌ریخت هستند.

### قضیه ۶.۱۰.۲

$$(۱) \quad \deg(D) < 0 \text{ اگر } \mathcal{L}(D) = 0$$

$$(۲) \quad l(D) := \dim_k \mathcal{L}(D) \leq 1 + \deg(D)$$

اثبات.

(۱) اگر  $\deg(D) < 0$ ، آن گاه 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  $f \in \mathcal{L}(D)$ ، آن گاه  $D' := D + (f)$  یک مقسوم‌علیه موثر است به طوری 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 بر روی 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 به دست 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  $Q = (0 : 1 : 1)$  است. این تابع شامل دوریشه است، هر یک با تکرار ۱؛ یعنی  $P_1 = (0 : \alpha : 1)$  و  $P_2 = (0 : 1 + \alpha : 1)$ . از نمایش  $f = (y^2 + yz + z^2)/x^2$  می‌بینیم که تنها قطب است؛ بنابراین، برطبق قضیه ۳.۱۰.۲ داریم  $(f) = P_1 + P_2 - 2Q$  و  $\deg((f)) = 0$ . 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  $\mathcal{L}(2Q)$  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  $\chi$  در  $\mathbb{A}^2$  تعریف شده با معادله  $F(x, y) = 0$  را در نظر بگیرید و فرض کنید  $P = (a, b)$  یک نقطه روی  $\chi$  باشد. مماس در  $T_P$  در نقطه  $P$  به صورت  $d_P F = 0$  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  $\chi$  یک عضو  $T_P^*$  تخصیص می‌دهند، در نظر می‌گیریم.

تعریف ۱.۱۰.۳. یک عضو  $\phi \in \Phi[\chi]$  یک فرم مشتق منظم<sup>۳۱</sup> (روی خم  $\chi$ ) نامیده می‌شود اگر هر نقطه  $P$  از  $\chi$  شامل یک همسایه  $U$  باشد به طوری که در این همسایه،  $\phi$  به صورت  $\phi = \sum_{i=1}^n f_i dg_i$  نمایش داده شود، که در آن تمامی توابع  $f_i$  و  $g_i$  در  $U$  منظم باشند.

فرم‌های مشتق منظم روی  $\chi$  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  $d(f+g) = df + dg$  و  $d(fg) = f dg + g df$  و  $da = 0$  برای  $a \in k$ . برای گسترش به فرم‌های مشتق گویا<sup>۳۲</sup> باید رابطه (معروف)  $d(f/g) = (gdf - fdg)/g^2$  را اضافه کنیم. می‌خواهیم تا یک فرم مشتق گویا روی یک خم تصویری هموار  $\chi$  تعریف کنیم. برای انجام دادن این کار، زوج‌های  $(U, \omega)$  و  $(V, \eta)$  را هم‌ارز می‌نامیم اگر  $\omega = \eta$  روی  $U \cap V$ . یک کلاس هم‌ارزی برای این رابطه یک فرم مشتق گویا نامیده می‌شود. از اینجا به بعد، فرم‌های مشتق گویا روی  $\chi$  را مشتق‌ها<sup>۳۳</sup> نامیده و فضای مشتق‌ها را با  $\Omega(\chi)$  نشان می‌دهیم. بدون اثبات

<sup>۳۱</sup>regular differential form

<sup>۳۲</sup>rational differential forms

<sup>۳۳</sup>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  $\omega$  می‌تواند به صورت  $\omega = f dt$  نوشته شود که در آن  $f$  یک تابع گویاست. خواننده ممکن است فکر کند که این مطلب به طور 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  $\chi$  در  $\mathbb{P}^2$  داده شده به صورت  $x^2 + y^2 + z^2 = 0$  می‌اندازیم ( $\text{cha}(k) \neq 3$ ). مجموعه باز  $U_x$  را به صورت  $U_x := \{(x : y : z) \in \chi : y \neq 0, z \neq 0\}$  و به طور مشابه  $U_y$  و  $U_z$  را تعریف کنید؛ در این صورت  $U_x, U_y, U_z$  و  $\chi$  را می‌پوشانند چون هیچ نقطه روی  $\chi$  وجود ندارد به طوری که دو تا از مختص‌های آن صفر باشد. به آسانی می‌توان بررسی نمود که سه نمایش:

$$U_x \text{ روی } \omega := \left(\frac{y}{z}\right)^2 d\left(\frac{x}{y}\right), \quad U_y \text{ روی } \eta := \left(\frac{z}{x}\right)^2 d\left(\frac{y}{z}\right), \quad U_z \text{ روی } \xi := \left(\frac{x}{y}\right)^2 d\left(\frac{z}{x}\right),$$

یک دیفرانسیل روی  $\chi$  تعریف می‌کنند. برای نمونه، برای نشان دادن این که  $\eta$  و  $\xi$  روی  $U_y \cap U_z$  برابر هستند، معاله  $0 = 1 + (x/z)^2 + (y/z)^2$ ، دیفرانسیل‌ها را گرفته و فرمول  $d(f^{-1}) = -f^{-2}df$  را برای  $f := y/z$  به کار ببریم. یک تابع منظم روی  $\chi$  ثابت است، بنابراین، نمی‌توان این دیفرانسیل را به صورت  $gdf$  به طوری که  $f$  و  $g$  توابعی منظم روی  $\chi$  باشند، نمایش داد.

تعریف ۴.۱۰.۳. مقسوم علیه  $(\omega)$  از مشتق  $\omega$  به صورت زیر تعریف می‌شود:

$$(\omega) := \sum_{P \in \chi} v_P(f_P)P,$$

که در آن  $\omega = f_P dt_P$  نمایش موضعی  $\omega$  بوده و  $v_P$  یک ارزیابی روی  $O_P$  است (گسترش یافته به  $k(\chi)$ ). البته باید نشان داد که این کد به انتخاب پارامتر موضعی وابسته نیست و نیز این که تنها تعداد متناهی از ضرایب، صفر نیستند.

فرض کنید  $\omega$  یک دیفرانسیل باشد و  $W = (\omega)$ ؛ در این صورت  $W$  یک مقسوم علیه کانونی<sup>۲۴</sup> نامیده می‌شود. اگر  $\omega'$  دیفرانسیل ناصفر دیگری باشد، آنگاه برای یک تابع گویای  $f$  خواهیم داشت  $\omega' = f\omega$ ؛

<sup>۲۴</sup>canonical divisor

بنابراین،  $(\omega') = W' \equiv W$  و از این رو مقسوم‌علیه‌های کانونی، تشکیل یک کلاس هم‌ارزی می‌دهند. این کلاس هم‌چنین با  $W$  نمایش داده می‌شود. حال فضای  $\mathcal{L}(W)$  را در نظر بگیرید. این فضای توابع گویا (ارجاع به تعریف ۵.۱۰.۲) می‌تواند بر روی یک فضای یک‌ریخت از فرم‌های دیفرانسیل به صورت  $f \rightarrow f\omega$  نگاشته شود. بنابر تعریف  $\mathcal{L}(W)$ ، تصویر  $f$  تحت این نگاشت، یک فرم دیفرانسیل منظم است؛ یعنی  $\mathcal{L}(W)$  یک‌ریخت با  $\Omega[X]$  است.

تعریف ۵.۱۰.۳ فرض کنید  $\chi$  یک خم تصویری هموار روی  $k$  باشد. گونای  $g$  از  $\chi$  را به صورت  $g := l(W)$  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<sup>۲۶</sup> را بیان می‌کنیم.

قضیه ۶.۱۰.۳. اگر  $\chi$  یک خم تصویری نامنفرد از درجه  $d$  در  $\mathbb{P}^2$  باشد، آن‌گاه:

$$g = \frac{1}{4}(d-1)(d-2).$$

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  $\chi$  ضرایب اسکالر از دیفرانسیل  $\omega$  در مثال ۳.۱۰.۳ هستند.

برای ساختن کدهای روی خم‌های جبری که کدهای گایا 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  $\omega$  داشتیم، تعریف می‌شود. فرض کنید  $P$  یک نقطه روی  $\chi$ ،  $t$  یک پارامتر موضعی در  $P$  و  $\omega = f dt$  نمایش موضعی  $\omega$  باشند. تابع  $f$  می‌تواند به صورت  $\sum_i a_i t^i$  نوشته شود. باقی‌مانده  $\text{Res}_P(\omega)$  از  $\omega$  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"<sup>۲۷</sup> شناخته شده است. ما تنها قضیه را بیان می‌کنیم.

قضیه ۷.۱۰.۳. اگر  $\omega$  یک دیفرانسیل روی یک خم تصویری هموار  $\chi$  باشد، آن‌گاه:

$$\sum_{P \in \chi} \text{Res}_P(\omega) = 0.$$

<sup>۲۵</sup>genus

<sup>۲۶</sup>Plücker formula

<sup>۲۷</sup>residue theorem

## ۱۰.۴ قضیه ریمن-روچ

قضیه مشهور زیر، معروف به قضیه ریمن-روچ<sup>۳۸</sup>، تنها یک نتیجه مرکزی در هندسه جبری با کاربردهایی در سایر موضوعات نیست، بلکه کلید نتایج جدید در نظریه کدگذاری هم هست.

قضیه ۱۰.۴.۱. فرض کنید  $D$  یک مقسوم‌علیه روی یک خم تصویری هموار از گونای  $g$  باشد؛ در این صورت، برای هر مقسوم‌علیه کانونی  $W$  داریم:

$$l(D) - l(W - D) = \deg(D) - g + 1$$

ما اثبات (کاملاً پیچیده) را نمی‌آوریم. این قضیه به ما اجازه می‌دهد تا درجه مقسوم‌علیه‌های کانونی را تعیین کنیم.

نتیجه‌گیری ۱۰.۴.۲. برای یک مقسوم‌علیه کانونی  $W$  داریم  $\deg(W) = 2g - 2$ .

اثبات. همواره توابع منظم روی یک خم تصویری ثابت هستند؛ یعنی  $\mathcal{L}(\circ) = k$ ، بنابراین،  $l(\circ) = 1$ .  $D = W$  را در قضیه ۱۰.۴ جای‌گزین کنید و نتیجه از تعریف ۱۰.۳ حاصل می‌گردد.  $\square$

حال واضح است که چرا در مثال ۱۰.۲ فضای  $\mathcal{L}(2Q)$  تنها دارای بعد ۲ است. با استفاده از قضیه ۱۰.۳، خم  $\chi$  دارای گونای ۱ است، درجه  $W - 2Q$  منفی است، بنابراین،  $l(W - 2Q) = 0$ . با استفاده از قضیه ۱۰.۴ داریم  $l(2Q) = 2$ .

در ابتدا، قضیه ۱۰.۴ خیلی مفید به نظر نمی‌آید. اما نتیجه ۱۰.۴ ابزاری برای به‌کارگیری موفق آن ارائه می‌دهد.

نتیجه‌گیری ۱۰.۴.۳. فرض کنید  $D$  یک مقسوم‌علیه روی یک خم تصویری هموار با گونای  $g$  باشد و فرض کنید  $\deg(D) > 2g - 2$ ؛ در این صورت:

$$l(D) = \deg(D) - g + 1.$$

<sup>۳۸</sup>Riemann-Roch theorem



اثبات. با استفاده از نتیجه ۲.۱۰.۴، داریم  $\deg(W - D) < 0$ ، بنابراین، با استفاده از قضیه ۶.۱۰.۲ قسمت (۱) داریم  $l(W - D) = 0$ . □

مثال ۴.۱۰.۴. کد موجود در قضیه ۱۶.۱۰.۱ را در نظر بگیرید. صفحه آفین را در یک صفحه تصویری بنشانید و توابع گویا روی خم تعریف شده توسط  $G$  را در نظر بگیرید. با استفاده از قضیه بزوت، این خم با خط دربی نهایت اشتراک دارد؛ یعنی خط تعریف شده به صورت  $z = 0$  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 ۶.۱۰.۳)، خم تعریف شده توسط  $G$  دارای گونای برابر با  $(m-1)$  است. اگر  $l \geq m - 2$  آن‌گاه نتیجه ۳.۱۰.۴ را به کار می‌بریم و نتیجه مشابهی همانند قضیه ۶.۱۰.۱ 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  $\chi$  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<sup>۳۹</sup>  $D$  نامیده می‌شود. ارتباط آن با توابع، توسط قضیه زیر برقرار می‌گردد.

$$\delta(D) = l(W - D) \quad \text{قضیه ۶.۱۰.۴.}$$

اثبات. اگر  $W = (\omega)$ ، آن‌گاه نگاشت خطی  $\phi : \mathcal{L}(W - D) \rightarrow \Omega(D)$  را به صورت  $\phi(f) := f\omega$  تعریف می‌کنیم. این نگاشت به وضوح یک‌ریختی است. □

مثال ۷.۱۰.۴. اگر در نظر بگیریم  $D = 0$ ، آن‌گاه با استفاده از تعریف ۵.۱۰.۳، دقیقاً  $g$  دیفرانسیل منظم به‌طور خطی مستقل روی یک خم  $\chi$  وجود دارد؛ بنابراین، دیفرانسیل موجود در مثال ۲.۱۰.۳ هم‌چنان که پس از قضیه ۶.۱۰.۳ ملاحظه شد، تنها دیفرانسیل منظم روی  $\chi$  (در حد یک عامل ثابت) است.

<sup>۳۹</sup>index of speciality

## ۱۰.۵ کدها از خم‌های جبری

حال به سراغ کاربردهایی در نظریه کدگذاری می‌آییم. الفبای ما مجدداً  $\mathbb{F}_q$  می‌باشد. قضایای موجود در بخش قبل را به کار خواهیم برد. انطباق‌های کمی نیاز هست، چون برای مثال فضای  $\mathcal{L}(D)$  روی یک میدان بسته جبری در نظر گرفته نخواهد شد؛ بلکه روی  $\mathbb{F}_q$  در نظر 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 در مورد پایه  $\mathcal{L}(D)$  (پایه‌ای روی بستار  $k$ ، شامل چند جمله‌ای‌های روی  $\mathbb{F}_q$ ) واضح خواهد شد.

فرض کنید  $\chi$  یک خم تصویری نامنفرد روی  $\mathbb{F}_q$  باشد. دو نوع از کدهای هندسه جبری از  $\chi$  را تعریف خواهیم کرد. نوع اول کدهای رید-سولومن را تعمیم می‌دهند، نوع دوم کدهای گاپا را تعمیم می‌دهند. در ادامه،  $P_1, P_2, \dots, P_n$  نقاط گویا روی  $\chi$  هستند و  $D$  مقسوم‌علیه  $P_1 + P_2 + \dots + P_n$  می‌باشد. علاوه بر این  $G$  مقسوم‌علیه دیگری است که دارای محمل  $4^\circ$  مجزا از  $D$  است. اگرچه انجام چنین کاری لازم نیست، اما ما محدودیت‌های بیشتری روی  $G$  قرار خواهیم داد؛ یعنی این که محمل  $G$  نیز شامل نقاط گویاست و علاوه بر این:

$$2g - 2 < \deg(G) < n. \quad (1)$$

تعریف ۱.۱۰.۵. کد خطی  $C(D, G)$  از درجه  $n$  روی  $\mathbb{F}_q$  تصویر نگاشت خطی  $\alpha : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$  تعریف شده به صورت  $\alpha(f) := (f(P_1), f(P_2), \dots, f(P_n))$  است. کدهای با این نوع "کدهای RS گسترش یافته هندسی  $4^1$ " 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  $\alpha$  باشد، آن گاه  $f \in \mathcal{L}(G - D)$  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.

$4^\circ$  support

$4^1$  geometric generalized RS codes

(۲) اگر  $\alpha(f)$  دارای وزن  $d$  باشد، آن گاه  $n - d$  نقطه  $P_i$ ، مانند  $P_{i_1}, P_{i_2}, \dots, P_{i_{n-d}}$ ، وجود دارند، به طوری که  $f(P_i) = 0$ ؛ بنابراین  $f \in \mathcal{L}(G - E)$ ، که در آن  $E = P_{i_1} + \dots + P_{i_{n-d}}$ . از این رو  $\deg(G) - n + d \geq 0$ .

□

به شباهتی که این اثبات با اثبات قضیه ۱۶.۱۰.۱ دارد توجه کنید.

مثال ۳.۱۰.۵. فرض کنید  $\chi$  خط تصویری روی  $\mathbb{F}_q$  باشد. در نظر بگیرید  $mQ := G$ ، که در آن نقطه  $(1 : 0)$  باشد،  $n = q$ ،  $P_i = (\alpha_i : 1)$ ، که در آن  $\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_q\}$ ؛ در این صورت، اگر  $m = k - 1$ ، آن گاه می بینیم که  $C(D, G)$  کد رید-سولومن گسترش یافته، آن چنان که در بخش ۶.۸ توصیف شد، است.

مثال ۴.۱۰.۵. فرض کنید  $\chi$  خم موجود در مثال های ۱۳.۱۰.۱ و ۷.۱۰.۲ باشد و  $2Q := G$ ، که در آن  $(0 : 1 : 1) := Q$ . در نظر می گیریم  $n = 8$  (بنابراین،  $D$  مجموع نقاط گویای باقی مانده است). این مختصات ها به صورت زیر داده شده اند:

$$\begin{array}{cccccccc} & Q & P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 \\ x & 0 & 0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & \alpha & \bar{\alpha} \\ y & 1 & \alpha & \bar{\alpha} & 0 & 0 & 0 & 1 & 1 & 1 \\ z & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{array},$$

که در آن  $\bar{\alpha} = 1 + \alpha$ . در مثال ۷.۱۰.۲ می بینیم که ۱ و  $x/(y+z)$  پایه ای از  $\mathcal{L}(2Q)$  روی  $k$  و از این رو روی  $\mathbb{F}_4$  نیز هستند. این مطلب منجر به ماتریس مولد زیر برای  $C(D, G)$  می گردد:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & \alpha & \bar{\alpha} \end{pmatrix}.$$

با استفاده از قضیه ۱.۱۰.۵، کمترین-فاصله، حداقل برابر با ۶ است و البته از ماتریس مولد دیده می شود که  $d = 6$ .

حال به سراغ دومین کلاس از کدهای هندسه جبری می آییم. ما این کدها را "کدهای گاپای هندسی" <sup>۴۲</sup> خواهیم نامید.

تعریف ۵.۱۰.۵. کد خطی  $C^*(D, G)$  با طول  $n$  روی  $\mathbb{F}_q$ ، تصویر نگاشت خطی  $\alpha^* : \Omega(G - D) \rightarrow \mathbb{F}_q^n$ ، تعریف شده به صورت زیر است:

$$\alpha^*(\eta) := (\text{Res}_{P_1}(\eta), \text{Res}_{P_2}(\eta), \dots, \text{Res}_{P_n}(\eta)).$$

پارامترها به صورت 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)، به کارگیری 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 در نظر بگیرید. فرض کنید  $P_i := (\gamma_i : 1)$ ، که در آن  $\gamma_i$ ها،  $0 \leq i \leq n-1$ ، مشابه با تعریف ۱.۹.۲ هستند. تعریف می‌کنیم  $D := P_0 + P_1 + \dots + P_{n-1}$  و  $G := (g)$ ، که در آن  $g(x, y)$  یک فرم همگن از چندجمله‌ای گاپای  $g(z)$  در تعریف ۱.۹.۲ است؛ در این صورت 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 در نظر گرفته و نشان دهیم که حاصل ضرب داخلی دو کلمه برابر با صفر است. فرض کنید  $\eta \in \Omega(G - D)$ ،  $f \in \mathcal{L}(G)$  با استفاده از تعریف‌های ۱.۱۰.۵ و ۵.۱۰.۵، مشتق  $f\eta$  شامل هیچ قطبی مگر احتمالاً قطب‌های مرتبه ۱ در نقاط  $P_1, P_2, \dots, P_n$  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 تمامی قطب‌ها، یعنی روی نقاط  $P_i$ ، برابر صفر است؛ بنابراین، داریم:

$$0 = \sum_{i=1}^n f(P_i)Res_{P_i}(\eta) = \langle \alpha(f), \alpha^*(\eta) \rangle .$$

□

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 به دست آوردن تمامی کدها کافی می‌باشند. اما، داشتن هر دو کلاس هنگام پرداختن به روش‌های کدگشایی مفید است. این روش‌ها ماتریس بررسی توازن را به کار 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 می‌بایم. به طور 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). در واقع، قضیه ۲.۱۰.۵ بیان می‌کند که  $d \geq n - k + 1 - g$ ، بنابراین، اگر  $g$  کوچک باشد، آن‌گاه ما نزدیک به کران سینگلتن 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. به جهت درک برخی مثال‌های موجود در این پاراگراف، کران هسه-ویل<sup>۴۳</sup> را بدون اثبات بیان می‌کنیم.

قضیه ۱.۱۰.۶. فرض کنید  $\chi$  یک خم با گونای  $g$  روی  $\mathbb{F}_q$  باشد. اگر  $N_q(\chi)$  معرف تعداد نقاط گویا روی  $\chi$  باشد، آن‌گاه:

$$|N_q(\chi) - (q + 1)| \leq 2g\sqrt{q}.$$

در ابتدا مثالی می‌آوریم که هیچ مطلب جدیدی را نتیجه نمی‌دهد.

مثال ۲.۱۰.۶. فرض کنید  $\chi$  خط تصویری روی  $\mathbb{F}_{q^m}$  باشد. فرض کنید  $n := q^m - 1$ . تعریف می‌کنیم  $P_\infty := (1 : 0)$ ،  $P_0 := (0 : 1)$  و مقسوم‌علیه  $D$  را به صورت  $\sum_{j=1}^n P_j$  تعریف می‌کنیم، که در آن  $(1 \leq j \leq n)$ ،  $P_j := (\beta^j : 1)$ . تعریف می‌کنیم  $G := aP_0 + bP_\infty$ ،  $a \geq 0$ ،  $b \geq 0$  (در اینجا  $\beta$  یک ریشه  $m$ ام اولیه واحد است). با استفاده از قضیه ۱.۱۰.۴،  $\mathcal{L}(G)$  دارای بعد  $a + b + 1$  است و فوراً دیده می‌شود

<sup>۴۳</sup>Hasse-Weil bound

که توابع  $(x/y)^i$ ،  $-a \leq i \leq b$ ، تشکیل یک پایه از  $\mathcal{L}(G)$  را می‌دهند. کد  $C(D, G)$  را در نظر بگیرید. یک ماتریس مولد برای این کد شامل سطرهای  $(\beta^i, \beta^{2i}, \dots, \beta^{ni})$  برای  $-a \leq i \leq b$  است. به آسانی بررسی می‌شود که  $(c_0, c_1, \dots, c_n)$  یک کدکلمه در  $C(D, G)$  است اگر و تنها اگر  $\sum_{j=1}^n c_j (\beta^l)^j = 0$  برای تمامی  $l$ هایی که  $a < l < n - b$  است. نتیجه می‌شود که  $C(D, G)$  یک کد رید-سولومن است. زیرمیدان با مختص‌های متعلق به  $\mathbb{F}_q$ ، یک کد BCH است.

مثال ۳.۱۰.۶. در این مثال، کدهایی را از خم‌های هرمیتی<sup>۴۴</sup> را در نظر می‌گیریم. فرض کنید  $q = r^2 = 2^l$ . یک خم هرمیتی  $\chi$  در  $\mathbb{P}^2$  روی  $\mathbb{F}_q$  با معادله زیر تعریف شده است:

$$x^{r+1} + y^{r+1} + z^{r+1} = 0. \quad (2)$$

با استفاده از قضیه ۶.۱۰.۳، گونای  $g$  از  $\chi$  برابر با  $\frac{1}{r}(q - \sqrt{q}) = \frac{1}{r}r(r-1)$  است. در ابتدا نشان خواهیم داد که  $\chi$  شامل بیشترین تعداد از نقاط گویاست؛ یعنی با استفاده از قضیه ۱.۱۰.۶ دقیقاً  $1 + q\sqrt{q}$  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  $\xi^{r+1} = 1$  است که شامل  $r+1$  جواب در  $\mathbb{F}_q$  می‌باشد. این مطلب نشان می‌دهد که  $\chi$  شامل  $3(r+1)$  نقطه با شرط  $xyz = 0$  است. اگر  $xyz \neq 0$  آنگاه ممکن است فرض کنیم  $z = 1$  و  $y$  عضوی از  $\mathbb{F}_q^*$  باشد به طوری که  $y^{r+1} \neq 0$ . برای هر انتخاب  $y$ ،  $r+1$  جواب  $x$  وجود دارد. این مطلب  $(r+1)^2(r-2)$  زوج  $(x, y)$  را نتیجه می‌دهد؛ بنابراین،  $\chi$  شامل  $1 + q\sqrt{q} = 1 + (r+1)^2(r-2) = 3(r+1) + (r-2)(r+1)^2$  نقطه گویاست (ملاحظه می‌کنیم که این نتیجه برای سایر اعداد اول به جز ۲ می‌تواند برقرار باشد).

گیریم  $G := mQ$ ، که در آن  $Q := (0 : 1 : 1)$  و  $q - \sqrt{q} < m < q\sqrt{q}$ . کد  $C(D, G)$  روی  $\mathbb{F}_q$  دارای طول  $n = q\sqrt{q}$ ، بعد  $k = m - g + 1$  و فاصله  $d \geq n - m$  است. برای دیدن این که این کدها چقدر خوب هستند، مثال  $q = 16$  را در نظر می‌گیریم. یک پایه برای  $\mathcal{L}(G)$  به آسانی یافت می‌شود. توابع  $f_{i,j}(x, y, z) := x^i y^j / (y+z)^{i+j}$ ،  $0 \leq i \leq 4$ ،  $4i + 5j \leq m$ ، این کار را انجام می‌دهند. در ابتدا، مشاهده می‌کنید که  $m - 5 = m - g + 1$  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 ۱۳.۱۰.۱، با نشان دادن این که  $f_{i,j}$  شامل یک قطب مرتبه  $4i + 5j$  در  $Q$  است، رفتار نمایند؛ بنابراین، این توابع مستقل هستند. از این رو، این کد به آسانی 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 (بگوئید  $10^9$  بیت) را روی

<sup>۴۴</sup> Hermitian curves

یک کانال با احتمال خطای  $p_e = 0.01$  (یک کانال کاملاً بد) ارسال نماییم. ما کدگذاری با استفاده از یک کد رید-سولومن با نرخ  $\frac{1}{4}$  روی  $\mathbb{F}_{16}$  را با کدگذاری با استفاده از  $C(D, G)$  مقایسه می‌کنیم که در آن  $m = 37$  تا مجدداً نرخ  $\frac{1}{4}$  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 کدگذاری به سختی برابر با  $3.10^{-4}$  است (درواقع یک بهبود مطلوب)؛ اما برای کد  $C(D, G)$ ، احتمال خطا پس از کدگذاری کمتر از  $2.10^{-7}$  است. در این مثال، به خاطر سپردن این مطلب مهم است که ما الفبا را ثابت نگه داشته‌ایم (در این حالت  $\mathbb{F}_{16}$ ). اگر ما کد  $C(D, G)$  را که در آن، کلمات، رشته‌هایی ۲۵۶ بیتی هستند با یک کد کد RS با نرخ  $\frac{1}{4}$  روی  $\mathbb{F}_{256}$  (کلمات دارای طول ۱۶۰ بیت هستند) مقایسه کنیم، آنگاه کد آخری به کارآیی (احتمال خطای  $2.10^{-6}$ ) نزدیک خواهد شد و یک کد RS با نرخ  $\frac{1}{4}$  روی  $\mathbb{F}_{256}$  (کلمات دارای طول ۳۸۴ بیت هستند) بهتر عمل می‌کند (تقریباً  $10^{-7}$ ). هم‌چنین می‌توانیم کد خود را با یک کد BCH دودویی به طول ۲۵۵ و نرخ  $\frac{1}{4}$  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<sup>۴۵</sup> باشیم، آنگاه کد  $C(D, G)$  می‌تواند خطاهای گروهی تا طول ۴۶ بیت را به دست گیرد (که حداکثر ۱۳ حرف یک کد کلمه 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 (به‌کاررفته توسط مولف) از جمله مطالبی بود که چندین مهندس را که به شدت 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 کدگذاری، مساله‌ای که ما در این کتاب از آن صرف نظر کردیم، اما به‌وضوح کاربردهایی اساسی دارد، منجر شده است.

مثال ۴.۱۰.۶. فرض کنید  $\chi$  چهارتایی کلاین روی  $\mathbb{F}_8$  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،  $\chi$  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 سیره<sup>۴۶</sup> [۹۸] این بهینه است). فرض کنید  $Q := (0 : 0 : 1)$  و فرض کنید  $D$  مجموع ۲۳ نقطه گویای دیگر باشد و  $G = 10Q$ . از قضیه ۲.۱۰.۵، داریم که  $C(D, G)$  دارای بعد  $8 = 10 - g + 1$  و کمترین-فاصله  $13 = 23 - 10$  است. حال این کد را با کد بررسی‌توازن واحد  $[4, 3, 2]$  به‌صورت زیر متصل کنید. سمبل‌های موجود در کدکلمات  $C(D, G)$ ، عناصر  $\mathbb{F}_8$  هستند

<sup>۴۵</sup>bursty channel

<sup>۴۶</sup>J.-P.Serre

که ما آنها را به عنوان بردارهای ستونی با طول ۳ روی  $\mathbb{F}_2$  تفسیر می‌کنیم و سپس بررسی توازن را اضافه می‌کنیم. کد حاصل  $C$  یک کد  $[92, 24, 26]$  دودویی است. کد پنچر شده حاصل، یک کد  $[91, 24, 25]$  (ساخته شده توسط بارگ ۴۷ [۸۲] در سال ۱۹۸۷) است که رکورد جهانی جدیدی برای کدهای با  $n = 91$ ،  $d = 25$  ایجاد نمود. چندین کد دیگر از این نوع در همان مقاله داده شده است.

مثال ۱۰.۶.۵. ما چگونگی ساخت یک ماتریس مولد برای کد موجود در مثال قبل را نشان می‌دهیم. توابع  $x/y$  و  $z/x$ ،  $y/z$  را در نظر می‌گیریم. نقاطی که این توابع می‌توانند دارای ریشه یا قطب باشند  $P_1 := (1 : 0 : 0)$ ،  $P_2 := (0 : 1 : 0)$  و  $Q = (0 : 0 : 1)$  هستند. چون خط با معادله  $y = 0$  (در مختصات آفین) در  $Q$  بر خم با معادله  $x^2y + y^2 + x = 0$  مماس نمی‌باشد، می‌بینیم که  $y/z$  یک پارامتر موضعی در  $Q$  (ایده‌ای که در مثال‌های اخیر به کار رفته است) است. به طور مشابه،  $z/x$  یک پارامتر موضعی در  $P_1$  است و  $x/y$  یک پارامتر موضعی در  $P_2$  می‌باشد. ما رفتار  $y/z$  در  $P_1$  و  $P_2$  را بررسی می‌کنیم. در  $P_1$  داریم:

$$\frac{y}{z} = \left(\frac{z}{x}\right)^2 \frac{x^3}{x^3 + y^2z},$$

بنابراین،  $y/z$  شامل یک ریشه با تکرار ۲ در  $P_1$  است. به طور مشابه، در  $P_2$  داریم:

$$\frac{y}{z} = \left(\frac{y}{x}\right)^2 \frac{y^3 + z^2x}{y^3},$$

بنابراین،  $P_2$  یک قطب مرتبه ۳ برای تابع  $y/z$  است. از این رو  $(\frac{y}{z}) = 2P_1 - 3P_2 + Q$ . به روش مشابه  $(\frac{z}{x}) = P_1 + 2P_2 - 3Q$  و  $(\frac{x}{y}) = -3P_1 + P_2 + 2Q$  را محاسبه می‌کنیم. از این مقسوم‌علیه‌ها، می‌توانیم نتیجه بگیریم که توابع  $(z/x)^i (y/x)^i$  برای  $0 \leq 3i + 2j \leq 10$  و  $0 \leq j \leq 2i$ ، متعلق به  $\mathcal{L}(10Q)$  هستند؛ بنابراین، توابع وزنی در  $\mathcal{L}(10Q)$  با قطب‌هایی در  $Q$  از مرتبه به ترتیب ۰، ۳، ۵، ۶، ۷، ۸، ۹ و ۱۰ داریم. از این رو آنها مستقل هستند و چون  $l(10Q) = 8$ ، آنها پایه‌ای از  $\mathcal{L}(10Q)$  هستند. با جای‌گزین نمودن مختص‌های نقاط گویای  $\chi$  در این توابع، ماتریس مولد ۸ در ۲۳ این کد را می‌یابیم.

مثال ۱۰.۶.۷. فرض کنید  $\mathbb{F}_4 = \{0, 1, \alpha, \bar{\alpha}\}$ ، که در آن  $\bar{\alpha} = \alpha + 1 = \alpha^2$ . خم  $\chi$  روی  $\mathbb{F}_4$  داده شده توسط معادله  $x^2y + \alpha y^2z + \bar{\alpha}z^2x = 0$  را در نظر بگیرید. این خم، یک خم نامنفرد با گونای ۱ است. ۹



نقطه گویای آن به صورت 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	$\alpha$	۱	۱
$y$	۰	۱	۰	$\alpha$	$\bar{\alpha}$	۱	۱	$\alpha$	۱
$z$	۰	۰	۱	$\bar{\alpha}$	$\alpha$	۱	۱	۱	$\alpha$

فرض کنید  $D := P_1 + P_2 + \dots + P_6$  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 این که خط با معادله  $x+y+\bar{\alpha}z=0$  با  $\chi$  در  $Q_2$  تلاقی دارد و بر  $\chi$  در  $Q_1$  مماس است. با به کار گیری قضیه ۱.۱۰.۵، کد  $C(D, G)$  از طول ۶ دارای کمترین-فاصله حداقل ۳ است. اما، این کد در واقع یک کد MDS است، یعنی کد شش تایی موجود در بخش ۴.۲.

## ۱۰.۷ بهبود کران گیلبرت-ورشامو

الفبای  $\mathbb{F}_q$  را ثابت نگه می‌داریم. کدهای  $C(D, G)$  آن چنان که در بخش ۱۰.۵ تعریف شد، با یک خم  $\chi$  را که شامل  $n+1$  نقطه گویای  $P_1, P_2, \dots, P_n, Q$  است، در نظر می‌گیریم. گیریم  $G = mQ$  به طوری که  $2 < m < n$ . تعریف می‌کنیم  $\gamma(\chi) := g/n$ . این مطلب توسط فاسمن<sup>۴۸</sup>، ولادوت<sup>۴۹</sup> و زینک<sup>۵۰</sup> [۹۸] نشان داده شده است که دنباله‌ای از خم‌های  $\chi$  وجود دارد، به طوری 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  $\chi_i$  روی  $\mathbb{F}_q$  وجود دارند؛ به طوری که  $\chi_i$  شامل  $n_i + 1$  نقطه گویا و گونای  $g_i$  است، که در آن  $n_i \rightarrow \infty$  وقتی  $i \rightarrow \infty$  و  $\bar{\gamma} = (q^{\frac{1}{2}} - 1)^{-1}$  برای  $\gamma(\chi_i) \rightarrow \bar{\gamma}$ .

همچنان که در قضیه ۲.۱۰.۵ دیدیم، کدهای متناظر  $C_i := C(D, G)$  روی  $\chi_i$  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 این رو با توجه به قضیه ۱.۱۰.۷ داریم:

<sup>۴۸</sup>Tsfasman

<sup>۴۹</sup>Vlăduț

<sup>۵۰</sup>Zink

$$\text{قضیه ۲.۱۰.۷. } \delta + \alpha(\delta) \geq 1 - \bar{\gamma}.$$

این یک تمرین مقدماتی در حسابان است که آیا خط مستقیم در صفحه  $(\delta, \alpha)$ ، 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  $q \geq 43$  و چون  $q$  باید یک مربع باشد، بهبودی از کران گیلبرت-ورشامو را برای  $q \geq 49$  داریم.

## ۱۰.۸ پیشنهادها

اولین روش‌های کدگشایی جالب در مقاله‌ای توسط جاستسن<sup>۵۱</sup> [۹۱] داده شد. این ایده‌ها توسط اسکروبوگاتو<sup>۵۲</sup> و ولادوت<sup>۵۳</sup> [۹۶] تعمیم داده شدند. از آن پس، این روش‌ها به‌طور قابل ملاحظه‌ای بهبود یافته (ر.ک. مرجع [۸۴]) و توسط فنگ<sup>۵۴</sup> 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 جستن کم و بیش از قضایای عمیق در هندسه جبری، تشریح شوند. این ایده‌ها توسط فنگ<sup>۵۵</sup> 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 به کار می‌برد.

بهبودهایی از کران گیلبرت-ورشامو (ر.ک. مرجع [۸۱])، نظریه خم‌های پیمانانه‌ای را به کار 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 به جای میدان‌ها و خواص جبری و تحلیلی خم‌ها، لازم به نظر می‌آید.

کار اخیر گارسیا<sup>۵۶</sup> و استیچتنوت<sup>۵۷</sup> [۸۷]، توصیفی روشن از دنباله خم‌ها با اثبات قضیه ۱.۱۰.۷ به‌وسیله ابزارهایی معتدل‌تر از هندسه جبری ارائه نمود.

<sup>۵۱</sup>J. Justesen

<sup>۵۲</sup>A. N. Skorobogatov

<sup>۵۳</sup>S. G. Vlăduț

<sup>۵۴</sup>G.-L.Feng

<sup>۵۵</sup>G.-L.Feng

<sup>۵۶</sup>Garcia

<sup>۵۷</sup>Stichtenoth

## مسائل ۱۰.۹

۱.۱۰.۹. خم موجود در مثال ۷.۱۰.۱ را در نظر بگیرید. رفتار تابع  $x/z$  در نقطه  $(1 : 0 : 0)$  چگونه است؟

۲.۱۰.۹. نشان دهید که اگر چهارتایی کلاین روی  $\mathbb{F}_p$  منفرد باشد، آن گاه  $p = 7$ . اگر  $p = 7$ ، آن گاه یک نقطه منفرد بیابید.

۳.۱۰.۹. سهمی  $\chi$  از مثال ۷.۱۰.۱ روی  $\mathbb{F}_4$  را در نظر بگیرید. فرض کنید  $g = (z^3 + xyz)/x^3$  مقسوم علیه  $g$  را تعیین کنید.

۴.۱۰.۹. فرض کنید  $\chi$  یک خم تصویری روی بستار جبری  $\mathbb{F}_7$  تعریف شده به وسیله معادله  $x^4y + y^4z + z^4x = 0$  باشد. مقسوم علیه  $f := x/z$  را تعیین کنید.

۵.۱۰.۹. نشان دهید که کد موجود در مثال ۶.۱۰.۶ در واقع هم‌ارز با کد شش‌تایی است.

۶.۱۰.۹. خم موجود در مثال ۴.۱۰.۶ را در نظر بگیرید. قضیه ریمن-روچ درباره  $l(3Q)$  چه می‌گوید؟ نشان دهید  $l(3Q) = 2$ .

# فصل ۱۱

## کدهای جبری به طور 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 در نظر بگیریم، آن‌گاه در مورد این کدها ناامید خواهیم شد. کدهای هادامارد موجود در بخش ۴.۱ دارای  $\delta = \frac{1}{p}$  بوده و اگر  $m \rightarrow \infty$ ، آن‌گاه نرخ آنان،  $R$ ، به سمت صفر میل می‌کند. برای کدهای همپنگ  $R$  به  $1$  میل می‌کند، اما  $\delta$  به صفر میل می‌کند. در مورد کدهای BCH نیز داریم  $\delta \rightarrow 0$ ، 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  $\delta \rightarrow 0$  یا  $R \rightarrow 0$ .

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  $R = \frac{1}{p}$  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 به صورت 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  $C_\alpha$  شامل کلمه ناصفر  $(a, \alpha a)$  با وزن کمتر از  $2m\lambda$  باشد، آن‌گاه این کلمه به طور یکتا  $\alpha$  را به عنوان خارج قسمت (در  $\mathbb{F}_{2^m}$ ) تقسیم  $\alpha a$  بر  $a$  تعیین می‌کند. نتیجه

می‌شود حداکثر  $\sum_{i < 2m\lambda} \binom{2m}{i}$  انتخاب برای  $\alpha$  منجر به یک کد  $C_\alpha$  خواهد شد که دارای کمترین-فاصله کمتر از  $2m\lambda$  است. حال در نظر می‌گیریم  $\lambda := H^{-1}(\frac{1}{4} - (1/\log m))$ . با استفاده از قضیه ۵.۱.۴، تعداد انتخاب‌های "بد" برای  $\alpha$  برابر است با  $o(2^m)$ ؛ بنابراین، برای حداکثر تمامی انتخاب‌های  $\alpha$  داریم:

$$d \geq 2mH^{-1}(\frac{1}{4} - \frac{1}{\log m}).$$

که در آن معرف کمترین-فاصله  $C_\alpha$  می‌باشد. با قرار دادن  $m \rightarrow \infty$  و در نظر گرفتن انتخاب‌های مناسب برای  $\alpha_m$ ، دنباله‌ای از کدهای با نرخ  $\frac{1}{4}$  را داریم؛ به طوری که  $\delta$  متناظر در رابطه زیر صدق می‌کند:

$$\delta = H^{-1}(\frac{1}{4}) + o(1), \quad (m \rightarrow \infty).$$

بنابراین، این دنباله به کران گیلبرت ۸.۵.۱ دست می‌یابد. اگر بتوانیم روش صریحی از انتخاب  $\alpha_m$  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<sup>۱</sup> در انجام این کار موفق گردید. ایده اصلی، تغییر ساختاری است که در بالا بیان شد. به جای آن (که در انتخاب مشکل است) مقدار  $\alpha$ ، تمامی مضارب  $\alpha$  در یک کدکلمه رخ می‌دهد. تاثیر متوسط، تقریباً به اندازه انتخاب زیرکانه  $\alpha$  خوب می‌باشد.

## ۱۱.۲ کدهای جاستسن

کدهایی که تشریح خواهیم کرد، تعمیمی از کدهای الحاقی<sup>۲</sup> هستند که توسط فُرنی<sup>۳</sup> در مرجع [۲۲] معرفی شدند. ایده آن، ساختن کد در دو مرحله با شروع از یک کد  $C_1$  و تعبیر کلمات  $C_1$  به عنوان سمبل‌های یک الفبای جدید که با آن  $C_2$  ساخته می‌شود، می‌باشد. ما این مطلب را با جزئیات بیشتر تشریح می‌کنیم. فرض کنید  $C_2$  کدی روی  $\mathbb{F}_2^m$  باشد. سمبل‌های  $c_i$  از یک کدکلمه  $(c_0, c_1, \dots, c_{n-1})$  می‌تواند به صورت  $m$ -تایی‌هایی روی  $\mathbb{F}_2$  نوشته شود؛ یعنی  $(c_{i1}, c_{i2}, \dots, c_{im})$   $(i = 0, 1, \dots, n-1)$  چنین  $m$ -تایی، دنباله‌ای از سمبل‌های اطلاعاتی برای یک کلمه متعلق به  $C_1$  معروف به کد داخلی<sup>۴</sup> است. بیاید ساده‌ترین حالت را در نظر بگیریم، که در آن نرخ برابر  $\frac{1}{4}$  است. متناظر با  $c_i = (c_{i1}, c_{i2}, \dots, c_{im})$  کلمه‌ای با طول  $2m$  در کد داخلی داریم.

<sup>۱</sup> J. Justesen

<sup>۲</sup> concatenated codes

<sup>۳</sup> G. D. Forney

<sup>۴</sup> inner code

نرخ کد الحاقی، نصف نرخ  $C_2$  است. ایده جاستسن، تغییر کد داخلی  $C_1$  بود؛ یعنی اجازه داشتن برای انتخاب  $C_1$  وابسته به  $i$ . مانند بخش قبل، کدهای داخلی طوری انتخاب شده‌اند که کلمه با طول  $2m$  با سمبل‌های  $c_i$  آغاز گردد. برای کد خارجی<sup>۵</sup>  $C_2$  ما یک کد رید-سولومن را در نظر می‌گیریم.

جزئیات ساختن در ادامه می‌آیند. چون مایلیم که  $m$  را به بی‌نهایت میل دهیم، باید یک ساختار ساده برای  $\mathbb{F}_{2^m}$  داشته باشیم. قضیه ۱۱.۱.۲۴ را به کار می‌بریم؛ بنابراین، قرار دهید  $m = 2^{l-1}$  و  $\mathbb{F}_{2^m}$  را در نمایشی به صورت  $\mathbb{F}_2[x]$  (در پیمانه  $g(x)$ ) در نظر بگیرید، که در آن  $g(x) = x^m + x^{m/2} + 1$ . کد رید-سولومن  $C_2$  که کد خارجی است، به صورت زیر تعبیر می‌شود (مراجعه به بخش ۶.۸). یک  $m$ -تایی از سمبل‌های اطلاعات  $(i_0, i_1, \dots, i_{m-1})$  به صورت عضو  $\mathbb{F}_{2^m}$   $i_0 + i_1x + \dots + i_{m-1}x^{m-1} \in \mathbb{F}_{2^m}$  تفسیر می‌شود.  $K$  مقدار متوالی  $m$ -تایی  $a_0, a_1, \dots, a_{K-1}$  را در نظر بگیرید و چندجمله‌ای  $a(Z) = a_0 + a_1Z + \dots + a_{K-1}Z^{K-1} \in \mathbb{F}_{2^m}[Z]$  را تشکیل دهید. برای  $N = 2^m - 1$ ،  $j = 1, 2, \dots, 2^m - 1$ ،  $j(x) = \sum_{i=0}^{m-1} \varepsilon_i x^i$  را با  $j(x) = \sum_{i=0}^{m-1} \varepsilon_i 2^i$  نمایش دودویی  $j$  باشد؛ در این صورت  $j(x)$  در میان عناصر ناصفر  $\mathbb{F}_{2^m}$  تغییر می‌کند. ما اینها را با  $a(Z)$  جانشین می‌کنیم؛ بنابراین، دنباله‌ای از  $N$  عضو  $\mathbb{F}_{2^m}$  را به دست می‌آوریم. این یک کد کلمه در کد خطی  $C_2$  است که دارای نرخ  $K/N$  است. چون  $a(Z)$  دارای درجه کمتری مساوی  $K - 1$  است، آن دارای حداکثر  $K - 1$  ریشه است؛ یعنی دارای کمترین-فاصله  $D \geq N - K + 1$  (ارجاع به بخش ۶.۸). 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  $j$ امین سمبل در یک کد کلمه در کد خارجی باشد (هنوز در نمایش به صورت چندجمله‌ای روی  $\mathbb{F}_2$ )، آن‌گاه ما آن را با  $(c_j, j(x)c_j)$  جای‌گزین می‌کنیم، که در آن، ضرب مجدداً در پیمانه  $g(x)$  در نظر گرفته می‌شود. سرانجام ما آن را به صورت یک  $2m$ -تایی از عناصر  $\mathbb{F}_2$  تفسیر می‌کنیم.

تعریف ۱۱.۱.۲. فرض کنید  $m = 2^{l-1}$ ،  $N = 2^m - 1$ ،  $K$  به روش مناسب زیر انتخاب خواهد شد؛  $D = N + 1 - K$ . کد دودویی با طول کلمه  $2mN$   $n := n_m := 2mN$  تعریف شده به صورت بالا، با  $\varphi_m$  نشان داده می‌شود. این کد، کد جاستسن<sup>۶</sup> گفته می‌شود. بعد  $\varphi_m$  برابر با  $k := mK$  و نرخ آن برابر با  $\frac{1}{4}K/N$  است.

در تحلیل ما از  $\varphi_m$ ، ایده مشابهی مانند بخش ۱۱.۱ را به کار می‌بریم؛ یعنی این واقعیت که یک  $2m$ -تایی ناصفر  $(c_j, j(x)c_j)$  واقع در یک کد کلمه  $\varphi_m$ ، مقدار  $j$  را مشخص می‌کند.

لم ۲.۱۱.۲. فرض کنید  $\gamma \in (0, 1)$  و  $\delta \in (0, 1)$ . فرض کنید  $(M_L)_{L \in \mathbb{N}}$  دنباله‌ای از اعداد طبیعی با

<sup>۵</sup> outer code

<sup>۶</sup> Justesen code

خاصیت  $M_L \cdot 2^{-L\delta} = \gamma + o(1)$  ( $L \rightarrow \infty$ ) باشد. فرض کنید  $W$  مجموع وزن‌های  $M_L$  کلمه متمایز در  $\mathbb{F}_2^L$  باشد؛ در این صورت:

$$W \geq \gamma L 2^{L\delta} \{H^{\leftarrow}(\delta) + o(1)\}, \quad (L \rightarrow \infty).$$

اثبات. برای  $L$  به قدر کافی بزرگ، تعریف می‌کنیم:

$$\lambda := H^{\leftarrow}\left(\delta - \frac{1}{\log L}\right).$$

با استفاده از قضیه ۵.۱.۴ داریم:

$$\sum_{0 \leq i \leq \lambda L} \binom{L}{i} \leq 2^{L(\delta - (1/\log L))}.$$

بنابراین:

$$\begin{aligned} W &\geq \{M_L - \sum_{0 \leq i \leq \lambda L} \binom{L}{i}\} \lambda L \geq \lambda L \{M_L - 2^{L(\delta - (1/\log L))}\} \\ &= \lambda L 2^{L\delta} \{\gamma + o(1)\} = \gamma L 2^{L\delta} \{H^{\leftarrow}(\delta) + o(1)\}, \quad (L \rightarrow \infty). \end{aligned}$$

□

یک نرخ  $R$ ،  $0 < R < \frac{1}{2}$ ، را انتخاب می‌کنیم. عدد  $K$  در تعریف ۱.۱۱.۲، کمترین مقداری در نظر گرفته شده است به طوری که  $R_m := \frac{1}{2}K/N \geq R$ . این ما را مطمئن می‌سازد که دنباله کدهای  $\varphi_m$  حاصل از در نظر گرفتن  $l = 1, 2, \dots$  در تعریف ۱.۱۱.۲ دارای نرخ  $R_m \rightarrow \infty$  ( $l \rightarrow \infty$ ) باشد. کمترین-فاصله  $\varphi_m$  چه طور است؟ یک کلمه ناصفر در کد خارجی دارای وزن حداقل  $N - K + 1 = D$  است. علاوه‌براین:

$$\begin{aligned} N - K + 1 &> N - K = N(1 - 2R_m) \\ &= (2^m - 1)\{1 - 2R + o(1)\}, \quad (m \rightarrow \infty). \end{aligned} \tag{۱}$$

هر سمبل ناصفر در یک کد کلمه از کد خارجی یک  $2m$ -تایی  $(c_j, j(x)c_j)$  در کد کلمه متناظر  $c$  از  $\varphi_m$  است و اینها همگی متفاوت خواهند بود (با استفاده از ملاحظه زیر ۱.۱۱.۲). لم ۲.۱۱.۲ را به کار گرفته تا وزن  $c$  را تخمین بزنیم. گیریم  $L = 2m$ ،  $\delta = \frac{1}{2}$ ،  $\gamma = 1 - 2R$ ، و  $M_L = D$ . با استفاده از رابطه ۱، شرایط لم، برقرار است؛ بنابراین:

$$w(c) \geq (1 - 2R) \cdot 2^m \cdot 2^m \{H^{\leftarrow}\left(\frac{1}{2}\right) + o(1)\}, \quad (m \rightarrow \infty).$$

از این رو:

$$d_m/n \geq (1 - 2R)\{H^{\leftarrow}\left(\frac{1}{\gamma}\right) + o(1)\}, \quad (m \rightarrow \infty).$$

بنابراین، قضیه زیر را ثابت کرده ایم.

**قضیه ۳.۱۱.۲.** فرض کنید  $\frac{1}{\gamma} < R < 1$ . کدهای جاستسن  $\varphi_m$  تعریف شده در بالا دارای طول کلمه  $n = 2m(2^m - 1)$  نرخ  $R_m$  و کمترین فاصله  $d_m$  هستند، که در آن:

$$(1) \quad R_m \rightarrow R \quad (m \rightarrow \infty);$$

$$(2) \quad \liminf_{m \rightarrow \infty} d_m/n \geq (1 - 2R)H^{\leftarrow}\left(\frac{1}{\gamma}\right).$$

حال با به کارگیری نماد موجود در فصل ۵، برای مقادیر  $R$  کمتر از  $\frac{1}{\gamma}$  داریم  $\delta \geq (1 - 2R)H^{\leftarrow}\left(\frac{1}{\gamma}\right)$ . برای اولین بار، برای  $m \rightarrow \infty$  به صفر میل نمی کند.

یک تغییر کوچک در ساختار قبل برای رسیدن به نرخ های بزرگ تر از  $\frac{1}{\gamma}$  لازم است. فرض کنید  $0 \leq s < m$  (را بعداً انتخاب خواهیم کرد).  $\varphi_m$  را در نظر بگیرید. برای هر  $2m$ -تایی  $(c_j, j(x)c_j)$  در کد کلمه  $c, s$  سمبل آخر را حذف می کنیم. کد حاصل با  $\varphi_{m,s}$  نشان داده می شود. فرض کنید  $R$  ثابت باشد،  $0 < R < 1$ . برای  $m$  و  $s$  داده شده،  $K$  را کوچک ترین عدد صحیحی انتخاب می کنیم، که در آن  $R_{m,s} := \lfloor m/(2^m - s) \rfloor (K/N) \geq R$  (اگر  $m(2^m - s) \geq R$  آنگاه این کار امکان پذیر است). در اثبات قضیه ۳.۱۱.۲، این واقعیت را که کد کلمه  $c$  شامل حداقل  $D$  تا  $2m$ -تایی متمایز ناصفر  $(c_j, j(x)c_j)$  است، به کار بردیم. با استفاده از برش  $\gamma$ ،  $(2^m - s)$ -تایی هایی را به دست آورده ایم که لزوماً دیگر متمایز نمی باشند، اما هر مقدار ممکن، حداکثر  $2^s$  بار رخ خواهد داد؛ بنابراین، حداقل  $M_s := 2^{-s}(N - K) = 2^{-s}N(1 - \frac{\gamma m - s}{m}R_{m,s})$  -تایی های متمایز در یک کد کلمه  $c$  از  $\varphi_{m,s}$  وجود خواهند داشت.

مجدداً لم ۲.۱۱.۲ را به کار می بریم؛ این بار با پارامترهای زیر:

$$L = 2^m - s, \quad \delta = \frac{m-s}{L}, \quad \gamma = 1 - \frac{\gamma m - s}{m}R, \quad M_L = M_s.$$

فرض کنید  $d_{m,s}$  کمترین فاصله  $\varphi_{m,s}$  باشد؛ داریم:

$$d_{m,s} \geq \left(1 - \frac{\gamma m - s}{m}R\right)(2^m - s)2^{m-s}\{H^{\leftarrow}\left(\frac{m-s}{\gamma m - s}\right) + o(1)\}2^s, \quad (m \rightarrow \infty)$$

$$\frac{d_{m,s}}{n} \geq \left(1 - \frac{\gamma m - s}{m}R\right)\{H^{\leftarrow}\left(\frac{m-s}{\gamma m - s}\right) + o(1)\}, \quad (m \rightarrow \infty) \quad (2)$$



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  $m/(2m - s) \geq R$  داریم. اگر  $r \geq R$ ، آن‌گاه هم‌چنین داریم  $s := \lfloor m(2r - 1)/r \rfloor + 1$  داریم:

$$\frac{d_{m,s}}{n} \geq (1 - \frac{R}{r})H^{\leftarrow}(1 - r) + o(1), \quad (m \rightarrow \infty) \quad (3)$$

طرف راست رابطه ۳ بیشترین است، اگر  $r$  در رابطه زیر صدق کند.

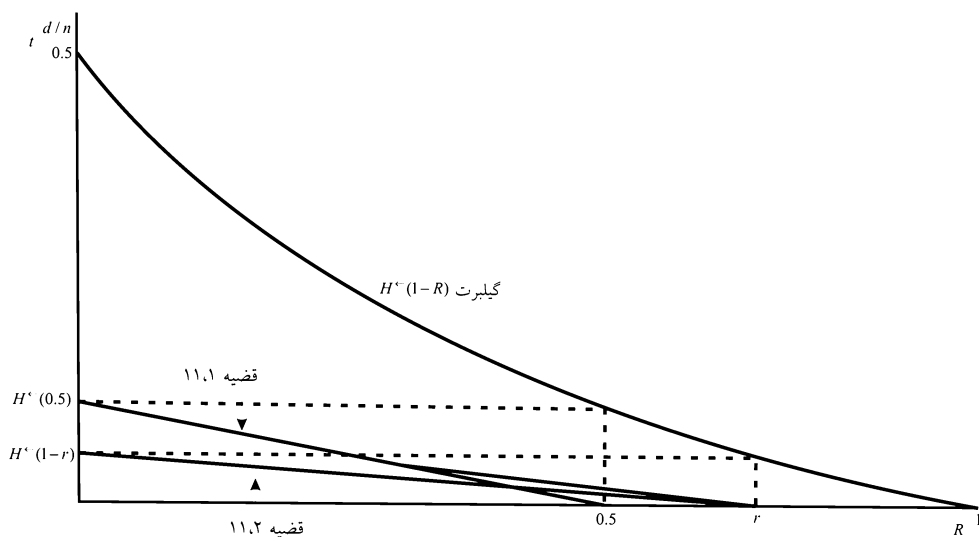
$$R = \frac{r^2}{1 + \log\{1 - H^{\leftarrow}(1 - r)\}}. \quad (4)$$

اگر جواب معادله ۴ کمتر از  $\frac{1}{2}$  باشد، آن‌گاه در نظر 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:

$$\liminf \frac{d_{m,s}}{n} \geq (1 - \frac{R}{r})H^{\leftarrow}(1 - r).$$

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 جدی تر ممکن است به کشف انتخاب‌های صریحی از  $\alpha$  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  $\mathbb{F}_{2^6}$  همان باشد که در بخش ۱۱.۲ نمایش داده شد. نشان دهید هیچ مقداری از  $\alpha$  برای ساختار بخش ۱۱.۱ وجود ندارد، به طوری که  $C_\alpha$  دارای فاصله بیشتر از ۳ باشد. آن را با سایر کدهای  $[12, k]$  معروف با نرخ بزرگ‌تر یا مساوی  $\frac{1}{4}$  مقایسه کنید.

۲.۱۱.۴. فرض کنید  $\alpha(x)$  چندجمله‌ای با درجه کمتر از  $k$  باشد. یک کد  $[2k, k]$  گردشی دوگانه<sup>۸</sup> دودویی شامل تمامی کلمات به شکل  $(a(x), \alpha(x)a(x))$  است، که در آن حاصل ضرب در پیمانه  $(x^k - 1)$  محاسبه شده است. در این حالت، کد، تحت یک شیفت دوری هم‌زمان از هر دو نیمه کلمات، پایا می‌باشد. یک کد  $[12, 6]$  از این نوع بسازید که دارای  $d = 4$  باشد.

۳.۱۱.۴. روش برش دادن<sup>۹</sup> موجود در بخش ۱۱.۲ را به کار 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.

<sup>۸</sup> double circulant

<sup>۹</sup> truncation

## فصل ۱۲

# کدهای حسابی

### ۱۲.۱ کدهای AN

در این فصل، مقدمه‌ای خلاصه‌وار درباره کدهایی که برای بررسی و تصحیح عمل‌گرهای حسابی استفاده شده توسط یک کامپیوتر به کار 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  $r$  ( $r \geq 2, r \in \mathbb{N}$ ) نمایش داده شده‌اند، محاسبه شده‌اند. برای اهداف عملی، حالت دودویی ( $r = 2$ ) و حالت ده‌تایی ( $r = 10$ ) مهم‌ترین می‌باشند. اولین چیزی که ما باید انجام دهیم یافتن یک تابع فاصله مناسب می‌باشد. در فصل‌های قبل، فاصله همینگ را به کار بردیم، اما آن یک تابع فاصله مناسب برای اهداف فعلی نمی‌باشد. یک خطا در یک جمع می‌تواند باعث ارقام نادرست بسیاری در پاسخ گردد، به دلیل 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<sup>۱</sup>  $w(x)$  از یک عدد صحیح  $x$  کوچک‌ترین  $t \geq 0$  است، به طوری که یک

<sup>۱</sup> 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  $|a_i| < r$ ،  $n(i) \geq 0$ ،  $(i = 1, 2, \dots, t)$ . فاصله حسابی<sup>۲</sup> دو عدد صحیح به صورت زیر تعریف می شود:

$$d(x, y) := w(x - y).$$

به آسانی چک می شود که این در واقع 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 نمی باشد. فاصله حسابی حداکثر برابر با فاصله همینگ است. کدهای  $C$  به شکل زیر را در نظر 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 می شوند. این کدها به روش زیر به کار رفته اند. فرض کنید می خواهیم دو عدد صحیح  $N_1$  و  $N_2$  (هر دو مثبت و کوچک در مقایسه با  $B$ ) را اضافه کنیم. این کدها به صورت  $AN_1$  و  $AN_2$  کد می شوند و سپس این دو عدد صحیح اضافه می شوند. فرض کنید  $S$  این مجموع باشد. اگر هیچ خطایی ایجاد نگردد، آن گاه  $N_1 + N_2$  را با تقسیم بر  $A$  داریم. اگر  $S$  بر  $A$  بخش پذیر نباشد؛ یعنی خطاهایی ایجاد شده اند، به دنبال کد کلمه  $AN_3$  می گردیم به طوری 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 بزرگ تریا مساوی  $2e + 1$  است. مانند قبل، این مطلب هم ارز با این شرط است که  $C$  دارای کمترین-وزن حداقل  $2e + 1$  باشد. این خصوصیات از کد  $C$  بر پایه شباهت  $C$  با زیرگروه  $H := \{AN \mid N \in \mathbb{Z}\}$  از  $\mathbb{Z}$  است. گرفتن  $H$  به عنوان کد، خود ایده خوبی نمی باشد، زیرا  $H$  دارای کمترین-وزن کمتر یا مساوی  $2$  است (مساله ۱.۱۲.۵ را ببینید).

به منظور اجتناب از این مشکل، کدهای معروف به کدهای پیمانه ای<sup>۳</sup>  $AN$  را در نظر خواهیم گرفت. تعریف کنید  $AB := m$ . حال می توانیم  $C$  را به عنوان زیرگروهی از  $\mathbb{Z}/m\mathbb{Z}$  در نظر بگیریم. این مطلب، تغییر تابع فاصله ما را لازم می سازد. عناصر  $\mathbb{Z}/m\mathbb{Z}$  را به صورت بردارهایی از یک گراف  $\Gamma_m$  در نظر بگیرید

<sup>۲</sup> arithmetic distance

<sup>۳</sup> modular codes

و فرض کنید  $x$  (در پیمانه  $m$ ) و  $x'$  (در پیمانه  $m$ ) با استفاده از یک یال به هم وصل شوند، اگر و تنها اگر:

$$x - x' \equiv \pm c.r^j \pmod{m},$$

برای برخی مقادیر صحیح  $c, j$  با شرط  $0 < c < r$ ،  $j \geq 0$ .

تعریف ۲.۱۲.۱. فاصله پیمانه‌ای<sup>۴</sup> دو عدد صحیح  $x$  و  $y$  (در نظر گرفته شده به صورت  $\mathbb{Z}/m\mathbb{Z}$ ) فاصله  $x$  و  $y$  در گراف  $\Gamma_m$  است. وزن پیمانه‌ای<sup>۵</sup>  $w_m(x)$  از  $x$  برابر با  $d_m(x, 0)$  است. توجه دارید که:

$$w_m(x) = \min\{w(y) \mid y \in \mathbb{Z}, y \equiv x \pmod{m}\}.$$

اگرچه در اینجا به شباهتی قوی با کدهای خطی دست یافته‌ایم، مشکل دیگری وجود دارد. توجه دارید که هر انتخابی برای  $m$  خوب است؛ برای مثال، اگر در نظر 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  $4 \equiv 3^1 \pmod{35}$ . اما خیلی منطقی نیست که زمانی که مجموع اعداد صحیح، کمتر از ۳۵ باشد، خطاها را در مکان متناظر با  $3^1$  در نظر بگیریم. محدود کردن  $j$  در تعریف یال‌های  $\Gamma_m$  نیز زیان‌بار است. ثابت می‌شود که اگر در نظر بگیریم  $m = r^n - 1$  ( $n \geq 2$ ،  $n \in \mathbb{Z}$ )، آن‌گاه می‌توانیم به نظریه‌ای قابل قبول 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 به صورت زیر است:

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{r^n - 1},$$

که در آن  $c_i \in \{0, 1, \dots, r-1\}$  ( $0 \leq i < n$ ) و تمامی  $c_i$ ها به طور هم‌زمان صفر نمی‌باشند؛ بنابراین،  $\mathbb{Z}/(r^n - 1)$  می‌تواند به صورت مجموعه‌ای از کلمات ناصفر به طول  $n$  روی الفبای  $\{0, 1, \dots, r-1\}$  تفسیر شود. البته لازم نیست که صفر را خارج کنیم، اگر در نظر 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  $c_0 = c_1 = \dots = c_{k-1} = 0$ . یک مقدار صحیح  $x$  (در پیمانه  $B$ ) با اضافه کردن  $k$  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

<sup>۴</sup> modular distance

<sup>۵</sup> modular weight

در حالت  $AB = m = r^n - 1$ ، فاصله پیمانه‌ای، یک تابع طبیعی برای محاسبه در  $\mathbb{Z}/m\mathbb{Z}$  است و این که  $C$  به صورت یک کد خطی عمل می‌کند. در واقع، حتی یک شباهت قوی‌تر با فصل‌های اخیر داریم.

تعریف ۳.۱۲.۱. یک کد  $AN$  دوری<sup>۶</sup> به طول  $n$  و پایه  $r$ ، یک زیرگروه  $C$  از  $\mathbb{Z}/(r^n - 1)$  است. چنین کدی یک ایده‌آل اصلی در این حلقه است؛ یعنی مقادیر صحیح  $A$  و  $B$  وجود دارند؛ به طوری که  $AB = r^n - 1$  و

$$C = \{AN \mid N \in \mathbb{Z}, 0 \leq N < B\}.$$

مانند بخش ۶.۱،  $A$  را مولد<sup>۷</sup> کد  $C$  می‌نامیم. تا به حال، این مطلب برای خواننده تعجب‌انگیز نبوده که ما در ابتدا به کدهای  $C$  با یک نرخ بزرگ  $(= (1/n) \log_r B)$  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  $rx \bmod r^n - 1$  نیز یک کدکلمه است، زیرا  $C$  یک گروه است و  $rx \bmod r^n - 1$  در واقع یک شیفت دوری از  $x$  است (هر دو در پایه  $r$  نمایش داده شده‌اند). عدد صحیح  $B$  می‌تواند با چند جمله‌ای بررسی یک کد دوری مقایسه شود.

ایده کدهای نادوری می‌تواند به روش یکسانی با در نظر گرفتن  $m = r^n + 1$  و سپس در نظر گرفتن زیرگروه‌های  $\mathbb{Z}/m\mathbb{Z}$  گسترش یابد.

مثال ۴.۱۲.۱. فرض کنید  $r = 2$ ،  $n = 11$ ؛ در این صورت  $m = r^n - 1 = 2047$ . فرض می‌کنیم  $A = 23$ ،  $B = 89$ . کد  $AN$  دوری شامل ۸۹ مضرب از ۲۳ تا ۲۰۴۷ را به دست می‌آوریم. ۲۲ روش برای ساختن یک خطا، متناظر با اعداد صحیح  $2^j \pm 1$  ( $0 \leq j < 11$ ) وجود دارد. اینها دقیقاً اعداد صحیح در پیمانه ۲۳ به جز صفر هستند؛ بنابراین، هر مقدار صحیح در بازه  $[1, 2047]$  دارای فاصله پیمانه‌ای  $0$  یا  $1$  تا دقیقاً یک کدکلمه است؛ بنابراین، این کد  $AN$  دوری، کامل<sup>۸</sup> است. این تعمیمی از کدهای همینگ است.

<sup>۶</sup> cyclic

<sup>۷</sup> generator

<sup>۸</sup> 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 به صورت زیر نوشته شود:

$$x = \sum_{i=1}^{w(x)} a_i r^{n(i)},$$

با مقادیر صحیح  $a_i$ ،  $n(i) < r$ ،  $|a_i| < r$ ،  $n(i) \geq 0$ ،  $(i = 1, \dots, w(x))$ . 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  $c \in \mathbb{Z}$ ،  $b \in \mathbb{Z}$ ،  $|c| < r$  و  $|b| < r$ . زوج  $(b, c)$  قابل قبول<sup>۹</sup> نامیده می‌شود، اگر یکی از شرایط زیر برقرار باشد:

$$(۱) \quad bc = 0$$

$$(۲) \quad bc > 0 \text{ و } |b+c| < r$$

$$(۳) \quad bc < 0 \text{ و } |b| > |c|$$

توجه دارید که اگر  $r = ۲$ ، آن‌گاه ما باید احتمال (۱) را داشته باشیم؛ بنابراین، یک نمایش  $x = \sum_{i=0}^{\infty} c_i 2^i$  به طوری که تمامی زوج‌های  $(c_{i+1}, c_i)$  قابل قبول باشند، دارای هیچ دو رقم ناصفر مجاوری نمی‌باشند. این منجر به نام فرم غیرمجاور<sup>۱۰</sup> (NAF) می‌گردد که ما اینک آن را تعمیم می‌دهیم.

تعریف ۲.۱۲.۲. نمایش:

$$x = \sum_{i=0}^{\infty} c_i r^i,$$

با  $c_i \in \mathbb{Z}$ ،  $|c_i| < r$  برای تمامی  $i$ ها و  $c_i = 0$  برای تمام  $i$ های بزرگ، یک NAF برای  $x$  نامیده می‌شود، اگر برای هر  $i \geq 0$ ، زوج  $(c_{i+1}, c_i)$  قابل قبول باشد.

<sup>۹</sup> admissible

<sup>۱۰</sup> 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، آن گاه:

$$w(x) = |\{i \mid i \geq 0, c_i \neq 0\}|.$$

اثبات.

(۱) فرض کنید  $x$  به صورت  $\sum_{i=0}^{\infty} b_i r^i$ ،  $|b_i| < r$  نمایش داده شود. فرض کنید  $i$  کمترین مقداری باشد که زوج  $(b_{i+1}, b_i)$  قابل قبول نباشد. بدون کاستن از کلیت  $b_i > 0$  (در غیر این صورت  $-x$  را در نظر بگیرید).  $b_i$  را با  $b'_i := b_i - r$  جایگزین کنید و  $b_{i+1}$  را با  $b_{i+1} + 1$  یا  $b'_{i+1} := b_{i+1} + 1$  (اگر  $b_{i+1} + 1 = r$ ، آن گاه این کار را ادامه می دهیم). اگر  $b_{i+1} > 0$  آن گاه داریم  $b'_{i+1} = 0$  یا  $b'_{i+1} < 0$  و  $b'_i b'_{i+1} < 0$  و  $|b'_i| = r - b_i = b_{i+1} + 1 > r - b_i = |b'_i|$  چون  $(b_i, b_{i+1})$  قابل قبول نبوده است. بنابراین،  $(b'_i, b'_{i+1})$  قابل قبول نیست و به روشی مشابه می توان بررسی کرد که  $(b'_{i+1}, b'_i)$  قابل قبول است. در این روش می توانیم یک NAF بسازیم و در این فرایند، وزن این نمایش افزایش نمی یابد.

(۲) تنها مطلبی که باقی می ماند این است که NAF یکتاست. فرض کنید برخی  $x$  ها دارای دو نمایش به صورت  $\sum_{i=0}^{\infty} c'_i r^i = \sum_{i=0}^{\infty} c_i r^i$  باشند. بدون کاستن از کلیت ممکن است فرض کنیم  $c'_0 \neq c_0$ ،  $c_0 > 0$ . بنابراین،  $c'_0 = c_0 - r$ . نتیجه می شود که  $c'_1 \in \{c_1 + 1 - r, c_1 + 1, c_1 + 1 + r\}$ . اگر  $c'_1 = c_1 + 1 - r$ ، آن گاه  $c_1 \geq 0$ ؛ بنابراین،  $c_0 + c_1 \leq r - 1$  چون  $c'_0 c'_1 > 0$  باید داشته باشیم  $c'_0 - c'_1 < r$ ، یعنی  $r - c_0 + r - c_1 - 1 < r$ ؛ بنابراین،  $c_0 + c_1 > r - 1$  که تناقض است. به روشی مشابه فرض های  $c'_1 = c_1 + 1$ ، به ترتیب  $c'_1 = c_1 + 1 + r$  به تناقض منجر می گردد؛ بنابراین، NAF یکتاست.  $\square$

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 نمایش های  $-r$ -تایی  $(r+1)x$  و  $x$  به صورت زیر باشد:

$$(r+1)x = \sum_{j=0}^{\infty} a_j r^j, \quad x = \sum_{j=0}^{\infty} b_j r^j.$$



با  $\{0, 1, \dots, r-1\}$  برای تمامی  $j$ ها و  $a_j = b_j = 0$  برای  $j$ های به اندازه کافی بزرگ؛ بنابراین، NAF برای  $x$  به صورت زیر است:

$$x = \sum_{j=0}^{\infty} (a_{j+1} - b_{j+1})r^j.$$

اثبات. ما اعداد  $a_j$  را با اضافه نمودن  $\sum_{j=0}^{\infty} b_j r^j$  و  $\sum_{j=0}^{\infty} b_j r^{j+1}$  محاسبه می کنیم. فرض کنید دنباله انتقالی به صورت  $\varepsilon_0, \varepsilon_1, \dots$  باشد؛ بنابراین،  $\varepsilon_0 = 0$  و  $\varepsilon_1 := \lfloor (\varepsilon_{i-1} + b_{i-1} + b_i)/r \rfloor$  داریم. حال باید بررسی کنیم که آیا  $(c_i, c_{i+1})$  یک زوج قابل قبول است یا نه. این مطلب که  $|c_{i+1} + c_i| < r$ ، نتیجه ای بدیهی از تعریف  $\varepsilon_i$  است. فرض کنید  $c_i > 0$ ،  $c_{i+1} < 0$ ؛ بنابراین،  $\varepsilon_i = 0$ . پس داریم  $c_i = \varepsilon_{i-1} + b_{i-1} + b_i - \varepsilon_i r$ . اگر  $a_i - b_i$  را با  $c_i$  نشان دهیم، آن گاه  $c_i = \varepsilon_{i-1} + b_{i-1} + b_i - \varepsilon_i r$ . این مطلب که  $|c_{i+1} + c_i| < r$  هم ارز با  $\varepsilon_{i-1} + b_{i-1} + b_i < r$  است؛ یعنی  $\varepsilon_i = 0$ . حالت آخر مشابه است.  $\square$

NAF متناظر با  $x$  به ما یک تخمین ساده از  $x$  آن چنان که در قضیه بعد نشان داده شده است، ارائه می دهد.

قضیه ۵.۱۲.۲. اگر بیشترین مقدار  $i$  را به طوری که  $c_i \neq 0$  در یک NAF برای  $x$  با  $i(x)$  نشان دهیم و تعریف کنیم  $i(0) := -1$  آن گاه:

$$i(x) \leq k \Leftrightarrow |x| < \frac{r^{k+2}}{r+1}.$$

اثبات کاملاً مقدماتی این قضیه را به خواننده واگذار می کنیم.

حال، از بخش ۱۲.۱ واضح خواهد بود که این ایده ها را باید به روش مشابهی برای نمایش های پیمانه ای گسترش دهیم؛ داریم  $n \geq 2$ ،  $m = r^n - 1$ .

تعریف ۶.۱۲.۲. نمایش:

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{m},$$

با  $c_i \in \mathbb{Z}$ ،  $|c_i| < r$  یک CNAF ( $\Rightarrow$  NAF دوری) برای  $x$  نامیده می شود، اگر  $(c_{i+1}, c_i)$  برای  $i = 0, 1, \dots, n-1$  قابل قبول باشد؛ بنابراین،  $c_n := c_0$ .

دو قضیه بعدی از CNAFها توسیع های سراسر است از قضیه ۳.۱۲.۲ می باشند و می توانند از این قضیه با به کارگیری قضیه ۴.۱۲.۲ به دست 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 پیمانانه  $m$  است؛ این CNAF یکتاست، مگر این که:

$$(r + 1)x \equiv 0 \not\equiv x \pmod{m},$$

که در این حالت، دو CNAF برای  $x$  (در پیمانانه  $m$ ) وجود دارد. اگر  $x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{m}$  یک CNAF برای  $x$  باشد، آن گاه:

$$w_m(x) = |\{i \mid 0 \leq i < n, c_i \neq 0\}|.$$

قضیه ۸.۱۲.۲. اگر  $(r + 1)x \equiv 0 \not\equiv x \pmod{m}$ ، آن گاه  $w_m(x) = n$ ؛ مگر این که  $n \equiv 0 \pmod{2}$  و  $w_m(x) = \frac{1}{2}n$  که در این حالت  $x \equiv \pm[m/(r + 1)] \pmod{m}$ .

قضیه ۹.۱۲.۲. اگر یک NAF برای  $x$  داشته باشیم، به طوری که  $c_{n-1} = 0$ ، آن گاه شرط اضافی برای این که این NAF یک CNAF باشد، برقرار است؛ بنابراین، قضیه ۵.۱۲.۲ قضیه زیر را ایجاب می کند. یک عدد صحیح  $x$  شامل یک CNAF با  $c_{n-1} = 0$  است، اگر و تنها اگر یک  $y \in \mathbb{Z}$  با  $x \equiv y \pmod{m}$  وجود داشته باشد.

این قضیه به روش دیگری برای یافتن وزن پیمانانه‌ای یک عدد صحیح منجر می شود.

قضیه ۱۰.۱۲.۲. برای  $x \in \mathbb{Z}$  داریم:

$$w_m(x) = |\{j \mid 0 \leq j < n, \exists y \in \mathbb{Z}, m/(r + 1) < y \leq m/(r + 1), y \equiv r^j x \pmod{m}\}|.$$

اثبات. به وضوح یک CNAF برای  $rx$  یک شیفت دوری از یک CNAF برای  $x$  است؛ یعنی  $w_m(rx) = w_m(x)$ . فرض کنید  $x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{m}$  یک CNAF باشد و  $c_{n-1-j} = 0$ ؛ در این صورت  $r^j x$  دارای یک CNAF با صفر به عنوان ضریب  $r^{n-1}$  است. با استفاده از قضیه ۹.۱۲.۲ این حالت مطلوب است، اگر وجود داشته باشد یک  $y$  با شرط  $y \equiv r^j x \pmod{m}$  و  $|y| \leq m/(r + 1)$ . چون وزن پیمانانه‌ای برابر با تعداد ضرایب ناصفر است، ادعا حاصل می گردد؛ مگر این که ما در یکی از حالات استثنایی قضیه ۷.۱۲.۲ باشیم، اما در این صورت نتیجه با توجه به قضیه ۸.۱۲.۲ نتیجه می شود.  $\square$

## ۱۲.۳ کدهای مندلبوم-باروس

حال کلاسی از کدهای AN دوری تصحیح‌کننده چند خطا را معرفی می‌کنیم که تعمیمی از کدهای معرفی‌شده توسط باروس<sup>۱۱</sup> و مندلبوم<sup>۱۲</sup> هستند. در ابتدا نیاز به قضیه‌ای درباره وزن پیمانهای در کدهای AN دوری داریم.

قضیه ۱.۱۲.۳. فرض کنید  $C \subset \mathbb{Z}/(r^n - 1)$  یک کد AN دوری با مولد  $A$  باشد و فرض کنید:

$$B := (r^n - 1)/A = |c|.$$

در این صورت:

$$\sum_{x \in C} w_m(x) = n \left( \left\lfloor \frac{rB}{r+1} \right\rfloor - \left\lfloor \frac{B}{r+1} \right\rfloor \right).$$

اثبات. فرض کنیم که هر  $x \in C$  شامل یک CNAF یکنای زیر باشد:

$$x \equiv \sum_{i=0}^{\infty} c_{i,x} r^i \pmod{r^n - 1}.$$

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 در نظر می‌گیریم، تعیین کنیم؛ جایی که در آن  $0 \leq i \leq n-1$  و  $x \in C$ . چون  $C$  دوری است هر ستون این ماتریس شامل تعداد یکسانی صفر است؛ بنابراین، تعداد تعیین‌شده، مساوی با  $n |\{x \in C | c_{n-1,x} \neq 0\}|$  است. با استفاده از قضیه ۹.۱۲.۲ داریم  $c_{n-1,x} \neq 0$ ، اگر و تنها اگر وجود داشته باشد یک  $y \in \mathbb{Z}$  به‌طوری که  $y \equiv x \pmod{r^n - 1}$  و  $m/(r+1) < y \leq mr/(r+1)$ . چون  $x$  دارای شکل AN (در پیمان  $r^n - 1$ )  $(0 \leq N < B)$  است، باید داشته باشیم  $B/(r+1) < N \leq Br/(r+1)$ .

عبارت موجود در قضیه ۱.۱۲.۳ تقریباً برابر با  $n|c|[(r-1)/(r+1)]$  است؛ بنابراین، این قضیه با نتیجه اخیرمان:

$$\sum_{x \in C} w(x) = n|c| \frac{q-1}{q},$$

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.

<sup>۱۱</sup>J. T. Barrows

<sup>۱۲</sup>D. Mandelbaum

قضیه ۲.۱۲.۳. فرض کنید  $B$  یک عدد اول باشد که بر  $r$  بخش پذیر نیست با این خاصیت که  $(\mathbb{Z}/B\mathbb{Z})$  توسط عناصر  $r$  و  $-1$  تولید شده است. فرض کنید  $n$  یک عدد صحیح مثبت با خاصیت  $r^n \equiv 1 \pmod{B}$  باشد و  $A := (r^n - 1)/B$ ؛ در این صورت کد  $C \subset \mathbb{Z}/(r^n - 1)$  تولید شده توسط  $A$  یک کد هم‌ارز با فاصله زیر است:

$$\frac{n}{(B-1)} (\lfloor \frac{rB}{r+1} \rfloor - \lfloor \frac{B}{r+1} \rfloor).$$

اثبات. فرض کنید  $x \in C$ ،  $x \neq 0$ ؛ در این صورت  $x = AN \pmod{r^n - 1}$ ، به طوری که  $N \not\equiv 0 \pmod{B}$ . فرض‌های ما ایجاب می‌کند که یک  $j$  به طوری که  $N \not\equiv \pm r^j \pmod{B}$  وجود دارد؛ بنابراین، وزن  $w_m(x) = w_m(\pm r^j A) = w_m(A)$  این مطلب نشان می‌دهد که  $C$  هم‌فاصله<sup>۱۳</sup> است؛ بنابراین، وزن ثابت، از قضیه ۱.۱۲.۳ نتیجه می‌شود.  $\square$

کدهای مندلبوم-باروس متناظر با کدهای دوری مینیمال  $M_i^-$  از بخش ۶.۲ هستند. توجه دارید که این کدها دارای طول کلمه حداقل  $\frac{1}{4}(B-1)$  هستند که این مقدار نسبت به تعداد کدکلمات که همان  $B$  است، بزرگ است؛ بنابراین، برای اهداف عملی، این کدها به نظر مهم نمی‌رسند.

## ۱۲.۴ پیشنهادها

خواننده علاقه‌مند به جزییات بیشتر درباره کدهای حسابی به مرجع [۵۳] توسط پترسون<sup>۱۴</sup> و ولدون<sup>۱۵</sup> و مرجع [۴۸] توسط مسی<sup>۱۶</sup> و گارسیا<sup>۱۷</sup> و مرجع [۵۸] توسط راثو<sup>۱۸</sup> ارجاع داده می‌شود. کدهای AN دوری کامل تصحیح‌کننده یک خطا به طور وسیعی مورد مطالعه قرار گرفته‌اند. در این زمینه مرجع [۲۸] توسط گوتو<sup>۱۹</sup>، مرجع [۲۹] توسط گوتو و فاکومارا<sup>۲۰</sup> و مرجع [۳۱] توسط گریتسنکو<sup>۲۱</sup> را معرفی می‌کنیم. یک کد AN دوری کامل تصحیح‌کننده یک خطا با  $r = 10$  یا  $r = 2^k$  ( $k > 1$ ) وجود ندارد.

<sup>۱۳</sup>equidistance

<sup>۱۴</sup>W. W. Peterson

<sup>۱۵</sup>E. J. Weldon

<sup>۱۶</sup>J. L. Massey

<sup>۱۷</sup>O. N. Garcia

<sup>۱۸</sup>T. R. N. Rao

<sup>۱۹</sup>M. Goto

<sup>۲۰</sup>T. Fukumara

<sup>۲۱</sup>V. M. Gritsenko

برای دیدن جزئیات بیشتر درباره NAF و CNAF، خواننده را به مراجع [۱۴] و [۱۵] توسط کلارک<sup>۲۲</sup> و لیانگ<sup>۲۳</sup> 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 می‌توانند در مرجع [۱۲] توسط چن<sup>۲۴</sup>، چین<sup>۲۵</sup> و لیو<sup>۲۶</sup>، یافت شوند.

برای یافتن اطلاعات بیشتر درباره کدهای حسابی کامل، خواننده را به کار مشترکی که عنوان آن توسط لنسترا<sup>۲۷</sup> در سمینار دلنگی-پیزت-پویتو<sup>۲۸</sup> (نظریه اعداد<sup>۲۹</sup>، ۱۹۷۷/۷۸) مطرح شده، ارجاع می‌دهیم.

## ۱۲.۵ مسائل

۱.۱۲.۵. ثابت کنید  $2 \leq \min\{w(AN) \mid N \in \mathbb{Z}, N \neq 0\}$  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 پیمانانه  $1 - 3^6$  را در نظر 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.

<sup>۲۲</sup>W. E. Clark

<sup>۲۳</sup>J. J. Liang

<sup>۲۴</sup>C. L. Chen

<sup>۲۵</sup>R. T. Chien

<sup>۲۶</sup>C. K. Liu

<sup>۲۷</sup>H. W. Lenstra

<sup>۲۸</sup>Séminaire Delange-Pisot-Poitou

<sup>۲۹</sup>Théorie des Nombres

## فصل ۱۳

# کدهای کانولوشن

### ۱۳.۱ مقدمه

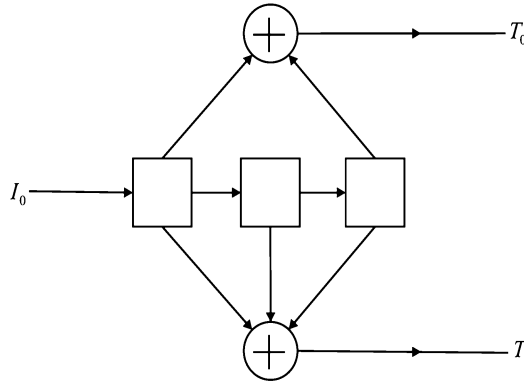
کدهایی که در این فصل در نظر می‌گیریم کاملاً با کدهایی که در فصل‌های قبل مطالعه کردیم، متفاوت هستند. آنها کدهای بلوکی نیستند، به این معنی که کلمات، طول ثابتی ندارند. اگرچه این کدها شباهت‌ها و ارتباط‌هایی با کدهای بلوکی دارند، اما یک تفاوت بزرگ بین آنها وجود دارد، به این معنا که تئوری ریاضی کدهای کانولوشن به خوبی توسعه نیافته است. این یکی از دلایلی است که ریاضی‌دانان به سختی به این کدها علاقه‌مند می‌شوند.

به هر حال، ما در مقدمه خود، مخبره اطلاعات توسط ماهواره‌ها را به عنوان یکی از مثال‌های بسیار موثر از کاربرد نظریه کدگذاری معرفی کردیم که در حال حاضر یکی از مهم‌ترین ابزارهای که در این زمینه استفاده می‌شود، کدگذاری کانولوشن است. بنابراین، یک مقدمه کوتاه در مورد این موضوع، مناسب به نظر 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  $\mathbb{F}_q$  سراسر است می‌باشد. به نظر می‌رسد هر مقدمه درباره کدگذاری کانولوشن، مثال یکسانی را به کار 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 به کار خواهیم برد.

در شکل ۱۳.۱، ابزار کدگذاری برای کدهای خود را تشریح می‌کنیم. سه مربع موجود در شکل، سلول‌های ذخیره‌ای<sup>۱</sup> (مدار دوضربه‌ای<sup>۲</sup>) 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).



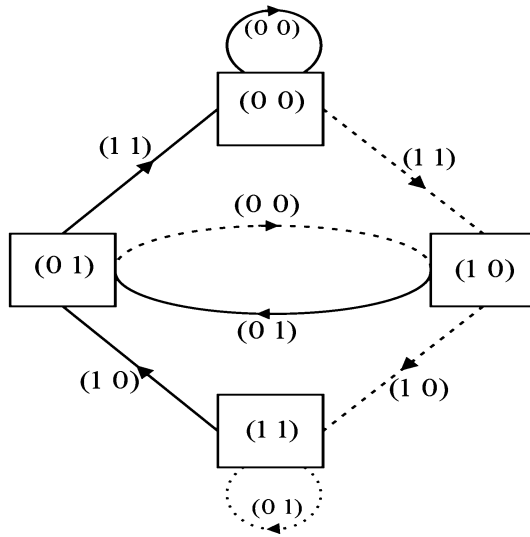
شکل ۱۳.۱:

اثر این سیگنال این است که محتویات مدارهای دوضربه‌ای در جهت پیکان‌ها به سوی عناصر بعدی حرکت می‌کند که آن در اصطلاح رجیستر تغییر مکان<sup>۳</sup> 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 به صورت 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 به کار می‌رود. عناصر دوم و سوم رجیستر تغییر مکان، 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 در دسترس می‌باشند. خروجی، به این سه سبیل ورودی بستگی دارد. در عمل، جریان‌های خروجی  $T_0$  و  $T_1$ ، برای تولید یک جریان خروجی، درهم آمیخته می‌شوند؛ بنابراین، اگر ما با حالت  $(0, 0, 0)$  در رجیستر شروع کنیم و یک جریان پیام شامل ۱ همراه با صفرها داشته باشیم، خواهیم دید که رجیستر در ابتدا به حالت  $(1, 0, 0)$  تغییر می‌یابد و خروجی  $(1, 1)$  را به وجود می‌آورد؛ سپس با خروجی  $(0, 1)$  به حالت

<sup>۱</sup> storage elements

<sup>۲</sup> flip-flops

<sup>۳</sup> shift register



شکل ۱۳.۲:

$(0, 1, 0)$  تغییر حالت می‌دهد؛ در ادامه به حالت  $(0, 0, 1)$  با خروجی  $(1, 1)$  و سپس به حالت اولیه و رشته‌ای از صفرها باز می‌گردد.

یک روش موثر برای توصیف طرز کار این کدگذار از طریق نمودار حالت<sup>۴</sup>، شکل ۱۳.۲، داده شده است. در اینجا محتویات دومین و سومین مدارهای دوضربه‌ای، حالت رجیستر نامیده می‌شود. ما دو حالت را توسط یک یال توپر به هم وصل می‌کنیم، اگر رجیستر از یکی به سمت دیگری با یک ورودی صفر حرکت کند. به طور 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 به صورت زیر باشد:

جریان ورودی  $i_0, i_1, i_2, \dots$  توسط سری توانی  $I_0(x) := i_0 + i_1x + i_2x^2 + \dots$  با ضرایبی در  $\mathbb{F}_2$  توصیف می‌شود. به همین شکل خروجی‌ها را در  $T_0$  و  $T_1$  توسط سری‌های توانی  $T_0(x)$ ، به ترتیب  $T_1(x)$  توصیف می‌کنیم. زمان را طوری هماهنگ می‌کنیم که اولین ورودی متناظر با اولین خروجی باشد. پس واضح است که:

$$T_0(x) = (1 + x^2)I_0(x),$$

$$T_1(x) = (1 + x + x^2)I_0(x).$$

<sup>۴</sup> State diagram



پس از آن ارتباط داده‌های  $T_0$  و  $T_1$  به صورت 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

$$11 \ 01 \ 11 \ 00 \ 00 \ \dots,$$

را به دست می‌آوریم که در نتیجه:

$$G(x) := 1 + x + x^2 + x^4 + x^5 = (1 + (x^2)^2) + x(1 + (x^2) + (x^2)^2).$$

بنابراین، اگر تعریف کنیم  $I(x) := I_0(x^2)$ ، آن‌گاه:

$$T(x) = G(x)I(x). \quad (1)$$

بنابر دلایلی که واضح هستند، می‌گوییم نرخ این کد کانولوشن برابر با  $\frac{1}{4}$  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 تغییر مکان، شش تا از سمبل‌های دنباله منتقل شده را تحت تاثیر قرار می‌دهد. این عدد، طول محدود<sup>۵</sup> کد نامیده می‌شود. این طول محدود برابر با درجه  $G(x)$  به علاوه 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 این صورت است: طول رجیستر تغییر مکان 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، زمانی که  $i_v$  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<sup>۶</sup> 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  $T_0(x)$ ،  $T_1(x)$ ،  $\dots$ ،  $T_{n-1}(x)$  وجود

<sup>۵</sup> constraint length

<sup>۶</sup> 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  $G_i(x)$  به دست می‌آید. دنباله منتقل شده  $T(x)$  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 این صورت  $T(x) = G(x)I(x)$  واضح است که انتخاب چندجمله‌ای‌های  $G_i(x)$ ،  $i = 0, 1, \dots, n-1$ ، خوب یا بد بودن کد را تعیین می‌کند، هر چند در هر صورت آن را با معنا می‌دانیم. حال اجازه دهید موقعیتی را که به وضوح 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<sup>۷</sup> نامیده می‌شود. روشی آسان برای اجتناب از فاجعه آمیز شدن یک کد کانولوشن با نرخ  $\frac{1}{n}$ ، وجود دارد؛ یعنی با برقراری شرط زیر:

$$\gcd(G_0(x), G_1(x), \dots, G_{n-1}(x)) = 1.$$

قبلاً دیده شده است که این تساوی وجود چندجمله‌ای‌های  $a_i(x)$ ،  $i = 0, \dots, n-1$ ، 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 علاوه بر آن 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  $I_0(x), I_1(x), \dots, I_{k-1}(x)$  داریم. متناظر با این ورودی‌ها  $n$  جریان خروجی  $T_i(x)$ ،  $i = 0, \dots, n-1$ ، 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  $G_{ij}$ ،  $i = 0, \dots, k-1$ ،  $j = 0, \dots, n-1$ ، برای تبیین این موقعیت داریم. اما:

$$T_j(x) := \sum_{i=0}^{k-1} G_{ij}(x)I_i(x).$$

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

<sup>۷</sup> catastrophic code

بلوکی روی یک میدان به طور مناسب انتخاب شده تبدیل می کند.

فرض کنید  $\mathbb{F}$  میدان خارج قسمتی  $\mathbb{F}[x]$  باشد؛ یعنی میدان تمامی سری های لوران <sup>۸</sup> به صورت:

$$\sum_{i=r}^{n-1} a_i x^i, \quad (r \in \mathbb{Z}, a_i \in \mathbb{F}).$$

$k$  بیت ورودی به رجیسترهای تغییر مکان متفاوت در زمان  $t$  به عنوان برداری در  $\mathbb{F}^k$  در نظر گرفته می شوند. این بدان معناست که دنباله های ورودی به عنوان برداری در  $\mathbb{F}^k$  تفسیر می شوند (مانند بخش ۳، بردارها، بردارهای سطری هستند). حال  $kn$  چند جمله ای  $G_{ij}(x)$  را به عنوان درایه های یک ماتریس مولد  $G$  در نظر می گیریم. البته،  $n$  دنباله خروجی می توانند به عنوان عناصر  $\mathbb{F}^n$  دیده شوند. این مطلب به تعریف زیر منتهی می شود.

تعریف ۱.۱۳.۱. یک کد کانولوشن دودویی  $C$  با نرخ  $\frac{1}{n}$  زیر فضای  $k$ -بعدی از فضای  $\mathbb{F}^n$  است که شامل پایه ای متشکل از  $k$  بردار متعلق به  $\mathbb{F}[x]^n$  می باشد. این بردارهای پایه، سطرهای  $G$  هستند.

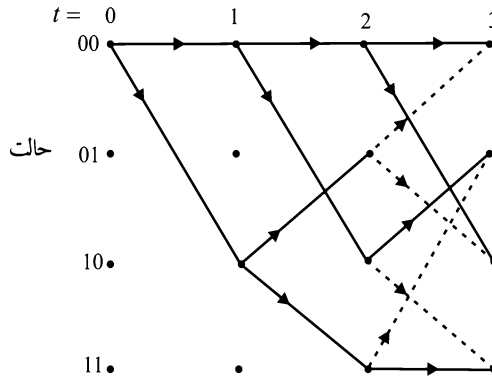
اگرچه این تعریف، برخی شباهت ها را با کدهای بلوکی نشان می دهد، دشواری آن را با به کارگیری  $\mathbb{F}$  مخفی می کنیم و علاوه بر این، محدود شدن روی عناصر  $G$  کاری کاملاً سخت گیرانه است. عملاً تمامی پیام ها متنهایی هستند و می توانیم فرض کنیم که در حالت  $t < 0$  در کار توقف وجود دارد. این بدان معناست که ما واقعاً به  $\mathbb{F}$  نیازی نداریم و هر کاری را می توانیم 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، انتخاب های متعددی از  $G$  وجود دارد که برخی از آنها ممکن است تحلیل  $C$  را آسان تر نماید. وضعیت یکسانی در مورد کدهای کانولوشن اتفاق می افتد. برای چنین عمل کردی از ماتریس مولد، خواننده را به مرجع [۲۳] ارجاع می دهیم. این یکی از اندک مثال های مربوط به تحلیل ریاضی کدهای کانولوشن است.

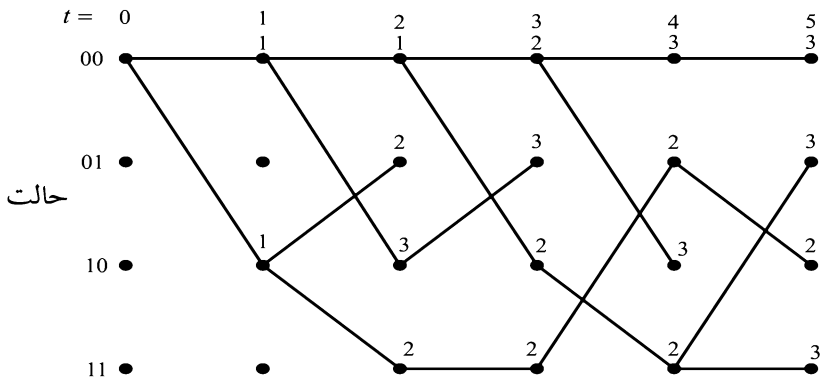
## ۱۳.۲ کدگشایی کدهای کانولوشن

چندین الگوریتم در عمل برای کدگشایی کدهای کانولوشن به کار رفته است. آنها کم و بیش شبیه به هم هستند و از نظر ریاضی زیاد عمیق نیستند. در واقع، 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

<sup>۸</sup> 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 معروف به الگوریتم ویتربی<sup>۹</sup> را با جزئیات بیشتر با به‌کارگیری مثال موجود در شکل‌های ۱۳.۱ و ۱۳.۲ مطرح می‌کنیم.

فرض کنید که پیام دریافتی به صورت ... ۰۰ ۱۰ ۰۱ ۰۰ ۱۰ باشد. نمودار شکل ۱۳.۳، حالت‌های ممکن در لحظه  $t = 0, 1, 2, 3$  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  $t = 3$  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 به معنی آن است که در لحظه  $t = 3$  دو خط رخ داده است. اگر از طرف دیگر، حالت ۰۰ از طریق ۱۰ و ۰۱ رخ دهد، خروجی ۱۱ ۰۱ ۱۱ به وجود می‌آید؛ بنابراین، در این لحظه سه خط وجود دارد. نمی‌دانیم که

<sup>۹</sup> Viterbi-algorithm

آیا رجیستر در حالت ۰۰ است یا نه و اگر این طور باشد، در این صورت مسیر افقی، مسیر محتمل تری برای رسیدن به آنجا است. به علاوه، این مسیر شامل دو خطاست. بیابید شکل ۱۳.۳ را به شکل ۱۳.۴ توسعه دهیم، که در آن  $t = 4$  و  $t = 5$  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 با احتمال یکسان برای رسیدن به یک حالت مشخص وجود داشته باشد، که در این صورت فرد باید یکی را انتخاب کند و دیگری را دور بیندازد. مطابق با هر زمان و هر حالت، فرد می‌تواند محتمل‌ترین خروجی‌ها را مطابق با آن فرض، گردآوری نماید؛ بنابراین، شکل ۱۳.۴ به لیست خروجی‌های زیر منتهی می‌شود:

	$t=1$	$t=2$	$t=3$	$t=4$	$t=5$
حالت ۰۰	۰۰	۰۰	۰۰	۰۰	۰۰
حالت ۰۱	۰۱	–	۱۱	۰۱	۰۰
حالت ۱۰	۱۰	۱۱	۰۰	۱۱	۰۰
حالت ۱۱	۱۱	–	۱۱	۱۰	۱۱

به وضوح در لحظه  $t = 5$ ، 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 به دست 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 بر روی تصمیمات کدگشایی بعدی و هم‌چنین فهمیدن عوامل موثر بر روی فاصله آزاد کد در تعیین صحت کدگشایی می‌باشد. برای تعیین جزئیات 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 در نظر بگیرید؛ یعنی آنهایی که به صورت زیر تعریف شده‌اند.  $k$  دنباله ورودی  $I_0(x), \dots, I_{k-1}(x)$  را در نظر گرفته و

$$I(x) := \sum_{i=0}^{k-1} I_i(x^n),$$

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 در نظر 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  $l + 1 = 1 + \deg(G(x))$  تعریف نموده و تنها کدهایی را در نظر می‌گیریم که  $l + 1 \leq mn$  و در آن  $m$  ثابت فرض شده است. ما علاقه‌مند به فاصله آزاد  $d_f$ ، برای چنین کدهایی هستیم. به‌وضوح  $d_f \leq l + 1$ . با شیفت دادن مقیاس زمان، می‌بینیم که در مطالعه روش کدگذاری، ممکن است محدودیت  $1 = t_0 = G(0) = 1$  را قرار دهیم. برای هر  $mn$ -تایی اولیه  $1 = t_0, t_1, \dots, t_{mn-1}$  از دنباله خروجی و هر  $mnk$ -تایی  $1 = i_0, i_1, \dots, i_{mnk-1}$  دقیقاً یک چندجمله‌ای  $G(x)$  از درجه کمتر یا مساوی  $mn$  وجود دارد، به طوری 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  $\sum_{i=0}^{d-2} \binom{mn-1}{i} 2^{mk-1}$  چندجمله‌ای با  $G(0) = 1$  را به‌عنوان مولد خارج می‌کنیم. بنابراین، یک انتخاب از  $G(x)$  وجود دارد که حداقل فاصله آزاد لازم را القا می‌کند، اگر:

$$2^{mk} \sum_{i=0}^d \binom{mn}{i} < 2^{mn}.$$

با در نظر گرفتن  $d = \lambda mn$  و نوشتن  $R := k/n$ ، از قضیه ۵.۱.۴ قسمت (۱)، با گرفتن لگاریتم داریم:

$$\frac{1}{mn} \log \sum_{i=0}^d \binom{mn}{i} < H(\lambda) < 1 - R,$$

اگر:

$$\lambda < H^{-1}(1 - R).$$

در اینجا  $\lambda$  خارج قسمت 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 برانگیز 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  $q = 2^r$ ،  $p(x) \in \mathbb{F}_q[x]$ ،  $c \in \mathbb{F}_q - \{0\}$ ،  $n \geq 0$  و  $N \geq 0$ ؛ در این صورت:

$$w(P(x)(x^n - c)^N) \geq w((x - c)^N) \cdot w(P(x) \bmod (x^n - c)).$$

اثبات.  $P(x)$  را به صورت  $\sum_{i=0}^{n-1} x^i Q_i(x^n)$  در نظر بگیرید؛ در این صورت با توجه به قضیه ۲.۴.۵ داریم:

$$\begin{aligned} w(P(x)(x^n - c)^N) &= \sum_{i=0}^{n-1} w(Q_i(x)(x - c)^N) \\ &\geq \sum_{i=0}^{n-1} w(Q_i(x))w((x - c)^N) \\ &= w((x - c)^N) \cdot w(\sum_{i=0}^{n-1} Q_i(c)x^i) \\ &= w((x - c)^N) \cdot w(P(x) \bmod (x^n - c)). \end{aligned}$$

□

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  $\mathbb{F}_q$  با کمترین فاصله  $d_q$  باشد و  $h(x)$  چندجمله‌ای بررسی توازن و  $d_h$  کمترین فاصله کد با چندجمله‌ای مولد  $h(x)$  باشد؛ در این صورت کد کانولوشن با نرخ  $1/(2m)$  روی میدان مشابه و با چندجمله‌ای مولد  $G(x) = g(x)$  فاجعه آمیز 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

$G_0(x), \dots, G_{2m-1}(x)$  از بخش ۱۳.۱ را در نظر بگیریم، در این صورت 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 فاجعه آمیز نمی‌باشد.

(۲) دنباله اطلاعاتی  $I_0(x)$  را در نظر بگیرید. داریم  $T(x) = G(x)(\hat{I}_0(x^m))^2$ ؛ بنابراین،  $T(x)$  به شکل زیر می‌باشد:

$$T(x) = P(x)(g(x))^{2i+1}(h(x))^{2j},$$

به طوری که  $i \geq 0, j \geq 0, P(x) \neq 0$  بر  $g(x)$  یا  $h(x)$  بخش‌پذیر نمی‌باشد. دو حالت را در نظر می‌گیریم:

الف) فرض کنید  $j \geq i$ ؛ در این صورت داریم:

$$T(x) = P(x)(g(x))^{2(i-j)+1}(x^n - 1)^{2j}.$$

و بنابراین ۱.۱۳.۴ داریم:

$$w(T(x)) \geq w((x-1)^{2j}) \cdot w(P(x)(g(x))^{2(i-j)+1} \bmod (x^n - 1)) \geq d_g.$$

زیرا عامل دوم بستگی به کدکلمه‌ای در کد دوری تولید شده توسط  $g(x)$  دارد.

ب) فرض کنید  $j < i$ ؛ در این صورت داریم:

$$T(x) = P(x)(h(x))^{2(j-i)-1}(x^n - 1)^{2i+1}.$$

و بنابراین ۱.۱۳.۴ داریم  $w(T(x)) \geq 2d_h$ ؛ زیرا:

$$w((x-1)^{2i+1}) \geq 2.$$

□

قبل از پرداختن به مثال‌های بیشتر درباره این بحث، کران بالایی را برای فاصله آزاد بیان می‌کنیم. یک کد کانولوشن با نرخ  $1/n$  روی  $\mathbb{F}_q$  با چند جمله‌ای مولد  $G(x) = \sum_{i=0}^{n-1} G_i(x^n)$  را در نظر بگیرید. فرض کنید:

$$L := n(1 + \max\{\deg(G_i(x)) \mid 0 \leq i \leq n-1\}).$$

(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  $1 + n - k \leq d$  برای کدهای بلوکی است. در اینجا ما ساختاری را بیان می‌کنیم که توسط جاستسن<sup>۱۰</sup> مرجع [۳۸] از کدهای کانولوشنی که به این کران دست می‌یابند، مطرح گردید. در ابتدا 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  $L \leq nq$ .

<sup>۱۰</sup>J. Justesen



اثبات. اگر  $d_f = L$ ، آن گاه هر یک از چندجمله‌ای‌های  $G_i(x)$  دارای وزن  $L/n$  می‌باشد. دنباله ورودی  $I_o(x) = 1 + \alpha x$  را در نظر می‌گیریم، که در آن  $\alpha$  متعلق به  $\mathbb{F}_q - \{0\}$  بوده و وزن متوسط  $\bar{\omega}$  از دنباله کدگذاری شده متناظر را تعیین می‌کند. داریم:

$$\begin{aligned}\bar{\omega} &= (q-1)^{-1} \sum_{\alpha \in \mathbb{F}_q - \{0\}} \sum_{i=0}^{n-1} w(G_i(x)(1 + \alpha x)) \\ &= (q-1)^{-1} n \{2(q-1) + (\frac{L}{n} - 1)(q-2)\}.\end{aligned}$$

چون  $\bar{\omega} \geq L$ ، باید داشته باشیم  $L \leq nq$ . □

با به کارگیری 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  $\alpha$  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 به هم اول می‌باشند. کد کانولوشن  $C$  با نرخ  $\frac{1}{4}$  روی  $\mathbb{F}_4$  با چندجمله‌ای مولد:

$$G(x) := g_1(x^2) + xg_2(x^2),$$

را در نظر بگیرید. این کد فاجعه آمیز نمی‌باشد. یک دنباله اطلاعاتی را به صورت  $I_o(x) = I'_o(x)(x^5 - 1)^N$  در نظر بگیرید، که در آن  $N$  ماکسیمال می‌باشد. با استفاده از لم ۱.۱۳.۴ داریم:

$$\begin{aligned}w(T(x)) &= w(g_1(x)I_o(x)) + w(g_2(x)I_o(x)) \\ &\geq w((x-1)^N) \cdot w(g_1(x)I'_o(x) \bmod (x^5 - 1)) \\ &\quad + w(g_2(x)I'_o(x) \bmod (x^5 - 1))\}.\end{aligned}$$

حال، اگر  $I'_o(x)$  مضربی از  $(x-1)g_1(x)$  یا  $(x-1)g_2(x)$  نباشد، آن گاه کران BCH نشان می‌دهد که هر دو جمله در عامل دوم در طرف راست بزرگ‌تر یا مساوی ۳ هستند. اگر از طرف دیگر  $I'_o(x)$  مضربی از  $(x-1)g_1(x)$  باشد، آن گاه هر دو جمله در طرف راست در خط بالا زوج می‌باشند (به خاطر عامل  $(x-1)$  و هر دو مثبت هستند. اگر دومی برابر با ۲ باشد، آن گاه 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 به منظور ساخت کدهای با نرخ  $\frac{1}{4}$  بر روی  $\mathbb{F}_q$  چندجمله‌ای‌های به شکل:

$$g_i(x) := (x - \alpha^m)(x - \alpha^{m+1}) \dots (x - \alpha^{m+d-2}),$$

را در نظر می‌گیریم، که در آن  $\alpha$  یک عضو اولیه از  $\mathbb{F}_q$  است.  $g_1(x)$  و  $g_2(x)$  را انتخاب می‌کنیم، به طوری که هر دو دارای درجه  $[\frac{1}{p}q]$  باشند و این که آنها دارای هیچ صفر مشترکی نمی‌باشند؛ در این صورت  $G(x) := g_1(x^2) + xg_2(x^2)$  یک کد کانولوشن  $C$  روی  $\mathbb{F}_q$  تولید می‌کند که فاصله آمیز نمی‌باشد. دو کد دوری با چند جمله‌ای‌های مولد  $g_1(x)$  و  $g_2(x)$  هر دو دارای کمترین-فاصله بزرگ‌تر یا مساوی  $d := [\frac{1}{p}q] + 1$  هستند. فرض کنید این کدها دارای چند جمله‌ای‌های بررسی توازن  $h_1(x)$  و  $h_2(x)$  هستند. یک دنباله اطلاعاتی  $I_0(x)$  برای  $C$  به صورت:

$$I_0(x) = (x^{q-1} - 1)^r (h_1(x))^s (h_2(x))^t p(x),$$

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:

$$\begin{aligned} w(T(x)) &= w(g_1(x)I_0(x)) + w(g_2(x)I_0(x)) \\ &\geq \sum_{i=1}^2 w((x-1)^r w(p(x)g_i(x) \bmod (x^{q-1} - 1))) \\ &\geq 2d. \end{aligned}$$

اگر  $s > 0$ ، آنگاه با روشی مشابه داریم:

$$\begin{aligned} w(T(x)) &= w((x^{q-1} - 1)^r (h_1(x))^s g_1(x)p(x)) + w((x^{q-1} - 1)^r (h_1(x))^s g_2(x)p(x)) \\ &\geq w((x-1)^{r+1} w(p(x)(h_1(x))^{s-1} \bmod (x^{q-1} - 1))) \\ &\quad + w((x-1)^r . w(p(x)(h_1(x))^s g_2(x) \bmod (x^{q-1} - 1))) \\ &\geq 2 + (q - [\frac{1}{p}q]) \geq 2 + 2[\frac{1}{p}q] = 2d. \end{aligned}$$

با توجه به این ساختار داریم  $L = 2(1 + [\frac{1}{p}q])$ ، 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 جزئیات 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 تعجب آور 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 جزئیات 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 این صورت او به کار پیرت<sup>۱۱</sup> (مراجع [۵۴] و [۵۵] را ببینید) ارجاع داده می‌شود. این کار توسط روس<sup>۱۲</sup> (ر.ک. مرجع [۵۹]) از نو طراحی شد. این ایده‌ها بر روی برخی کدهای نسبتاً خوب به کار گرفته شد و آنها به طور قطع در تحقیقات بعدی مفید خواهند بود.

یک کد کانولوشن را همانند آنچه در تعریف ۱.۱۳.۱ آمده در نظر می‌گیریم. چنین کدی را دوری می‌نامیم، اگر یک شیفت دوری هم‌زمان از ضرایب  $a_i$  از  $x^i$  ( $a_i \in \mathbb{F}_p^l$ )، کد مذکور را حفظ کند. در این حالت ما چیز جالبی به دست نمی‌آوریم. در واقع، به آسانی 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 به صورت زیر انجام می‌دهیم. فرض کنید  $K$  گروه جای‌گشت‌های روی  $\mathbb{F}_p^l$  باشد.  $K^{\mathbb{Z}}$ ، یعنی مجموعه تمامی توابع  $\varphi: \mathbb{Z} \rightarrow K$ ، را در نظر بگیرید که با تعریف  $\varphi_1 \varphi_2(n) := \varphi_1(n) \varphi_2(n)$  به یک گروه تبدیل کرده‌ایم.  $\varphi_n$  را به جای  $\varphi(n)$  خواهیم نوشت. دقت کنید که  $\varphi_n \in K$ ؛ در این صورت عملی از  $\varphi$  را روی عناصر  $\mathbb{F}_p^l$  به صورت:

$$\varphi\left(\sum_{i=r}^{\infty} a_i x^i\right) := \sum_{i=r}^{\infty} \varphi_i(a_i) x^i, \quad (2)$$

تعریف می‌کنیم.

تعریف ۱.۱۳.۵. اگر  $C$  یک کد کانولوشن باشد، آن‌گاه مجموعه تمام عناصر  $K^{\mathbb{Z}}$   $\varphi$ ، که در آن  $\varphi(C) = C$ ، گروه خودریختی  $C$  نامیده می‌شود.

از تعریف کدهای کانولوشن، این مطلب بدیهی است که کد  $C$  تحت حاصل ضرب در  $x$  پایاست؛ بنابراین، اگر  $\varphi$  یک خودریختی باشد، آن‌گاه  $\varphi^x := x^{-1} \varphi x$  نیز یک خودریختی است. علاوه بر این، این مطلب واضح است که اگر ما تنها عملی را در نظر بگیریم که روی یک مکان، ثابت باشد و آن را  $\varphi_i$  بنامیم، یک گروه جای‌گشتی روی  $\mathbb{F}_p^l$  به دست می‌آوریم که تصویر گروه خودریختی روی  $\mathbb{F}_p^l$  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 به نظر می‌آید. ما این مطلب را با به‌کارگیری تقریب جبری یکسان همانند آنچه در مورد کدهای بلوکی انجام دادیم،

<sup>۱۱</sup>Ph. Piret

<sup>۱۲</sup>C. Roos

انجام می‌دهیم. متغیر  $z$  را معرفی نموده و  $\mathbb{F}_q^{\mathbb{N}}$  را با  $\mathbb{F}_q[z]$  در پیمانه  $(z^n - 1)$  یکی می‌کنیم. فرض کنید  $\pi$  عدد صحیحی باشد، به طوری که  $(\pi, n) = 1$  و فرض کنید  $\sigma$  خودریختی  $\mathbb{F}_q^{\mathbb{N}}$  تعریف شده به صورت  $\sigma : f(Z) \rightarrow f(z^\pi)$  باشد. حال عناصر  $\mathbb{F}_q^{\mathbb{N}}$  می‌توانند به صورت  $\sum_{i=0}^{\infty} a_i x^i$  نوشته شوند، که در آن  $a_i = a_i(z)$  یک چندجمله‌ای با درجه کمتر از  $n$  است. در  $\mathbb{F}_q^{\mathbb{N}}$  جمع را به طور طبیعی و ضرب (نشان داده شده با  $*$ ) را به صورت زیر تعریف می‌کنیم:

$$\sum_i a_i x^i * \sum_j b_j x^j := \sum_i \sum_j \sigma^j(a_i) b_j x^{i+j}. \quad (3)$$

فرض کنید عامل سمت چپ برابر با  $z$  باشد؛ یعنی  $a_0 = z$ ،  $a_i = 0$  برای  $i \neq 0$ ؛ در این صورت از رابطه ۳ داریم:

$$z * \sum_j b_j x^j := \sum_j (z^{\pi^j} b_j) x^j. \quad (4)$$

این بدان معناست که ضرایب  $b_j$  از  $x^j$  به طور دوری روی مکان‌های  $\pi^j$  در پیمانه  $n$  شیف‌ت داده شده‌اند. نکته اصلی تعریف بالا این است که  $(\mathbb{F}_q^{\mathbb{N}}, +, *)$  یک جبر است که آن را با  $A(n, \pi)$  نشان می‌دهیم.

تعریف ۲.۱۳.۵. یک کد کانولوشن دوری (نماد CCC) یک ایده‌آل چپ در جبر  $A(n, \pi)$  است که پایه‌ای شامل چندجمله‌ای‌ها دارد.

در اینجا مشاهده می‌کنید که با استفاده از رابطه ۴، در واقع گروهی از خودریختی‌های  $\mathbb{F}_q^{\mathbb{N}}$  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  $\frac{4}{V}$  با حافظه یک توسط ماتریس  $G$  به صورت زیر داده شده است:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1+x & 1 & 1 & x & 1 & x & x \\ 0 & 1 & 1+x & 1 & x & 1+x & x \\ 0 & x & 1 & 1+x & 1+x & x & 1 \end{pmatrix}. \quad (5)$$

حال می‌خواهیم عناصر  $\mathbb{F}_q^{\mathbb{N}}$  با چندجمله‌ای‌هایی در  $\mathbb{F}_q[z]$  به پیمانه  $(z^V - 1)$  را مشخص نماییم. با نوشتن  $z^V - 1 = (1+z)(1+z+z^2)(1+z^2+z^3) = m_0(z)m_1(z)m_2(z)$  می‌توانیم  $G$  را به صورت زیر خلاصه نماییم:

$$G = \begin{pmatrix} m_1 m_2 \\ m_0 m_2 \\ z m_0 m_2 \\ z^2 m_0 m_2 \end{pmatrix} + \begin{pmatrix} 0 \\ m_0^2 m_1 \\ z^{-1} m_0^2 m_1 \\ z^{-2} m_0^2 m_1 \end{pmatrix} x. \quad (6)$$

ادعا می‌کنیم که  $G$  ماتریس مولد برای یک CCC در  $A(7, -1)$  است. چون  $\pi = -1$ ، با توجه به رابطه ۴ داریم:

$$z * \sum_i c_i x^i = \sum_i (z^{(-1)^i} c_i) x^i. \quad (7)$$

برای نشان دادن این که این کد یک CCC است، کافی است کلمات  $(1000)G$ ،  $(0100)G$ ،  $(0010)G$  را در نظر بگیریم. سپس آنها را از طرف چپ در  $z$  ضرب نموده و نشان دهیم که این حاصل ضرب، متعلق به کد می‌باشد. برای سه‌تای اول این مطلب با توجه به روابط ۶ و ۷ واضح است؛ برای مثال:

$$\begin{aligned} z * (0100)G &= z * (m_0 m_3 + m_0^3 m_1 x) \\ &= z m_0 m_3 + z^{-1} m_0^3 m_1 x = (0010)G. \end{aligned}$$

علاوه بر این:

$$\begin{aligned} z * (0001)G &= z * (z^2 m_0 m_3 + z^{-2} m_0^3 m_1 x) \\ &= z^3 m_0 m_3 + z^{-2} m_0^3 m_1 x \\ &= (1+z) m_0 m_3 + (1+z^6) m_0^3 m_1 x \\ &= (0110)G. \end{aligned}$$

نکته اصلی از قضیه پیرت آن است که یک CCC همیشه دارای یک ماتریس مولد با یک شکل "ساده" مشابه با رابطه ۶ است. این مطلب، امکان ساخت مثال‌هایی به نسبت آسان و مطالعه خواص آنها نظیر فاصله آزاد را ممکن می‌سازد.

## ۱۳.۶ پیشنهادها

کدهای کانولوشن توسط الیاس<sup>۱۳</sup> در سال ۱۹۹۵ (ر.ک. [۲۰]) معرفی شدند. بحث‌های نسبتاً زیادی در مورد این سوال که آیا کدهای کانولوشن "بهتر" از کدهای بلوکی هستند یا خیر، مطرح شد. به رقم کمبود یک دید ریاضی عمیق، کدهای کانولوشن در عمل به‌طور موفق به‌کار برده شدند. بسیاری از این کدها به آسانی به‌طور تصادفی انتخاب شده‌اند. برای ماموریت یکی از ماهواره‌ها در عمق فضا (ر.ک. [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

<sup>۱۳</sup>P. Elias

نموده و این بلوک‌ها را توسط کد گلی گسترش‌یافته [۱۲, ۲۴] 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<sup>۱۴</sup> و تیلبرگ<sup>۱۵</sup>، مرجع [۶۶]، 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<sup>۱۶</sup> (ارجاع به تعریف ۵.۳.۲) بود. ایده مشابهی به‌طور خیلی موفق برای کدهای کانولوشن به‌کار رفت. برای مشاهده جزئیات بیشتر درباره این ایده، خواننده را به مقاله‌ای از شالکویچ<sup>۱۷</sup> و پاست<sup>۱۸</sup>، مرجع [۶۵]، 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<sup>۱۹</sup>، 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 در نظر بگیریم که  $g(x) = G_0(x^2) + xG_1(x^2)$ ، آن‌گاه به واسطه رابطه ۱، تمامی دنباله‌های گذشته، 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 ۶ را تعیین کنید.

<sup>۱۴</sup>G. Solomon

<sup>۱۵</sup>H. C. A. Van Tilborg

<sup>۱۶</sup>syndrome

<sup>۱۷</sup>J. P. M. Schalkwijk

<sup>۱۸</sup>K. A. Post

<sup>۱۹</sup>Ph. Piret

# فصل ۱۴

## راهنمایی‌ها و حل مسائل

فصل ۲

۱.۲.۵

$$\begin{aligned} \sum_{0 \leq k < N/2} \binom{N}{k} q^k p^{n-k} &< (pq)^{N/2} \sum_{0 \leq k < N/2} \binom{N}{k} \\ &= 2^{N-1} (pq)^{N/2} < (0.07)^N. \end{aligned}$$

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 وجود دارد.  $(s_1, s_2, s_3)$  یک احتمال، به‌طور مثال  $(1, 1, 0)$  را در نظر بگیرید. این احتمال می‌تواند توسط الگوهای خطای  $(101011)$ ،  $(011101)$ ،  $(110000)$ ،  $(010011)$ ،  $(100101)$ ،  $(000110)$ ،  $(111110)$  و البته  $(001000)$  که محتمل‌ترین آنها می‌باشد، ایجاد شود. تصمیم ما این است که فرض کنیم  $e_3 = 1$ ؛ بنابراین، در اینجا دو سمبل اطلاعاتی درست با احتمال  $2p^4q^2 + p^2q^4$  و یک سمبل اطلاعاتی درست با احتمال  $2p^2q^2 + p^5q$  را به دست می‌آوریم.

با بررسی سایر حالات به روش مشابه، احتمال خطای سمبل را به صورت زیر داریم:

$$\begin{aligned} &\frac{1}{4}(22p^2q^4 + 36p^2q^2 + 24p^4q^2 + 12p^5q + 2p^6) \\ &= \frac{1}{4}(22p^2 - 52p^2 + 48p^4 - 16p^5). \end{aligned}$$

در مثال ما، این مقدار برابر با  $0.000007$  است که می‌توان آن را با مقدار  $0.001$  بدون کدگشایی مقایسه نمود.

۳.۲.۵. به عنوان کدکلمه، تمامی ۸-تایی‌ها به صورت زیر را در نظر 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 اضافه نمودن 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  $(e_1, e_2, \dots, e_7)$  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، به طوری که هر یک از آنان می‌توانند توسط ۳ الگوی متفاوت خطا با دو خطا تشریح شوند؛ به طور مثال  $(s_1, s_2, s_3, s_4) = (1, 1, 0, 0)$  متناظر با  $(e_1, e_2, \dots, e_7)$  که به صورت  $(0010001)$ ،  $(1100000)$  یا  $(0001100)$  است، می‌باشد. بیشترین توصیف محتمل برای  $(1, 1, 1, 0)$ ، وقوع سه خطا می‌باشد. بنابراین احتمال کدگشایی درست به صورت زیر است.

$$q^7 + 7q^6p + 7q^5p^2 + q^4p^3.$$

آن حدوداً برابر با  $1 - 14p^2$  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 پاک شده، نمی‌تواند ضرری برساند. در واقع، بررسی تمام الگوهای خطای ممکن با سه مکان پاک شده نشان می‌دهد که ۱۶ تا از اینها نیز ضرری نمی‌رسانند. این مطلب، به احتمال دریافت صحیح  $0.996 = (1 - p)^2(1 + 3p + 6p^2 + 6p^3)$  منجر می‌شود. این مقدار بهبود قابل ملاحظه‌ای با در نظر گرفتن این واقعیت است که دو کد بسیار مشابه هستند.



۵.۲.۵. با پاک شده، مانند صفرها برخورد کنید. حاصل ضرب‌های 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 به صورت ماتریس‌های ۴ در ۴ است. یک سطر و ستون را ثابت نگه دارید؛ ۱ها را در این سطر و ستون، مگر جایی که با یکدیگر تلافی کنند، مستقر کنید. در این روش، ما ۱۶ کلمه با وزن ۶ یافته‌ایم که در واقع هر دو تایی آنها دارای فاصله ۸ هستند.

۷.۲.۵. برای هر  $x$ ، حداکثر  $n/2$  کدکلمه وجود دارند، به طوری 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، به طوری که با  $x$  در دو مکان متفاوت هستند (زیرا  $n$  زوج است). برای هر کدکلمه  $c$ ، دقیقاً  $n$  کلمه وجود دارند، به طوری که با  $x$  در یک مکان متفاوت است و  $\binom{n}{2}$  کلمه وجود دارند، به طوری که در دو مکان متفاوت هستند.

زوج‌های  $(x, c)$  را به دور روش بشمارید، داریم:

$$|c| \cdot \binom{n}{2} \leq |c| \cdot n \cdot \frac{n-2}{2} + (2^n - |c| \cdot (n+1)) \cdot \frac{n}{2},$$

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  $\sum_{i=0}^2 \binom{n}{i} = 2^l$  برای برخی مقادیر صحیح  $l$ . این معادله به  $(n+1)(n^2 - n + 6) = 3 \cdot 2^{l+1}$ ، یعنی  $\{(n+1)\}^2 - 3(n+1) + 8 = 3 \cdot 2^{l+1}$ ، 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 ۲۳ یا ۱۱،  $n=7$ ، 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<sup>۱</sup> (کد MDS) نامیده می‌شود.

۳.۳.۸. چون  $C \subset C^\perp$ ، هر  $c \in C$  دارای این خاصیت است که  $\langle c, c \rangle = 0$ ، یعنی  $w(c)$  زوج است؛ بنابراین،  $\langle c, 1 \rangle = 0$  اما  $\langle 1, 1 \rangle = 1$ ، چون طول کلمه فرد است؛ بنابراین،  $C^\perp \setminus C$  با اضافه نمودن ۱ به تمامی کلمات  $C$  به دست آمده است.

۴.۳.۸. چون  $|B_1(x)| = 1 + 6 = 7$ ، ممکن است کسی فکر کند چنین کدی وجود دارد. اما، اگر چنین  $C$ ی 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 به طول 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 این رو 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، به طوری 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 اضافه نمودن سطر ۱ به ماتریس بررسی توازن  $C$  به دست 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  $(0, 0, 0)$ ،  $(0, 0, 1)$ ،  $(1, 0, 1)$  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  $p \equiv 1 \pmod{4}$ ، آنگاه یک  $\alpha \in \mathbb{F}_p$  وجود دارد، به طوری که  $\alpha^2 = -1$ ؛ در این صورت  $G = (I_4, \alpha I_4)$  یک ماتریس مولد از کد موردنظر است.

<sup>۱</sup> maximum distance separable code

(۲) اگر  $p \equiv 3 \pmod{4}$ ، آنگاه از این واقعیت استفاده می‌کنیم که تمامی عناصر  $\mathbb{F}_p$  مربعی نیستند؛ بنابراین، یک  $\alpha$  وجود دارد که مربعی است، گوئیم  $\alpha = \beta^2$ ، که در آن  $\alpha + 1$  مربعی نیست؛ یعنی

$$\alpha + 1 = -\gamma^2 \text{، لذا } \beta^2 + \gamma^2 = -1 \text{؛ پس:}$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \beta & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 & -\gamma & \beta & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \beta & \gamma \\ 0 & 0 & 0 & 1 & 0 & 0 & -\gamma & \beta \end{pmatrix},$$

این کار را انجام می‌دهد.

(۳) اگر  $p = 2$ ، آنگاه مثال ۳.۳.۳ را ببینید.

۹.۳.۸.

(۱) فرض کنید  $(\bar{A}_0, \bar{A}_1, \dots, \bar{A}_n, \bar{A}_{n+1})$  توزیع وزنی  $\bar{C}$  باشد؛ در این صورت  $\bar{A}_{2k} = 0$  و  $\bar{A}_{2k-1} = 0$ ، چون  $\sum A_{2k-1} z^{2k-1} = \frac{1}{2} \{A(z) - A(-z)\}$  و  $\sum A_{2k} z^{2k} = \frac{1}{2} \{A(z) + A(-z)\}$  داریم  $\bar{A}(z) = \frac{1}{2} \{(1+z)A(z) + (1-z)A(-z)\}$ .

(۲) از (۱) و رابطه (۲)، شمارنده وزنی کد گسترش یافته با طول  $n+1 = 2^k$  به صورت زیر می‌باشد:

$$\frac{1}{2} \left\{ \frac{(1+z)^{n+1} + (1-z)^{n+1}}{n+1} \right\} + \frac{n}{n+1} (1-z^2)^{(n+1)/2}.$$

حال قضیه ۲.۳.۵ را به کار می‌گیریم. شمارنده وزنی کد دوگان برابر با  $1 + 2nz^{(n+1)/2} + z^{n+1}$  است؛ یعنی تمامی کلمات این کد به جز  $0$  و  $1$  دارای وزن  $2^{k-1}$  هستند.

۱۱.۳.۸. این الگوی خطا، یک کد کلمه ناصفر  $c$  است. اگر  $w(c) = i$ ، آنگاه احتمال این الگوی خطا برابر با  $p^i(1-p)^{n-i}$  است؛ بنابراین، احتمال یک خطای تشخیص داده نشده برابر با  $\{(1-p)^n \{-1 + A(p/(1-p))\}\}$  است.

۱۲.۳.۸. فرض کنید  $G_i$  ( $i = 1, 2$ ) یک ماتریس مولد برای  $C_i$  در فرم استاندارد باشد. تعریف کنید  $A_{ij} \in \mathcal{R}$  ( $1 \leq j \leq k_2$ ,  $1 \leq i \leq k$ ) آن چنان که در ادامه می‌آید.  $k_1$  سطر اول  $A_{ij}$ ، جز سطر  $i$  که برابر با  $\delta_{ij}$  است، برابر با صفر هستند و به طور مشابه  $k_2$  ستون اول، جز ستون  $j$  که ترانهاده  $\delta_{ij}$  است، برابر با صفر هستند. به آسانی دیده می‌شود که این مطلب به طور یکتا یک عضو  $A_{ij}$  در  $\mathcal{R}$  را تعیین می‌کند.  $A_{ij}$ ها  $k_1 k_2$  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  $d_1$  است؛ یعنی شامل حداقل  $d_1$  ستون با وزن بزرگتر یا مساوی  $d_2$ ؛ بنابراین،  $C$  دارای کمترین فاصله بزرگتر یا مساوی  $d_1 d_2$  است. در واقع 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 همپینگ [۷، ۴] است که هم‌چنین کامل است؛ بنابراین، روش یکتایی در تصحیح حداکثر یک خطا روی هر یک از این دوزیرمجموعه 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 در نظر بگیرید. برای  $k = 1$ ، این ادعا درست است. فرض کنید  $A_k$  برای برخی مقادیر  $k$  درست باشد. کد کلمه  $c_{2^k}$  را در نظر بگیرید. لیست کلمات انتخاب‌شده شبیه زیر است:

$$A \begin{cases} c_0 & = 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & & \\ c_{2^{k-1}-1} & = * & * & 1 & 0 & 0 \\ B \begin{cases} c_{2^{k-1}} & = * & * & * & 1 & 1 \\ \vdots & & & & & \\ c_{2^k-1} & = * & * & * & 1 & 1 \end{cases} \end{cases}$$

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  $d(c_{2^k} + c_j, c_{2^k} + c_i) = d(c_{2^{k-1}} + x, c_{2^{k-1}} + c_i) = d(x, c_i)$  که در آن  $0 \leq i < 2^{k-1}$ ، نشان می‌دهد که ما باید  $x$  را به جای  $c_{2^{k-1}}$  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  $c_{2^k} + c_j = c_{2^k} + c_i$  برای  $0 \leq i < j$  (این مطلب برای  $i = 0$  درست است). داریم  $d(c_{2^k} + c_j, c_{2^k} + c_i) = d(c_i, c_j) \geq d$ . برای مقداری  $v$ ، این مطلب اثبات می‌کند که  $c_{2^k} + c_j$  یک انتخاب ممکن برای کد کلمه  $c_{2^k} + c_j = c_v$  است. این مطلب اثبات می‌کند که  $d(c_{2^k} + c_j, c_i) = d(c_{2^k}, c_i + c_j) \geq d$  چون با استفاده از فرض خطی بودن داریم  $c_i + c_j = c_v$ . برای مقادیر  $v$ ، این مطلب اثبات می‌کند که  $c_{2^k} + c_j$  یک انتخاب ممکن برای کد کلمه  $c_{2^k} + c_j = c_v$  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  $c_{2^k} + x < c_{2^k} + c_j$  (نماد  $<$  را برای ترتیب الفبایی به‌کار می‌بریم). با استفاده از فرض استقرای داریم  $c_j > x$ . این نامساوی ایجاب می‌کند  $x, c_j$  و  $c_{2^k}$  شبیه زیر باشند.

$$\begin{array}{l} c_j = * \quad * \quad 0 \quad a_1 a_2 \quad a_t \quad 0 \quad 0 \quad 0 \quad 0 \\ x = * \quad * \quad 1 \quad a_1 a_2 \quad a_t \quad 0 \quad 0 \quad 0 \quad 0 \\ c_{2^k} = * \quad * \quad 1 \quad ** \quad \quad \quad \quad \quad * \quad 1 \end{array}$$

فرض این که  $c_{2^k} + x$  یک انتخاب قابل قبول است، ایجاب می کند (مجدداً با به کارگیری خطی بودن) که:

$$d(c_{2^k} + x, c_j + c_i) \geq d, \quad 0 \leq i < 2^k \text{ برای}$$

یعنی:

$$d(c_{2^k} + x + c_j, c_i) \geq d, \quad 0 \leq i < 2^k \text{ برای.}$$

اما  $c_{2^k} + x + c_j < c_{2^k}$  یعنی این انتخاب  $c_{2^k}$  کمترین نبوده است که یک تناقض است. این مطلب، اثبات ادعای  $A_k$  را با توجه به استقرا کامل می کند.

(۲) حال، حالت  $d = 3$  را در نظر بگیرید. فرض کنید  $n_k$  طول کد پس از انتخاب  $2^k$  بردار باشد. اگر  $C_k$  کامل نباشد، آن گاه یک بردار  $x$  به طول  $n_k$  وجود دارد که دارای فاصله بزرگتر یا مساوی ۲ با هر کلمه از  $C_k$  است؛ بنابراین،  $(x, 1)$  یک انتخاب ممکن برای  $c_{2^k}$  است. این به ما  $n_{k+1} = n_k + 1$  را می دهد. اگر، از طرف دیگر،  $C_k$  کامل باشد، آن گاه واضح است که  $n_{k+1} = n_k + 2$  و  $(1, 1)$  و  $c_{2^k} = (1, 0, 0, \dots, 0, 1, 1)$  و  $k = 2^a - a - 1 + i$  برای  $n_k$  "طول ادعای  $B_\alpha =$  طول  $n_k$  برای  $1 \leq i < 2^a$  برابر با  $2^a + i$  است." با استفاده از استقرا در مشاهده فوق نتیجه می شود. در هر یک از دنباله های مذکور در  $B_\alpha$ ، کد نهایی یک کد همینگ است.

۱۵.۳.۸. اگر  $C$  یک کد  $[15, 8, 5]$  باشد، آن گاه  $C$  باید شامل یک کلمه به وزن ۵ باشد، زیرا در غیر این صورت می توانیم یک کد  $[14, 8, 5]$  را پنجر کنیم که نمی تواند وجود داشته باشد، زیرا  $2^8$  گوی با شعاع ۲ شامل نقاط بسیار زیادی است (قضیه ۹.۵.۲ را ببینید). چنین کلمه ای را به عنوان سطر اول ماتریس مولد در نظر بگیرید. روی مکان هایی که این سطر شامل صفر است، هفت سطر دیگر یک کد  $[10, 7]$  تولید می کنند که باید شامل کمترین فاصله ۳ باشد. مجدداً، این شرط گوی-پوششی را نقض می کند. (قسمت کدهای باقی مانده در بخش ۴.۴ را ببینید).

## فصل ۴

۱.۴.۸. با استفاده از تعریف ۶.۴.۵،  $\mathcal{R}(1, m)$  دارای بعد  $m + 1$  است؛ یعنی آن شامل  $2^{m+1}$  کلمه به طول  $n = 2^m$  است. با استفاده از قضیه ۹.۴.۵، هر یک از  $2(2^m - 1)$  ابرصفحه  $AG(m, 2)$  یک کد کلمه  $\mathcal{R}(1, m)$  را ایجاب می کند؛ یعنی جز برای  $0$  و  $1$ ، هر کد کلمه تابع مشخصه ای از یک ابرصفحه است. کد کلمه صفر و کد کلمات متناظر با ابرصفحه مار بر مبدا را در نظر بگیرید. در هر یک از این مختصات، سمبل صفر را با  $-1$  جایگزین کنید. چون دو ابرصفحه در  $2^{m-1}$  نقطه تلاقی دارند، این  $n$  بردار دوجه دو متعامد هستند.

۲.۴.۸. چون این کد کامل است، هر کلمه با وزن ۳ در  $\mathbb{F}_2^4$  دارای فاصله ۲ با یک کدکلمه به وزن ۵ است؛ بنابراین،  $A_5 = 2^3 \binom{4}{3} / \binom{5}{3} = 132$ . مجموعه ۵ تایی متناظر با  $x$  را با  $B(x)$  نشان دهید. فرض کنید  $x$  و  $y \notin \{x, 2x\}$ ، کدکلمای به وزن ۵ باشند، به طوری 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 این رو ۶۶ مجموعه  $B(x)$  به تعداد  $\binom{5}{4} = 5$  مجموعه ۴ تایی، یعنی تمام مجموعه‌های ۴ تایی 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  $(111, 111, 000, 000)$  و  $(111, 000, 111, 000)$  می‌باشند. در این صورت هر سطر دیگر  $A$  باید از سنخ  $(100, 110, 110, 100)$  یا  $(110, 100, 100, 110)$  باشد. ۶۶ کلمه  $x_i$  به ترتیب  $x_j + x_k$  را در نظر بگیرید. با استفاده از دو کاربرد شکل استاندارد فوق (برای هر سه تایی  $(x_i, x_j, x_k)$  داریم  $d(x_i, x_j + x_k) = w(x_i + x_j + x_k) = 4$  یا  $8$ ،  $d(x_i, x_i + x_k) = w(x_k) = 6$  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 بگیرید.

۵.۴.۸.

(۱) نشان دهید این زیرکد متناظر با زیرکد کد ۶ تایی تولیدشده توسط  $(1, \omega, 1, \omega, 1, \omega)$  است.

(۲) مانند اثبات برای  $G_{24}$ ، 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  $D$  به ترتیب دارای وزن‌های ۵، ۶، ۸ و ۹ هستند. برای دو کلمه  $a, b$  داریم  $d(a, b) = w(a) + w(b) - 2 \langle a, b \rangle$  که در آن  $\langle a, b \rangle$  در  $\mathbb{Z}$  محاسبه شده است. با استفاده از ضرب

بلوکی داریم:

$$AA^T = M(4I + J, 2J), \quad BB^T = M(3I + 3J, 3J - I),$$

$$AB^T = M(5J, 3J) - 2B^T, \quad \text{یک ماتریس با درایه‌های ۳ یا ۱}$$

نتیجه می‌شود که دو سطر  $A$ ، به ترتیب  $B$ ، دارای فاصله ۶ یا ۸ هستند و این که یک سطر از  $A$  و یک سطر از  $B$  دارای فاصله ۵ یا ۹ می‌باشند. به روش مشابه، این واقعیت که فاصله‌های باقی‌مانده حداقل برابر با ۵ هستند از روابط زیر نتیجه می‌شود:

$$CA^T = (4J - 2I, 4J - 2I, 4J - 2I, 4J - 2I),$$

$$CB^T = (4J, 4J, 4J, 4J),$$

$$DA^T = 3J + D, \quad DB^T = 3J + 2D,$$

$$CC^T = 4J + 4I, \quad DD^T = 3I + 6J, DC^T = 6J.$$

(این ساختار توسط ون‌لینت<sup>۲</sup> مرجع [۴۳] ارائه شد).

۸.۴.۸. از قضیه ۸.۱.۳ داریم  $A^T = -A$  و  $AA^T = 11I$ . چنین بر می‌آید که روی  $\mathbb{F}_3$  هر دو سطر  $G$  دارای ضرب داخلی صفر هستند؛ یعنی  $G$  یک کد خوددوگان [۲۴, ۱۲] تولید می‌کند؛ بنابراین،  $(A \ I)$  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  $12 = 11 + 1$  است و یک ترکیب خطی از دو سطر دارای وزن  $9 = 7 + 2$  است (این مطلب از  $AA^T = 11I$  نتیجه می‌شود)؛ بنابراین، یک ترکیب خطی از این سه سطر دارای وزن حداقل  $(11 - 7) + 3 = 7$  است و از این رو 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<sup>۳</sup> هستند. این کدها توسط پلس<sup>۴</sup> (۱۹۷۲) معرفی شدند. کلمات با وزن ثابت در چنین کدهایی اغلب،  $t$ -طرح‌ها (حتی با  $t = 5$ ) 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  $v_0, \dots, v_{m-1}$  بردارهای پایه از  $\mathcal{R}(1, m)$  باشند. پس از ۳.۴.۵ قسمت (۱) و (۲) می‌بینیم که  $1 = (1, 1)$ ،  $w_0 = (v_0, v_0)$ ،  $\dots$ ،  $w_{m-1} = (v_{m-1}, v_{m-1})$ ،  $w_m = (0, 1)$  بردارهای

<sup>۲</sup> J. H. van Lint

<sup>۳</sup> symmetry codes

<sup>۴</sup> V. Pless

پایه (با طول  $2^{m+1}$ ) از  $\mathcal{R}(1, m+1)$  هستند؛ بنابراین، یک بردار پایه  $(\nabla + \infty, \uparrow + \infty)$  به شکل  $w_{i_1} \cdots w_{i_s}$  از نوع  $(u, u)$  با  $u$  به عنوان یک بردار پایه از  $\mathcal{R}(r+1, m)$  است، اگر  $w_m$  در این حاصل ضرب رخ ندهد و آن از نوع  $(\circ, v)$  است، که در آن  $v$  یک بردار پایه از  $\mathcal{R}(r, m)$  باشد، اگر  $w_m$  در حاصل ضرب رخ دهد. اگر  $d(r, m)$  کمترین فاصله  $\mathcal{R}(r, m)$  باشد آن گاه از  $(u, u+v)$  ساختار می‌دانیم که

$$d(r+1, m+1) = \min\{2d(r+1, m), d(r, m)\}$$

۱۰.۴.۸

(۱) بردارهای  $x^*$  و  $c^* = \pm a_i$  را به عنوان بردارهایی در  $\mathbb{R}^n$  در نظر می‌گیریم. واضح است که  $\langle x^*, c^* \rangle = n - 2d(x, c)$  ممکن است فرض کنیم که  $a_i$ ها طوری انتخاب شده‌اند که  $\langle x^*, a_i \rangle$  مثبت است ( $1 \leq i \leq n$ ). بردارهای  $x^*$  و تمامی  $a_i$ ها دارای طول  $\sqrt{n}$  هستند؛ بنابراین،  $\sum_{i=1}^n \langle x^*, a_i \rangle^2 = n^2$ ، زیرا  $a_i$ ها دوه‌دو متعامد هستند. نتیجه می‌شود که یک  $i$  وجود دارد، به طوری که  $\langle x^*, a_i \rangle$  حداقل برابر با  $\sqrt{n}$  است.

(۲) حال فرض کنید  $m = 2k$  و  $c \in \mathcal{R}(1, m)$ . با استغاده از تعریف  $c$  لیست مقادیر یک تابع خطی روی  $\mathbb{F}_2^m$  است و بنابراین،  $d(x, c)$  تعداد نقاط متعلق به  $\mathbb{F}_2^m$  است، که در آن مجموع  $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$  و این تابع خطی مقدار ۱ را می‌گیرند. توجه داشته باشید که:

$$x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k} + x_1$$

$$x_1\bar{x}_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k},$$

که در آن  $\bar{x}_2 := x_2 + 1$ ؛ بنابراین، دنباله‌ای از تبدیلات مختصات  $\bar{x}_i := x_i + 1$  (برای  $\mathbb{F}_2^m$ ) این مجموع را به عبارتی هم‌ارز با  $x_1x_2 + \cdots + x_{2k-1}x_{2k}$  یا مکمل آن (رگر جمله ۱ در این تابع خطی رخ دهد) تغییر می‌دهد. نقاط  $x$ ی را می‌شماریم، که در آن  $x_1x_2 + \cdots + x_{2k-1}x_{2k} = 1$ . این تعداد را با  $n_k$  نشان دهید. به وضوح  $n_k = 2^{2k-2} - n_k$ ، که از آن داریم  $n_k = 2^{2k-1} - 2^{k-1}$ . این مقدار هم‌چنین می‌تواند با در نظر گرفتن بردار  $(x_1, x_2, \dots, x_{2k-1})$  محاسبه گردد. اگر این صفر نباشد، آن گاه  $2^{k-1}$  انتخاب برای  $(x_2, x_4, \dots, x_{2k})$  امکان‌پذیر است. از این رو  $n_k = (2^k - 1)2^{k-1}$ .

۱۱.۴.۸. از آنجا که کد همینگ سه‌تایی خوددوگان می‌باشد نتیجه می‌شود که  $C$  خوددوگان است؛  $J+I$  دارای رتبه ۴ است و از این رو  $C$  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 بررسی توازن 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  $i \leq d-2$ ، نیست، بیابیم. این روش تضمین می‌کند که هیچ  $(d-1)$ -تایی از ستون‌های ماتریس بررسی توازن وابسته خطی نباشند؛ یعنی این کد دارای کمترین فاصله حداقل  $d$  است. این روش کار می‌کند، اگر تعداد ترکیبات خطی حداکثر  $d-2$  ستون از  $m$  ستون انتخاب شده کمتر از  $q^{n-k}$  (برای هر  $m \leq n-1$ ) باشد. پس یک شرط کافی به صورت زیر است:

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}.$$

سمت چپ نامساوی موجود در قضیه ۶.۵.۱، حداقل  $n(q-1)/(d-1)$  برابر بزرگ است، سمت راست معده 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  $A(10, 5) = A(11, 6)$ . بهترین کران با استفاده از قضیه ۴.۵.۲ به دست می‌آید (نیز مثال پس از قضیه ۶.۵.۳ را ببینید). داریم  $A(11, 6) \leq 12$ . از رابطه ۲۰ (هم‌چنین جواب مساله ۳.۴.۸ را ببینید) یک کد  $(11, 12, 6)$  داریم؛ بنابراین،  $A(10, 5) = 12$ . ۳.۵.۵ تساوی در قضیه ۴.۵.۲ تنها زمانی می‌تواند برقرار باشد که برای نامساوی‌های به کار رفته در این اثبات نیز برقرار باشد و این نیز تنها زمانی ممکن است که  $M^2 \not\equiv 1 \pmod{q}$  یک عدد صحیح باشد؛ بنابراین،  $M = l$  غیرممکن است.

۴.۵.۵ با استفاده از مساله ۴.۴.۸ داریم  $A(17, 8) \geq 36$ . بهترین تخمین از بخش ۵.۲ با به کارگیری کران پلانکین به دست می‌آید. داریم  $A(17, 8) \leq 4A(15, 8) \leq 64$ . یک نتیجه بهتر با به کارگیری قضیه ۴.۵.۳ به دست می‌آید. خواننده می‌تواند بررسی کند که این نتیجه به صورت  $A(17, 8) \leq 50$  است. بهترین کران به دست آمده با تصحیح روش قضیه ۴.۵.۳ به صورت  $A(17, 8) \leq 37$  (ر.ک. مرجع [۶]) است.

۵.۵.۵ ستون‌های ماتریس مولد، نقاط  $(x_1, x_2, x_3, x_4, x_5)$  از  $PG(4, 2)$  است. می‌دانیم (ارجاع به مساله ۱۰.۳.۸) که تمامی کدکلمات ناصفر کد  $[31, 5]$  دارای وزن ۱۶ هستند. با به کارگیری نتیجه‌ای مشابه، مکان‌های متناظر با  $x_1 = x_2 = 0$ ، زیرکدی با طول ۷ شامل تمامی وزن‌های ناصفر برابر با ۴ است و مکان‌هایی که  $x_3 = x_4 = x_5 = 0$ ، زیرکدی با طول ۳ شامل تمامی وزن‌های ناصفر برابر با ۲ است.

اگر ما کد را در این ده مکان پنجر کنیم، آنگاه در کد [۲۱، ۵] باقی مانده داریم  $d = ۱۶ - ۴ - ۲ = ۱۰$ . از قضیه ۷.۵.۲ داریم  $n \geq ۱۰ + ۵ + ۳ + ۲ + ۱ = ۲۱$  یعنی کد پنجر شده 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  $|c| \cdot \binom{w}{2} / \binom{n}{2} = A(n-2, 2k, w-2)$  است و هیچ زوجی نمی‌تواند بیشتر از این تعداد رخ دهد).

۷.۵.۵. فرض کنید  $n = 2^k - 2$ . با استفاده از لم ۱۸.۵.۲ داریم  $A(n, 3, 3) \leq \frac{1}{3}n(n-2)$ . این رو قضیه ۱۹.۵.۲ ایجاب می‌کند:

$$A(n, 3) \leq 2^n / \left\{ 1 + n + \left( \binom{n}{2} - \frac{3n(n-2)}{6} \right) / \binom{n}{2} \right\} = 2^{n-k}.$$

بنابراین، کد همینگ کوتاه شده  $[n, n-k, 3]$  بهینه است.

۸.۵.۵. اگر دو کلمه  $c$  و  $c'$  با وزن  $w$  دارای فاصله ۲ باشند، گوئیم  $c'_j = c_k = 0$ ،  $c_j = c'_k = 1$ . آنگاه  $\sum_{i=0}^{n-1} ic_i - \sum_{i=0}^{n-1} ic'_i \equiv j - k \pmod{n}$ . نتیجه می‌شود که هر یک از کدهای  $C_l$  ( $0 \leq l \leq n-1$ ) دارای کمترین-فاصله ۴ است؛ بنابراین،  $A(n, 4, w) \geq 1/n \binom{n}{w}$ ، چون  $\sum_{l=0}^{n-1} |c_l| = \binom{n}{w}$ . با استفاده از لم ۱۸.۵.۲ داریم  $A(n, 4, w) \leq \binom{n}{w} / (n-w+1)$ . 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  $(n, M, 2k)$  دودویی باشد؛ تعریف کنید:

$$S := \{(c, x) | c \in C, x \in \mathbb{F}_2^n, d(x, c) = w\}.$$

به وضوح  $|S| = \binom{n}{w} M$ . برای یک  $x$  ثابت، حداکثر  $A(n, 2k, w)$  کلمه  $c$  در  $C$  وجود دارند، به طوری که  $d(x, c) = w$ ؛ بنابراین،  $\binom{n}{w} M \leq 2^n A(n, 2k, w)$ . 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:

$$2k \binom{M}{2} \leq \sum_{i=1}^n m_i (M - m_i) \leq M^2 w - n \left( \frac{Mw}{n} \right)^2.$$

(۲) فرض کنید  $2k/n \rightarrow \delta$  وقتی  $n \rightarrow \infty$ . فرض کنید  $w/n \rightarrow \omega$  وقتی  $n \rightarrow \infty$ . پس  $A(n, 2k, w)$  وقتی  $n \rightarrow \infty$  کراندار است و مساله ۹.۵.۵ ایجاب می‌کند  $\alpha(\delta) \leq 1 - H_2(\omega)$ . شرط  $1 - (w/k)(1 - (w/n)) > 0$  هنوز باید برقرار باشد؛ بنابراین، بهترین نتیجه حاصل می‌شود، اگر  $1 - (2\omega/\delta)(1 - \omega) = 0$ ، یعنی  $\omega = \frac{1}{2} - \frac{1}{2}\sqrt{1 - 2\delta}$  که قضیه ۱۶.۵.۲ است.

۱۱.۵.۵. داریم  $K_2(i) = 2i^2 - 2ni + \binom{n}{2}$  و این مقدار برای  $d \leq i \leq n - d$ ، کمتر از  $\binom{n}{2} - 2nd + 2d^2$  است. چون  $A_0 = A_n = 1$  (بدون کاستن از کلیت) و  $A_i = 0$  برای سایر مقادیر  $i$  خارج از  $[d, n - d]$ ، با توجه به لم ۳.۵.۳ داریم:

$$2 \binom{n}{2} + (2d^2 - 2nd + \binom{n}{2}) \sum_{i=d}^{n-d} A_i \geq 0.$$

این مطلب، نامساوی موردنیاز را ایجاب می‌کند.

۱۲.۵.۵. مساله تعیین  $A(9, 4)$  با قضیه ۴.۵.۳ را در نظر بگیرید. ما چهار نامساوی برای  $A_7, A_6, A_8$  و  $A_8$  یافتیم. ممکن است نامساوی بدیهی  $A_8 \leq 1$  به این دستگاه اضافه کنیم. یک محاسبه نسبتاً کسل‌کننده، جواب بهینه  $\frac{1}{4} \cdot 20$  را  $A_4 + A_7 + A_8 \leq 20$  را ایجاب می‌کند؛ بنابراین، ما باید احتمال یک کد  $(9, 21, 4)$  را محاسبه کنیم. در نظر گرفتن  $\omega = -1$  در اثبات لم ۳.۵.۳ نامساوی زیر را نتیجه می‌دهد:

$$21 \sum_{i=0}^9 A_i K_k(i) \geq \binom{9}{k},$$

یعنی با استفاده از:

$$K_k(0) = \binom{9}{k},$$

داریم:

$$\frac{20}{21} K_k(0) + \sum_{i=1}^9 A_i K_k(i) \geq 0.$$

چون این کد دارای ۲۱ کلمه است، حداکثر ۱۰ زوج کدکلمه با فاصله ۸ وجود دارند؛ یعنی  $A_8 \leq \frac{20}{21}$ ؛ بنابراین، مقادیر  $A_i$  باید در نامساوی مشابهی که ما آن را برای شروع حل کردیم، صدق کند. این مطلب ایجاب می‌کند  $20 < \frac{20}{21} \cdot \frac{71}{3} \leq A_4 + A_7 + A_8$  که یک تناقض است.

## فصل ۶

۱.۶.۱۳. ما بخش‌های ۶.۱ و ۶.۲ را گسترش می‌دهیم. روی  $\mathbb{F}_3$  داریم  $x^4 + 1 = (x^2 + 2x + 2)(x^2 + x + 2)$ ؛ بنابراین،  $x^2 + x + 2$  مولد یک کد نادوری  $[4, 2]$  با ماتریس مولد  $\begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix}$  است. با استفاده از تعریف ۱.۳.۳ این یک کد همینگ  $[4, 2]$  است.

۲.۶.۱۳. چون  $x^4 + x + 1$  اولیه است، می‌توانیم آن را به‌عنوان مولد کد همینگ  $[15, 11]$  در نظر بگیریم. حال روند اثبات قضیه ۱.۶.۴ را برای یافتن  $a(x)(x^4 + x + 1)$  پیروی کنید که ثابت می‌شود آن برابر با  $(x^{12} + x^9 + x^6 + x^3) + (x^8 + x^4 + x^2 + x) + 1$ ، مجموعی از سه خودتوان متناظر با

هم مجموعه‌های دوری، است. روش توصیف شده پس از قضیه ۴.۶.۴ پ مثال داده شده در آنجا، یک جواب دوم تهیه می‌کند.

۳.۶.۱۳. ماتریس  $E$  معرفی شده در بخش ۴.۵ را در نظر بگیرید و اولین ستون آن را حذف کنید. حال یک لیست از نقاط مخالف با  $(0, 0, \dots, 0)$  در  $AG(m, 2)$  داریم که به صورت بردارهای ستونی نوشته شده‌اند. نیز می‌توانیم این را به صورت لیستی از عناصر  $\mathbb{F}_m^*$  در نظر بگیریم. این یک گروه دوری تولید شده توسط یک عضو اولیه  $\xi$  از  $\mathbb{F}_m$  است. نگاشت  $A: \mathbb{F}_m \rightarrow \mathbb{F}_m$  تعریف شده به صورت  $A(x) := \xi x$  به وضوح یک تبدیل خطی نامنفرد از  $AG(m, 2)$  به خودش است و به عنوان جای‌گشتی از نقاط  $AG(m, 2) \setminus \{0\}$  دارای مرتبه  $m - 1$  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 کوتاه شده ایجاد می‌کند.

۴.۶.۱۳.  $x^2 + 2x + 1$  را برای تولید  $\mathbb{F}_4$  به کار برید. اگر  $\beta$  یک عضو اولیه باشد، آن‌گاه  $x^2 + 2x + 1$  چندجمله‌ای مینیمال آن است. با استفاده از جدول میدان متناظر آن، چندجمله‌ای مینیمال  $\beta^2$  را می‌یابیم که به صورت  $(x - \beta^2)(x - \beta^4)(x - \beta^8) = x^2 + x^2 + x + 2$  است و چندجمله‌ای مینیمال  $\beta^4$  به صورت  $(x^2 + x^2 + 2)$  است. حاصل ضرب این توابع شامل ریشه‌های  $\beta, \beta^2, \beta^3$  و  $\beta^4$  است؛ بنابراین، این کد مطلوب را ایجاد می‌کند. چندجمله‌ای مولد به صورت زیر است:

$$1 + x + 2x^2 + 2x^3 + 2x^4 + x^5 + x^6 + x^7 + 2x^8 + x^9.$$

بعد کد برابر با ۱۷ است.

۵.۶.۱۳. در ابتدا، جدولی از  $\mathbb{F}_{25}$  بسازید. با جای‌گذاری داریم  $E(\alpha^i) = R(\alpha^i)$  برای  $i = 1, 2, 3, 4$ . اینها به ترتیب  $\alpha^{28}, \alpha^{25}, \alpha^{19}$  و  $\alpha^{19}$  هستند. ما باید  $\sigma(z) = 1 + \sigma_1 z + \sigma_2 z^2$  را از معادلات  $1 + \sigma_1 \alpha^{25} + \sigma_2 \alpha^{28} = 0$  و  $\alpha^{19} + \sigma_1 + \sigma_2 \alpha^{25} = 0$  داریم  $\sigma_1 = \alpha^{28}$  و  $\sigma_2 = \alpha^{19}$ ؛ یعنی:

$$\sigma(z) = (1 - \alpha^{19} z)(1 - \alpha^{28} z).$$

بنابراین، این کد کلمه برابر است با:

$$(1001011011110010110101010110111).$$

مولد این کد برابر با  $(1 + x^2 + x^5)(1 + x^2 + x^3 + x^4 + x^5)$  است؛ یعنی:

$$g(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10}.$$

کدکلمه مذکور به صورت زیر است:

$$g(x)(1 + x^{11} + x^{20}).$$

۶.۶.۱۳. چون مجموعه تعریف  $C$  شامل  $\{\beta^j \mid j = -2, -1, 1, 2\}$  است، از مثال ۱۲.۶.۶ (با  $d_A = 3$  و  $|B| = 2$ ) نتیجه می‌شود که  $d \geq 4$ . زیرکد  $C'$  از  $C$  شامل کلمات زوج را در نظر بگیرید. کلمات این کد دارای ریشه‌های  $\beta^2, \beta^1, \beta^0, \beta^{-1}, \beta^{-2}$  هستند؛ بنابراین، با استفاده از کران BCH،  $C'$  دارای کمترین-فاصله حداقل ۶ است. نتیجه می‌شود  $d \geq 5$ .

۷.۶.۱۳. کد  $C'$  را که یک کد  $[q+1, 2, q]$  است، در نظر بگیرید. این کد روی هر دو مکانی متقارن است (ارجاع به مساله ۲.۳.۸). برای ضرایب شمارنده وزنی این مطلب ایجاب می‌کند که:

$$(q+1)A_{q+1} + aA_q = (q+1)(q^2 - q).$$

چون  $1 - q = A_{q+1} + A_q$  داریم  $A_{q+1} = 0$ ؛ یعنی هر کدکلمه ناصفر دارای وزن  $q$  است. کدکلمه یکتای  $c = (c_0, c_1, \dots, c_q)$  طوری که  $c_0 = c_{(q+1)/2} = 1$  وجود دارد. چون دقیقاً یکی از مختص‌های  $c$  برابر صفر است، یک شیفت دوری از  $c$  روی  $(q+1)/2$  مکان، کلمه مشابه  $c$  را القا نمی‌کند؛ بنابراین،  $C'$  دوری نمی‌باشد.

۸.۶.۱۳. روی  $\mathbb{F}_3$  داریم:

$$x^{11} - 1 = (x-1)(x^5 - x^3 + x^2 - x - 1)(x^5 + x^4 - x^3 + x^2 - 1),$$

که در آن این عوامل تحویل‌ناپذیر هستند؛ بنابراین، مشابه با تعریف ۱.۶.۹،  $g_0(x) = x^5 - x^3 + x^2 - x - 1$  را به عنوان مولد کد QR  $[11, 6]$  سه‌تایی  $C$  در نظر می‌گیریم. هم کران BCH و هم قضیه ۲.۶.۹ نتیجه می‌دهند  $d \geq 4$ ؛ در حالت آخر، محدودیت  $c(1) \neq 0$  وجود دارد. کد  $C^\perp$  دارای مولد  $(x-1)g_0(x)$  است (ارجاع به بخش ۶.۲). حال کد  $\bar{C}$  حاصل از اضافه‌نمودن یک بررسی‌توازن سراسری به روش معمول را در نظر بگیرید. اگر  $G$  یک ماتریس مولد برای  $C^\perp$  باشد، آنگاه یک ماتریس مولد برای  $C$  با اضافه‌نمودن سطر ۱ به دست می‌آید و یک ماتریس مولد برای  $\bar{C}$  به صورت زیر داده می‌شود:

$$\left( \begin{array}{c|c} G & \begin{matrix} \circ \\ \circ \\ \vdots \\ \circ \end{matrix} \\ \hline 1 & 1 \dots 1 \end{array} \right)$$

می‌بینیم که  $\bar{C}$  خوددوگان است. حاصل ضرب 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  $d \geq 5$ . این که  $C$  کامل است از تعریف و به‌کارگیری رابطه  $3^5 = 2^2 \binom{11}{2} + \binom{11}{1} + 1$  نتیجه می‌شود.

۱۳.۶.۹. با استفاده از نتیجه ۵.۶.۹ داریم  $d$  فرد است. با استفاده از قضیه ۲.۶.۹ قسمت (۲) و (۳) داریم  $d^2 - d + 1 \geq 47$  (یعنی  $d \geq 8$ ) و  $d \equiv 3 \pmod{4}$ ؛ بنابراین،  $d \geq 11$ . با استفاده از کران همینگ (قضیه ۹.۵.۲) برای  $d = 2e + 1$  داریم:

$$\sum_{i=0}^e \binom{47}{i} \leq 2^{47}/|C|.$$

چون  $C$  دارای بعد ۲۴ است، داریم  $e \leq 5$ . نتیجه می‌شود  $d = 11$ .

۱۳.۶.۱۰. در مثال بیان‌شده در بخش ۶.۹ و در مساله ۸.۶.۱۳ از قبل دیدیم که کد همینگ  $[7, 4]$  و دو کد گلی، نمونه‌هایی از کدهای QR کامل بودند. یک کد QR کامل دیگر نیز وجود دارد. این که برای  $e > 1$  کد دیگری وجود ندارد، نتیجه مستقیمی از نتیجه فصل ۷ است. فرض کنید  $C$  یک کد QR به طول  $n$  روی  $\mathbb{F}_q$  بوده و  $C$  یک کد کامل با  $d = 3$  باشد؛ در این صورت با استفاده از ۶.۳.۱ داریم:

$$1 + n(q-1) = q^{(n-1)/2}, \quad (q^{(n+1)/2} \text{ یا } q^{(n-1)/2})$$

دو حالت مشابه هستند. در اولی، داریم:

$$n = 1 + q + q^2 + \dots + q^{(n-3)/2}.$$

اگر  $n > 5$  آن‌گاه طرف راست حداقل برابر است با:

$$1 + 2 + \frac{n-5}{2} \cdot 4 = 2n - 7,$$

یعنی  $n = 7$  و  $q = 2$  و  $C$  کد همینگ  $[7, 4]$  است. آنچه باقی می‌ماند امتحان  $n = 3$  و  $n = 5$  است؛ داریم:

$$1 + 3(q-1) = q, \quad 1 + 5(q-1) = q^2.$$

بنابراین، تنها جواب برابر با  $n = 5$ ،  $q = 4$  است.

۱۳.۶.۱۱. فرض کنید  $\beta$  یک ریشه اولیه از  $\mathbb{F}_n$  باشد. تعریف کنید  $R_v := \{\beta^i \in \mathbb{F}_n \mid i \equiv v \pmod{e}\}$ ،

$0 \leq v < e$ . فرض کنید  $\alpha$  یک ریشه  $n$ ام اولیه واحد در یک توسیع میدان  $\mathbb{F}_q$  باشد. تعریف می‌کنیم:

$$g_v(x) := \prod_{r \in R_v} (x - \alpha^r), \quad 0 \leq v < e.$$

چون  $q \in R_0$ ، هر یک از  $g_v$ ها دارای ضرایبی در  $\mathbb{F}_q$  است. علاوه بر این، این چند جمله‌ای‌ها دارای درجه  $(n-1)/e$  است و

$$x^n - 1 = (x-1)g_0(x)g_1(x)\cdots g_{e-1}(x).$$

$e$  امین توان کد باقی مانده  $C$  دارای  $m$  لده  $g_0(x)$  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  $5^3 \equiv -1 \pmod{31}$ ، علاوه بر این توسط کران همینگ داریم  $d < 7$ . در واقع، حتی کران همینگ نشان می‌دهد که کد شامل  $2^2$  کلمه از  $C$  با وزن فرد نمی‌تواند دارای  $d = 7$  باشد. از این رو  $d = 5$ .

۱۲.۶.۱۳

(۱) چون  $\alpha, \alpha^2, \alpha^4, \alpha^5$  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  $0, i, j$  وجود خواهد داشت. فرض کنید  $\xi = \alpha^i, \eta = \alpha^j$ ؛ در این صورت  $1 + \xi + \eta = 0, 1 + \xi^2 + \eta^2 = 0$ . پس داریم  $1 = (\xi + \eta)^5 = (\xi^5 + \eta^5) + \xi\eta(\xi^2 + \eta^2)$ ؛ یعنی  $\xi^3 + \eta^3 = 0$ . این یک تناقض است، زیرا  $2^m - 1 \not\equiv 0 \pmod{3}$ ، بنابراین،  $x^3 = 1$  دارای جواب یکتای  $x = 1$  است، در حالی که  $\xi \neq \eta$ .

(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  $\xi, \xi + 1, \eta, \eta + 1$  است. مجموع توان‌های پنجم این عناصر برابر صفر است. این مطلب ایجاب می‌کند  $1 = (\xi + \eta)^3$ ، یعنی  $\xi + \eta = 1$  که یک تناقض است.

۱۲.۶.۱۳. نمایش مساله ۸.۶.۱۳ را در نظر بگیرید. فرض کنید  $\alpha$  یک عضو اولیه از  $\mathbb{F}_{35}$  باشد؛ در این صورت  $\alpha^{22}$  یک ریشه ۱۱ ام اولیه واحد است؛ یعنی یک ریشه از  $g_0(x)$  یا  $g_1(x)$ ؛ بنابراین، نمایش‌های  $1, \alpha^{22}, \alpha^{44}, \dots, \alpha^{220}$  به عنوان عناصر  $(\mathbb{F}_3)^5$ ، ستون‌هایی از یک ماتریس بررسی توازن  $C$  هستند. ستون‌های متناظر با  $\alpha^{22i}$  برای  $i > 5$  را در  $\alpha^{121} = 1 - \alpha$  ضرب کنید و آنها را نگه داشته تا مقادیر  $1, \alpha^{11}, \alpha^{22}, \dots, \alpha^{110}$  متناظر با یک ریشه  $1 + \alpha^{11}$  به دست آید. این کد هم‌ارز با  $C$  است که یکتایی آن شناخته شده است و این نمایش نادوری است.

۱۴.۶.۱۳. مجموعه تعریف این کد به صورت 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  $A = \{\alpha^i \mid i = 8, 9, 10\}$  و  $B = \{\beta^j \mid j = 0, 1, 3\}$ ،  $\beta = \alpha^10$ . این مطلب ایجاب می‌کند  $d \geq 6$ . برای زیرکد شامل وزن‌های زوج، در نظر بگیرید  $\beta = \alpha^8$ ،  $B = \{\beta^j \mid j = 0, 3, 4\}$ ،  $A = \{\alpha^i \mid i = 4, 7, 8, 9\}$  را برای  $|I| = 6$  به کار بگیرید.

## فصل ۷

۱.۷.۷. فرض کنید  $C$  کد مذکور باشد. چون کد همینگ با طول  $n + 1 = 2^m - 1$  برای  $n = 1$  کامل است،  $C$  دارای شعاع پوششی ۲ است.  $|c| = 2^{n-m}$ ،  $n = 2^m - 2$ ،  $e = 1$  را در رابطه ۳ جای‌گزین کنید. ما به تساوی دست می‌یابیم. نتیجه می‌شود که  $C$  تقریباً کامل است.

۲.۷.۷. فرض کنید  $\rho(u, C) = 2$ ، یعنی  $u = c + e$  که در آن  $c \in C$  و  $e$  دارای وزن ۲ است. چون  $c(\alpha) = c(\alpha^3) = 0$  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  $x_1, x_2, x_3$  محاسبه نموده و بدین گونه یک کدکلمه می‌یابیم؛ بنابراین، ما تعداد جواب‌های دستگاه زیر را محاسبه می‌کنیم:

$$x_1 + x_2 + x_3 + \alpha^i + \alpha^j = 0,$$

$$x_1^3 + x_2^3 + x_3^3 + \alpha^{3i} + \alpha^{3j} = 0.$$

$y_i := x_i + e(\alpha)$  را جای‌گزین می‌کنیم؛ داریم:

$$y_1 + y_2 + y_3 = 0,$$

$$y_1^3 + y_2^3 + y_3^3 = s := \alpha^{i+j}(\alpha^i + \alpha^j),$$

که در آن  $s \neq 0$  و  $y_k \notin \{\alpha^i, \alpha^j\}$ .

از معادله اول داریم  $y_3 = y_1 + y_2$  که ما آن را در معادله دوم جای‌گزین می‌کنیم. نتیجه برابر است با:

$$y_1 y_2 (y_1 + y_2) = s.$$

چون  $s \neq 0$  داریم  $y_2 \neq 0$ . تعریف کنید  $y := y_1 / y_2$ . این معادله به صورت زیر ساده می‌شود.

$$y(1 + y) = s / y_2^3.$$

چون  $(3, n) = (3, 2^{2m+1} - 1) = 1$  نتیجه می‌شود که برای هر مقدار  $y$ ، به جز  $y = 0$ ،  $y = 1$  این معادله دارای جواب یکتای  $y_2$  (در  $\mathbb{F}_{2^{2m+1}}$ ) است؛ بنابراین،  $n - 1$  جواب  $\{y_1, y_2\}$  را یافته و سپس  $y_3$  نتیجه می‌شود. به وضوح، هر سه تایی، شش‌بار یافت می‌شود. علاوه بر این، ما باید جواب  $y_1 = \alpha^i$ ،  $y_2 = \alpha^j$



را رد کنیم، زیرا اینها متناظر با  $x_1 = \alpha^j, x_2 = \alpha^i, x_3 = 0$  (یا هر جای گشت) می‌باشند؛ بنابراین،  $\rho(u, C) = 2$  نتیجه می‌دهد که  $\frac{1}{4}(n-1) - 1$  کدکلمه دارای فاصله ۳ با  $u$  هستند. به روش مشابه، می‌توان حالت  $\rho(u, C) > 2$  را بررسی نمود.

۳.۷.۷. کد  $C$ ، کد پریازاتا به طول 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 پنجر کنید تا کد  $C$  (۱۵، ۲۵۶، ۵) را به دست آورید. این پارامترها در رابطه ۳ صدق می‌کنند.

۴.۷.۷. این که  $C$  با یک کد خطی هم‌ارز نیست، به آسانی دیده می‌شود. اگر چنین بود، آن‌گاه  $C$  در واقع یک کد خطی می‌بود، زیرا  $C \in \mathbb{F}_2$ . پس مجموع دو کلمه از  $C$  مجدداً در  $C$  می‌باشد. این مطلب آشکارا درست نمی‌باشد. برای دیدن این که  $C$  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 در نظر بگیریم. اگر  $c = c'$  و  $x \neq y$ ، آن‌گاه واضح است که  $d(a, b) \geq 3$ . اگر  $c \neq c'$ ، آن‌گاه  $d(a, b) \geq w(x-y) + w(x+c-y-c') \geq w(c-c') \geq 3$  چون  $|c| = 2^{11}$  و  $d = 3$ ، تساوی را در شرط ۶.۳.۱ داریم؛ یعنی  $C$  کامل است.

۵.۷.۷. برای دوریشه  $\Psi_2$ ، از روابط ۲۰ و ۲۴ داریم:

$$x_1 + x_2 = n + 1 \quad \text{و} \quad x_1 x_2 = 2^{l-1}.$$

بنابراین،  $x_1 = 2^a, x_2 = 2^b$  (با توجه به شرط ۶.۳.۱ داریم  $2^c = 2^a + 2^b + 2 = n^2 + n + 2$  (که در آن  $c \geq 2$  چون  $n \geq 2$ )).

$$(2^a + 2^b)(2^a + 2^b - 1) + 2 = 2^c,$$

چون در طرف چپ معادله فوق، یک جمله ۲ داریم، جمله دیگر بر ۴ بخش پذیر نیست؛ بنابراین،  $a = 0$  یا  $a = 1$ . اگر  $a = 0$ ، آن‌گاه داریم  $2^c = 2^b(2^b + 1) + 2$ ، یعنی  $b = 1$  و  $n = 2$  متناظر با کد  $C = \{(00)\}$  است. اگر  $a = 1$ ، آن‌گاه داریم  $2^c = 2^2b + 3 \cdot 2^b + 4$ ، یعنی  $b = 2$  و از این رو  $n = 5$  متناظر با کد تکرار  $C = \{(00000), (11111)\}$  است.

۶.۷.۷. در ابتدا قضیه ۴.۷.۳ و رابطه ۱۱ را به کار برید. معادله زیر را داریم:

$$4x^2 - 4(n+1)x + (n^2 + n + 12) = 0,$$

با ریشه‌های  $x_{1,2} = \frac{1}{4}(n+1 \pm \sqrt{n-11})$ .

در نتیجه  $m^2 = n - 11$  برای برخی مقادیر صحیح  $m$ . از رابطه ۱۹ داریم:

$$12 \cdot 2^n = |c| \cdot (n^2 + n + 12) = |c|(n+1+m)(n+1-m).$$

بنابراین،  $n + 1 + m = a \cdot 2^{\alpha+1}$ ،  $n + 1 - m = b \cdot 2^{\beta+1}$  یا  $ab = 1$  در ابتدا قرار دهید  $a = b = 1$ . داریم  $n + 1 = 2^\alpha + 2^\beta$ ،  $m = 2^\alpha - 2^\beta$ ؛ از این‌رو:

$$2^\alpha + 2^\beta - 12 = 2^{2\alpha} - 2^{\alpha+\beta+1} + 2^{2\beta},$$

یعنی:

$$-12 = 2^\alpha(2^\alpha - 2^{\beta+1} - 1) + 2^\beta(2^\beta - 1),$$

یک تناقض آشکار است.

سپس قرار دهید  $b = 3$ . در نتیجه  $n + 1 = a \cdot 2^\alpha + 3 \cdot 2^\beta$ ،  $m = a \cdot 2^\alpha - 3 \cdot 2^\beta$ ؛ از این‌رو:

$$3 \cdot 2^\beta(3 \cdot 2^\beta - 2^{\alpha+1} - 1) + 2^\alpha(2^\alpha - 1) + 12 = 0.$$

اگر  $\alpha > 2$ ، آنگاه باید داشته باشید  $\beta = 2$  و در نتیجه  $\alpha = 4$ . چون  $\alpha \leq 2$  جواب نمی‌دهد و حالت آخر  $a = 3$  نیز چیزی را ایجاد نمی‌کند، ثابت کرده‌ایم که  $n + 1 = 2^4 + 3 \cdot 2^2$ ؛ یعنی  $n = 27$ . ساختار چنین کدی مشابه با مطلب موجود درباره یک کد RM پنچر شده (۲.۷.۴) است. فرم به کار رفته در ۲.۷.۴ را با  $x_1x_2 + x_3x_4 + x_5x_6 + x_5 + x_6 = 0$  جای‌گزین کنید. مابقی اثبات مشابه است. مایک کد دووزنی با طول ۲۷ با وزن‌های ۱۲ و ۱۶ یافته و سپس قضیه ۵.۷.۳ را به کار می‌گیریم.

۷.۷.۷

(۱) فرض کنید  $N$  تعداد زوج‌های  $(x, c)$  باشد، طوری که  $x \in \mathbb{F}_4^4$ ،  $c \in C$ ،  $d(x, c) = 2$ . با اولین انتخاب  $c$  داریم  $N = |c| \cdot \binom{4}{2}$ . برای هر  $x$  با شرط  $d(x, c) = 2$  حداکثر هفت کدکلمه ممکن وجود دارد که  $d(x, c) = 2$ ؛ از این‌رو:

$$N \leq (3^4 - |c|(1 + 2 \cdot 14)).$$

با مقایسه این نتایج، می‌بینیم که در دومی، باید تساوی برقرار باشد. هر  $x \in \mathbb{F}_4^4$  دارای فاصله حداکثر ۱ تا  $C$  یا فاصله ۲ تا دقیقاً هفت کدکلمه است.

(۲)  $\binom{4}{2}$  کلمه با وزن ۲ در  $\mathbb{F}_4^4$  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  $A_4 = 364$ .

(۳) با توجه به (۲) می‌بینیم که  $4A_4 = 1456$  کلمه با وزن ۳ دارای فاصله ۱ تا  $C$  هستند. زوج‌های  $(x, c)$  را، که در آن  $w(x) = 3$  و  $c \in C$ ،  $d(x, c) = 2$  می‌شماریم. آشکارا  $1456 - \binom{4}{2} \cdot 23 = 1456 - 182 = 1274$  کلمه با وزن ۳ وجود دارد.

انتخاب برای  $x$  وجود دارند. با شروع از کدکلمه  $c$  با وزن ۴، ۱۲ انتخاب برای  $x$  وجود دارد. اگر  $w(c) = 5$ ، آن گاه ۱۰ انتخاب برای  $x$  وجود دارد؛ بنابراین، داریم:

$$12A_4 + 10A_5 = 7.1456,$$

یعنی  $A_5 = 582\frac{2}{5}$  که بی معنی است.  $C$  وجود ندارد!

۸.۷.۷. در متریک لی، حجم گوی با شعاع ۱ برابر است با  $V_1 = 1 + 2n = m^2$ . کلمات متعلق به مجموعه  $\mathbb{Z}_m^n \setminus \{(0, 0)\}$  را به زوج‌های  $(x, -x)$  تفکیک نموده و یکی را به عنوان ستونی از یک ماتریس بررسی توازن  $H$ ، ۲ در  $n$ ، در نظر بگیرید. با تعمیم نظریه کدهای همینگ، کد خطی  $C$  را به صورت زیر تعریف کنید:

$$c \in C \Leftrightarrow cH^T = 0.$$

به وضوح  $C$  یک کد تصحیح کننده ۱ خطاست و  $C$  کامل است، زیرا  $|c| \cdot V_1 = m^n$ .

## فصل ۸

۱.۸.۵. در ابتدا توجه دارید که در یک کد چهارتایی خوددوگان به طول ۶، کلمات دارای مختصات فرد شامل چهارتا مختصات این چنینی هستند. چون این کد باید شامل ۴۳ کلمه باشد، ماتریس مولد در فرم ۱ دارای  $6 = 2k_1 + k_2$  است. به وضوح،  $k_1 = 3$  غیرممکن است.

برای  $k_1 = 0$  مثال بدیهی  $\mathbb{F}_2^6$  را داریم. شمارنده وزنی لی آن  $(x^2 + y^2)^6$  یکی از دو جواب مستقل برای معادله موجود در قضیه ۴.۳.۶ در حالت خوددوگانگی است. دیگری برابر با  $(x^4 - y^4)^2 x^2 y^2$  است (اینها به آسانی با استفاده از این واقعیت که تمامی وزن‌ها زوج هستند، یافت می‌شوند). تمامی ترکیبات خطی با جمله  $x^{12}$  نیز شامل جمله  $y^{12}$  هستند، بنابراین، این کد شامل  $(2, 2, 2, 2, 2, 2)$  است.

حال  $k_1 = k_2 = 2$  را امتحان می‌کنیم. سطرهای  $(A \ B)$  هر یک باید سه درایه فرد داشته باشند. به آسانی می‌توان مثالی یافت، به طور نمونه:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

شمارنده وزنی، جواب معادله موجود در قضیه ۴.۳.۶ است که شامل جمله  $x^{10}y^2$  نباشد؛ یعنی  $x^{12} + 15x^8y^4 + 32x^6y^6 + 15x^4y^8 + y^{12}$  دو سطر  $A$  می‌توانند رابطه‌ای غیرخطی ایجاد کنند، زیرا  $\sigma(1) + \sigma(1) \neq \sigma(2)$ . کدکلمه  $(002200)$  آن را جبران می‌کند. توجه دارید که تصاویر دودویی از دو بردار پایه اول، متعامد نمی‌باشند.

برای  $k_1 = 1$ ،  $k_2 = 4$ ، به آسانی 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  $(I_3 - 2J_3 - I_3)$  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 کد با مولد  $(I_7 - J_7 - I_7)$  است.

۲.۸.۵. فرض کنید بردارهای  $v_i$  ( $0 \leq i \leq m-2$ ) 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 ۱ یا  $\varepsilon_i = 0$ .

با استفاده از قضیه ۶.۸.۲ (و این واقعیت که  $\mathcal{R}(2, m)$  خطی است)، تنها باید بررسی کنیم که آیا حاصل ضرب مختصات وار 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. به آسانی دیده می‌شود  $a = n - i$ ،  $b = n - 2i + j$ .

۴.۸.۵. با به‌کارگیری لم ۲.۴.۶، کد نرداستروم-راینسن دارای شمارنده وزنی زیر است:

$$1 + 112z^6 + 30z^8 + 112z^{10} + z^{12}.$$

قضیه ۲.۳.۵ را به‌کار بگیرید. در اینجا، محاسبه کردن با فرم همگن آسان‌تر است.

۵.۸.۵. تعداد زوج‌های  $(x, c)$ ، که در آن  $c \in \mathcal{P}$  و  $w(x) = 2$  و  $d(x, c) = 3$ ، برابر با  $10A_5$  است. با

استفاده از ۱.۷.۳ آن هم‌چنین برابر با  $\binom{n}{2} \frac{n-2}{3} = \binom{n}{2} (r-1)$  است؛ از این‌رو:

$$A_5 = \frac{n(n-1)(n-3)}{6}.$$

$\binom{n}{2}$  کلمه با وزن ۳ وجود دارد. البته،  $10A_5$  دارای فاصله ۲ تا این کد و از این‌رو فاصله ۳ تا  $\frac{n-1}{3}$  کلمه با وزن ۶ است.  $10A_5 - \binom{n}{2}$  کلمه با وزن ۳ دارای فاصله ۳ تا  $\frac{n-2}{3} = r-1$  کلمه با وزن ۶ است. چون یک کلمه با وزن ۶ دارای فاصله ۳ تا  $20$  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-راینسن تحت فاصله پایاست؛ بنابراین، شمارنده وزنی مذکور دارای  $A_i = A_{16-i}$  است. می‌دانیم  $112 = A_6 = A_{10}$  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 پریاراتای توسیع‌یافته مشمول در کد همینگ توسیع‌یافته است؛ بنابراین، دارای فاصله ۴ است.

$GR(4^m)$  را در نظر بگیرید. می‌دانیم  $1 + \xi$  می‌تواند به صورت  $2\xi^j + \xi^i$  نوشته شود؛ بنابراین،  $C_m$  شامل کدکلمه  $a$  با مختص‌های  $1, 1, 1, 3, 2$  در مکان‌های متناظر با  $0, 1, \xi, \xi^2$  است. با یک شیفت دوری، یک کدکلمه مشابه  $b$  می‌یابیم با یک  $1$  در مکان  $0$  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  $m = 3$  کار نمی‌کند.

## فصل ۹

۱.۹.۸. در قضیه ۱.۹.۳، نشان داده شد که اگر ما  $g(z)$  را با  $z + 1$  جای‌گزین کنیم، آن‌گاه کد مشابهی به دست می‌آوریم؛ بنابراین،  $\Gamma(L, g)$  دارای بعد حداقل ۴ و کمترین-فاصله  $d \geq 3$  است. آن‌چنان که در قسمت اول بخش ۹.۳ نشان داده شده است،  $d$  ممکن است بزرگتر باشد. ماتریس بررسی توازن  $H = (h_0 \quad h_1 \quad \dots \quad h_{\nu})$  را که  $h_i$  متعلق به مجموعه مقادیر  $(\alpha^j + 1)^{-1}$  با شرط  $(j, 15) = 1$  است. می‌دانیم  $H$  شامل تمامی بردارهای ستونی با یک  $1$  در مکان آخر است؛ یعنی  $\Gamma(L, g)$  کد همینگ گسترش‌یافته  $[8, 4, 4]$  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  $X^{n-1} \circ A(X)$ ، یعنی  $X^{-1}A(X)$ ، بر  $g(X)$  بخش‌پذیر است. چون  $C$  دوری است، از رابطه ۲ می‌فهمیم که  $X^{-1}A(X)$  بر  $g(\alpha^i X)$ ، برای  $0 < i \leq n-1$ ، نیز بخش‌پذیر است. اگر  $g(X)$  دارای یک ریشه متفاوت با صفر در یک میدان گسترش‌یافته از  $\mathbb{F}_2$  باشد، آن‌گاه  $n-1$  ریشه متمایز از  $X^{-1}A(X)$  داریم که یک تناقض است، زیرا  $X^{-1}A(X)$  دارای درجه کمتر از  $n-1$  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  $(b_0, b_1, \dots, b_{n-1})$  داریم  $\sum_{i=0}^{n-1} b_i \gamma_i^r = 0$  برای  $0 \leq r \leq d_1 - 2$ ، که در آن  $\gamma_i = \alpha^i$  (یک عضو اولیه است)؛ بنابراین، کمترین-فاصله بزرگتر یا مساوی  $d_1 + d_2 - 1 = (d_1 - 2) + (d_2 - 1) + 2$  است. ۴.۹.۸. فرض کنید  $G^{-1}(X)$  معرف معکوس  $G(X)$  در حلقه  $(T, +, \circ)$  باشد. تعریف کد GBCH می‌تواند به صورت زیر خوانده شود:

$$P(X) \cdot (\Phi a)(X) = Q(X)G(X) + R(X)(X^n - 1),$$

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  $\deg Q(X) < n - t$  به دست می‌آید، اگر زوج  $(\hat{P}(X), X^t)$  را در نظر بگیریم، که در آن:

$$\hat{P}(X) = x^t \circ G^{-1}(X) \circ P(X).$$

جواب دوم: به منظور اطمینان از این که ما دارای کد مشابهی هستیم، برای آن می‌بینیم که ماتریس بررسی توازن یکسانی مشابه با بخش ۹.۶ به دست 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  $\hat{P}(X) = \Phi \hat{p}$ .

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  $x^2 + 1 \in C$ ، داریم  $d = 2$ . اگر در تعریف ۱.۹.۲،  $g(x)$  را با درجه بیشتر از ۱ در نظر 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  $(1 : 0 : 0)$ ،  $(y, z)$  را به صورت مختص‌های آفین در نظر می‌گیریم. معادله به صورت  $z = y^2$  می‌شود. بنابراین، می‌بینیم که  $y$  یک پارامتر موضعی است (و  $z$  نیست)؛ بنابراین، در  $(1 : 0 : 0)$ ،  $y/x$  را به صورت پارامتر موضعی در نظر می‌گیریم. چون  $x/z = (x/y)^2$ ، می‌بینیم که یک قطب مرتبه ۲ در  $(1 : 0 : 0)$  وجود دارد.

۲.۱۰.۹. اگر  $f$  و سه مشتق جزئی در  $(x : y : z)$  صفر باشند، آن‌گاه  $xyz \neq 0$  و سه معادله  $2x^2 = y^2 z$  و غیره را می‌یابیم. این سه به ما  $\lambda(xyz)^2 = (xyz)^2$  را می‌دهند، پس  $p = 7$ . ممکن است فرض کنیم  $x = 1$ ؛ در این صورت معادلات  $y^2 z = 2$  و  $y = 2z^2$  جواب  $y = 2$  و  $z = 4$  را می‌دهند. از این رو یک نقطه منفرد وجود دارد.

۳.۱۰.۹.  $X$  دارای پنج نقطه است:  $P = (0 : 0 : 1)$ ،  $Q = (1 : 0 : 0)$  و  $R_i = (\alpha^i : \alpha^{2i} : 1)$  ( $0 \leq i \leq 2$ ). به وضوح، هر نقطه  $R_i$  یک ریشه با تکرار ۱ است. در  $Q$ ،  $y/x$  را به صورت یک پارامتر موضعی داریم و

$$g = \left(\frac{y}{x}\right)^2 \frac{x^2 + y^2}{x^3},$$

از این رو  $Q$  یک ریشه با تکرار ۳ است. در  $P$ ، یک پارامتر موضعی،  $y/x$  است و

$$g = \left(\frac{z}{y}\right)^3 \frac{z^2 + y^2}{z^3},$$

بنابراین،  $P$  یک قطب مرتبه ۶ است. از این رو  $R_1 + R_2 + R_3 = -6P + 3Q$ .

۴.۱۰.۹. ما تنها مجبوریم نگاهی به این سه نقطه بیندازیم، که در آن دو مختصات صفر هستند،  $P = (0 : 0 : 1)$ ،  $Q = (1 : 0 : 0)$  و  $R = (0 : 1 : 0)$ . آسانترین همان  $Q$  است، که در آن  $z/x$  یک پارامتر موضعی است. از این رو  $Q$  یک قطب مرتبه ۱ است. در  $P$ ، پارامتر موضعی  $y/z$  و

$$\frac{x}{z} = \left(\frac{y}{z}\right)^4 \frac{z^4}{x^3 y + z^4},$$

را داریم، که در آن دومین عامل یک یکه است؛ بنابراین،  $P$  یک ریشه با تکرار ۴ است. در  $R$ ، یک پارامتر موضعی،  $x/y$  است. از

$$\frac{x}{z} = \left(\frac{y}{x}\right)^3 \frac{y^4 + z^2 x}{y^4},$$

می بینیم که  $R$  یک قطب مرتبه ۳ است؛ داریم:

$$(f) = 4P - Q - 3R.$$

۵.۱۰.۹. تنها مختصات نقاط  $P_1$  تا  $P_6$  را در سه پایه جایگزین کنید. نشان داده شده است که با ضرب سطرها و ستون‌های معین در مقادیر ثابت مناسب و یک جای‌گشت، دو ماتریس مولد متعلق به کدهای هم‌ارز هستند.

۶.۱۰.۹. چون  $g = 3$ ، از قضیه ۱.۱۰.۴ داریم  $l(3Q) \geq 1$ . از نتیجه ۳.۱۰.۴ نتیجه می‌شود که  $l(5Q) = 3$ . از مثال ۵.۱۰.۶ می‌بینیم که توابع ۱ و  $z/x$  در  $\mathcal{L}(3Q)$  هستند و نیز آنها یک پایه می‌باشند.

## فصل ۱۱

۱.۱۱.۴. کلمات  $C_\alpha$  دارای شکل  $(a(x), \alpha(x)a(x))$  هستند، که در آن  $a(x)$  و  $\alpha(x)$  چندجمله‌ای‌هایی در پیمانۀ  $1 + x^2 + x^6$  می‌باشند. برای رسیدن به  $d > 3$ ، باید آن  $\alpha(x)$ ‌هایی را که در آن یک ترکیب  $\alpha(x)a(x) = x^j + x^k$ ،  $a(x) = x^i$  و همچنین معکوس‌های این  $\alpha(x)$ ‌ها محتمل است، خارج کنیم. چون  $(1+x)^{-1} = 1 + x^{-1}(x+x^2) = 1 + x^{-1}(x+x^2) = 1 + x^{-1}(x+x^2)$ ، به آسانی دیده می‌شود که هر عضو ناصفر  $\mathbb{F}_{2^6}$  دارای یک نمایش یکتای  $x^i(1+x)^j$  است؛ که در آن:

$$i \in \{0, \pm 1, \pm 2, \pm 3, \pm 4\}, \quad j \in \{0, \pm 1, \pm 2, \pm 4\}.$$

بنابراین، شرط  $d > 2$ ، نه مقدار  $\alpha(x)$  را خارج می‌کند و شرط  $d > 3$ ،  $54$  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  $14.3.8$ ، یک کد  $[12, 7]$  گسترش‌یافته با کمترین ترتیب الفبایی با  $d = 4$  وجود دارد. در لم  $1.4.6$  دیدیم که یک کد غیرخطی با  $n = 12$ ،  $d = 4$  حتی با تعداد کلمات بیشتر وجود دارد.

$2.11.4$ . فرض کنید  $\alpha(x)$  یک چندجمله‌ای با وزن ۳ باشد؛ در این صورت در  $(a(x), \alpha(x)a(x))$  وزن‌های دو نیمه دارای توازن یکسان می‌باشد. از این رو تنها  $d < 4$  ممکن است، اگر یک انتخاب  $a(x) = x^i + x^j$  وجود داشته باشد طوری که  $\alpha(x)a(x) \equiv 0 \pmod{x^3 - 1}$ . این برقرار است، اگر  $\alpha(x)$  متناوب باشد؛ یعنی  $1 + x^2 + x^4$  یا  $x + x^3 + x^5$ . برای تمامی انتخاب‌های دیگر داریم  $d = 4$ .

$3.11.4$ . فرض کنید نرخ  $R$  در رابطه  $1/l < R \leq l/(l+1)$  ( $l \in \mathbb{N}$ ) صدق کند. فرض کنید  $s$  کمترین مقدار صحیح باشد که  $m/[(l+1)m - s] \geq R$ . کد  $C$  را با انتخاب  $l$ -تایی  $(\alpha_1, \alpha_2, \dots, \alpha_l) \in (\mathbb{F}_2^m)^l$  و سپس تشکیل  $(a, \alpha_1 a, \dots, \alpha_l a)$  برای تمامی  $a \in \mathbb{F}_2^m$  و سرانجام حذف  $s$  سمبل آخر می‌سازیم. طول کلمه کد برابر  $n = (l+1)m - s$  است.

یک کلمه ناصفر  $c \in C$  متناظر با  $2^s$  مقدار ممکن  $l$ -تایی  $(\alpha_1, \dots, \alpha_l)$  است. برای اطمینان از این که کمترین فاصله بزرگتر یا مساوی  $\lambda n$  است، باید حداکثر  $2^s \sum_{i < \lambda n} \binom{n}{i}$  مقدار  $(\alpha_1, \dots, \alpha_l)$  را خارج کنیم. خوشحال خواهیم شد، اگر این رابطه به ما یک انتخاب برای  $(\alpha_1, \dots, \alpha_l)$  بدهد؛ یعنی اگر:

$$2^s \sum_{i < \lambda n} \binom{n}{i} < 2^{ml}.$$

آنگاه از قضیه  $5.1.4$  داریم:

$$s + nH(\lambda) < ml,$$

یعنی:

$$H(\lambda) < \frac{ml - s}{n} = 1 - \frac{m}{n} = 1 - R + o(1), \quad (m \rightarrow \infty).$$

## فصل ۱۲

$1.12.5$ . دنباله  $er, er^2, er^3, \dots$  را در نظر بگیرید. دو عضو در این دنباله وجود دارد که در پیمانه  $A$  هم‌نهیست می‌باشند، گوئیم  $r^n - r^m \equiv 0 \pmod A$  ( $n > m$ ).

$2.12.5$ . فرض کنید  $AB = r^n - 1 = cm$  که در آن  $A$  یک عدد اول بزرگتر از  $r^2$  می‌باشد. فرض کنید  $r$  زیرگروه  $H$  از  $\mathbb{F}_A^*$  با  $|H| = n$  را تولید می‌کند که شامل  $\{\pm c | c = 1, 2, \dots, r-1\}$  به‌عنوان مجموعه کاملی از معرف‌های هم‌مجموعه‌ای است. کد AN دوری  $C$  با طول  $n$  و پایه  $r$  را در نظر بگیرید.



به وضوح، هر مقدار صحیح در بازه  $[1, m]$  دارای فاصله پیمانه‌ای  $0$  یا  $1$  تا دقیقاً یک کدکلمه است؛ بنابراین،  $C$  یک کد کامل است (چون  $w_m(A) \geq 3$  باید داشته باشیم  $A > r^2$ ). یک مثال بدیهی برای  $r = 3$  کد دوری  $\{13, 26\}$  است. در اینجا فرض کرده‌ایم  $m = 33 - 1$  و  $A = 13$ .

زیرگروه تولیدشده توسط  $3$  در  $\mathbb{F}_{13}^*$  دارای شاخص  $4$  است و معرف‌های هم‌مجموعه‌ای برابر با  $1 \pm$  و  $2 \pm$  هستند.

۳.۱۲.۵. داریم  $455 = \sum_{i=0}^5 b_i 3^i$ ، که در آن  $(b_5, b_4, b_3, b_2, b_1, b_0) = (2, 1, 2, 1, 2, 1)$ . الگوریتم توصیف شده در تعریف ۳.۱۰.۱ مقادیر اولیه  $2, 1$  را با  $-1$ ،  $2$  جای‌گزین می‌کند. در این روش، دنباله زیر از معرف‌ها را داریم:

$$(2, 1, 2, 1, 2, 1) \rightarrow (-1, 2, 2, 1, 2, 1) \rightarrow (-1, -1, 0, 2, 2, 1)$$

$$\rightarrow (-1, -1, 0, -1, 0, 2) \rightarrow (0, -1, 0, -1, 0, -1).$$

بنابراین، این نمایش در CNAF به صورت زیر است:

$$455 \equiv -273 = -3 - 3^2 - 3^5.$$

۴.۱۲.۵. شرایط موجود در قضیه ۲.۱۰.۲ را بررسی می‌کنیم. در  $\mathbb{F}_{11}^*$ ، عضو  $3$  زیرگروه  $\{1, 3, 9, 5, 4\}$  را تولید می‌کند؛ ضرب در  $-1$ ، پنج عضو دیگر را ایجاد می‌کند.  $r^n = 3^5 = 243 = 1 + 11 \times 22$  چون داریم  $A = 22$ ، در نمایش سه‌تایی  $A = 1 + 1 \times 3 + 2 \times 3^2$  برای CNAF برابر با  $1 + 1 \times 3^2 + 0 \times 3^4 + 0 \times 3^3 + 1 \times 3^2 + 0 \times 3 + 1$  (در پیمانه ۲۴۲) است. این کد شامل ده کلمه است؛ یعنی شیفتهای دوری  $(1, -2, 0, 1, 0)$ ، به ترتیب  $(-1, 2, 0, -1, 0)$ . تمام وزن‌ها  $2$  هستند.

## فصل ۱۳

۱.۱۳.۷. با به‌کارگیری نماد موجود در بخش ۱۱.۱ داریم:

$$G(x) = (1 + (x^2)^2) + x(1 + x^2) = 1 + x + x^3 + x^4.$$

رشته اطلاعاتی  $\dots 1 \ 1 \ 1 \ 1 \ 1 \ 1$  می‌دهد  $I_0(x) = (1 + x)^{-1}$ ؛ از این‌رو:

$$T(x) = (1 + x^2)^{-1} G(x) = 1 + x + x^2,$$

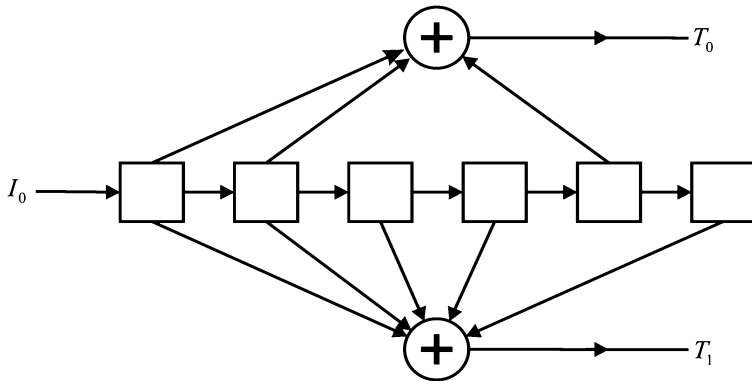
یعنی گیرنده  $\dots 0 \ 0 \ 0 \ 1 \ 1 \ 1$  را دریافت می‌کند.

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 به وجود 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  $\dots 0 0 0 0 1 0 0 1 0 0 1 0 0 0 1$  را در نظر بگیرید؛ یعنی  $I_0(x) = h(x)$ ؛ در این صورت 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  $1 + x + x^2 + x^3 + x^5 + x^7 + x^8 + x^{11} = g(x)$ ؛ بنابراین،  $G_0(x) = 1 + x + x^4$ ،  $G_1(x) = 1 + x + x^2 + x^3 + x^5$  کدگذار به شکل زیر است:



شکل ۱۴.۱:

و

یک خروجی ایجاد می‌کند  $I_0 = 1 1 0 0 1 0 0 0$

$T = 11 00 10 00 00 00 01 10 01 00 00$

۲.۱۳.۷. یک دنباله خروجی متناهی در نظر بگیرید. این دنباله به شکل  $(a_0 + a_1x + \dots + a_lx^l)G$  می‌باشد، که در آن  $a_i$ ها بردارهای سطری در  $\mathbb{F}_q^k$  هستند. مانند رابطه ۶،  $G$  را به صورت  $G_1 + xG_2$  می‌نویسیم. به وضوح هفت تایی 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 هفت تایی ناصفر نهایی باشد، آن‌گاه آن برابر با  $(11 \dots 1)$  است و وزن آن ۷ می‌باشد. اگر هفت تایی ناصفر نهایی،  $a_lG$  باشد، آن‌گاه آن کدکلمه ناصفری در کد تولیدشده توسط  $m_0m_1$  است و از این رو دارای وزن حداقل ۴ می‌باشد. اما،

اگر  $a_l = (1000)$ ، آن‌گاه  $a_l G = 0$  و هفت‌تایی ناصفر نهایی، کدکلمه ناصفیری در کد تولیدشده توسط  $m_1$  است و آن دارای وزنی بزرگتر یا مساوی ۳ می‌باشد؛ بنابراین، فاصله آزاد برابر با ۶ است. این مطلب با توجه به ورودی  $x(1000) * (1100)$  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: Mathe-matical 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. 767-770 (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] Gallager, 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 Louvain, 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  $Z_4$ -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 algebrigue 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 قابل قبول
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	

- design	طرح بلوکی
- length	طول بلوکی
bound	
- BCH	کران BCH
- Carlitz-Uchiyama	کران کارلیتز-یوچياما
- Elias	کران الیاس
- Gilbert-Varshamov	گیلبرت-ورشامو
- Grey	کران گری
- Griesmer	کران گریسمر
- Hamming	کران همینگ
- Johnson	کران جانسن
- linear programming	برنامه‌ریزی خطی
- McEliece	کران مک‌الیس
- Plotkin	کران پلاتکین
- Singleton	کران سینگلتون
- sphere packing	کران گوی پوششی
burst	گروهی
byte	بایت
character principal	سرشت اصلی
characteristic	
- numbers	اعداد مشخصه
- polynomial	چندجمله‌ای مشخصه
Chebyshev's inequality	نامساوی چیپشیف
check polynomial	چندجمله‌ای بررسی
Christoffel-Darboux formula	فرمول کریستوفل-داربوکس
code	
- algebraic geometry	کد هندسه جبری
- alternant	کد متناوب
- arithmetic	کد حسابی
- asymptotically good	کد به‌طور مجانبی خوب
- BCH	کد BCH
- narrow sense	کد کم‌عرض
- primitive	کد اولیه

- Best ..... کد بست
- block ..... کد بلوکی
- catastrophic ..... کد فاجعه آمیز
- completely regular ..... کد کاملا منظم
- concatenated ..... کد الحاقی
- constacyclic ..... کد پایادوری
- convolutional ..... کد کانولوشن
- cyclic ..... کد دوری
- AN ..... کد دوری AN
- convolutional, ..... کد دوری کانولوشن
- cyclic over  $\mathbb{Z}_4$  ..... کد دوری روی  $\mathbb{Z}_4$
- direct product ..... حاصل ضرب مستقیم
- double circulant ..... کد گردشی دوگانه
- dual ..... کد دوگان
- Elias ..... کد الیاس
- equidistant ..... کد هم فاصله
- equivalent ..... کد هم ارز
- error-correcting ..... کد تصحیح/کننده خطا
- error-detecting ..... کد تشخیص دهنده خطا
- extended ..... کد گسترش یافته
- generalized BCH ..... کد BCH گسترش یافته
- generalized Reed-Muller ..... کد رید-مولر گسترش یافته
- generalized Reed-Solomon ..... کد رید-سولومن گسترش یافته
- geometric generalized Reed-Solomon ..... کد رید-سولومن گسترش یافته هندسی
- geometric Goppa ..... کد گاپای هندسی
- Golay ..... کد گلی
- binary ..... کد گلی دودویی
- ternary ..... کد گلی سه تایی
- Goppa ..... کد گاپا
- group ..... کد گروهی
- Hadamard ..... کد هادامارد
- Hamming ..... کد همینگ
- inner ..... کد داخلی

- irreducible cyclic ..... کد تحویل‌ناپذیر سطری
- Justesen ..... کد جاستسن
- Kerdock ..... کد کرداک
- lexicographically least ..... آخرین کد با ترتیب الفبایی
- linear ..... کد خطی
- Mandelbaum-Barrows ..... کد مندلبوم-باروس
- maximal ..... کد ماکسیمال
- cyclic ..... کد ماکسیمال دوری
- maximum distance separable ..... کدهای تفکیک‌پذیر با بیشترین فاصله
- MDS ..... کد MDS
- minimal cyclic ..... کد مینیمال دوری
- modular arithmetic ..... کد حسابی پیمانهای
- Nadler ..... کد نادلر
- narrow sense BCH ..... کد BCH کم‌عرض
- nearly perfect ..... کد تقریباً کامل
- negacyclic ..... کد نادوری
- Nordstrom-Robinson ..... کد نرداستروم-رابینسن
- optimal ..... کد بهینه
- outer ..... کد خارجی
- perfect ..... کد کامل
- Preparata ..... کد پریاراتا
- primitive BCH ..... کد BCH اولیه
- projective ..... کد تصویری
- punctured ..... کد پنچر شده
- QR ..... کد QR
- quadratic residue ..... کد باقی‌مانده مربعی
- quasi-perfect ..... کد شبه-کامل
- quaternary ..... کد چهارتایی
- Reed-Muller ..... کد رید-مولر
- Reed-Solomon ..... کد رید-سولومن
- regular ..... کد منظم
- repetition ..... کد تکراری
- residual ..... کد باقی‌مانده

- RM	کد RM
- self-dual	کد خوددوگان
- separable	کد تفکیک پذیر
- shortened	کد کوتاه شده
- Srivastava	کد اسریواستاوا
- symmetry	کد متقارن
- systematic	کد سیستماتیک
- ternary	کد سه تایی
- trivial	کد بدیهی
- two-weight	کد دو وزنی
- uniformly packed	کد به طور یکنواخت بسته بندی شده
- uniquely decodable	کد به طور یکتا کدگشایی شونده
codeword	کد کلمه
coding gain	بهره کدگذاری
collaborating codes	کدهای هم کار
conference matrix	ماتریس کنفرانس
constraint length	طول محدود
coordinate ring	حلقه مختصات
coset	
- leader	سردسته هم مجموعه
- representative	معرف هم مجموعه
covering radius	شعاع پوششی
curve,	
- Hermitian	خم هرمیتی
- nonsingular	خم نامنفرد
- smooth	خم هموار
cyclic nonadjacent form	فرم دوری غیر مجاور
cyclotomic coset	هم مجموعه دوری
decision (hard, soft)	تصمیم (سخت، نرم)
decoder Berlekamp	کدگشای برلیکمپ
decoding	
- complete	کدگشایی کامل
- incomplete	کدگشایی غیر کامل



- majority logic.....	کدگشایی با منطق اکثریت
- maximum likelihood.....	کدگشایی با بیشترین درست‌نمایی
- multistep majority .....	کدگشایی اکثریت چند مرحله‌ای
- Viterbi .....	کدگشایی ویتربی
defining set .....	مجموعه تعریف
derivative.....	مشتق
design block .....	طرح بلوکی
differential.....	دیفرانسیل
direct product .....	حاصل ضرب مستقیم
distance	
- arithmetic .....	فاصله حسابی
- distribution .....	توزیع فاصله
- enumerator .....	شمارنده فاصله
- external.....	فاصله بیرونی
- free.....	فاصله آزاد
- Hamming.....	فاصله همینگ
- invariant .....	پایافاصله
- minimum.....	کمترین-فاصله
divisor	
- canonical.....	مقسوم‌علیه کانونی
- degree of.....	درجه مقسوم‌علیه
- effective .....	مقسوم‌علیه موثر
- principal.....	مقسوم‌علیه اصلی
encoder .....	کدگذار
entropy.....	آنتروپی
erasure.....	پاک‌کننده
error locator polynomial.....	چندجمله‌ای تشخیص خطا
Euler indicator .....	شاخص اویلر
expected value .....	مقدار متوس
factor group.....	گروه خارج‌قسمتی
finite field.....	میدان منتهای
flat.....	مسطر
function field.....	میدان تابعی

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 گرافف
Gray map	نگاشت گری
group	
- abelian	گروه آبدلی
- 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	اب‌صفحه
ideal	
- maximal	ایده آل ماکسیمال
- prime	ایده آل اول
- principal	ایده آل 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 ..... حاصل ضرب داخلی

integral domain ..... دامنه صحیح

irreducible polynomial ..... چندجمله‌ای تحویل‌ناپذیر

Jet Propulsion Laboratory ..... آزمایشگاه پرتاب جت

Klein quartic ..... چهارتایی کلاین

Krawtchouk

- expansion ..... توسعه کراچوک  
- polynomial ..... چندجمله‌ای کراچوک

Kronecker product ..... حاصل ضرب 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 مویبوس

- inversion formula.....	فرمول معکوس مویوس
monic polynomial.....	چندجمله‌ای تکین
multiplicative group of a field.....	گروه ضربی یک میدان
nonadjacent form.....	فرم غیرمجاور
normal distribution.....	توزیع نرمال
order.....	رتبه
orthogonal parity checks.....	بررسی توازن‌های متعامد
outer distribution.....	توزیع خارجی
Paley matrix.....	ماتریس پالی
parameter	
- local.....	پارامتر موضعی
- uniformizing.....	پارامتریکنواخت‌کننده
parity check	
- equation.....	معادله بررسی توازن
- matrix.....	ماتریس بررسی توازن
- symbol.....	سمبل بررسی توازن
permutation matrix.....	ماتریس جای‌گشتی
Plücker formula.....	فرمول پلاکر
point	
- at infinity.....	نقطه در بی‌نهایت
- nonsingular.....	نقطه نامنفرد
- rational.....	نقطه گویا
- simple.....	نقطه ساده
pole.....	قطب
primitive	
- element.....	عضو اولیه
- idempotent.....	خودتوان اولیه
- polynomial.....	چندجمله‌ای اولیه
- root of unity.....	ریشه اولیه واحد
principal	
- character.....	سرشت اصلی
- ideal.....	ایده آل اصلی
- ideal ring.....	حلقه ایده آل اصلی

projective	
- geometry	هندسه تصویری
- plane	صفحه تصویری
quadratic residue	مانده مربعی
quotient field	میدان خارج قسمتی
redundancy	افزونگی
regular function	تابع منظم
representative	معرف
residue	
- class	کلاس باقی مانده
- ring	حلقه باقی مانده
- theorem	قضیه باقی مانده
Riemann-Roch theorem	قضیه ریمن-روچ
ring	حلقه
Shannon theorem	قضیه شانون
shift register	رجیستر تغییر مکان
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 .....	مقسوم علیه 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